Cylance Endpoint Security

Guide d'administration

Contents

Utilisation des tableaux de bord

Les tableaux de bord offrent des visualisations et des résumés statistiques utiles des données collectées et analysées par différents services Cylance Endpoint Security. Pour afficher les tableaux de bord, cliquez sur Tableau de bord dans la barre de menus et sélectionnez le tableau de bord à afficher. Par défaut, les tableaux de bord sont disponibles pour les données réseau CylancePROTECT Desktop, CylancePROTECT Mobile et CylanceGATEWAY.

Vous pouvez également créer vos propres tableaux de bord personnalisés en sélectionnant des widgets qui affichent les données collectées par divers services. Plusieurs widgets comportent des éléments interactifs que vous pouvez manipuler pour filtrer les données ou afficher plus d'informations, ainsi que des liens pour afficher des informations détaillées dans des écrans dédiés de la console de gestion.

Vous pouvez partager les tableaux de bord que vous créez ou modifiez avec d'autres utilisateurs administrateurs.

Principales fonctionnalités des tableaux de bord Cylance Endpoint Security

Tableau de bord	Fonctionnalités
Protection de terminal (CylancePROTECT Desktop)	• Menaces en cours : affiche le nombre de menaces qui s'exécutent actuellement sur les terminaux. • Menaces automatiques : affiche le nombre de menaces qui sont configurées pour s'exécuter automatiquement. • Menaces mises en quarantaine : affiche le nombre de menaces mises en quarantaine. • Unique à Cylance : affiche le nombre de menaces qui ont été identifiées de manière unique par CylancePROTECT Desktop. • Total des fichiers analysés : affiche le nombre total de fichiers analysés par CylancePROTECT Desktop. • Évènements de menace : affiche les menaces détectées au cours des 30 derniers jours, classées en dangereuse, anormale, mise en quarantaine, dispensée et effacée. • Protection contre les menaces : affiche le pourcentage de menaces sur lesquelles vous avez pris des mesures (par exemple, mettre en quarantaine, dispenser ou ajouter à la liste sécurisée). • Protection des terminaux : affiche le pourcentage de terminaux dont les fichiers dangereux et anormaux sont configurés pour la mise en quarantaine automatique dans les stratégies des terminaux. Si la mise en quarantaine automatique est désactivée pour un ou les deux types de fichiers, le terminal est considéré comme non protégé lors du calcul du pourcentage. • Menaces par priorité : affiche le nombre total de menaces, regroupées par priorité, qui n'ont pas encore été traitées et qui nécessitent une attention particulière. • Classifications de menaces : affiche une carte thermique des types de menaces détectées. • Listes top dix : affiche les dix principales menaces détectées sur le plus grand nombre de terminaux, les dix principaux terminaux présentant le plus de menaces et les dix principales zones présentant le plus de menaces.

Tableau de bord	Fonctionnalités

Protection mobile (CylancePROTECT Mobile)	• Alertes mobiles détectées : affiche le nombre d'alertes mobiles détectées et le nombre d'alertes mobiles non résolues.
	• Terminaux mobiles avec alertes : affiche le nombre de terminaux mobiles avec alertes détectées par l'application CylancePROTECT Mobile.
	• Terminaux mobiles activés pour la détection des alertes : affiche le nombre de terminaux mobiles sur lesquels l'application CylancePROTECT Mobile est installée et activée.
	• Alertes mobiles par catégorie : affiche des diagrammes et des graphiques des alertes mobiles par catégorie.
	• Systèmes d'exploitation mobiles avec vulnérabilités : affiche un graphique des systèmes d'exploitation mobiles présentant des vulnérabilités, telles qu'identifiées, définies et suivies par la base de données nationale des vulnérabilités.
	• Alertes d'applications mobiles : affiche les statistiques des applications malveillantes et mises en ligne détectées.
	• Alertes de réseau mobile : affiche les statistiques relatives aux réseaux non sécurisés et aux détections Wi-Fi non sécurisées.
	• Alertes de sécurité des terminaux mobiles : affiche les statistiques pour les détections de sécurité des terminaux (verrouillage de l'écran désactivé, échec de l'attestation, etc.).
	• Afficher les listes et les statistiques des principales menaces dans les catégories suivantes :
	  • Principaux terminaux avec alertes mobiles
	  • Principaux réseaux Wi-Fi non sécurisés
	  • Principales applications malveillantes
	  • Principales détections d'alertes mobiles
	  • Principales applications chargées latéralement
	  • Principales URL de messages non sécurisés
	  • Principaux réseaux non sécurisés
	  • Principaux modèles de terminaux non pris en charge
	  • Principaux systèmes d'exploitation non pris en charge
	  • Principaux correctifs de sécurité non pris en charge

Tableau de bord	Fonctionnalités
Réseau (CylanceGATEWAY)	• Nombre total d'utilisateurs de la passerelle active : affiche le nombre d'utilisateurs actifs. • Connexions réseau : affiche un graphique des connexions réseau autorisées et bloquées. • Octets transférés : affiche un graphique des octets transférés (chargés et téléchargés). • Accès au réseau privé, Accès au réseau public : affiche des graphiques d'accès au réseau privé et public. • Principales destinations du réseau privé, Principales destinations du réseau public : affiche les listes des principales destinations de réseaux privés et publics et les actions les plus importantes. • Historique de connexion des connecteurs : affiche un graphique des connecteurs CylanceGATEWAY Connectors en ligne et hors ligne. • État du connecteur : affiche l'état de connexion du CylanceGATEWAY Connectors dans votre environnement. • Risque lié à la réputation de la destination : affiche une liste des alertes de risque de destination faible, moyen et élevé. • Catégories de risque de sécurité : affiche les catégories de risque autorisées, bloquées et combinées des catégories de risque autorisées et bloquées pour une catégorie donnée. • Versions TLS : affiche un graphique des versions TLS dans votre environnement. • Principales catégories bloquées : affiche un graphique des destinations autorisées, bloquées et une combinaison des destinations autorisées et bloquées pour le niveau de risque de destination spécifié. • Principaux consommateurs de bande passante : affiche une liste des principaux consommateurs de bande passante dans les chemins publics, privés et combinés publics et privés.

Tableau de bord	Fonctionnalités
Protection des informations (CylanceAVERT)	• Informations sur les évènements d'exfiltration : affiche le nombre d'évènements d'exfiltration CylanceAVERT, regroupés par type d'exfiltration. Ce widget peut être filtré selon une heure personnalisée. • 10 principaux évènements d'exfiltration par catégorie : affiche le nombre des 10 principaux évènements d'exfiltration par catégorie (politiques, utilisateurs, terminaux, fichiers et types de données). Ce widget peut être filtré selon une heure personnalisée. • 10 premiers articles de l'inventaire des dossiers par catégorie : affiche le nombre des 10 éléments de l'inventaire les plus importants par catégorie (politiques, extensions de fichiers, types d'informations et types de données). • 10 principaux évènements d'exfiltration par emplacement : affiche le nombre des 10 principaux évènements d'exfiltration par emplacement (domaines Web, domaines de messagerie et supports amovibles). Ce widget peut être filtré selon une heure personnalisée. • Inventaire des fichiers : affiche le nombre de fichiers sensibles dans l'inventaire des fichiers. • Casier de preuves : affiche le nombre de fichiers sensibles dans le casier de preuves. • Total des utilisateurs CylanceAVERT actifs : affiche le nombre total d'utilisateurs CylanceAVERT connectés. • Total des terminaux CylanceAVERT actifs : affiche le nombre total de terminaux CylanceAVERT connectés.

Créer un tableau de bord

1. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Créer un tableau de bord personnalisé	**a.** Dans la barre de menus de la console de gestion, cliquez sur **Tableau de bord > Protection mobile** ou **Tableau de bord > Réseau**. **b.** Cliquez sur ⊕ **> Ajouter un nouveau tableau de bord**. **c.** Si vous souhaitez commencer avec un tableau de bord vide, cliquez sur **Nouveau tableau de bord** dans la liste déroulante. Si vous souhaitez que le tableau de bord dispose des widgets par défaut de CylancePROTECT Mobile, CylanceGATEWAY (réseau) ou CylanceAVERT (protection des informations), cliquez sur cette option dans la liste déroulante. **d.** Saisissez un titre. **e.** Cliquez sur **Ajouter**.
Copier un tableau de bord	**a.** Dans la barre de menus de la console de gestion, cliquez sur **Tableau de bord**, puis sur le tableau de bord à copier. **b.** Cliquez sur ⊕ **> Copier ce tableau de bord**. **c.** Saisissez un titre. **d.** Cliquez sur **Enregistrer**.

2. Cliquez sur ⊕ **> Ajouter des widgets**. Pour en savoir plus sur les widgets disponibles, consultez la section Principales fonctionnalités des tableaux de bord Cylance Endpoint Security.
3. Dans le panneau **Ajouter des widgets**, faites glisser et déposez les widgets que vous souhaitez ajouter au tableau de bord.

   Vous pouvez déplacer des widgets et les redimensionner. Pour supprimer un widget, passez la souris dessus et cliquez sur ⋮ **> Supprimer**.

Partager un tableau de bord

Vous pouvez partager les tableaux de bord que vous créez ou modifiez avec d'autres utilisateurs administrateurs.

Avant de commencer :

- Vous devez disposer du rôle Administrateur pour partager un tableau de bord avec d'autres administrateurs.
- Créer un tableau de bord.

1. Dans la console de gestion, accédez au tableau de bord que vous souhaitez partager.
2. Cliquez sur ··· > **Partager le tableau de bord**.
3. Indiquez si vous souhaitez partager le tableau de bord avec tous les administrateurs ou sélectionnez les administrateurs. Si vous choisissez de partager avec des administrateurs spécifiques, recherchez et ajoutez les administrateurs à la liste.
4. Cliquez sur **Partager**.

Les administrateurs avec lesquels vous avez partagé le tableau de bord recevront une notification lorsqu'ils se connecteront à la console de gestion. Ils peuvent ajouter le tableau de bord partagé à leur menu Tableau de bord en accédant au tableau de bord par défaut de CylancePROTECT Mobileou au tableau de bord de CylanceGATEWAYou à n'importe quel tableau de bord personnalisé, en cliquant sur ⊕ > **Ajouter un nouveau tableau de bord**, puis en sélectionnant le tableau de bord partagé dans la liste déroulante Nouveau tableau de bord. Les utilisateurs avec lesquels vous partagez un tableau de bord ne peuvent pas apporter de modifications au tableau de bord partagé, mais ils peuvent le copier pour créer un nouveau tableau de bord qu'ils peuvent modifier.

La couleur de l'icône en regard du nom du tableau de bord indique si vous êtes le propriétaire d'un tableau de bord partagé (vert), si vous disposez d'un accès en lecture seule à un tableau de bord partagé (marron) ou si le tableau de bord est partagé avec tous les administrateurs (orange).

À la fin :

- Si vous souhaitez modifier les personnes avec lesquelles vous partagez un tableau de bord, accédez au tableau de bord et cliquez sur ··· > **Gérer les paramètres de partage**.
- Si vous souhaitez arrêter le partage d'un tableau de bord, cliquez sur ··· > **Arrêter le partage de ce tableau de bord**.

Gestion des alertes sur les services Cylance Endpoint Security

La vue Alertes constitue un moyen efficace d'examiner les alertes détectées et corrélées entre les services Cylance Endpoint Security, ce qui vous permet d'identifier et de suivre plus facilement les modèles de menaces en vigueur dans votre écosystème d'entreprise et de résoudre plus efficacement les ensembles d'alertes. La vue Alertes élimine la nécessité d'examiner les alertes provenant de différentes sections de la console qui sont chacune dédiées à un service spécifique tel que CylancePROTECT Desktop ou CylanceOPTICS. Vous pouvez utiliser la vue Alertes pour examiner et gérer les alertes de tous les services Cylance Endpoint Security pris en charge par votre environnement.

Service	Pris en charge par la vue Alertes
CylancePROTECT Desktop	Télémétrie des menaces, alertes de protection de la mémoire et alertes de contrôle de script de l'agent CylancePROTECT Desktop sur les terminaux de bureau.
CylancePROTECT Mobile	Alertes détectées par l'application CylancePROTECT Mobile.
CylanceOPTICS	Alertes détectées par l'agent CylanceOPTICS sur les ordinateurs de bureau.
CylanceGATEWAY	Paramètres de protection du réseau que vous avez configurés ou réputations de destination que CylanceGATEWAY a déterminées comme étant à haut risque.
CylanceAVERT	Évènements d'exfiltration de l'agent CylanceAVERT sur les terminaux de bureau.
Connecteur Okta	Télémétrie des évènements utilisateur Okta à l'aide du connecteur BlackBerry Okta. Requiert une licence CylanceENDPOINT Pro.
Connecteur Mimecast	Télémétrie de protection des pièces jointes Mimecast à l'aide du connecteur BlackBerry Mimecast. Requiert une licence CylanceENDPOINT Pro.

La vue Alertes initiale est un résumé qui regroupe les alertes similaires en fonction de divers critères tels que la priorité, la classification des alertes, les réponses configurées et d'autres attributs d'alerte clés. Pour en savoir plus sur ces critères, consultez la section Comment Cylance Endpoint Security regroupe les alertes.

Le regroupement automatisé des alertes reflète à la fois la fréquence et la prévalence des alertes, offrant aux analystes une vision claire de la fréquence des menaces et des zones sur lesquelles elles se produisent. Par défaut, les groupes d'alertes sont triés par ordre décroissant de priorité pour fournir une vue descendante de toutes les télémétries de sécurité pertinentes. Chaque groupe affiche des icônes pour les types d'artéfacts d'indicateurs clés associés au groupe (par ex., fichier, processus, e-mail, etc.). Vous pouvez cliquer sur une icône d'indicateur clé pour en consulter les attributs et, le cas échéant, vous pouvez copier ou filtrer ces valeurs. Lorsque de nouvelles alertes sont détectées et traitées à partir des sources de télémétrie, elles sont ajoutées à un groupe existant ou à un nouveau groupe.

La vue Alertes prend en charge les alertes à détection unique et à détection multiple. Les règles de détection des alertes peuvent parfois effectuer plusieurs détections avant de générer une alerte et de l'afficher dans la vue Alertes. Chaque détection est modélisée à l'aide d'un évènement (par exemple, fichier ouvert, clé de registre ajoutée, etc.).

Vous pouvez cliquer sur un groupe d'alertes pour accéder aux informations suivantes :

- L'onglet Présentation des alertes, qui récapitule les détails de la détection et les indicateurs clés pertinents pour le groupe.
- L'onglet Indicateurs clés affiche les attributs de détection qui sont identiques dans chaque alerte individuelle comprise dans le groupe. Par exemple, si l'indicateur clé est un hachage de fichier, ce hachage est détecté dans chaque alerte, que le terminal soit identique ou différent. Les indicateurs clés sont représentés visuellement pour indiquer la relation entre les objets parents, enfants et frères. Pour les alertes à détection multiple, les indicateurs clés sont inclus dans chaque évènement et résumés dans l'ordre d'exécution.
- La liste des alertes individuelles du groupe. Vous pouvez cliquer sur une alerte individuelle pour ouvrir des détails granulaires. Vous pouvez également afficher l'ensemble complet des artéfacts, représentés sous forme d'icônes, associés à l'alerte. Les artéfacts contiennent l'ensemble complet des facettes capturées par le moteur de détection sous-jacent. Comme les indicateurs clés, ces artéfacts sont représentés visuellement pour indiquer la relation entre les objets parents, enfants et frères. Pour les alertes à détection multiple, les indicateurs clés sont inclus dans chaque évènement et résumés dans l'ordre d'exécution.
- Vous pouvez utiliser Cylance Assistant optimisé par l'IA pour fournir une analyse récapitulative d'un groupe d'alertes et une analyse détaillée des artefacts de processus au sein d'un groupe d'alertes (par exemple, les processus de ligne de commande). L'Cylance Assistant tire parti de sources de connaissances approfondies en matière de cybersécurité pour fournir des informations précieuses qui vous aideront dans vos enquêtes sur les menaces. Pour plus d'informations, reportez-vous à Utiliser Cylance Assistant optimisé par l'IA pour examiner les alertes.

Selon les types d'alertes d'un groupe, vous pouvez également effectuer des actions de gestion. Par exemple, pour les alertes de menace CylancePROTECT Desktop, vous pouvez ajouter ou supprimer un fichier de la liste sécurisée globale ou de la liste de quarantaine globale.

Comment Cylance Endpoint Security regroupe les alertes

Cylance Endpoint Security utilise les critères suivants pour regrouper les alertes de différents services, en automatisant le processus afin de définir et d'optimiser vos activités de recherche et de résolution des menaces en regroupements logiques d'alertes connexes. Créée et gérée par BlackBerry, la logique de regroupement est conçue de manière dynamique pour gérer les alertes provenant d'une gamme de services intégrés. Vous bénéficiez ainsi d'une expérience sans intervention qui automatise l'analyse de la fréquence et de la prévalence, ce qui vous permet de trier et de hiérarchiser plus facilement vos efforts en matière de cybersécurité.

Une nouvelle alerte est ajoutée à un groupe d'alertes existant lorsque toutes les conditions suivantes sont remplies :

- La priorité, la classification, la sous-classification, la description, les indicateurs clés et la réponse de l'alerte correspondent à ce groupe.
- L'alerte est détectée dans les 7 jours (168 heures) suivant l'alerte la plus ancienne de ce groupe.

Un nouveau groupe d'alertes est créé lorsqu'une alerte qui ne remplit pas toutes ces conditions est détectée.

Priorité

La priorité d'une alerte, qui correspond à l'urgence du problème et son impact potentiel sur l'environnement de votre entreprise, est prise en compte dans le mode de regroupement des alertes. La vue Alertes regroupe les alertes prioritaires parmi les sources de télémétrie pour vous aider à afficher et à résoudre en premier lieu les alertes les plus urgentes.

Les facteurs qui déterminent la priorité d'une alerte varient selon le service :

Service	Facteurs
CylancePROTECT Desktop	• Pour les alertes de menace, la priorité est toujours élevée dans la vue Alertes, même si la priorité de l'alerte est inférieure dans Protection > Menaces de la console de gestion. L'objectif de cette priorité élevée dans la vue Alertes est d'indiquer l'urgence de la détection des programmes malveillants. • Pour les alertes de protection de la mémoire et de contrôle de script, la priorité est déterminée par la nature de l'événement, telle qu'elle est configurée par les analystes de cybersécurité BlackBerry. La priorité dépend de la gravité globale et de la pertinence de l'enquête.
CylancePROTECT Mobile	Les alertes utilisent une valeur de priorité correspondant à la gravité spécifiée dans la console de gestion et dans l'application CylancePROTECT Mobile.
CylanceOPTICS	La priorité est déterminée par la configuration des règles de détection CylanceOPTICS.

CylanceGATEWAY	La priorité est basée sur les paramètres de protection réseau que vous configurez ou sur la réputation d'une destination, telle qu'elle est déterminée par CylanceGATEWAY, avec un niveau de risque élevé. Par exemple, CylanceGATEWAY peut générer des alertes à afficher dans la vue Alertes dans les cas suivants :
	• Détections de réputation de destination :
	  • Lorsque cette option est activée, les alertes sont générées en fonction du niveau de risque que vous avez défini. Par exemple, si vous définissez le niveau de risque sur « Moyen à élevé », des alertes sont générées pour toutes les détections avec des niveaux de risque moyen et élevé.
	  • Lorsque cette option n'est pas activée, les alertes dont le niveau de risque est élevé sont générées par défaut.
	• Détections de signature :
	  • Lorsque cette option est activée, des alertes sont générées pour les détections de signature bloquées et s'affichent avec un niveau de risque élevé.
	  • Lorsque cette option n'est pas activée, CylanceGATEWAY ne génère pas d'alertes.
	• En ce qui concerne les détections Tunnellisation DNS et Jour zéro, des alertes sont générées si les détections présentent un niveau de risque élevé.

CylanceAVERT	La priorité est toujours élevée dans la vue Alertes.
Mimecast	La priorité est déterminée par l'évaluation des risques liés aux pièces jointes Mimecast.
Okta	La priorité est configurée par des analystes de cybersécurité BlackBerry.

Classification et sous-classification

La classification et la sous-classification des alertes identifient et cataloguent le type de détection sous-jacent pour fournir un contenu d'alerte structuré qui décrit plus précisément l'alerte détectée par un service

donné. Chaque service définit un ensemble spécifique de classifications et de sous-classifications pour clarifier la nature de l'alerte.

Les données de classification et de sous-classification servent à identifier et à regrouper les alertes similaires.

Les facteurs qui déterminent la classification et la sous-classification d'une alerte varient selon le service :

Service	Facteurs
CylancePROTECT Desktop	• Pour les alertes de menace, la classification et la sous-classification correspondent aux classifications de fichiers des alertes de menace CylancePROTECT Desktop. • Pour les alertes de protection de la mémoire, la classification et la sous-classification correspondent aux types de violations de protection de la mémoire. • Pour les alertes de contrôle de script, la classification indique le type d'alerte global (par exemple, contrôle des scripts, programme potentiellement indésirable, programme malveillant) et la sous-classification fournit des détails supplémentaires (par exemple, script exécuté, script bloqué).
CylancePROTECT Mobile	La classification correspond à une catégorie globale d'alertes (par exemple, Sécurité du terminal ou Menaces réseau) et la sous-classification correspond au type d'alerte spécifique qui s'affiche dans la console de gestion et dans l'application (par exemple, Application malveillante, Application chargée latéralement, Wi-Fi non sécurisé, etc.).
CylanceOPTICS	Les règles de détection contiennent des tactiques, des techniques et des sous-techniques MITRE pour définir la classification et la sous-classification d'une alerte.
CylanceGATEWAY	La classification correspond à la catégorie globale des alertes (par exemple, Contrôle d'accès réseau) et la sous-classification correspond au type d'alerte spécifique qui s'affiche dans la console de gestion (par exemple, Réputation, Tunnellisation DNS, Détection de signature et Détection du jour zéro).
CylanceAVERT	La classification est déterminée par l'évènement d'exfiltration.
Mimecast	La classification d'une alerte est la tactique MITRE d'accès initial (TA0001). La sous-classification de la même alerte est la technique MITRE d'hameçonnage (T1566).
Okta	La classification d'une alerte est soit le contrôle d'accès utilisateur (par exemple, si le nombre maximal de tentatives de connexion est dépassé), soit le contrôle d'accès réseau (par exemple, si la demande IP est bloquée en raison d'une règle de liste de blocage). Si la classification d'alerte est le contrôle d'accès utilisateur, la sous-classification sera le verrouillage utilisateur. Si la classification d'alerte est le contrôle d'accès réseau, la sous-classification sera le blocage de l'adresse IP.

Description

La description d'une alerte est une caractéristique qui fournit un court segment d'informations sur l'alerte. Les alertes avec des descriptions sont davantage susceptibles d'être regroupées.

Indicateurs clés

Les indicateurs clés sont le contenu de détection commun à chaque alerte spécifique d'un groupe d'alertes. Le processus d'agrégation compare les indicateurs clés des alertes pour déterminer si celles-ci doivent être regroupées. Par exemple, si un fichier contient un hachage SHA256 d'indicateur clé, la valeur de hachage est identique dans chaque alerte comprise dans un groupe d'alertes.

Les indicateurs clés d'une alerte varient selon le service :

Service	Facteurs
CylancePROTECT Desktop	• Pour les alertes de menace, l'indicateur clé est le hachage SHA256. • Pour les alertes de protection de la mémoire, les indicateurs clés sont les caractéristiques uniques de l'évènement (par exemple, les données de fichier telles que le hachage SHA256 et la valeur de risque). • Pour les alertes de contrôle de script, les indicateurs clés sont les caractéristiques uniques de l'événement (par exemple, un hachage SHA256 de fichier, un type de script et un nom de script).
CylancePROTECT Mobile	Les indicateurs clés correspondent aux caractéristiques uniques d'une alerte mobile donnée (par exemple, le nom de package d'une application chargée latéralement, le SSID d'un réseau Wi-Fi non sécurisé, le modèle d'un terminal non pris en charge, etc.).
CylanceOPTICS	Les indicateurs clés sont les facettes des artéfacts d'identification unique associés à une alerte. Par exemple, pour les artéfacts de processus, les indicateurs clés sont les facets suivants : hachage SHA256, chemin d'accès au fichier et argument de ligne de commande. Ces facets établissent une signature unique pour le type d'artéfact de processus qui peut être comparé à d'autres alertes. Les facets d'indicateur clé d'un groupe d'alertes sont communs à toutes les alertes individuelles du groupe.
CylanceGATEWAY	Les indicateurs clés sont Connexion réseau et Demande DNS.
CylanceAVERT	Les indicateurs clés varient en fonction du type d'artéfact. Pour les artéfacts d'alerte par e-mail, l'indicateur clé est l'ID de conversation. Pour les artéfacts d'alerte d'exfiltration de fichiers et de navigateur, l'indicateur clé est le nom d'utilisateur.
Mimecast	Les indicateurs clés sont les facettes des artéfacts associés à une alerte. Par exemple, pour les artéfacts de pièces jointes d'e-mail, les indicateurs clés sont le hachage SHA256 de la pièce jointe d'e-mail.
Okta	Les indicateurs clés sont les comptes associés aux demandes de connexion des utilisateurs et l'adresse IP associée aux tentatives de connexion bloquées.

Réponse

Pour les services qui exécutent des actions d'atténuation, il s'agit de l'action que vous avez configurée pour exécuter le service en réponse à la détection. Par exemple, pour les alertes de menace CylancePROTECT Desktop, la réponse peut être l'une des suivantes : ignorée, en quarantaine, dangereuse ou anormale.

Pour les services qui n'exécutent pas d'actions d'atténuation, des informations pertinentes sont collectées à partir du service intégré. Les alertes avec des réponses correspondantes sont davantage susceptibles d'être regroupées.

Heure

L'heure à laquelle une alerte se produit par rapport aux autres alertes est prise en compte dans le mode de regroupement des alertes. Une alerte est ajoutée à un groupe existant si la priorité, la classification, la sous-classification, la description, les indicateurs clés et la réponse de l'alerte correspondent à ce groupe, et si l'alerte se produit dans les 7 jours (168 heures) suivant l'alerte la plus ancienne de ce groupe. Si l'alerte correspond aux critères ci-dessus mais se produit en dehors de la période de 7 jours suivant l'alerte la plus ancienne du groupe, elle est ajoutée à un nouveau groupe. Le délai de 7 jours garantit que les groupes d'alertes ont une période fixe et ne croissent pas indéfiniment.

Afficher et gérer les alertes agrégées

Avant de commencer : Vérifiez que votre rôle d'administrateur dispose des autorisations requises pour utiliser la vue Alertes. L'autorisation Afficher les alertes fournit un accès en lecture seule à la vue Alertes. Vous devez disposer des autorisations Modifier les alertes et Supprimer les alertes pour apporter des modifications aux groupes d'alertes et aux alertes individuelles dans cette vue. Pour utiliser la vue Alertes afin d'ajouter un fichier des alertes de menace CylancePROTECT Desktop à la liste sécurisée globale ou à la liste de quarantaine globale, ou de supprimer un fichier de ces listes, votre rôle nécessite les autorisations associées à la liste globale en question. Pour en savoir plus, consultez la section Configuration des administrateurs dans le contenu relatif à la configuration.

1. Dans la barre de menus de la console de gestion, cliquez sur **Alertes**.

   Pour sélectionner les colonnes que vous souhaitez afficher, faites défiler l'écran vers la droite et cliquez sur |||.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Filtrez et triez les groupes d'alertes.	**a.** Cliquez sur sur une colonne et saisissez ou sélectionnez les critères de filtre. Vous pouvez effectuer l'une des opérations suivantes : • Appliquez plusieurs critères de filtre à la fois. Pour supprimer un filtre, cliquez sur le signe x en regard du filtre. • Si vous souhaitez filtrer par classification, sous-classification, description ou indicateurs clés, effectuez l'une des opérations suivantes : ◦ Pour trouver des correspondances exactes, cliquez sur > **est égal à**. Saisissez une valeur pour afficher les correspondances. Cliquez sur jusqu'à 5 correspondances en vue de les ajouter à la liste de filtrage, puis cliquez sur **Appliquer**. ◦ Pour rechercher des correspondances contenant la valeur spécifiée, cliquez sur > **contient**. Saisissez une ou plusieurs valeurs (cliquez sur + pour ajouter des valeurs supplémentaires). Cliquez sur **Apply** (Appliquer). Lorsque vous affichez les résultats, vous pouvez cliquer sur le filtre qui figure en haut de l'écran pour ajouter ou supprimer des critères de filtre. • Si vous filtrez par **Nombre**, cliquez sur pour obtenir des options supplémentaires (supérieur à, inférieur à, etc.). • Filtrez par **Produit** pour appliquer les résultats à des services Cylance Endpoint Security spécifiques. • Filtrez par **Temps de détection** pour appliquer les résultats à une plage de dates et d'heures spécifique. **b.** Pour trier les groupes d'alertes dans l'ordre croissant ou décroissant en fonction d'une colonne, cliquez sur le nom de celle-ci (le cas échéant).
Affichez les détails des indicateurs clés d'un groupe d'alertes et filtrez les groupes d'alertes par type ou valeur d'indicateur clé.	**a.** Passez le curseur sur une icône d'indicateur clé pour connaitre le type d'objet ou d'évènement. Cliquez sur une icône pour afficher les détails. **b.** Le cas échéant, pour afficher le texte complet d'une valeur de chaine tronquée, passez le curseur dessus et cliquez sur . **c.** Le cas échéant, pour copier une valeur, passez le curseur dessus et cliquez sur . **d.** Pour filtrer les groupes d'alertes en fonction d'un indicateur clé, placez le pointeur de la souris dessus, puis cliquez sur .

Tâche	Étapes
Affichez les détails d'un groupe d'alertes et d'alertes individuelles.	**a.** Cliquez sur un groupe d'alertes. **b.** Dans le volet de gauche, faites défiler vers le bas pour afficher les relations entre les objets déclencheurs et cibles. Cette vue affiche un ensemble unique d'indicateurs clés associés à des évènements spécifiques (fichiers, utilisateurs, exécutables, processus, etc.). **c.** Dans le volet de gauche, faites défiler vers le bas pour afficher les relations entre les objets déclencheurs et cibles. Cette vue affiche un ensemble unique d'indicateurs clés associés à des évènements spécifiques (fichiers, utilisateurs, exécutables, processus, etc.). Par exemple, vous pouvez afficher un objet de processus parent ou un fichier exécutable qui est le processus à l'origine d'un processus enfant. Les évènements ou objets au même niveau sont considérés comme des éléments frères sous le même parent. Si besoin, vous pouvez passer le curseur sur les valeurs et cliquer sur pour afficher les chaines de texte intégral ou sur pour copier la valeur. Pour les artefacts de processus, cliquez sur pour générer une analyse par l'Cylance Assistant. Pour plus d'informations, reportez-vous à Utiliser Cylance Assistant optimisé par l'IA pour examiner les alertes. **d.** Pour les alertes de terminaux individuelles, effectuez l'une des opérations suivantes : • Triez et filtrez les informations d'alerte. • Modifiez l'état des alertes. Reportez-vous à la section Changements d'état pour les alertes. • Attribuez les alertes à un utilisateur. • Ajoutez ou modifiez les libellés des alertes. **e.** Pour ouvrir le panneau de détails d'une alerte individuelle, cliquez sur celle-ci. Effectuez l'une des opérations suivantes : • Le cas échéant, vous pouvez cliquer sur **Détails de détection** pour afficher d'autres détails et actions dans d'autres zones de la console (par exemple, dans la vue Détections de CylanceOPTICS). Le lien Détails de détection reste actif pendant 60 jours pour les alertes de menace CylancePROTECT Desktop et pendant 30 jours pour les autres types d'alertes. • Développez les artéfacts associés à l'alerte pour examiner les détails et afficher les relations entre les objets et évènements déclencheurs et cibles. L'ensemble complet des objets associés à une règle de détection est inclus dans la vue des artéfacts. Si besoin, vous pouvez passer le curseur sur les valeurs et cliquer sur pour afficher les chaines de texte intégral ou sur pour copier la valeur. Pour les artefacts de processus, cliquez sur pour générer une analyse par l'Cylance Assistant. Pour plus d'informations, reportez-vous à Utiliser Cylance Assistant optimisé par l'IA pour examiner les alertes.

Tâche	Étapes
Demande de prise en charge de CylanceMDR	Cette fonction est disponible pour les abonnements CylanceMDR à la demande uniquement. Si vous avez observé une alerte qui vous semble suspecte et que vous souhaitez que la menace soit analysée par un expert, vous pouvez demander de l'aide à un analyste CylanceMDR. L'alerte sera transmise à un analyste pour enquête. Vous pouvez utiliser le portail CylanceMDR (CylanceGUARD) pour communiquer avec l'analyste au sujet de l'alerte transmise à partir de l'écran Escalades. Par exemple, il peut vous être demandé de fournir des détails supplémentaires sur l'alerte. **a.** Cliquez sur un groupe d'alertes contenant des alertes de menace CylancePROTECT Desktop. **b.** Dans le volet de droite, cliquez sur le bouton **Assistance CylanceMDR**. **c.** Cliquez sur **Demande d'assistance** pour confirmer que vous souhaitez transmettre l'alerte à un analyste. **d.** Effectuez un suivi de la demande via le portail CylanceMDR (CylanceGUARD). Voir la documentation CylanceMDR Si vous souhaitez bénéficier d'une surveillance des menaces 24 h/24, 7 j/7, envisagez des abonnements CylanceMDR Standard ou Avancé. Pour plus d'informations, reportez-vous à la présentation de CylanceMDR.
Alertes de menace CylancePROTECT Desktop : ajoutez un fichier à la liste sécurisée globale ou à la liste de quarantaine globale ou le supprimer.	**a.** Cliquez sur un groupe d'alertes contenant des alertes de menace CylancePROTECT Desktop. **b.** Cliquez sur **Actions > Gérer la liste globale**. Le hachage SHA256 du fichier associé aux alertes de menace s'affiche. Une notification est fournie si le fichier figure déjà dans la liste sécurisée globale ou dans la liste de quarantaine globale. **c.** Sélectionnez l'action appropriée pour ajouter le fichier dans la liste sécurisée globale ou dans la liste de quarantaine globale, ou pour ou l'en supprimer. Si le fichier figure déjà dans la liste de sécurité globale ou dans la liste de quarantaine globale, vous pouvez le déplacer vers l'autre liste. **d.** Si vous ajoutez le fichier à la liste de sécurité globale, cliquez sur la catégorie appropriée dans la liste déroulante **Catégorie**. **e.** Si vous ajoutez le fichier à une liste, saisissez-en le motif. **f.** Cliquez sur **Enregistrer**. Les modifications sont appliquées à la liste sécurisée ou de quarantaine appropriée. Le groupe d'alertes n'a pas été modifié dans la vue Alertes.
Modifiez l'état des groupes d'alertes.	Effectuez l'une des opérations suivantes : • Pour modifier l'état d'un groupe d'alertes, dans la liste déroulante **État**, cliquez sur l'état approprié. • Pour modifier l'état de plusieurs groupes d'alertes, sélectionnez-les, cliquez sur **Modifier l'état**, cliquez sur l'état approprié, puis cliquez sur **Appliquer**. Reportez-vous à la section Changements d'état pour les alertes.

Tâche	Étapes
Attribuez des groupes d'alertes à un utilisateur.	Effectuez l'une des opérations suivantes : • Pour attribuer un groupe d'alertes à un utilisateur, dans la colonne **Destinataire**, cliquez sur +, recherchez un utilisateur et cliquez dessus, puis cliquez sur **Attribuer**. • Pour attribuer plusieurs groupes d'alertes à un utilisateur, sélectionnez-les, cliquez sur **Attribuer une alerte**, recherchez et sélectionnez un utilisateur, puis cliquez sur **Attribuer**.
Ajoutez ou modifiez le libellé des groupes d'alertes.	Vous pouvez ajouter des libellés personnalisés aux groupes d'alertes pour fournir des notes ou des rappels, ou des critères de filtre. Pour afficher les libellés, vous devez activer l'affichage de la colonne Libellés. **a.** Sélectionnez un ou plusieurs groupes d'alertes. **b.** Cliquez sur **Modifier les libellés**. **c.** Saisissez un libellé et appuyez sur la touche ENTRÉE ou recherchez et sélectionnez un libellé existant. **d.** Cliquez sur **Apply** (Appliquer). Pour supprimer un libellé, cliquez dessus, cliquez sur l'icône x, puis cliquez sur **Appliquer**.
Exportez les données d'alerte.	Effectuez l'une des opérations suivantes : • Pour exporter les détails de tous les groupes d'alertes, cliquez sur . Saisissez le nom du fichier et saisissez et cliquez sur **Exporter**. • Pour exporter les détails de toutes les alertes d'un groupe, cliquez sur un groupe d'alertes, puis sur . Saisissez le nom du fichier et saisissez et cliquez sur **Exporter**.
Supprimez les groupes d'alertes.	**a.** Sélectionnez un ou plusieurs groupes d'alertes. **b.** Cliquez sur **Supprimer**. **c.** Cliquez à nouveau sur **Supprimer** pour confirmer.
Supprimer des groupes d'alertes des résultats filtrés	**a.** Filtrez les groupes d'alertes selon les critères appropriés. **b.** Effectuez l'une des opérations suivantes : • Pour supprimer tous les groupes d'alertes des résultats filtrés, cochez la case en haut à gauche et cliquez sur **Tout supprimer**. Cliquez à nouveau sur **Tout supprimer** pour confirmer. • Pour supprimer des groupes d'alertes spécifiques des résultats filtrés, sélectionnez les groupes d'alertes et cliquez sur **Supprimer**. Cliquez à nouveau sur **Supprimer** pour confirmer.

Utiliser Cylance Assistant optimisé par l'IA pour examiner les alertes

Vous pouvez utiliser Cylance Assistant optimisé par l'IA pour fournir une analyse récapitulative d'un groupe d'alertes et une analyse détaillée des artefacts de processus au sein d'un groupe d'alertes (par exemple, les processus de ligne de commande). L'Cylance Assistant tire parti de sources de connaissances approfondies en matière de cybersécurité pour fournir des informations précieuses qui vous aideront dans vos enquêtes sur les menaces.

Remarque :

- Pour accéder à l'Cylance Assistant dans la vue Alertes, vous devez contacter le représentant de votre compte BlackBerry pour demander l'activation de cette fonction.
- Actuellement, l'Cylance Assistant n'est disponible que pour les alertes CylanceOPTICS. Les futures mises à jour permettront d'étendre cette fonctionnalité à d'autres produits et services Cylance.
- BlackBerry n'utilise aucune donnée client pour former l'IA qui alimente l'Cylance Assistant.

1. Dans la barre de menus de la console de gestion, cliquez sur **Alertes**.
2. Dans la colonne **Produit**, cliquez sur et sélectionnez **CylanceOPTIC**.
3. Cliquez sur un groupe d'alertes.

Tâche	Étapes
Générez une analyse récapitulative du groupe d'alertes.	**a.** Dans la section **Présentation** du volet de gauche, cliquez sur **Résumé de l'alerte**. **b.** Cliquez sur pour copier le résumé.
Générez une analyse d'un processus déclencheur ou cible pour le groupe d'alertes.	**a.** Dans le volet de gauche, faites défiler vers le bas pour afficher les relations entre les objets déclencheurs et cibles. **b.** Passez le curseur sur un artefact de processus déclencheur ou cible et cliquez sur . **c.** Cliquez sur pour copier l'analyse.
Générez une analyse d'un processus déclencheur ou cible pour une alerte spécifique dans le groupe.	**a.** Cliquez sur une alerte individuelle dans le groupe d'alertes. **b.** Dans le volet de droite, faites défiler vers le bas pour afficher les relations entre les objets déclencheurs et cibles. **c.** Passez le curseur sur un artefact de processus déclencheur ou cible et cliquez sur . **d.** Cliquez sur pour copier l'analyse.

Changements d'état pour les alertes

L'état des alertes individuelles dans d'autres sections de la console (par exemple, Protection > Menaces, CylanceOPTICS > Détections, et Protection > Alertes Protect Mobile) correspond à un état équivalent dans la vue Alertes. Lorsqu'un état d'alerte change dans une autre vue, il est également mis à jour dans la vue Alertes. Par exemple, si l'état d'une alerte dans Détections est remplacé par Faux positif, l'état de la vue Alertes indique Fermé.

Lorsque vous modifiez l'état de chaque alerte dans la vue Alertes, un changement d'état équivalent s'affiche dans la vue CylanceOPTICS > Détections. Actuellement, les changements d'état que vous initiez dans la vue Alertes ne s'affichent pas dans la vue Protection > Menaces ou dans la vue Protection > Alertes Protect Mobile.

Notez les états équivalents suivants pour les alertes de menace CylancePROTECT Desktop :

- Les alertes dans Protection > Menaces avec un état Dangereux, Anormal ou En quarantaine apparaissent avec l'état Nouveau dans la vue Alertes.
- Les alertes dans Protection > Menaces avec un état Ignoré apparaissent avec l'état Fermé dans la vue Alertes.

Si vous définissez un état pour un groupe d'alertes, les alertes individuelles de ce groupe se voient attribuer l'état que vous avez sélectionné. Si les alertes individuelles d'un groupe d'alertes ont des états différents, qu'il s'agisse de changements d'état manuels ou de changements d'état provenant d'une autre vue (par exemple, CylanceOPTICS > Détections), le groupe d'alertes passe à l'état Multiple. Si toutes les alertes individuelles d'un

groupe d'alertes ont le même état, le groupe d'alertes a également le même état. Par exemple, si toutes les alertes individuelles sont définies sur l'état Fermé, le groupe d'alertes est également défini sur l'état Fermé.

Gestion d'utilisateurs, de terminaux et de groupes

Cette section fournit des informations sur l'affichage et la gestion des utilisateurs et des terminaux activés pour les services Cylance Endpoint Security et les groupes que vous utilisez pour appliquer les paramètres et les stratégies.

Gérer les terminaux CylancePROTECT Desktop et CylanceOPTICS

Vous pouvez utiliser la console de gestion pour afficher et gérer les terminaux dotés de l'agent CylancePROTECT Desktop et de l'agent CylanceOPTICS à partir de l'écran Actifs > Terminaux. Les terminaux apparaissent sur cet écran s'ils ont correctement installé l'agent et sont donc inscrits auprès de la console de gestion. Vous pouvez rechercher des terminaux, y effectuer des actions et exporter un rapport connexe. Par exemple, vous pouvez exporter une liste de terminaux exécutant des agents non pris en charge. Vous pouvez également ajouter rapidement des terminaux à une autre zone pour vous assurer qu'une stratégie de terminal appropriée leur est attribuée en fonction de leur zone.

La section suivante décrit la nouvelle vue de grille des terminaux sur l'écran Terminaux. L'écran Terminaux offre une expérience de recherche basée sur des requêtes pour simplifier la recherche des terminaux requis, l'enregistrement et le chargement de requêtes, ainsi que la possibilité d'ajuster la densité d'information et d'épingler des colonnes pour améliorer la lisibilité.

Les requêtes enregistrées sont utilisées pour construire des règles de zone. Vous pouvez charger une requête enregistrée et vérifier la liste des terminaux dans les résultats avant de l'utiliser pour les règles de zone. Pour plus d'informations, reportez-vous à la section Configuration des zones pour gérer des terminaux CylancePROTECT Desktop et CylanceOPTICS dans le contenu relatif à la configuration.

Avant de commencer : Dans la vue héritée, cliquez sur **Basculer vers la nouvelle vue** en haut à droite de l'écran pour passer à la nouvelle vue de la grille des terminaux.

1. Dans la barre de menus de la console de gestion , cliquez sur **Actifs > Terminaux**.
   La liste de tous les terminaux s'affiche.
2. Vous pouvez également personnaliser les colonnes affichées dans la grille des terminaux.
   - Pour ajouter ou supprimer des colonnes, cliquez sur ⚙ et sélectionnez les colonnes de votre choix. Vous pouvez également utiliser le curseur pour régler la densité d'information affichée sur la grille et cliquer sur 📌 pour épingler des colonnes.
   - Pour réorganiser l'ordre des colonnes, faites glisser leur nom vers l'emplacement souhaité.
   - Pour trier les colonnes dans l'ordre croissant ou décroissant, cliquez sur le nom de l'une d'elles.
3. Pour filtrer la liste des terminaux, effectuez l'une des opérations suivantes :

Tâche	Étapes
Recherche simple de terminaux	Pour effectuer une recherche simple, saisissez du texte dans la barre de recherche vide, sans spécifier de colonne. La méthode de recherche simple filtre rapidement les résultats des colonnes Nom du terminal, Nom DNS, Adresse IP, Adresse MAC et Dernier utilisateur signalé. La recherche simple utilise le champ `Text` ; en revanche, elle ne permet pas de filtrer les résultats en combinaison avec d'autres champs. Pour effectuer une recherche sur d'autres champs, effectuez plutôt une recherche avancée.

Tâche	Étapes
Recherche avancée de terminaux	**a.** Cliquez sur la barre de recherche. Une liste de champs filtrables s'affiche. Le cas échéant, vos recherches enregistrées et récentes apparaissent en haut de la liste. **b.** Sélectionnez un champ à filtrer. **c.** Sélectionnez un opérateur de comparaison (par exemple, `~ = <`). **Remarque :** Le champ d'adresse IP ne fonctionne actuellement qu'avec les opérateurs « est égal à » (=) et « commence par » (^=). Si vous souhaitez rechercher des terminaux dans une plage d'adresses IP, vous pouvez utiliser l'opérateur « est égal à » et utiliser des virgules pour les lister ou utiliser l'opérateur « commence par » et essayer de faire correspondre la première partie des adresses IP (par exemple, `"IP Address" ^= 192.168` trouverait des terminaux avec des adresses 192.168.x.x). La prise en charge du filtrage de la liste des terminaux par plages d'adresses IP sera ajoutée dans une prochaine version. **d.** Saisissez une valeur de paramètre pour le champ que vous filtrez. Vous pouvez séparer plusieurs paramètres par une virgule (par exemple, `Platform ~ macOS, Windows` ou `"IP Addresses" = 192.168.1.100, 192.168.1.101, 192.168.1.102`). Si des valeurs de paramètre contiennent une chaine de plusieurs mots, placez-la entre guillemets (par ex., `"Windows 11"`). **e.** Pour ajouter une autre expression, ajoutez un opérateur booléen (`and or`) à la fin de la requête. Actuellement, les opérateurs booléens de la requête doivent être identiques au premier que vous sélectionnez. Par exemple, `A=B and C=D and E~F` est pris en charge. Ou encore, `A=B or C=D or E~F` est également pris en charge. En revanche, `A=B and C=D or E~F` ne l'est actuellement pas. **f.** Cliquez sur **Rechercher**.
Enregistrer une requête	Pour l'enregistrer, une requête figurant dans la barre de recherche doit être valide. **a.** Effectuez une recherche pour vous assurer que la requête est valide et qu'elle produit les résultats attendus. **b.** Cliquez sur dans la barre de recherche. **c.** Saisissez un nom pour la requête. **d.** Cliquez sur **Enregistrer**.
Charger une requête enregistrée ou récente	Vous pouvez charger une requête enregistrée ou que vous avez récemment effectuée. Les requêtes enregistrées et récentes apparaissent uniquement lorsque la barre de recherche est vide. **a.** Cliquez sur la barre de recherche vide. Vous pouvez cliquer sur pour la vider. **b.** En haut de la liste, cliquez sur une requête récente () ou enregistrée (). La requête est chargée dans la barre de recherche. **c.** Cliquez sur **Rechercher**.

Tâche	Étapes
Renommer une requête enregistrée	**a.** Cliquez sur la barre de recherche vide. Vous pouvez cliquer sur ⊗ pour la vider. **b.** En haut de la liste, près d'une requête enregistrée, cliquez sur ✎. **c.** Saisissez un nouveau nom pour la requête. La requête ne peut pas être modifiée. **d.** Cliquez sur **Enregistrer**.
Exporter les résultats dans un fichier .csv	**a.** Cliquez sur ⇥. **b.** Saisissez un nom pour le fichier. **c.** Cliquez sur **Exporter**.

4. Pour effectuer des actions sur les terminaux, effectuez l'une des opérations suivantes :

Tâche	Étapes
Afficher les détails du terminal	Cliquez sur le nom d'un terminal.
Attribuer une stratégie de terminal aux terminaux	Un terminal ne peut être associé qu'à une seule stratégie de terminal. Si vous attribuez une nouvelle stratégie de terminal à un terminal, elle remplace la stratégie de terminal précédente. **a.** Sélectionnez un ou plusieurs terminaux. **b.** Cliquez sur **Attribuer la stratégie**. **c.** Cliquez sur une stratégie de terminal. **d.** Cliquez sur **Enregistrer**.
Ajouter des terminaux à une zone.	Vous pouvez utiliser des zones pour gérer l'application de paramètres et d'une stratégie de terminal à plusieurs terminaux. Pour plus d'informations sur les zones, consultez le contenu relatif à la configuration Cylance Endpoint Security. **a.** Sélectionnez un ou plusieurs terminaux. **b.** Cliquez sur **Ajouter à des zones**. **c.** Sélectionnez une ou plusieurs zones. **d.** Cliquez sur **Enregistrer**.
Supprimer des terminaux	Lorsque vous supprimez un terminal, vous annulez l'enregistrement de l'agent CylancePROTECT Desktop et les données de ce terminal sont supprimées de la console de gestion. L'utilisateur reçoit une notification indiquant que l'agent n'est pas enregistré et qu'il doit fournir un jeton d'installation pour réenregistrer l'agent. **a.** Sélectionnez un ou plusieurs terminaux. **b.** Cliquez sur **Supprimer.**. **c.** Cliquez sur **Oui** pour confirmer.

Tâche	Étapes
Excluez des terminaux de la gestion du cycle de vie.	Si vous souhaitez que certains terminaux ne soient pas automatiquement supprimés de la console en raison d'une inactivité, vous pouvez les exclure manuellement de la gestion du cycle de vie des terminaux. Les terminaux inactifs inclus dans la gestion du cycle de vie peuvent être automatiquement supprimés. **a.** Sélectionnez un ou plusieurs terminaux. **b.** Cliquez sur **Gestion du cycle de vie**. **c.** Cliquez sur **Exclure de la gestion du cycle de vie** (ou **Inclure dans la gestion du cycle de vie**). **d.** Cliquez sur **Oui** pour confirmer. Vous pouvez configurer les paramètres de gestion du cycle de vie pour spécifier quand l'état d'un terminal passe de hors ligne à inactif et quand les terminaux inactifs sont supprimés. Pour plus d'informations, consultez Configurer la gestion du cycle de vie des terminaux.
Réinitialiser la période d'inactivité des terminaux	Cette fonction définit l'état du terminal sur hors ligne, réinitialise le compteur de dates hors ligne et définit la date hors ligne sur la date actuelle. Cela n'affecte pas les terminaux en ligne. **a.** Sélectionnez un ou plusieurs terminaux. **b.** Cliquez sur **Réinitialiser la période d'inactivité**. **c.** Cliquez sur **Oui** pour confirmer.
Lancer une analyse de détection des menaces en arrière-plan sur un terminal (Vue héritée uniquement)	Vous pouvez lancer une analyse de détection des menaces en arrière-plan pour un terminal à la demande. Cette fonctionnalité requiert que les terminaux exécutent l'agent CylancePROTECT Desktop 3.2 ou une version ultérieure. Si une autre analyse est en cours sur un terminal, elle est interrompue avant le démarrage d'une analyse d'ar-rière-plan avec cette option. Cette fonctionnalité est actuellement disponible dans la vue héritée uniquement. **a.** Sélectionnez un ou plusieurs terminaux. **b.** Cliquez sur **Analyse d'arrière-plan**. **c.** Cliquez sur **Oui** pour confirmer. Les date et heure de la dernière analyse d'arrière-plan terminée sont consignées dans la console. Si la détection récurrente des menaces en arrière-plan est définie dans la stratégie de terminal attribuée, la prochaine heure d'analyse planifiée est recalculée en conséquence. Notez que si des analyses de détection des menaces en arrière-plan sont exécutées simultanément sur plusieurs terminaux de machine virtuelle provenant du même hôte de machine virtuelle, les performances des terminaux seront affectées en raison du partage des ressources.

Gérer les zones

Vous pouvez utiliser des zones pour regrouper et gérer des terminaux CylancePROTECT Desktop et CylanceOPTICS. Vous pouvez regrouper ces terminaux en fonction de la zone géographique (par exemple, l'Asie et l'Europe), de la fonction (par exemple, le personnel des ventes et du service informatique) ou de tout critère requis par votre organisation.

Vous pouvez attribuer une stratégie de terminal à une zone et l'appliquer aux terminaux CylancePROTECT Desktop et CylanceOPTICS dans la zone. Vous pouvez également ajouter une règle de zone qui peut attribuer des terminaux à une zone en fonction de critères sélectionnés, tels que le nom de domaine, la plage d'adresses IP ou le système d'exploitation. Une règle de zone ajoute de nouveaux terminaux à la zone si le terminal répond aux exigences de la règle.

1. Dans la console de gestion, cliquez sur **Zones** sur la barre de menu. Effectuez l'une des opérations suivantes :
   - Pour trier les zones dans l'ordre croissant ou décroissant par colonne, cliquez sur le nom de la colonne.
   - Pour filtrer les zones, cliquez sur une colonne et saisissez ou sélectionnez les critères de filtre.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Affichez les informations relatives à une zone.	Cliquez sur le nom d'une zone.
Ajouter une nouvelle zone.	**a.** Cliquez sur **Ajouter une nouvelle zone**. **b.** Dans le champ **Nom de la zone**, saisissez un nom. **c.** Dans la liste déroulante **Stratégie**, cliquez sur une stratégie de terminal à associer à la zone. **d.** Dans le champ **Valeur**, cliquez sur le niveau de priorité approprié pour la zone. Ce paramètre n'a aucun impact sur la gestion des zones. **e.** Cliquez sur **Enregistrer**.
Supprimer une zone.	**a.** Sélectionnez une ou plusieurs zones. **b.** Cliquez sur **Supprimer.**. **c.** Cliquez sur **Oui**.
Créez une règle de zone.	Créez une règle de zone pour ajouter automatiquement des terminaux à une zone s'ils répondent aux critères spécifiés. Les conditions de règle que vous spécifiez sont traitées de haut en bas. **a.** Cliquez sur le nom d'une zone. **b.** Cliquez sur **Créer une règle**. **c.** Configurez la règle de zone. **d.** Cliquez sur **Enregistrer**.

Tâche	Étapes
Ajoutez des terminaux à une zone.	Un terminal peut appartenir à un maximum de 75 zones. Si un terminal comporte plus de 75 zones, il peut y avoir des résultats inattendus avec l'attribution de la stratégie et de l'agent ou un message d'erreur indiquant « Échec lors de l'ajout des terminaux sélectionnés aux zones sélectionnées ». **a.** Cliquez sur le nom d'une zone. **b.** Sous l'onglet **Terminaux**, cliquez sur **Ajouter un terminal à la zone**. **c.** Sélectionnez les terminaux à ajouter. **d.** Si vous souhaitez appliquer de zone aux terminaux sélectionnés, cochez la case **Appliquer la stratégie de zone aux terminaux sélectionnés**. **e.** Cliquez sur **Enregistrer**.
Appliquez la stratégie de terminal de zone à tous les utilisateurs de la zone.	Cette action remplace toutes les stratégies de terminal actuellement attribuées aux terminaux par la stratégie de terminal actuellement attribuée à la zone. **a.** Cliquez sur le nom d'une zone. **b.** Cochez la case **Appliquer à tous les terminaux de cette zone**. **c.** Cliquez sur **Enregistrer**.
Copiez des terminaux dans une autre zone.	**a.** Cliquez sur le nom d'une zone. **b.** Dans l'onglet **Terminaux**, sélectionnez un ou plusieurs terminaux. **c.** Cliquez sur **Copier un terminal**. **d.** Sélectionnez une ou plusieurs zones. **e.** Cliquez sur **Enregistrer**.
Supprimez des terminaux d'une zone.	**a.** Cliquez sur le nom d'une zone. **b.** Dans l'onglet **Terminaux**, sélectionnez un ou plusieurs terminaux. **c.** Cliquez sur **Supprimer le terminal de la zone**. **d.** Cliquez sur **Oui**.
Utilisez des zones pour gérer les mises à jour des agents.	Vous pouvez créer des règles de mise à jour basées sur des zones pour mettre à jour les agents CylancePROTECT Desktop et CylanceOPTICS sur des terminaux. Pour plus d'informations, reportez-vous au contenu relatif à la configuration de Cylance Endpoint Security.

Gérer les terminaux avec l'application CylancePROTECT Mobile

Vous pouvez utiliser la console de gestion pour afficher et gérer les terminaux mobiles avec l'application CylancePROTECT Mobile. Vous pouvez également afficher le niveau de risque actuel des terminaux, déterminé à l'aide du mappage des menaces vers les niveaux de risque dans la stratégie d'évaluation des risques attribuée aux utilisateurs (Il existe une stratégie d'évaluation par défaut.). Pour plus d'informations sur les stratégies d'évaluation des risques, consultez le contenu relatif à la configuration Cylance Endpoint Security.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Terminaux mobiles**. Effectuez l'une des opérations suivantes :

- Pour trier les terminaux dans l'ordre croissant ou décroissant en fonction d'une colonne, cliquez sur le nom de celle-ci.
- Pour filtrer les terminaux, cliquez sur dans une colonne et saisissez ou sélectionnez les critères de filtre.

2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Afficher les alertes CylancePROTECT Mobile d'un terminal	**a.** Cliquez sur un terminal. **b.** Affichez l'onglet **Alertes Protect Mobile**. Pour afficher les alertes ayant entraîné le niveau de risque actuel du terminal, dans le volet de gauche, cliquez sur le niveau de risque.
Afficher les événements CylanceGATEWAY d'un terminal	**a.** Cliquez sur un terminal. **b.** Dans le menu, cliquez sur **Événements**.
Afficher les détails de conformité d'un terminal	**a.** Cliquez sur un terminal. **b.** Dans le menu, cliquez sur **Conformité**.
Supprimer des terminaux	**a.** Sélectionnez un ou plusieurs terminaux. **b.** Cliquez sur **Supprimer.**. **c.** Cliquez à nouveau sur **Supprimer** pour confirmer. Le terminal ainsi que les alertes et événements qui lui sont associés sont supprimés des services Cylance Endpoint Security et de la console de gestion. Si vous souhaitez ajouter à nouveau le terminal, l'utilisateur doit réactiver l'application CylancePROTECT Mobile. Reportez-vous à la page Gérer l'application CylancePROTECT Mobile et les utilisateurs CylanceGATEWAY pour obtenir des instructions sur l'envoi d'un nouvel e-mail d'activation.

Gérer l'application CylancePROTECT Mobile et les utilisateurs CylanceGATEWAY

Vous pouvez afficher et gérer les comptes utilisateur activés pour l'application CylancePROTECT Mobile et pour CylanceGATEWAY dans la console de gestion.

1. Dans la console de gestion, cliquez sur **Actifs > Utilisateurs** sur la barre de menu. Effectuez l'une des opérations suivantes :
   - Pour trier les utilisateurs dans l'ordre croissant ou décroissant par colonne, cliquez sur le nom de la colonne.
   - Pour filtrer les utilisateurs, cliquez sur une colonne et saisissez ou sélectionnez les critères de filtre.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Afficher les alertes d'un utilisateur.	**a.** Cliquez sur le nom d'utilisateur. **b.** Dans le menu, cliquez sur **Alertes**. **c.** Cliquez sur l'onglet approprié.
Afficher les événements d'un utilisateur	**a.** Cliquez sur le nom d'utilisateur. **b.** Dans le menu, cliquez sur **Événements**.
Afficher les détails du terminal d'un utilisateur.	**a.** Cliquez sur le nom d'utilisateur. **b.** Dans le menu, cliquez sur **Terminaux**. **c.** Cliquez sur un terminal pour afficher les alertes, les événements et les informations de conformité associés.
Ajouter un utilisateur à un groupe	Les groupes de répertoire sont gérés dans votre répertoire d'entreprise. Vous ne pouvez donc pas utiliser les étapes ci-dessous pour ajouter des utilisateurs à des groupes de répertoire. Ces étapes s'appliquent aux groupes locaux uniquement. **a.** Cliquez sur le nom d'utilisateur. **b.** Dans le menu, cliquez sur **Configuration**. **c.** Cliquez sur **Assigner des groupes d'utilisateurs**. **d.** Recherchez et sélectionnez un ou plusieurs groupes. **e.** Cliquez sur **Attribuer**.
Supprimer un utilisateur d'un groupe.	Les groupes de répertoire sont gérés dans votre répertoire d'entreprise. Vous ne pouvez donc pas utiliser les étapes ci-dessous pour supprimer des utilisateurs de groupes de répertoire. Ces étapes s'appliquent aux groupes locaux uniquement. **a.** Cliquez sur le nom d'utilisateur. **b.** Dans le menu, cliquez sur **Configuration**. **c.** Cliquez sur 🗑 en regard du groupe. **d.** Cliquez sur **Désattribuer**.
Attribuer une politique à un utilisateur.	**a.** Cliquez sur le nom d'utilisateur. **b.** Dans le menu, cliquez sur **Configuration**. **c.** Cliquez sur **Attribuer des stratégies utilisateur**. **d.** Dans la liste déroulante des stratégies, cliquez sur le nom de la stratégie. **e.** Recherchez et sélectionnez la stratégie. **f.** Cliquez sur **Attribuer**. Si une stratégie de ce type est déjà attribuée à l'utilisateur, la nouvelle sélection remplace la stratégie précédemment attribuée.
Supprimer la stratégie d'un utilisateur.	**a.** Cliquez sur le nom d'utilisateur. **b.** Dans le menu, cliquez sur **Configuration**. **c.** Cliquez sur 🗑 en regard de la stratégie. **d.** Cliquez sur **Désattribuer**.

Tâche	Étapes
Supprimez l'inscription One-Time Password d'un utilisateur.	L'utilisateur doit être inscrit pour utiliser la procédure One-Time Password. **a.** Cliquez sur le nom d'utilisateur. **b.** Dans la liste déroulante **Actions**, cliquez sur **Supprimer l'inscription TOTP**. **c.** Dans la boite de dialogue **Supprimer l'inscription TOTP**, cliquez sur **Confirmer**.
Envoyer un nouvel e-mail d'activation pour l'application CylancePROTECT Mobile.	Une stratégie d'inscription doit être attribuée à l'utilisateur avec la plate-forme mobile applicable activée. **a.** Sélectionnez un ou plusieurs utilisateurs. **b.** Cliquez sur **Envoyer à nouveau l'invitation**. **c.** Cliquez une nouvelle fois sur **Envoyer à nouveau l'invitation.** pour confirmer.
Faire expirer le mot de passe d'activation d'un utilisateur pour l'application CylancePROTECT Mobile.	**a.** Sélectionnez un ou plusieurs utilisateurs. **b.** Cliquez sur **Faire expirer le code d'accès**. **c.** Cliquez sur **Expirer** pour confirmer.
Supprimer des utilisateurs.	**a.** Sélectionnez un ou plusieurs utilisateurs. **b.** Cliquez sur **Supprimer des utilisateurs**. **c.** Cliquez sur **Supprimer** pour confirmer. Le compte utilisateur et toutes les applications CylancePROTECT Mobile, ainsi que tous les événements CylanceGATEWAY et alertes associés à cet utilisateur sont supprimés de la console de services et de gestion Cylance Endpoint Security. Si vous avez configuré la synchronisation et l'intégration des répertoires, modifiez le groupe de répertoire selon les besoins afin que l'utilisateur ne soit plus ajouté à Cylance Endpoint Security lors de la synchronisation.

Afficher les informations sur l'utilisateur CylanceAVERT

Vous pouvez afficher des informations sur vos utilisateurs CylanceAVERT et les évènements, terminaux et stratégies associés à partir de la page **Utilisateurs CylanceAVERT** de la console de gestion. Lorsque vous sélectionnez un utilisateur dans la liste Utilisateurs CylanceAVERT, vous pouvez afficher les détails de l'utilisateur, les évènements d'exfiltration de données associés à cet utilisateur, les détails des terminaux de l'utilisateur, ainsi que les groupes d'utilisateurs et les stratégies auxquels l'utilisateur est affecté.

1. Dans la barre de menus de la console de gestion, cliquez sur **Actifs > Utilisateurs Avert**.
2. Cliquez sur le nom d'un utilisateur dans la liste Utilisateurs Avert pour afficher les détails d'un utilisateur spécifique. Vous pouvez afficher le nom de chaque utilisateur, son adresse e-mail et le nombre de terminaux attribués à l'utilisateur dans la liste Utilisateurs Avert.

   Remarque : Vous ne pouvez pas ajouter, mettre à jour ou supprimer des utilisateurs de cette page. Si vous souhaitez gérer vos utilisateurs, cliquez sur **Gérer les utilisateurs**.
3. Sur la page des détails de l'utilisateur, effectuez l'une des opérations suivantes :

- Pour afficher des détails sur les évènements d'exfiltration de données associés à l'utilisateur, cliquez sur l'onglet **Évènements**. Cet onglet s'affiche par défaut.
- Pour afficher des détails sur les terminaux des utilisateurs, notamment le nom du terminal, la version du système d'exploitation, la version de l'agent CylanceAVERT, la date d'inscription de l'agent et la date d'attribution de la dernière stratégie, cliquez sur l'onglet **Terminaux**.
- Pour afficher les groupes d'utilisateurs et les stratégies d'utilisateurs attribués à l'utilisateur, cliquez sur l'onglet **Configuration**. Pour attribuer l'utilisateur à des groupes d'utilisateurs, cliquez sur **Attribuer des groupes d'utilisateurs**, puis sélectionnez le groupe dans la liste. Pour attribuer l'utilisateur à une stratégie d'utilisateur, cliquez sur **Attribuer des stratégies d'utilisateur**, puis sélectionnez la stratégie dans le menu déroulant.

Gérer les groupes d'utilisateurs

Vous pouvez gérer les groupes d'utilisateurs pour les utilisateurs qui sont activés pour l'application CylancePROTECT Mobile et pour les utilisateurs CylanceGATEWAY. Un groupe d'utilisateurs est un ensemble d'utilisateurs partageant des propriétés communes. L'administration d'utilisateurs sous forme de groupe est plus efficace que l'administration d'utilisateurs individuels car elle permet d'ajouter des propriétés, de les modifier ou de les supprimer simultanément de tous les membres du groupe. Lorsque vous attribuez des stratégies à des groupes d'utilisateurs, elles s'appliquent à tous les membres du groupe.

Cylance Endpoint Security possède deux types de groupes d'utilisateurs :

- Les groupes de répertoires lient les groupes à votre annuaire d'entreprise. L'appartenance au groupe est synchronisée avec la liste d'appartenance du répertoire. Pour plus d'informations, reportez-vous à la section Configurer l'intégration et la suppression.
- Les groupes locaux sont créés et gérés dans la console de gestion. Vous pouvez attribuer n'importe quel utilisateur local ou utilisateur de répertoire à un groupe local.

Pour en savoir plus sur la création de groupes, consultez le contenu relatif à la configuration.

1. Dans la console de gestion, cliquez sur **Actifs > Groupes d'utilisateurs** sur la barre de menu.
2. Pour attribuer des stratégies au groupe, sous stratégies, cliquez sur ⊕ et sélectionnez la stratégie que vous souhaitez attribuer.

   Vous pouvez également attribuer des stratégies à des utilisateurs et des groupes à partir des paramètres de stratégie.
3. Pour gérer les utilisateurs du groupe, cliquez sur l'onglet **Utilisateurs**.

Configurer la gestion du cycle de vie des terminaux

L'état des agents CylancePROTECT Desktop et CylanceOPTICS est « hors ligne » s'ils ne communiquent pas avec la console de gestion, par exemple lorsque l'utilisateur éteint son terminal. Si un agent reste hors ligne pendant une période prolongée, cela peut indiquer que le terminal n'est plus utilisé. La gestion du cycle de vie des appareils ne s'applique pas aux agents des appareils mobiles (par exemple, CylancePROTECT Mobile) ou à l'agent CylanceGATEWAY.

À l'aide de la gestion du cycle de vie des terminaux, vous pouvez spécifier le nombre de jours pendant lesquels un terminal peut rester hors ligne avant d'être signalé comme étant inactif dans la console de gestion. Vous pouvez également configurer la gestion du cycle de vie pour qu'elle supprime automatiquement les terminaux marqués comme inactifs de la console après un autre nombre de jours spécifié. Par exemple, vous pouvez configurer la fonction de gestion du cycle de vie des terminaux pour signaler un terminal hors ligne comme étant inactif s'il

est resté hors ligne pendant 30 jours. Vous pouvez par ailleurs configurer cette fonctionnalité pour supprimer un terminal de la console après 15 jours supplémentaires d'inactivité.

Lorsque la fonctionnalité de gestion du cycle de vie des terminaux est activée ou modifiée, le système vérifie la date de déconnexion de chaque terminal hors ligne et met à jour son état dans les 24 heures. Par exemple, si un terminal est hors ligne depuis 40 jours, que la fonctionnalité de gestion du cycle de vie des terminaux est activée et que le champ Jours hors ligne est défini sur 30 jours, le terminal passe à l'état « inactif » dans un délai de 24 heures. Dans un autre exemple, si un terminal est hors ligne depuis 25 jours et que le champ Jours hors ligne est défini sur 30 jours, le terminal passe à l'état « inactif » au bout de 5 jours, en supposant qu'il soit resté hors ligne. Les terminaux marqués comme inactifs continuent d'être protégés, même s'ils ne communiquent pas avec la console.

La console effectue le suivi du nombre de jours pendant lesquels le terminal est resté hors ligne ou inactif. Lorsque le terminal communique à nouveau avec la console, il passe à l'état en ligne et le compteur est remis à zéro.

1. Dans la console de gestion, cliquez sur **Paramètres > Cycle de vie des terminaux**.
2. Activez le paramètre **Activer la gestion automatisée du cycle de vie des terminaux**.
   a) Dans le champ **Jours hors ligne**, spécifiez le nombre de jours (entre 7 et 180) pendant lesquels un terminal doit être hors ligne avant de passer à l'état inactif.
3. Pour supprimer des terminaux inactifs, activez le paramètre **Supprimer les terminaux inactifs**.
   a) Dans le champ **Jours d'inactivité**, spécifiez le nombre de jours (entre 7 et 180) pendant lesquels un terminal doit être inactif avant d'être automatiquement supprimé de la console.

   Lorsque vous supprimez un terminal de la console, ses données sont supprimées de la console, mais l'agent ne supprime pas le terminal.
4. Cliquez sur **Enregistrer**.

À la fin :

- Pour afficher l'état d'un terminal, dans **Actifs > Terminaux**, consultez la colonne **État**.
- Pour savoir si un terminal est inclus dans la gestion du cycle de vie des terminaux, dans **Actifs > Terminaux**, consultez la colonne **Gestion du cycle de vie**. Si cette colonne n'est pas disponible, vous devrez peut-être l'afficher manuellement
- Pour exclure un terminal de la gestion du cycle de vie des terminaux afin qu'il ne soit pas signalé comme étant inactif après sa déconnexion, consultez la section Gérer les terminaux CylancePROTECT Desktop et CylanceOPTICS.

Afficher une liste des applications installées sur les terminaux CylancePROTECT Desktop

L'agent CylancePROTECT Desktop 3.2 envoie à la console une liste des applications logicielles installées sur le terminal. Cette fonctionnalité vous permet d'identifier les applications installées sur les terminaux qui peuvent être une source de vulnérabilités, de hiérarchiser les actions contre les vulnérabilités et de les gérer en conséquence. Vous pouvez afficher toutes les applications installées sur les terminaux et afficher une liste des applications installées sur des terminaux spécifiques. Cette fonctionnalité peut être activée à partir de la stratégie de terminal.

Avant de commencer :

- L'agent CylancePROTECT Desktop version 3.2 ou ultérieure doit être exécuté sur un terminal Windows pour envoyer une liste d'applications à la console.
- Une stratégie de terminal avec la fonction d'inventaire logiciel activée doit être attribuée aux terminaux.

Effectuez l'une des opérations suivantes :

Tâche	Étapes
Afficher la liste de toutes les applications installées sur les terminaux de votre locataire	**a.** Dans la console, accédez à **Actifs > Applications installées**. **b.** Cliquez sur le nom d'une application pour afficher la liste des terminaux sur lesquels elle est installée. Vous pouvez cliquer sur le nom d'un terminal pour en afficher les détails, y compris la liste des applications qui y sont installées.
Afficher la liste des applications installées sur un terminal spécifique	**a.** Dans la console, cliquez sur **Actifs > Terminaux**. **b.** Cliquez sur le nom d'un terminal. **c.** Dans la section **Menaces et activités**, cliquez sur l'onglet **Applications installées**.

Supprimer un terminal FIDO enregistré pour un compte utilisateur

Vous pouvez supprimer FIDOles terminaux qu'un utilisateur a enregistrés. Par exemple, vous pouvez supprimer un terminal enregistré s'il est perdu ou si l'utilisateur a quitté votre entreprise.

1. Dans la console de gestion, cliquez sur **Actifs > Utilisateurs** sur la barre de menu.
2. Dans la liste déroulante **Actions**, cliquez sur **Gérer les terminaux FIDO**.
3. Dans la boite de dialogue **Gérer les terminaux FIDO**, sélectionnez les terminaux et cliquez sur **Supprimer**.

Découvrir les terminaux non protégés

Vous pouvez utiliser la console de gestion pour afficher la liste des terminaux connus, détectés à partir de Active Directory, qui ne sont pas protégés par CylancePROTECT Desktop. Les terminaux connus exécutant une version du système d'exploitation prenant en charge l'installation de CylancePROTECT sont indiqués. Vous pouvez également exporter la liste des terminaux et prendre les mesures nécessaires (par exemple, installer CylancePROTECT) sur ces terminaux pour protéger ces derniers et votre réseau contre les menaces potentielles.

Avant de commencer : Vérifiez que vous avez activé le service de détection des terminaux non protégés. Pour plus d'informations, consultez Activer la détection de terminaux non protégés.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Terminaux non protégés**.
   L'état de contrôle de protection du terminal peut être l'un des suivants :
   - Pris en charge : le terminal détecté exécute une version du système d'exploitation prise en charge par CylancePROTECT Desktop.
   - Non pris en charge : le terminal détecté n'exécute pas une version du système d'exploitation prise en charge par CylancePROTECT Desktop.
   - Informations insuffisantes : pas assez d'informations disponibles pour déterminer si la version du système d'exploitation qui s'exécute sur le terminal est prise en charge par CylancePROTECT Desktop.
2. Effectuez l'une des opérations suivantes :
   - Pour ajouter ou supprimer des colonnes, cliquez sur ||| et sélectionnez les colonnes que vous souhaitez afficher.
   - Pour filtrer l'une des colonnes, cliquez sur l'en-tête de colonne.

- Pour exporter les informations sur les terminaux non protégés dans un fichier .csv, cliquez sur . Vous pouvez exporter toutes les colonnes du tableau ou sélectionner **Filtres actuels** pour exporter uniquement les colonnes filtrées. Cliquez sur **Exporter**.

Activer la détection de terminaux non protégés

Vous devez activer le service de détection de terminaux non protégés pour analyser le locataire nouvellement ajouté afin de détecter et de répertorier les terminaux connus qui ne sont pas protégés par CylancePROTECT Desktop sur l'écran Terminaux non protégés. L'option permettant d'activer ce service sera disponible dans les 24 heures suivant la configuration de la connexion au répertoire avec le BlackBerry Connectivity Node.

Sur les locataires nouvellement ajoutés, l'option n'est pas disponible pendant 24 heures maximum pendant que le service fonctionne sur un planificateur qui actualise la liste des locataires et les données des autres services. Cette actualisation a lieu toutes les 24 heures. Une fois les informations du locataire mises à jour, elles sont disponibles pour le service de détection de terminaux non protégés et vous pouvez l'activer. Lorsque le service est activé pour la première fois, les terminaux non protégés sont répertoriés dans un délai de 2 minutes. Une fois le service activé, la console de gestion met à jour la liste des terminaux non protégés toutes les 24 heures. Par défaut, cette fonctionnalité est désactivée pour chaque locataire.

Avant de commencer :

- Assurez-vous que vous avez configuré une connexion de répertoire à l'aide de la dernière version de BlackBerry Connectivity Node. Pour plus d'informations, consultez la section Installation de BlackBerry Connectivity Node dans le contenu relatif à la configuration.
- Configurez votre environnement pour afficher le système d'exploitation du terminal et la version du système d'exploitation des terminaux non protégés gérés.
- Assurez-vous que l'utilisateur dispose des autorisations appropriées pour activer cette fonctionnalité. Pour plus d'informations sur les autorisations, reportez-vous à la section Autorisations pour les rôles d'administrateur dans le contenu relatif à la configuration. Les autorisations suivantes sont requises :
  - Pour afficher les connexions au répertoire, l'utilisateur doit disposer de l'autorisation « Afficher les connexions au répertoire ».
  - Pour activer et désactiver cette fonctionnalité, l'utilisateur doit disposer de l'autorisation « Modifier les connexions au répertoire ».

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions à l'annuaire**.
2. Dans la liste **Connexion au répertoire**, cliquez sur la connexion pour laquelle vous souhaitez activer la découverte de terminaux non protégés.
3. Dans l'onglet **Paramètres de synchronisation**, sélectionnez **Découverte de terminaux non protégés**.
4. Lorsque vous y êtes invité, cliquez sur **Confirmer** pour appliquer ce paramètre à toutes les connexions de répertoire de votre environnement.

Configurez votre environnement pour afficher le système d'exploitation du terminal et la version du système d'exploitation des terminaux non protégés gérés

Pour que la fonction des terminaux non protégés affiche le système d'exploitation et la version du système d'exploitation, vous devez configurer le schéma pour autoriser la synchronisation des attributs requis entre le contrôleur de domaine et le catalogue global.

1. Sur le contrôleur de domaine Active Directory, procédez comme suit pour enregistrer Schmmgmt.dll et ajouter l'option Schéma au MMC :
   a) Sur le contrôleur de domaine, cliquez sur **Démarrer > Exécuter**.
   b) Dans le champ de recherche, saisissez `regsvr32 schmmgmt.dll`. Cliquez sur **OK**.
   c) À l'issue des opérations, cliquez sur **OK**.
2. Dans le MMC, ouvrez le schéma Active Directory et procédez comme suit :

a) Cliquez sur **Démarrer > Exécuter**.
b) Dans le champ de recherche, saisissez `mmc.exe`. Cliquez sur **OK**.
c) Dans le menu **Fichier**, cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.
d) Cliquez sur **Schéma Active Directory** .
e) Cliquez sur **Ajouter**.
f) Cliquez sur **Fermer**. Cliquez sur **OK**.

3. Pour mettre à jour les attributs à synchroniser avec le catalogue global, procédez comme suit :
a) Dans la colonne de gauche de la vue de schéma Active Directory, cliquez sur **Attributs**.
b) Dans la liste des attributs, recherchez et cliquez sur **operatingSystem**.
c) Cochez la case **Répliquer cet attribut dans le catalogue global**.
d) Cliquez sur **OK**.
e) Répétez les étapes a à d pour les attributs suivants :
- operatingSystemServicePack
- operatingSystemVersion

Gestion des menaces détectées par CylancePROTECT Desktop

Les terminaux sont des points de terminaison sur lesquels l'agent CylancePROTECT Desktop est installé (ordinateurs de bureau ou serveurs). Les terminaux peuvent être gérés à l'aide de la console de gestion ou de l' API Cylance User. Les actions de gestion comprennent l'examen des évènements de menace et d'autres alertes, la vérification de l'attribution de la stratégie et des paramètres corrects aux terminaux, et l'utilisation de zones pour regrouper et simplifier la gestion des terminaux.

Gérer les alertes de menace CylancePROTECT Desktop

Vous pouvez utiliser la console de gestion pour afficher et gérer les alertes de menace détectées par l'agent CylancePROTECT Desktop. Les fichiers considérés comme dangereux ou anormaux s'affichent dans la console de gestion. Les fichiers considérés comme surs ne s'affichent pas dans la console.

1. Sur la barre de menus de la console de gestion, cliquez sur **Protection > Menaces**. Effectuez l'une des opérations suivantes :
   - Pour ajouter ou supprimer des colonnes, cliquez sur ||| et sélectionnez les colonnes que vous souhaitez afficher.
   - Pour regrouper les informations d'alerte de menace par une ou plusieurs colonnes, faites glisser ces colonnes dans l'espace au-dessus des noms de colonnes.
   - Pour trier les alertes de menace dans l'ordre croissant ou décroissant par colonne, cliquez sur la colonne.
   - Pour filtrer les alertes de menace par colonne, utilisez le champ de filtre et l'icône de la colonne. Après avoir filtré les alertes de menace, enregistrez ces filtres en marquant la page comme signet. L'enregistrement de vos filtres en tant que signet ne fonctionne que pour les alertes de menace.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Afficher les détails de l'alerte de menace.	Cliquez sur la ligne de l'alerte de menace.
Afficher la page des détails de la menace.	Cliquez sur le nom du fichier.
Utilisez les filtres de menace.	Cliquez sur un filtre de menace. Cliquez sur l'icône de fermeture pour effacer le filtre de menace.
Affichez les indicateurs de menace.	Développez la section **Indicateurs de menace**. Pour en savoir plus sur les indicateurs de menace, consultez Indicateurs de menace.

Tâche	Étapes
Ajouter des fichiers à la liste globale.	Ajouter des fichiers à la liste de quarantaine globale ou à la liste sécurisée globale. **a.** Cochez les cases correspondant aux fichiers à ajouter à une liste globale. **b.** Cliquez sur **Quarantaine globale** pour ajouter les fichiers à la liste de quarantaine globale. Cliquez sur **Sécurisé** pour ajouter les fichiers à la liste sécurisée globale.
Ajoutez un fichier à la liste locale.	Ajoutez un fichier à une liste de quarantaine locale ou à une liste sécurisée locale. Les listes locales sont prioritaires sur les listes globales. Par exemple, vous pouvez bloquer un fichier de son organisation, mais l'autoriser sur des terminaux spécifiques. **a.** Cliquez sur la ligne de l'alerte de menace. **b.** Dans la liste de terminaux, sous **Non sécurisé** ou **Anormal**, cochez les cases correspondant aux terminaux appropriés. **c.** Cliquez sur **Quarantaine** pour ajouter le fichier à la liste de quarantaine locale. Cliquez sur **Ignorer** pour ajouter le fichier à la liste sécurisée locale.
Modifier la liste locale d'un fichier.	Vous pouvez modifier un fichier de la quarantaine locale à la liste sécurisée locale ou de la liste sécurisée locale à la quarantaine locale. **a.** Cliquez sur la ligne de l'alerte de menace. **b.** Dans la liste de terminaux, sous **En quarantaine** ou **Ignorés**, cochez les cases correspondant aux terminaux appropriés. **c.** Si vous êtes dans la liste **Ignorés**, cliquez sur **Quarantaine** pour ajouter le fichier à la liste de quarantaine locale. Si vous êtes sur la liste **En quarantaine**, cliquez sur **Ignorer** pour ajouter le fichier à la liste sécurisée locale.

À la fin : Pour exporter les informations sur la menace dans un fichier .csv, cliquez sur  . Sélectionnez la portée de l'exportation et cliquez sur **Exporter**.

Indicateurs de menace

Chaque catégorie représente une zone fréquemment observée dans les logiciels malveillants.

Anomalies

Ces indicateurs représentent les situations dans lesquelles le fichier comporte des éléments incohérents ou anormaux. Il s'agit souvent d'incohérences dans les éléments structurels du fichier.

Indicateur	Description
16bitSubsystem	Ce fichier utilise le sous-système 16 bits. Les logiciels malveillants l'utilisent dans une partie moins sécurisée et moins surveillée du système d'exploitation, et souvent pour lancer des attaques par escalade des privilèges.

Indicateur	Description
Anachronisme	Ce fichier exécutable semble mentir quant au moment où il a été écrit, ce qui n'est pas classique pour les logiciels écrits de manière professionnelle.
AppendedData	Ce fichier exécutable comporte un contenu supplémentaire qui lui a été ajouté, au-delà des zones normales du fichier. Les données ajoutées peuvent fréquemment être utilisées pour intégrer des données ou des codes malveillants, et elles sont souvent négligées par les systèmes de protection.
AutoitDbgPrivilege	Le script AutoIt peut procéder à des activités de débogage.
AutoitManyDllCalls	Le script AutoIt utilise de nombreux appels à des DLL externes. Le moteur d'exécution AutoIt possède déjà de nombreuses fonctions communes. Par conséquent, l'utilisation de fonctionnalités supplémentaires provenant de DLL externes peut être un signe de malveillance.
AutoitMutex	Le script AutoIt crée des objets de synchronisation. Ce script est habituellement utilisé par les logiciels malveillants pour éviter d'infecter plusieurs fois la même cible.
AutoitProcessCarving	Le script AutoIt est susceptible de reconstituer le processus pour exécuter son propre code qui semble provenir d'un autre processus. Cela est souvent le cas pour entraver la détection.
AutoitProcessInjection	Le script AutoIt est susceptible de procéder à une injection de processus pour exécuter du code dans le contexte d'autres processus, afin de ne pas être détecté ou de dérober des données.
AutoitRegWrite	Le script AutoIt écrit dans le registre Windows.
Base64Alphabet	Le fichier contient des preuves d'utilisation du codage Base64 d'un alphabet. Les logiciels malveillants tentent ainsi d'éviter les pratiques de détection courantes ou d'attaquer d'autres programmes qui utilisent le codage Base64.
CommandlineArgsImport	Le fichier importe des fonctions capables de lire des arguments à partir d'une ligne de commande. Les logiciels malveillants utilisent cette fonctionnalité pour recueillir des informations sur les exécutions suivantes.
ComplexMultipleFilters	Le fichier contient plusieurs flux avec divers filtres.
ComplexObfuscatedEncoding	Le fichier contient un nombre anormalement élevé de noms obscurcis.
ComplexUnsupportedVersion EmbeddedFiles	Le fichier utilise les fonctionnalités EmbeddedFiles provenant de versions plus récentes de la norme PDF qu'il déclare.

Indicateur	Description
ComplexUnsupportedVersionFlate	Le fichier utilise la fonctionnalité FlateDecode provenant de versions plus récentes de la norme PDF qu'il déclare.
ComplexUnsupportedVersionJbig2	Le fichier utilise la fonctionnalité JBIG2Decode provenant de versions plus récentes de la norme PDF qu'il déclare.
ComplexUnsupportedVersionJs	Le fichier utilise les fonctionnalités JavaScript provenant de versions plus récentes de la norme PDF qu'il déclare.
ComplexUnsupportedVersionXFA	Le fichier utilise les fonctionnalités XFA provenant de versions plus récentes de la norme PDF qu'il déclare.
ComplexUnsupportedVersionXobject	Le fichier utilise les fonctionnalités XOBject provenant de versions plus récentes de la norme PDF qu'il déclare.
ContainsFlash	Le fichier contient des objets flash.
ContainsPE	Le fichier contient des fichiers exécutables intégrés.
ContainsU3D	Le fichier contient des objets U3D.
InvalidCodePageUsed	Le fichier utilise un environnement local non valide ou non reconnu, probablement pour éviter la détection.
InvalidData	Les métadonnées du fichier sont de toute évidence fausses ou endommagées.
InvalidStructure	La structure du fichier n'est pas valide. La table d'allocation des tailles, des métadonnées ou du secteur interne est incorrecte, ce qui peut indiquer une faille de sécurité.
ManifestMismatch	Le manifeste du fichier est incohérent. Le logiciel malveillant évite d'être détecté, mais brouille rarement les pistes de manière optimale.
NontrivialDLLEP	Ce fichier exécutable est une DLL avec un point d'entrée non trivial. Ils sont communs dans les DLL, mais une DLL malveillante peut utiliser ce point d'entrée pour s'installer dans un processus.
NullValuesInStrings	Certaines chaines du fichier contiennent des caractères nuls.
PDFParserArraysContainsNullCount	Le fichier contient un nombre anormalement élevé de valeurs nulles dans les matrices.
PDFParserArraysHeterogeneous Nombre	Le fichier contient un nombre anormalement élevé de matrices comprenant différents types d'éléments.
PDFParserMailtoURICount	Le fichier contient un nombre anormalement élevé de liens d'e-mail (mailto:).

Indicateur	Description
PDFParserMinPageCount	Le fichier présente une structure inhabituelle d'objets de page, notamment un nombre élevé d'objets de page enfant par nœud.
PDFParserNamesPoundName MaxLength	Le fichier peut tenter d'obscurcir son contenu en utilisant de longues chaines codées.
PDFParserNamesPoundName MinLength	Le fichier contient une longueur minimale de nom d'échappement anormalement élevée.
PDFParserNamesPoundName TotalLength	Le fichier peut tenter d'obscurcir son contenu en stockant une grande partie de son contenu dans des chaines codées.
PDFParserNamesPoundName UpperCount	Le fichier contient un nombre anormalement élevé de noms d'échappement avec des caractères hexadécimaux en majuscules.
PDFParserNamesPoundName ValidCount	Le fichier contient un nombre anormalement élevé de noms d'échappement valides.
PDFParserNamesPoundPerName MaxCount	Le fichier contient un nombre maximal de caractères d'échappement par nom unique anormalement élevé.
PDFParserNamesPound UnnecessaryCount	Le fichier contient un nombre anormalement élevé de noms d'échappement inutiles.
PDFParserNumbersLeading DigitTallies8	Le fichier contient un nombre anormalement élevé de nombres commençant par 8 dans la représentation décimale.
PDFParserNumbersPlusCount	Le fichier contient un nombre anormalement élevé de nombres avec le signe plus explicite.
PDFParserNumbersRealMax RawLength	Le fichier contient une longueur maximale de nombres réels anormalement élevée.
PDFParserPageCounts	Le fichier contient un nombre anormalement élevé d'objets de page enfant.
PDFParserPageObjectCount	Le fichier contient un nombre anormalement élevé d'objets de page.
PDFParserSizeEOF	Le fichier contient une ou plusieurs séquences de fin de fichier anormalement longues.
PDFParserStringsHexLowerCount	Le fichier contient un nombre anormalement élevé de chaines d'échappement avec des chiffres hexadécimaux en minuscules.

Indicateur	Description
PDFParserStringsLiteralString MaxLength	Le fichier contient une longueur maximale de chaine littérale anormalement élevée.
PDFParserStringsOctalZero PaddedCount	Le fichier contient un nombre de caractères d'échappement octaux anormalement élevé dans des chaines qui sont inutilement complétées à zéro.
PDFParserTrailerSpread	Le fichier contient une propagation anormalement importante entre les objets de fin.
PDFParserWhitespaceComment MaxLength	La longueur maximale d'un commentaire dans le fichier est anormalement élevée.
PDFParserWhitespaceComment MinLength	Le fichier contient de brefs commentaires inhabituels qui ne sont pas utilisés par le logiciel de lecture.
PDFParserWhitespaceComment TotalLength	Le fichier contient une quantité anormalement importante de données commentées.
PDFParserWhitespaceEOL0ACount	Le fichier contient un nombre anormalement élevé de caractères de fin de ligne courts.
PDFParserWhitespaceWhitespace 00Count	Le fichier contient un nombre anormalement élevé d'octets nuls utilisés comme espaces.
PDFParserWhitespaceWhitespace 09Count	Le fichier contient un nombre anormalement élevé d'octets 09 utilisés comme espace.
PDFParserWhitespaceWhitespace LongestRun	Le fichier contient une zone d'espace anormalement longue.
PDFParserWhitespaceWhitespace TotalLength	Le fichier contient un nombre d'espaces anormalement élevé.
PDFParseru3DObjectsNames AllNames	Le fichier contient un nombre anormalement élevé d'objets U3D.
PossibleBAT	Le fichier contient la preuve qu'un fichier batch Windows standard est inclus. Le logiciel malveillant évite les techniques d'analyse courantes et assure sa persistance.
PossibleDinkumware	Le fichier inclut certains composants de DinkumWare. Dinkumware est fréquemment utilisé dans divers composants malveillants.
PropertyImpropriety	Le fichier contient des propriétés OOXML suspectes.

Indicateur	Description
RaiseExceptionImports	Le fichier importe des fonctions utilisées pour générer des exceptions au sein d'un programme. Les logiciels malveillants mettent en place des tactiques pour rendre l'analyse de code dynamique standard difficile à suivre.
ReservedFieldsViolation	Le fichier enfreint la spécification concernant l'utilisation de champs réservés.
ResourceAnomaly	La section des ressources de ce fichier contient une anomalie. Les logiciels malveillants contiennent souvent des bits dont le format est incorrect ou des bits impairs dans la section des ressources d'une DLL.
RWXSection	Ce PE peut contenir un code modifiable, qui est dans le meilleur des cas non orthodoxe et dans le pire des cas symptomatique d'une infection virale. Cette fonction implique souvent que le fichier n'a pas été créé à l'aide d'un compilateur standard ou qu'il a été modifié après sa création initiale.
SectorMalfeasance	Le fichier contient des anomalies structurelles avec l'allocation de secteur OLE.
StringInvalid	L'une des références à une chaine dans une table de chaines pointe vers un décalage négatif.
StringTableNotTerminated	Une table de chaines ne se termine pas par un octet nul. Cela peut entrainer une erreur lors de l'exécution en raison d'une chaine qui ne se termine pas.
StringTruncated	L'une des références à une chaine dans une table de chaines a pointé vers un emplacement après la fin du fichier.
SuspiciousPDataSection	Ce PE masque un élément difficile à identifier dans la zone pdata. La section « pdata » d'un fichier PE est généralement utilisée pour traiter les structures d'exécution, mais ce fichier particulier contient autre chose.
SuspiciousRelocSection	Ce PE masque un élément difficile à identifier dans la zone « relocations ». La zone « relocations » d'un fichier PE est généralement utilisée pour déplacer des symboles particuliers, mais ce fichier particulier contient autre chose.
SuspiciousDirectoryNames	Le fichier contient des noms de répertoire OLE associés à une malveillance.
SuspiciousDirectoryStructure	Le fichier signale des anomalies dans la structure de répertoire OLE.
SuspiciousEmbedding	Le fichier utilise une intégration suspecte d'OLE.
SuspiciousVBA	Le fichier contient un code VBA suspect.
SuspiciousVBALib	Le fichier indique une utilisation suspecte de la bibliothèque VBA.

Indicateur	Description
SuspiciousVBANames	Le fichier contient des noms suspects associés aux structures VBA.
SuspiciousVBAVersion	Le fichier contient des versions VBA suspectes.
SWFOddity	Le fichier contient certaines utilisations suspectes du SWF intégré.
TooMalformedToProcess	Le fichier est incorrectement formé, à tel point qu'il est impossible à analyser dans son intégralité.
VersionAnomaly	Le fichier rencontre des problèmes avec la façon dont il présente ses informations de version. Les logiciels malveillants procèdent ainsi pour ne pas être détectés.

Collection

Ces indicateurs représentent les situations dans lesquelles le fichier contient des éléments qui indiquent des fonctions ou des preuves de collecte de données. Il peut s'agir de l'énumération de la configuration du système ou de la collecte d'informations sensibles spécifiques.

Indicateur	Description
BrowserInfoTheft	Le fichier contient la preuve d'une intention de lire les mots de passe stockés dans le cache du navigateur. Les logiciels malveillants utilisent cette fonctionnalité pour recueillir les mots de passe pour exfiltration.
CredentialProvider	Le fichier contient la preuve d'une interaction avec un fournisseur d'informations d'identification ou le souhait d'apparaitre comme tel. Les logiciels malveillants procèdent de cette manière lorsque les fournisseurs d'informations d'identification accèdent à de nombreux types de données sensibles, tels que les noms d'utilisateur et les mots de passe. Ce faisant, ils peuvent compromettre l'intégrité de l'authentification.
CurrentUserInfoImports	Le fichier importe des fonctions utilisées pour collecter les informations sur l'utilisateur actuellement connecté. Les logiciels malveillants déterminent des moyens d'action pour escalader les privilèges et mieux adapter les futures attaques.
DebugStringImports	Le fichier importe des fonctions utilisées pour générer les chaines de débogage. En général, cette fonction est désactivée dans les logiciels de production, mais reste activée dans les logiciels malveillants en cours de test.
DiskInfoImports	Le fichier importe des fonctions pouvant être utilisées pour collecter les détails des volumes sur le système. Les logiciels malveillants l'utilisent conjointement avec la liste pour déterminer des éléments sur les volumes en vue d'une nouvelle attaque.
EnumerateFileImports	Le fichier importe des fonctions utilisées pour répertorier les fichiers. Les logiciels malveillants l'utilisent pour rechercher des données sensibles ou d'autres points d'attaque.

Indicateur	Description
EnumerateModuleImports	Le fichier importe des fonctions pouvant être utilisées pour dresser la liste de toutes les DLL qu'un processus en cours d'exécution utilise. Les programmes malveillants utilisent cette fonctionnalité pour localiser et cibler des bibliothèques spécifiques à charger dans un processus et pour mapper un processus qu'ils souhaitent injecter.
EnumerateNetwork	Le fichier démontre une capacité à tenter d'énumérer les réseaux et cartes réseau connectés. Les logiciels malveillants le font pour déterminer l'emplacement d'un système cible par rapport aux autres et pour rechercher d'éventuels chemins latéraux.
EnumerateProcessImports	Le fichier importe des fonctions pouvant être utilisées pour dresser la liste de tous les processus en cours d'exécution sur un système. Les logiciels malveillants l'utilisent pour localiser les processus dans lesquels injecter ou ceux qu'ils souhaitent supprimer.
EnumerateVolumeImports	Le fichier importe des fonctions pouvant être utilisées pour répertorier les volumes sur le système. Les logiciels malveillants l'utilisent pour trouver toutes les zones dont ils pourraient avoir besoin pour rechercher des données ou propager une infection.
GinaImports	Le fichier importe des fonctions utilisées pour accéder à Gina. Un logiciel malveillant l'utilise pour tenter de violer le système de saisie de mot de passe sécurisé Ctrl+Alt+Suppr ou d'autres fonctions de connexion au réseau.
HostnameSearchImports	Le fichier importe des fonctions utilisées pour collecter des informations relatives aux noms d'hôte sur le réseau et au nom d'hôte de la machine proprement dite. Le logiciel malveillant utilise cette fonctionnalité pour mieux cibler d'autres attaques ou rechercher de nouvelles cibles.
KeystrokeLogImports	Le fichier importe des fonctions pouvant capturer et consigner les frappes de touches à partir du clavier. Les logiciels malveillants tentent ici de capturer et d'enregistrer les frappes de touches afin de trouver des informations sensibles telles que les mots de passe.
OSInfoImports	Le fichier importe des fonctions utilisées pour collecter des informations sur le système d'exploitation actuel. Les logiciels malveillants utilisent cette fonctionnalité pour déterminer comment mieux adapter les attaques et transmettre des informations à un contrôleur.
PossibleKeylogger	Le fichier contient des preuves d'activité de type enregistreur de frappe. Les logiciels malveillants utilisent des enregistreurs de frappe pour recueillir des informations sensibles à partir du clavier.
PossiblePasswords	Le fichier inclut des mots de passe communs ou une structure permettant le forçage brut des mots de passe communs. Les logiciels malveillants tentent ici de pénétrer dans un réseau en accédant à d'autres ressources à l'aide de mots de passe.

Indicateur	Description
ProcessorInfoWMI	Le fichier importe des fonctions pouvant être utilisées pour déterminer des informations détaillées sur le processeur. Les logiciels malveillants l'utilisent pour adapter les attaques et exfiltrer ces données vers une infrastructure de commande et de contrôle commune.
RDPUsage	Le fichier interagit avec le protocole RDP (Remote Desktop Protocol). Les logiciels malveillants l'utilisent pour se déplacer latéralement et offrir des fonctionnalités de commande et de contrôle directes.
SpyString	Le fichier exécute probablement un logiciel espion qui surveille le presse-papiers ou les actions de l'utilisateur lors de l'utilisation de l'API d'accessibilité.
SystemDirImports	Le fichier importe des fonctions servant à localiser le répertoire système. Les logiciels malveillants tentent ici de localiser un grand nombre de fichiers binaires système installés, car ils se cachent souvent parmi eux.
UserEnvInfoImports	Le fichier importe des fonctions servant à collecter des informations sur l'environnement de l'utilisateur actuellement connecté. Les logiciels malveillants tentent ici de déterminer les détails de l'utilisateur connecté et de rechercher d'autres informations pouvant être obtenues à partir des variables d'environnement.

Perte de données

Ces indicateurs représentent les situations dans lesquelles le fichier contient des éléments qui indiquent des fonctions ou des preuves d'exfiltration de données. Il peut s'agir de connexions réseau sortantes, de preuves d'agissement en tant que navigateur ou d'autres communications réseau.

Indicateur	Description
AbnormalNetworkActivity	Le fichier implémente une méthode de mise en réseau non standard. Les programmes malveillants tentent ici d'éviter la détection d'approches réseau plus courantes.
BrowserPluginString	Le fichier indique la capacité d'énumérer ou d'installer des plug-ins de navigateur.
ContainsBrowserString	Le fichier contient la preuve d'une tentative de création d'une chaine UserAgent personnalisée. Les logiciels malveillants utilisent fréquemment des chaines UserAgent courantes pour ne pas être détectés dans les requêtes sortantes.
DownloadFileImports	Le fichier importe des fonctions pouvant être utilisées pour télécharger des fichiers sur le système. Les logiciels malveillants l'utilisent pour déclencher une attaque et exfiltrer les données via l'URL sortante.
FirewallModifyImports	Le fichier importe des fonctions capables de modifier le pare-feu Windows local. Les logiciels malveillants l'utilisent pour ouvrir des brèches et éviter d'être détectés.

Indicateur	Description
HTTPCustomHeaders	Le fichier contient des preuves de la création d'autres entêtes HTTP personnalisés. Les logiciels malveillants tentent ici de faciliter les interactions avec les infrastructures de commande et de contrôle et d'éviter toute détection.
IRCCommands	Le fichier contient des preuves d'interaction avec un serveur IRC. Les logiciels malveillants utilisent généralement IRC pour faciliter une infrastructure de commande et de contrôle.
MemoryExfiltrationImports	Le fichier importe des fonctions qui peuvent être utilisées pour lire la mémoire à partir d'un processus en cours d'exécution. Les logiciels malveillants l'utilisent pour déterminer les emplacements appropriés dans lesquels s'insérer ou pour extraire des informations utiles de la mémoire d'un processus en cours d'exécution, telles que des mots de passe, des données de carte de crédit ou d'autres informations sensibles.
NetworkOutboundImports	Le fichier importe des fonctions qui peuvent être utilisées pour envoyer des données hors du réseau ou d'Internet. Les logiciels malveillants l'utilisent pour exfiltrer des données ou comme méthode de commande et de contrôle.
PipeUsage	Le fichier importe des fonctions qui permettent la manipulation de canaux nommés. Les logiciels malveillants l'utilisent comme méthode de communication et d'exfiltration des données.
RPCUsage	Le fichier importe des fonctions qui lui permettent d'interagir avec une infrastructure RPC (Remote Procedure Call). Les logiciels malveillants l'utilisent pour diffuser ou envoyer des données à des systèmes distants à des fins d'exfiltration.

Tromperie

Ces indicateurs représentent les situations dans lesquelles le fichier contient des éléments qui indiquent des fonctions ou des preuves d'un fichier trompeur. La tromperie peut prendre la forme de sections masquées, d'inclusion de code pour éviter la détection ou d'indications qu'elle est mal étiquetée dans les métadonnées ou d'autres sections.

Indicateur	Description
AddedHeader	Le fichier contient un entête PE obscurci supplémentaire qui peut être une charge utile malveillante masquée.
AddedKernel32	Le fichier contient une référence obscurcie supplémentaire à kernel32.dll, une bibliothèque qui peut être utilisée par une charge utile malveillante.
AddedMscoree	Le fichier contient une référence obscurcie supplémentaire à mscoree.dll, une bibliothèque qui peut être utilisée par une charge utile malveillante.

Indicateur	Description
AddedMsvbvm	Le fichier contient une référence obscurcie supplémentaire à msvbvm, une bibliothèque qui peut être utilisée par une charge utile malveillante compilée pour Microsoft Visual Basic 6.
AntiVM	Le fichier présente des caractéristiques susceptibles de déterminer si le processus est en cours d'exécution sur une machine virtuelle. Les logiciels malveillants l'utilisent pour éviter de s'exécuter dans des bacs à sable virtualisés qui deviennent de plus en plus courants.
AutoitDownloadExecute	Le script AutoIt peut télécharger et exécuter des fichiers. Cette opération permet souvent de livrer des charges utiles malveillantes supplémentaires.
AutoitObfuscationStringConcat	Le script AutoIt est probablement obscurci par la concaténation de chaines. Cela permet souvent d'éviter la détection de commandes suspectes complètes.
AutoitShellcodeCalling	Le script AutoIt utilise la fonction d'API Windows CallWindowProc(), qui peut indiquer l'injection d'un shellcode.
AutoitUseResources	Le script AutoIt utilise des données provenant de ressources stockées avec le script. Les logiciels malveillants stockent souvent des parties importantes d'eux-mêmes sous forme de données de ressources, qu'ils décompactent lors de l'exécution, ce qui éveille la suspicion.
CabinentUsage	Le fichier inclut visiblement un fichier CAB. Les logiciels malveillants l'utilisent pour regrouper les composants sensibles de manière à ne pas être détectés.
ClearKernel32	Le fichier contient une référence à kernel32.dll, une bibliothèque qui peut être utilisée par une charge utile malveillante.
ClearMscoree	Le fichier contient une référence à mscoree.dll, une bibliothèque qui peut être utilisée par une charge utile malveillante.
ClearMsvbvm	Le fichier contient une référence à msvbvm.dll, une bibliothèque qui peut être utilisée par une charge utile malveillante compilée pour Microsoft Visual Basic 6.
ComplexInvalidVersion	Le fichier déclare la version PDF incorrecte.
ComplexJsStenographySuspected	Le fichier peut contenir du code JavaScript masqué dans des chaines littérales.
ContainsEmbeddedDocument	Le fichier contient un document incorporé dans l'objet. Les logiciels malveillants peuvent l'utiliser pour propager une attaque à plusieurs sources ou pour dissimuler sa véritable forme.

Indicateur	Description
CryptoKeys	Le fichier contient des preuves de la présence d'une clé cryptographique intégrée. Le logiciel malveillant procède ainsi pour éviter toute détection ou peut-être pour fournir une authentification avec des services à distance.
DebugCheckImports	Le fichier importe des fonctions qui lui permettent d'agir comme un débogueur. Les logiciels malveillants utilisent cette fonctionnalité pour lire et écrire à partir d'autres processus.
EmbeddedPE	Le PE en contient d'autres PE, ce qui est généralement le cas uniquement avec les programmes d'installation de logiciels. Les logiciels malveillants intègrent souvent un fichier PE qu'ils déposent sur le disque, puis exécutent. Cette technique est souvent utilisée pour éviter les scanneurs de protection en regroupant les fichiers binaires dans un format que la technologie de numérisation sous-jacente ne comprend pas.
EncodedDosStub1	Le fichier PE contient un élément de remplacement DOS PE obscurci qui peut appartenir à une charge utile malveillante masquée.
EncodedDosStub2	Le fichier PE contient un élément de remplacement DOS PE obscurci qui peut appartenir à une charge utile malveillante masquée.
EncodedPE	Le fichier PE contient des PE supplémentaires, ce qui est extrêmement suspect. Cet indicateur est similaire à l'indicateur EmbeddedPE, mais utilise un schéma de codage pour tenter de masquer davantage le code binaire à l'intérieur de l'objet.
ExecuteDLL	Le fichier PE contient une fonctionnalité permettant d'exécuter une DLL à l'aide de méthodes courantes. Les programmes malveillants utilisent cette méthode pour éviter les pratiques de détection courantes.
FakeMicrosoft	Le fichier PE prétend être écrit par Microsoft, mais il ne ressemble pas à un fichier PE Microsoft. Les logiciels malveillants se font généralement passer pour des fichiers PE Microsoft pour passer inaperçus.
HiddenMachO	Le fichier contient un autre fichier exécutable MachO, qui n'est pas correctement déclaré. Il peut s'agir d'une tentative visant à éviter que la charge utile ne soit facilement détectée.
HTTPCustomUserAgent	Le fichier contient des preuves de manipulation de la chaine UserAgent du navigateur. Les logiciels malveillants tentent ici de faciliter les interactions avec les infrastructures de commande et de contrôle et d'éviter toute détection.
InjectProcessImports	Le fichier PE peut injecter du code dans d'autres processus. Cette fonctionnalité implique souvent qu'un processus tente d'être trompeur ou hostile d'une manière ou d'une autre.

Indicateur	Description
InvisibleEXE	Le fichier PE semble s'exécuter de manière invisible, mais il ne s'agit pas d'un service en arrière-plan. Il peut être conçu pour rester caché.
JSTokensSuspicious	Le fichier contient un JavaScript inhabituellement suspect.
MSCertStore	Le fichier présente des signes d'interaction avec le magasin de certificats Windows principal. Les logiciels malveillants procèdent ainsi pour recueillir des informations d'identification et insérer des clés indésirables dans le flux, afin de faciliter des attaques par interception.
MSCryptoImports	Le fichier importe des fonctions pour utiliser la bibliothèque de cryptographie Windows de base. Les logiciels malveillants utilisent cette fonctionnalité pour exploiter la cryptographie installée en local et ne pas avoir à utiliser la leur.
PDFParserDotDotSlash1URICount	Le fichier peut effectuer une tentative Path Traversal à l'aide de chemins relatifs tels que « ../ ».
PDFParserJavaScriptMagicseval~28	Le fichier peut contenir un JavaScript obscurci ou exécuter un JavaScript chargé de manière dynamique avec eval().
PDFParserJavaScriptMagic sunescape~28	Le fichier peut contenir un JavaScript obscurci.
PDFParserjsObjectsLength	Le fichier contient un nombre anormalement élevé de scripts JavaScript individuels.
PDFParserJSStreamCount	Le fichier contient un nombre anormalement élevé de flux liés à JavaScript.
PDFParserJSTokenCounts0 cumulativesum	Le fichier contient un nombre anormalement élevé de jetons JavaScript.
PDFParserJSTokenCounts1 cumulativesum	Le fichier contient un nombre anormalement élevé de jetons JavaScript.
PDFParserNamesAllNames Suspicious	Le fichier contient un nombre anormalement élevé de noms suspects.
PDFParserNamesObfuscated NamesSuspicious	Le fichier contient un nombre anormalement élevé de noms obscurcis.
PDFParserPEDetections	Le fichier contient un ou plusieurs fichiers PE intégrés.
PDFParserSwfObjectsxObservations SWFObjectsversion	Le fichier contient un objet SWF avec un numéro de version inhabituel.

Indicateur	Description
PDFParserSwfObjectsxObservation sxSWFObjectsxZLibcmfSWFObjectsx ZLibcmf	Le fichier contient un objet SWF avec des paramètres de compression inhabituels.
PDFParserswfObjectsxObservations xSWFObjectsxZLibflg	Le fichier contient un objet SWF avec des paramètres d'indicateur de compression inhabituels.
PE_ClearDosStub1	Le fichier contient un élément de remplacement DOS, ce qui indique l'inclusion du fichier PE.
PE_ClearDosStub2	Le fichier contient un élément de remplacement DOS, ce qui indique l'inclusion du fichier PE.
PE_ClearHeader	Le fichier contient des données d'entête de fichier PE qui n'appartiennent pas à la structure du fichier.
PEinAppendedSpace	Le fichier contient un fichier PE qui n'appartient pas à la structure du fichier.
PEinFreeSpace	Le fichier contient un fichier PE qui n'appartient pas à la structure du fichier.
ProtectionExamination	Le fichier semble rechercher des systèmes de protection communs. Le programme malveillant procède ainsi pour lancer une action antiprotection adaptée à celle installée sur le système.
SegmentSuspiciousName	Un segment contient une chaine non valide, notamment un nom ou un nom non standard inhabituel. Cela peut indiquer une altération postcompilation ou l'utilisation de conditionneurs ou d'obscurcisseurs de code.
SegmentSuspiciousSize	La taille du segment est sensiblement différente de celle de l'ensemble des sections du contenu. Cela peut être le signe de l'utilisation d'une zone non référencée ou de la réservation d'espace pour la décompression du code malveillant pendant l'exécution.
SelfExtraction	Le fichier semble être une archive à extraction automatique. Les logiciels malveillants utilisent souvent cette tactique pour brouiller leurs véritables intentions.
ServiceDLL	Le fichier semble être une DLL de service. Les DLL de service sont chargées dans les processus svchost.exe et constituent une méthodologie de persistance courante pour les logiciels malveillants.
StringJsSplitting	Le fichier contient des jetons JS suspects.
SWFinAppendedSpace	Le fichier contient un objet flash Shockwave qui n'appartient pas à la structure du document.

Indicateur	Description
TempFileImports	Le fichier importe des fonctions utilisées pour accéder aux fichiers temporaires et les manipuler. Les logiciels malveillants procèdent ainsi, car les fichiers temporaires ont tendance à éviter la détection.
UsesCompression	Certaines parties du code du fichier semblent être compressées. Les logiciels malveillants utilisent ces techniques pour éviter la détection.
VirtualProtectImports	Le fichier importe des fonctions servant à modifier la mémoire d'un processus en cours d'exécution. Les logiciels malveillants procèdent ainsi pour s'injecter dans les processus en cours d'exécution.
XoredHeader	Le fichier contient un entête PE obscurci xor qui peut être une charge utile malveillante masquée.
XoredKernel32	Le fichier contient une référence obscurcie xor à kernel32.dll, une bibliothèque qui peut être utilisée par une charge utile malveillante.
XoredMscoree	Le fichier contient une référence obscurcie xor à mscoree.dll, une bibliothèque qui peut être utilisée par une charge utile malveillante.
XoredMsvbvm	Le fichier contient une référence obscurcie xor à msvbvm, une bibliothèque qui peut être utilisée par une charge utile malveillante compilée pour Microsoft Visual Basic 6.

Destruction

Ces indicateurs représentent les situations dans lesquelles le fichier contient des éléments qui indiquent des fonctions ou des preuves de destruction. Les fonctionnalités destructrices incluent la possibilité de supprimer des ressources système telles que des fichiers ou des répertoires.

Indicateur	Description
action_writeByte	Le script VBA dans le document écrit probablement des octets dans un fichier. Cette action est inhabituelle pour un document légitime.
action_hexToBin	Le script VBA du fichier utilise probablement une conversion hexadécimale en binaire, ce qui peut indiquer le décodage d'une charge utile malveillante masquée.
appended_URI	Le fichier contient un lien qui n'appartient pas à la structure du fichier.
appended_exploit	Le fichier contient des données suspectes en dehors de la structure du fichier, ce qui peut révéler la présence d'une faille.
appended_macro	Le fichier contient un script de macro qui n'appartient pas à la structure du fichier.
appended_90_nopsled	Le fichier contient un nop-sled qui n'appartient pas à la structure du fichier, ce qui sert vraisemblablement à faciliter l'exploitation d'une faille.

Indicateur	Description
AutorunsPersistence	Le fichier tente d'interagir avec les méthodes courantes de persistance (par exemple, les scripts de démarrage). Les logiciels malveillants utilisent généralement ces tactiques pour parvenir à la persistance.
DestructionString	Le fichier dispose de fonctionnalités permettant d'interrompre des processus ou d'arrêter la machine par l'intermédiaire de commandes shell.
FileDirDeleteImports	Le fichier PE importe des fonctions qui peuvent servir à supprimer des fichiers ou des répertoires. Les programmes malveillants utilisent cette méthode pour arrêter les systèmes et brouiller les pistes.
JsHeapSpray	Le fichier contient probablement un code HeapSpray.
PossibleLocker	Le fichier démontre la volonté de verrouiller les outils courants par stratégie. Les logiciels malveillants procèdent ainsi pour conserver la persistance et rendre la détection et le nettoyage plus difficiles.
RegistryManipulation	Le fichier importe des fonctions utilisées pour manipuler le registre Windows. Les logiciels malveillants procèdent ainsi pour parvenir à la persistance et éviter la détection, entre autres nombreuses raisons.
SeBackupPrivilege	Le fichier PE peut tenter de lire les fichiers auxquels il n'a pas accès. Le privilège SeBackup permet d'accéder aux fichiers sans respecter les contrôles d'accès. Il est fréquemment utilisé par les programmes qui gèrent les sauvegardes et se limite souvent aux administrateurs, mais peut être utilisé de manière malveillante pour accéder à des éléments spécifiques habituellement difficiles d'accès.
SeDebugPrivilege	Le fichier PE peut tenter d'altérer les processus système. Le privilège SeDebug permet d'accéder à des processus autres que les vôtres et se limite souvent aux administrateurs. Il est souvent associé à la lecture et à l'écriture dans d'autres processus.
SeRestorePrivilege	Le fichier PE peut tenter de modifier ou de supprimer les fichiers auxquels il n'a pas accès. Le privilège SeRestore permet l'écriture sans tenir compte du contrôle d'accès.
ServiceControlImports	Le fichier importe des fonctions pouvant contrôler les services Windows sur le système actuel. Un programme malveillant utilise cette fonctionnalité soit pour s'exécuter en arrière-plan (en s'installant en tant que service) soit pour désactiver d'autres services censés protéger le système.
SkylinedHeapSpray	Le fichier contient une version non modifiée du code HeapSpray de Skylined.

Indicateur	Description
SpawnProcessImports	Le fichier PE importe des fonctions pouvant être utilisées pour générer un autre processus. Les programmes malveillants utilisent cette fonctionnalité pour lancer les phases suivantes d'une infection, généralement téléchargées sur Internet.
StringJsExploit	Le fichier contient du code JavaScript capable de lancer des exploits.
StringJsObfuscation	Le fichier contient des jetons d'obfuscation JavaScript.
TerminateProcessImports	Le fichier importe des fonctions pouvant être utilisées pour arrêter un processus en cours d'exécution. Les programmes malveillants utilisent cette fonctionnalité pour tenter de supprimer des systèmes de protection ou pour endommager un système en cours d'exécution.
trigger_AutoClose	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la fermeture du fichier.
trigger_Auto_Close	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la fermeture du fichier.
trigger_AutoExec	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement.
trigger_AutoExit	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la fermeture du document.
trigger_AutoNew	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la création d'un document.
trigger_AutoOpen	Le script VBA dans le fichier est susceptible de s'exécuter dès l'ouverture du fichier.
trigger_Auto_Open	Le script VBA dans le fichier est susceptible de s'exécuter dès l'ouverture du fichier.
trigger_DocumentBeforeClose	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement juste avant la fermeture du fichier.
trigger_DocumentChange	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la modification du fichier.
trigger_Document_Close	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la fermeture du fichier.
trigger_Document_New	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la création d'un fichier.
trigger_DocumentOpen	Le script VBA dans le fichier est susceptible de s'exécuter dès l'ouverture du fichier.

Indicateur	Description
trigger_Document_Open	Le script VBA dans le fichier est susceptible de s'exécuter dès l'ouverture du fichier.
trigger_NewDocument	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la création d'un fichier.
trigger_Workbook_Close	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de la fermeture d'une feuille de calcul Microsoft Excel.
trigger_Workbook_Open	Le script VBA dans le fichier est susceptible de s'exécuter automatiquement lors de l'ouverture d'une feuille de calcul Microsoft Excel.
UserManagementImports	Le fichier importe des fonctions pouvant être utilisées pour changer d'utilisateur sur le système local. Il peut ajouter, supprimer ou modifier des informations clés sur l'utilisateur. Les logiciels malveillants peuvent utiliser cette fonctionnalité pour assurer la persistance ou nuire au système local.
VirtualAllocImports	Le fichier importe des fonctions utilisées pour créer une mémoire dans un processus en cours d'exécution. Les logiciels malveillants procèdent ainsi pour s'injecter dans le processus en cours d'exécution.

Shellcodes

Ces indicateurs représentent les situations où un petit élément de code est utilisé comme charge utile dans l'exploitation d'une vulnérabilité logicielle. Cet élément est appelé « shellcode », car il démarre généralement un shell de commande à partir duquel l'utilisateur malveillant peut contrôler la machine compromise, bien que tout code qui effectue une tâche similaire puisse être appelé shellcode.

Indicateur	Description
ApiHashing	Le fichier contient une séquence d'octets ressemblant à un shellcode qui tente de détecter furtivement les API de bibliothèque chargées dans la mémoire.
BlackholeV2	Le fichier semble provenir du kit d'exploitation Blackhole.
ComplexGotoEmbed	Le fichier peut forcer un navigateur à accéder à une adresse ou à exécuter une action.
ComplexSuspiciousHeaderLocation	L'entête PDF est situé à un décalage différent de zéro, ce qui peut indiquer une tentative d'empêcher le fichier d'être reconnu comme un document PDF.
EmbeddedTiff	Le fichier peut contenir une image TIFF créée avec nop-sled pour faciliter l'exploitation d'une faille.
EmbeddedXDP	Le fichier contient probablement un autre PDF en tant que fichier XDP (XML Data Package).

Indicateur	Description
FindKernel32Base1	Le fichier contient une séquence d'octets ressemblant à un shellcode qui tente de localiser kernel32.dll dans la mémoire.
FindKernel32Base2	Le fichier contient une séquence d'octets ressemblant à un shellcode qui tente de localiser kernel32.dll dans la mémoire.
FindKernel32Base3	Le fichier contient une séquence d'octets ressemblant à un shellcode qui tente de localiser kernel32.dll dans la mémoire.
FunctionPrologSig	Le fichier contient une séquence d'octets qui est une fonction prolog classique susceptible de contenir un shellcode.
GetEIP1	Le fichier contient une séquence d'octets s'apparentant à un shellcode qui résout sa propre adresse pour localiser d'autres éléments en mémoire et faciliter l'exploitation.
GetEIP4	Le fichier contient une séquence d'octets s'apparentant à un shellcode qui résout sa propre adresse pour localiser d'autres éléments en mémoire et faciliter l'exploitation.
IndirectFnCall1	Le fichier contient une séquence d'octets qui s'apparente à un appel de fonction indirect, probablement un shellcode.
IndirectFnCall2	Le fichier contient une séquence d'octets qui s'apparente à un appel de fonction indirect, probablement un shellcode.
IndirectFnCall3	Le fichier contient une séquence d'octets qui s'apparente à un appel de fonction indirect, probablement un shellcode.
SehSig	Le fichier contient une séquence d'octets classique d'une gestion structurée des exceptions, qui contient probablement un shellcode.
StringLaunchAction Browser	Le fichier peut forcer un navigateur à accéder à une adresse ou à exécuter une action.
StringLaunchActionShell	Le fichier peut exécuter des actions de shell.
StringSingExploit	Le fichier peut contenir une exploitation.

Indicateurs divers

Cette section répertorie les indicateurs qui ne correspondent pas aux autres catégories.

Indicateur	Description
AutoitFileOperations	Le script AutoIt peut exécuter plusieurs actions sur les fichiers. Il peut être utilisé pour la collecte, la persistance ou la destruction d'informations.

Indicateur	Description
AutorunString	Le fichier a la capacité d'obtenir une persistance à l'aide d'un ou de plusieurs mécanismes d'exécution automatique.
CodepageLookupImports	Le fichier importe des fonctions utilisées pour rechercher la page de codes (emplacement) d'un système en cours d'exécution. Les programmes malveillants utilisent cette fonctionnalité pour différencier le pays/la région où un système est exécuté afin de mieux cibler des groupes particuliers.
MutexImports	Le fichier importe des fonctions pour créer et manipuler des objets mutex. Les logiciels malveillants utilisent fréquemment des objets mutex pour éviter d'infecter un système à plusieurs reprises.
OpenSSL statique	Le fichier contient une version d'OpenSSL compilée de telle manière qu'elle semble furtive. Les logiciels malveillants procèdent ainsi pour inclure la fonctionnalité de cryptographie sans paraitre suspects.
PListString	Le fichier a la capacité d'interagir avec les listes de propriétés utilisées par le système d'exploitation. Il peut donc obtenir une persistance ou compromettre divers processus.
PrivEscalationCryptBase	Le fichier tente d'utiliser une escalade de privilèges à l'aide de CryptBase. Les programmes malveillants procèdent ainsi pour obtenir plus de privilèges sur le système affecté.
ShellCommandString	Le fichier a la capacité d'utiliser des commandes shell sensibles à des fins de reconnaissance, d'élévation de privilèges ou de destruction de données.
SystemCallSuspicious	Le fichier a la capacité de surveiller et/ou de contrôler le système et d'autres processus, et d'effectuer des actions de type débogage.

Gérer les alertes de contrôle de script CylancePROTECT Desktop

Vous pouvez utiliser la console de gestion pour afficher et gérer les alertes de contrôle de script détectées par l'agent CylancePROTECT Desktop. Les scripts considérés comme dangereux s'affichent dans la console de gestion.

1. Dans la barre de menus de la console de gestion, cliquez sur **Protection > Contrôle de script**. Effectuez l'une des opérations suivantes :
   - Pour ajouter ou supprimer des colonnes, cliquez sur ||| et sélectionnez les colonnes que vous souhaitez afficher.
   - Pour trier les alertes de contrôle de script dans l'ordre croissant ou décroissant par colonne, cliquez sur la colonne.
   - Pour filtrer les alertes de contrôle de script par colonne, utilisez le champ de filtre et l'icône de la colonne.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Affichez les détails de l'alerte de contrôle de script.	**a.** Cliquez sur la ligne d'alerte de contrôle de script, mais pas sur la case à cocher. **b.** Affichez les terminaux affectés par l'alerte de contrôle de script. La liste des terminaux concernés s'affiche sous la liste des alertes de contrôle de script.
Ajoutez un script à la liste sécurisée globale.	Ajoutez un script à la liste sécurisée globale. **a.** Cochez les cases des scripts à ajouter à une liste globale. **b.** Cliquez sur **Sécurité**.
Affichez la page des détails du terminal.	**a.** Cliquez sur le nom du terminal pour afficher la page contenant ses détails.

À la fin : Pour exporter les informations de contrôle de script dans un fichier .csv, cliquez sur  . Sélectionnez la portée de l'exportation et cliquez sur **Exporter**.

Gérer les alertes de terminal externe CylancePROTECT Desktop

Vous pouvez utiliser la console de gestion pour afficher et gérer les alertes de terminal externe détectées par l'agent CylancePROTECT Desktop. Les smartphones, les clés USB, les disques durs externes et les appareils photo numériques sont des exemples de terminaux externes. Les paramètres des terminaux externes sont également appelés contrôle de terminal.

Avant de commencer : Avant d'exclure un terminal externe, tenez compte des points suivants :

- L'ajout d'une exclusion contenant des traits de soulignement dans le numéro de série n'est pas pris en charge à partir de la page des alertes de terminal externe. Vous devez ajouter l'exclusion dans la stratégie de terminal.
- L'ajout d'une exclusion à partir de la page des alertes de terminal externe affecte la stratégie actuellement attribuée au terminal, qui peut ne pas être la stratégie utilisée lorsque l'alerte s'est produite.

1. Dans la barre de menus de la console de gestion, cliquez sur **Protection > Terminaux externes**. Effectuez l'une des opérations suivantes :
   - Pour ajouter ou supprimer des colonnes, cliquez sur  et sélectionnez les colonnes que vous souhaitez afficher.
   - Pour regrouper les informations d'alerte de terminal externe par une ou plusieurs colonnes, faites glisser ces colonnes dans l'espace au-dessus des noms de colonne.
   - Pour trier les alertes de terminal externe dans l'ordre croissant ou décroissant par colonne, cliquez sur la colonne.
   - Pour filtrer les alertes de terminal externe par colonne, utilisez le champ de filtre et l'icône de la colonne.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Ajoutez le terminal externe à la liste d'exclusion des stratégies de terminal.	Les exclusions de terminaux externes sont configurées dans une stratégie de terminal. L'ajout d'une exclusion à partir de la page des alertes de terminal externe ajoute l'exclusion à la stratégie de terminal attribuée au terminal sur lequel l'alerte a été détectée. **a.** Cliquez sur ⊕ pour l'alerte de terminal externe pour laquelle ajouter une exclusion de stratégie de terminal. **b.** Vous pouvez également modifier l'ID du produit et le numéro de série du terminal externe. L'ID fournisseur ne peut pas être modifié. **c.** Vous pouvez également ajouter un commentaire. Vous pouvez fournir un motif d'exclusion ou d'autres informations pertinentes. **d.** Sélectionnez l'un des types d'accès suivants : • Accès complet : permet au terminal externe de se connecter au point de terminaison et fournit un accès complet au terminal externe (accès en lecture et en écriture). • Lecture seule : permet au terminal externe de se connecter au point de terminaison et fournit un accès en lecture seule au terminal externe. • Bloquer : ne permet pas au terminal externe de se connecter au point de terminaison. **e.** Cliquez sur **Enregistrer l'exclusion**.
Affichez la page des détails du terminal.	**a.** Cliquez sur le nom du terminal pour afficher la page contenant ses détails.

À la fin : Pour exporter les informations des terminaux externes dans un fichier .csv, cliquez sur  . Sélectionnez la portée de l'exportation et cliquez sur **Exporter**.

Protection contre les menaces

CylancePROTECT Desktop peut faire plus que simplement classer les fichiers comme dangereux ou anormaux. Il peut fournir des détails sur les caractéristiques statiques et dynamiques des fichiers. Cela vous permet non seulement de bloquer les menaces, mais également de comprendre leur comportement afin de mieux les atténuer ou y répondre.

Score Cylance

Le score Cylance représente le niveau de confiance selon lequel le fichier constitue un réel danger pour votre environnement. Plus le score est élevé, plus le niveau de confiance selon lequel le fichier peut être utilisé à des fins malveillantes est élevé. En fonction du score, les menaces sont considérées comme dangereuses ou anormales.

Le score des fichiers identifiés comme présentant une menace potentielle s'affichent en rouge (dangereux ou anormal). Le score des fichiers identifiés comme sécurisés s'affichent en vert. Dans des circonstances normales, les fichiers sécurisés (vert) ne s'affichent pas sur la console. Les fichiers sécurisés qui s'affichent sur la console ont généralement été ajoutés à votre liste de quarantaine globale et mis en quarantaine sur un terminal.

Les fichiers qui seraient considérés comme dangereux/anormaux (rouge) sont traités comme sécurisés si vous les ajoutez à votre liste sécurisée globale et ne s'afficheront pas sur la console.

Parfois, un fichier peut être classé comme dangereux ou anormal même si le score affiché ne correspond pas à la plage de score. Cela peut être dû à des résultats de mise à jour ou à une analyse de fichier supplémentaire qui peut avoir eu lieu après la détection initiale. Pour obtenir une analyse des menaces à jour, activez le chargement automatique dans la stratégie.

Le score Cylance ne dépend pas de la classification des menaces. La plupart des classifications de menaces sont des processus manuels réalisés par un chercheur de menaces et attribués fichier par fichier. Il est possible qu'un fichier présente un score Cylance sans classification avant une date ultérieure.

Fichiers dangereux et anormaux

BlackBerry regroupe les alertes de menace CylancePROTECT Desktop à l'aide du score Cylance pour la menace. Cela simplifie les actions telles que l'ajout automatique de menaces dangereuses et anormales à la liste de quarantaine globale à l'aide d'une stratégie de terminal.

- **Dangereux :** fichier dont le score est compris entre 60 et 100. Les attributs d'un fichier non sécurisé sont très similaires à un programme malveillant.
- **Anormal :** fichier dont le score est compris entre 1 et 59. Un fichier anormal possède quelques attributs de programme malveillant, mais ils sont moins nombreux que ceux d'un fichier non sécurisé ; il est donc moins susceptible d'être un programme malveillant.

Parfois, un fichier peut être classé comme dangereux ou anormal même si le score affiché ne correspond pas à la plage de classification. Cela peut être dû à des résultats mis à jour ou à une analyse de fichier supplémentaire suite à la détection initiale. Pour obtenir une analyse des menaces à jour, activez le chargement automatique dans la Terminal stratégie de terminal.

Classification des fichiers

Le tableau suivant répertorie les entrées d'état de fichier possibles pouvant s'afficher pour chaque menace CylancePROTECT Desktop.

État du fichier	Description
Fichier non disponible	En raison d'une contrainte de chargement (par exemple, le fichier est trop volumineux), le fichier n'est pas disponible pour analyse. Contactez le support technique BlackBerry pour obtenir une autre méthode de transfert du fichier.
Entrée vide	Le fichier n'a pas encore été analysé. Lorsqu'une analyse est terminée, un nouvel état est attribué.
Approuvé : local	Le fichier est considéré comme sûr. Vous pouvez ajouter le fichier à la liste sécurisée globale afin qu'il soit autorisé à s'exécuter et ne génère pas d'alertes lorsqu'il est identifié sur d'autres terminaux.

État du fichier	Description
PUP	Le fichier est un programme potentiellement indésirable (PUP), indiquant qu'il peut être dangereux même si un utilisateur a consenti à le télécharger. L'exécution de certains PUP peut être autorisée sur un ensemble limité de systèmes de votre organisation (par exemple, une application VNC autorisée à s'exécuter sur des terminaux d'administrateurs de domaine). Vous pouvez choisir d'ignorer ou de bloquer les PUP par terminal, ou de les ajouter à la liste de quarantaine globale ou à la liste sécurisée en fonction des normes de votre organisation. Le fichier peut avoir l'une des sous-classes suivantes : • Logiciel de publicité • Corrompu • Jeu • Générique • Outil de piratage • Application portable (ne nécessite pas d'installation) • Outil de script • Barre d'outils
Utilisation double	Le fichier peut être utilisé à des fins malveillantes et non malveillantes. Par exemple, bien que PsExec soit un outil utile pour exécuter des processus sur un autre système, cette même fonctionnalité peut être utilisée pour y exécuter des fichiers malveillants. Le fichier peut avoir l'une des sous-classes suivantes : • Piratage (modifie une autre application pour contourner les limitations de licence) • Générique • Keygen (générer, révéler ou récupérer des clés de produit) • Outil de surveillance • Piratage de mot de passe • Accès à distance • Outil (programmes administratifs pouvant faciliter une attaque)

État du fichier	Description
Logiciels malveillants	Le fichier a été identifié comme un logiciel malveillant conçu pour perturber, endommager ou obtenir un accès non autorisé à votre réseau. Il doit être supprimé dès que possible. Le fichier peut avoir l'une des sous-classes suivantes : • Porte dérobée • Bot • Téléchargeur • Programme malveillant de diffusion • Exploitation • Fausse alerte • Générique • Programme renifleur d'informations • Parasite • Rançon • Restant • Rootkit • Cheval de Troie • Virus • Ver informatique
Éventuel logiciel malveillant	Le fichier a été identifié comme logiciel suspect et est considéré comme anormal ou dangereux. Vous pouvez l'ajouter à la liste de quarantaine globale ou à la liste sécurisée en fonction des normes de votre organisation.

Évaluer le niveau de risque d'un fichier

Vous pouvez utiliser la console de gestion pour évaluer le niveau de risque d'un fichier, tel qu'analysé et déterminé par les services cloud CylancePROTECT. Cette fonctionnalité vous donne un aperçu de la manière dont l'agent CylancePROTECT Desktop classifie un fichier qu'il identifie sur un terminal. Actuellement, les exécutables Windows, macOS et Linux sont pris en charge.

Avant de commencer : Vous devez disposer du rôle Administrateur pour accéder à cette fonctionnalité dans la console.

1. Dans la barre de menus de la console de gestion, cliquez sur **Protection > Analyse des menaces**.
2. Effectuez l'une des opérations suivantes :

Action	Étapes
Recherchez un fichier par hachage.	Dans le champ **Hachages**, saisissez ou collez les hachages SHA256, en séparant chaque hachage sur une nouvelle ligne. Vous pouvez ajouter jusqu'à 32 hachages.
Chargez un fichier	La taille maximale d'un fichier que vous pouvez charger est de 10 Mo. **a.** Dans l'onglet **Charger un fichier**, cliquez sur **Parcourir les fichiers**. **b.** Accédez au fichier à analyser et sélectionnez-le. Cliquez sur **Ouvrir**.

3. Cliquez sur **Analyser**.

4. Vérifiez l'état du fichier pour déterminer si une menace a été trouvée ou si le fichier est considéré comme sûr.

   Si vous recevez l'état **Fichier requis** après avoir effectué une recherche de fichier par hachage SHA256, chargez le fichier dans l'onglet **Charger le fichier**.

À la fin : Si nécessaire, ajoutez un fichier à la liste de quarantaine globale ou à la liste de sécurité globale. Pour obtenir des instructions, reportez-vous à Ajouter un fichier à la liste de quarantaine globale CylancePROTECT Desktop ou à la liste sécurisée globale.

Utilisation des rapports CylancePROTECT Desktop

Dans la barre de menus, vous pouvez cliquer sur Rapports pour afficher les rapports CylancePROTECT Desktop suivants. Les rapports sont interactifs, ce qui vous permet de sélectionner des données pour afficher plus de détails.

Signaler	Description
Aperçu CylancePROTECT	Ce rapport fournit un résumé analytique de l'utilisation de CylancePROTECT Desktop, notamment le nombre de zones et de terminaux, le pourcentage de terminaux couverts par la mise en quarantaine automatique et la protection de la mémoire, ainsi que des résumés des évènements de menace, des violations de mémoire, des versions d'agent et un décompte hors ligne des terminaux CylancePROTECT Desktop.
Résumé des évènements de menace	Ce rapport indique le nombre de fichiers identifiés comme étant des programmes malveillants ou potentiellement indésirables (PUP), et comprend une répartition des sous-catégories spécifiques. Les dix principales listes des propriétaires de fichiers et des terminaux avec des menaces affichent le nombre d'évènements de menace pour les programmes malveillants, les PUP et les familles de menaces à double usage.
Résumé du terminal	Ce rapport affiche les données récapitulatives des terminaux CylancePROTECT Desktop.
Évènements de menace	Ce rapport fournit des données détaillées sur les évènements de menace identifiés par l'agent CylancePROTECT Desktop.
Terminaux	Ce rapport affiche le nombre de terminaux CylancePROTECT Desktop par système d'exploitation.

Les rapports affichent les menaces de manière basée sur les évènements. Un évènement représente une instance individuelle d'une menace. Par exemple, si un fichier particulier se trouve dans trois emplacements de dossier différents sur un terminal, le nombre d'évènements de menace sera égal à trois. Les données de rapport sont actualisées toutes les trois minutes environ. Vous pouvez exporter les rapports d'aperçu CylancePROTECT, de résumé des évènements de menace et de résumé du terminal au format .png, et les rapports des évènements de menace et des terminaux au format .csv.

Récupération des rapports de données sur les menaces avec une application tierce

Vous pouvez également accéder à des rapports détaillés sur les données de menace et les télécharger à l'aide des URL répertoriées dans la section Rapport sur les données de menace dans Paramètres > Application. Les URL utilisent un jeton unique généré par la console de gestion et affiché dans Paramètres > Application. Vous pouvez supprimer et régénérer le jeton si nécessaire. Notez que la régénération du jeton rend les jetons précédents non valides. Si vous souhaitez utiliser une application tierce pour récupérer des rapports à partir de ces URL, l'application et le système d'exploitation hôte doivent utiliser :

- TLS 1.2
- Les codages supportés par la stratégie TLSv1.2_2021

Gestion des menaces détectées par CylancePROTECT Mobile

Vous pouvez utiliser la console de gestion pour afficher une liste collective des menaces mobiles que l'application CylancePROTECT Mobile a détectées sur les terminaux des utilisateurs. Les alertes sont stockées pendant 120 jours maximum. Si vous désactivez le service CylancePROTECT Mobile pour un utilisateur, toutes les alertes qui lui sont associées sont supprimées de la console de gestion.

Afficher les alertes CylancePROTECT Mobile

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Alertes Protect Mobile**.

   Pour plus d'informations sur les alertes CylancePROTECT Mobile pouvant s'afficher sur cet écran, reportez-vous à Menaces mobiles détectées par l'application CylancePROTECT Mobile.
2. Vous pouvez également effectuer l'une des opérations suivantes :
   - Pour afficher les détails disponibles pour une alerte (par exemple, le temps de détection ou l'heure de la première installation), cliquez sur l'alerte.
   - Pour regrouper des alertes, cliquez sur la liste déroulante **Critère de groupement**, puis sur une option.
   - Pour trier les alertes dans l'ordre croissant ou décroissant en fonction d'une colonne, cliquez sur le nom de celle-ci.
   - Pour filtrer les alertes, cliquez sur dans une colonne et saisissez ou sélectionnez les critères de filtre.
   - Pour ignorer une ou plusieurs alertes, sélectionnez-les et cliquez sur **Ignorer**. Cliquez à nouveau sur **Ignorer** pour confirmer.
   - Pour exporter les résultats dans un fichier .csv, cliquez sur . Cliquez sur **Exporter**.

Vous pouvez utiliser les informations suivantes pour ajouter une application ou des certificats à la liste sécurisée ou restreinte CylancePROTECT Mobile :

- Dans le cas de menaces d'application chargée latéralement sous iOS, la colonne **Nom** affiche le nom commun du certificat de développeur.
- Dans le cas de menaces d'application chargée latéralement sous Android, la colonne **Description** affiche le hachage SHA256 de l'application.

Menaces mobiles détectées par l'application CylancePROTECT Mobile

Le tableau suivant répertorie les alertes pouvant être signalées dans la console de gestion dans Protection > Protéger les alertes mobiles :

Menace de sécurité mobile	Type d'alerte UI	Nom de l'alerte UI	Description de l'UI
Sécurité des applications : applications malveillantes	Application malveillante	Nom de l'application	Nom du package, version du package, hachage SHA256

Menace de sécurité mobile	Type d'alerte UI	Nom de l'alerte UI	Description de l'UI
Sécurité des applications : applications chargées latéralement	Application chargée latéralement	Android : nom de l'application iOS : clé de signature	Android : nom du package, version du package, source du programme d'installation, hachage SHA256
Sécurité des applications : applications limitées	Application limitée	Android : nom de l'application iOS : clé de signature	Android : nom du package, version du package, source du programme d'installation, hachage SHA256
Protection réseau : sécurité Wi-Fi	Wi-Fi non sécurisé	SSID de réseau Si désactivé par l'utilisateur : fonction désactivée par l'utilisateur	Algorithmes d'accès Wi-Fi
Protection réseau : connexion réseau	Réseau compromis	Type de réseau	SSID de réseau
Sécurité du terminal : modèle de terminal non pris en charge	Modèle de terminal non pris en charge	Nom de modèle	NA
Sécurité du terminal : système d'exploitation non pris en charge	Système d'exploitation non pris en charge	Nom du système d'exploitation, version du système d'exploitation	NA
Sécurité du terminal : correctif de sécurité non pris en charge	Correctif de sécurité non pris en charge	Version du correctif Lorsque la vérification du certificat d'attestation échoue : non approuvé	NA
Sécurité du terminal : détection flash/crack	Terminal compromis	Android : flashé iOS : cracké	Nom du système d'exploitation, version du système d'exploitation
Sécurité du terminal : chiffrement complet du disque	Cryptage désactivé	Cryptage désactivé	Nom du système d'exploitation, version du système d'exploitation
Sécurité du terminal : verrouillage de l'écran	Verrouillage d'écran désactivé	Verrouillage d'écran désactivé	Nom du système d'exploitation, version du système d'exploitation

Menace de sécurité mobile	Type d'alerte UI	Nom de l'alerte UI	Description de l'UI
Sécurité du terminal : options de développement	Mode développeur	Le mode développeur est activé	Nom du système d'exploitation, version du système d'exploitation
Sécurité du terminal : attestation Android SafetyNet ou Play Integrity	Échec d'attestation SafetyNet ou Play Integrity	Android SafetyNet Android Play Integrity	Type d'attestation, état d'attestation
Sécurité du terminal : Android attestation de certificat matériel	Échec de l'attestation matérielle	Matériel Android	Attestation de clé matérielle : type d'attestation, état d'attestation, échec de règle Autres détections : type d'attestation, état d'attestation
Sécurité des terminaux : attestation améliorée Samsung Knox	Échec de l'attestation améliorée Knox	Attestation améliorée Knox	Knox, échec du terminal
Sécurité du dispositif : contrôle d'intégrité iOS	Échec de l'attestation d'intégrité de l'application	Vérification de l'intégrité de l'application iOS	Type d'attestation, état d'attestation
Analyse des messages (s'affiche uniquement pour Android uniquement)	Message dangereux	SMS malveillant	Liste des URL malveillantes

Gestion des listes sécurisées et dangereuses pour CylancePROTECT Desktop et CylancePROTECT Mobile

Cette section fournit des informations sur l'ajout de fichiers et de certificats à des listes de quarantaine ou sécurisées pour CylancePROTECT Desktop, ainsi que sur l'ajout d'applications, de certificats de développeur, d'adresses IP et de domaines à des listes sécurisées ou restreintes pour CylancePROTECT Mobile.

Ajouter un fichier à la liste de quarantaine globale CylancePROTECT Desktop ou à la liste sécurisée globale

Vous pouvez ajouter un fichier à la liste de quarantaine globale pour le bloquer sur tous les terminaux CylancePROTECT Desktop. Ajoutez un fichier à la liste sécurisée globale pour l'autoriser sur tous les terminaux CylancePROTECT Desktop. La liste des fichiers non attribués est destinée aux fichiers répertoriés dans la console de gestion qui n'ont pas été mis en quarantaine globalement ou mis sur liste sécurisée.

Pour ajouter des fichiers à une liste de quarantaine locale ou à une liste sécurisée locale pour un terminal, reportez-vous à Ajoutez un fichier à la liste sécurisée locale ou à la liste de quarantaine locale CylancePROTECT Desktop.

Effectuez l'une des opérations suivantes :

Tâche	Étapes
Ajoutez un fichier à la liste de quarantaine ou de sécurité globale à partir de la page menaces.	**a.** Sur la barre de menus de la console de gestion, cliquez sur **Protection > Menaces**. **b.** Sélectionnez le fichier. **c.** Effectuez l'une des opérations suivantes : • Pour ajouter le fichier à la liste de quarantaine globale, cliquez sur **Quarantaine globale**. • Pour ajouter le fichier à la liste sécurisée globale, cliquez sur **Sécurisé**. **d.** Spécifiez les informations suivantes. **e.** Cliquez sur **Oui**.
Ajoutez manuellement un fichier à une liste de quarantaine globale ou à une liste sécurisée.	**a.** Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Liste globale**. **b.** Cliquez sur l'onglet **Quarantaine globale** ou **Sécurisé**. **c.** Cliquez sur **Ajouter un fichier**. **d.** Spécifiez les informations sur le fichier. **e.** Cliquez sur **Envoyer**.

Tâche	Étapes
Ajoutez un fichier à la liste de quarantaine globale ou à la liste sécurisée à partir de la liste non attribuée.	**a.** Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Liste globale**. **b.** Dans l'onglet **Non attribué**, sélectionnez le fichier. **c.** Effectuez l'une des opérations suivantes : • Pour ajouter le fichier à la liste de quarantaine globale, cliquez sur **Quarantaine globale**. • Pour ajouter le fichier à la liste sécurisée globale, cliquez sur **Sécurisé**. **d.** Spécifiez un motif pour l'ajout du fichier à la liste globale. **e.** Cliquez sur **Oui**.
Déplacer un fichier d'une liste globale à une autre.	**a.** Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Liste globale**. **b.** Cliquez sur l'onglet **Quarantaine globale** ou **Sécurisé**. **c.** Sélectionnez le fichier à déplacer. **d.** Effectuez l'une des opérations suivantes : • Pour déplacer le fichier dans la liste de quarantaine globale, cliquez sur **Quarantaine globale**. • Pour déplacer le fichier vers la liste sécurisée globale, cliquez sur **Sécurisé**. • Pour déplacer le fichier vers la liste non attribuée, cliquez sur **Supprimer de la liste**. **e.** Spécifiez les informations suivantes. **f.** Cliquez sur **Oui**.

Ajoutez un fichier à la liste sécurisée locale ou à la liste de quarantaine locale CylancePROTECT Desktop

Ajoutez un fichier à la liste de quarantaine locale pour le bloquer sur ce terminal. Ajoutez un fichier à la liste de dispense locale (sécurisée locale) pour ce terminal. Ces actions affectent uniquement le terminal, mais n'affectent pas les autres terminaux de l'organisation.

Pour ajouter des fichiers à la liste de quarantaine globale ou à la liste sécurisée globale CylancePROTECT Desktop, reportez-vous à la section Ajouter un fichier à la liste de quarantaine globale CylancePROTECT Desktop ou à la liste sécurisée globale.

1. Dans la barre de menus de la console de gestion , cliquez sur **Actifs > Terminaux**.
2. Cliquez sur un terminal.
3. Sous **Menaces**, sélectionnez le fichier.
4. Cliquez sur **Quarantaine** pour ajouter le fichier à la liste de quarantaine locale. Cliquez sur **Dispenser** pour ajouter le fichier à la liste de dispense locale (sécurisée locale).
5. Saisissez les informations requises.
6. Cliquez sur **Oui**.

Ajouter un certificat à la liste sécurisée globale CylancePROTECT Desktop

Pour les logiciels personnalisés correctement signés, ajoutez le certificat à la liste des certificats pour permettre au logiciel de s'exécuter sans interruption. Cela permet aux administrateurs de créer une liste sécurisée par certificat signé, représentée par l'empreinte SHA1 du certificat. Lors de l'ajout d'informations de certificat à la console de gestion, le certificat lui-même n'est pas téléchargé ni enregistré sur la console de gestion ; les informations sur le certificat sont extraites et enregistrées sur la console de gestion (horodatage, objet, émetteur et empreinte). L'horodatage du certificat représente le moment où le certificat a été créé. La console de gestion ne vérifie pas si le certificat est à jour ou a expiré. Si le certificat change (par exemple, il est renouvelé ou il s'agit d'un nouveau), il doit être ajouté à la liste sécurisée dans la console de gestion. La fonctionnalité de liste sécurisée par certificat fonctionne avec les macros PowerShell, ActiveScript et Office.

Cette fonctionnalité est actuellement compatible avec Windows et macOS uniquement.

Avant de commencer : Identifiez l'empreinte de certificat pour le fichier exécutable portable (PE) signé.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Certificats**.
2. Cliquez sur **Ajouter le certificat**.
3. Cliquez sur **Rechercher les certificats à ajouter** ou faites glisser le certificat dans la boîte de message. Si vous recherchez les certificats, la fenêtre Ouvrir s'affiche pour vous permettre de sélectionner les certificats.
4. Vous pouvez également sélectionner le type de fichier auquel s'applique le certificat avec l'option **S'applique à**, Exécutable ou Script. Cela vous permet d'ajouter un exécutable ou un script en fonction d'un certificat au lieu d'un emplacement de dossier.
5. Vous pouvez également ajouter des notes sur le certificat.
6. Cliquez sur **Envoyer**. L'émetteur, l'objet, l'empreinte numérique et les notes (le cas échéant) sont ajoutés au référentiel.

À la fin : Lorsqu'un certificat a expiré ou a été révoqué, vous devez le supprimer et ajouter un nouveau certificat émis. Pour supprimer un certificat, sélectionnez-le et cliquez sur **Supprimer de la liste**, puis cliquez sur **Oui** pour confirmer. Pour ajouter à nouveau un certificat valide, suivez les étapes ci-dessus.

Ajouter une application, un certificat, une adresse IP, un domaine ou une source de programme d'installation à une liste sécurisée ou restreinte CylancePROTECT Mobile

Vous pouvez utiliser les listes sécurisées et restreintes CylancePROTECT Mobile pour gérer les opérations suivantes :

- Ne pas soumettre une application ou un certificat de signature de développeur spécifique à la détection de logiciels malveillants et de chargements latéraux.
- Classer une application ou un certificat de signature de développeur spécifique comme une menace lors de la détection de logiciels malveillants et de charges latérales.
- Exempter une adresse IP ou un domaine de l'analyse des messages.
- Classer une adresse IP ou un domaine spécifique comme une menace pour l'analyse des messages.
- Ne pas soumettre une source spécifique de programme d'installation à la détection de charge latérale.
- Classer une source spécifique de programme d'installation comme une menace pour la détection de charge latérale.

Avant de commencer :

- Dans **Protection > Protéger les alertes mobiles**, vous pouvez cliquer sur les alertes pour afficher des détails tels que le hachage de l'application, les détails du certificat, les détails du package, etc. Vous pourrez avoir besoin de ces informations lorsque vous suivrez les étapes ci-dessous pour ajouter des éléments à la liste sécurisée ou restreinte.
- Si vous souhaitez ajouter un certificat de développeur Android à la liste sécurisée ou restreinte, vous devez obtenir l'empreinte du certificat à partir du binaire de l'application. Pour obtenir des instructions, reportez-vous à l'article KB 70577.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Liste globale (Mobile)**.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Ajoutez un certificat de développeur à la liste sécurisée de détection chargée latéralement ou de détection de programmes malveillants.	**a.** Dans l'onglet **Sécurité**, cliquez sur **Développeurs**. **b.** Cliquez sur **Ajouter le certificat**. **c.** Effectuez l'une des opérations suivantes : • Pour ajouter le certificat de signature à partir d'un fichier d'application, cliquez sur **Sélectionner une application pour obtenir les informations de certificat**. Accédez au fichier .apk ou .ipa et sélectionnez-le, puis cliquez sur **Envoyer**. • Pour saisir manuellement les informations du certificat, cliquez sur **Saisir manuellement les informations de certificat**. Spécifiez les détails du certificat et cliquez sur **Ajouter**. • Pour importer une liste de certificats à partir d'un fichier .csv, cliquez sur **Importer la liste de certificats à partir du fichier .csv**. Accédez au fichier et cliquez sur **Charger**. Lorsqu'un certificat a expiré ou a été révoqué, vous devez le supprimer manuellement et l'ajouter à nouveau. Pour supprimer un certificat, sélectionnez-le et cliquez sur **Supprimer**, puis sur **Oui** pour confirmer. Pour ajouter à nouveau un certificat valide, répétez les étapes ci-dessus.
Ajoutez un certificat de développeur à la liste restreinte de détection de charge latérale ou de détection de programmes malveillants. (Android uniquement)	**a.** Dans l'onglet **Restreint**, cliquez sur **Développeurs**. **b.** Cliquez sur **Ajouter le certificat**. **c.** Effectuez l'une des opérations suivantes : • Pour ajouter le certificat de signature à partir d'un fichier d'application, cliquez sur **Sélectionner une application pour obtenir les informations de certificat**. Accédez au fichier .apk et sélectionnez-le, puis cliquez sur **Envoyer**. • Pour saisir manuellement les informations du certificat, cliquez sur **Saisir manuellement les informations de certificat**. Spécifiez les détails du certificat et cliquez sur **Ajouter**. • Pour importer une liste de certificats à partir d'un fichier .csv, cliquez sur **Importer la liste de certificats à partir du fichier .csv**. Accédez au fichier et cliquez sur **Charger**. Lorsqu'un certificat a expiré ou a été révoqué, vous devez le supprimer manuellement et l'ajouter à nouveau. Pour supprimer un certificat, sélectionnez-le et cliquez sur **Supprimer**, puis sur **Oui** pour confirmer. Pour ajouter à nouveau un certificat valide, répétez les étapes ci-dessus.

Tâche	Étapes
Ajoutez une application à la liste sécurisée de détection chargée latéralement ou de détection de programmes malveillants.	**a.** Dans l'onglet **Sécurité**, cliquez sur **Applications**. **b.** Cliquez sur **Ajouter une application**. **c.** Effectuez l'une des opérations suivantes : • Pour ajouter un fichier d'application, cliquez sur **Sélectionner un fichier d'application**. Accédez au fichier .apk ou .ipa et sélectionnez-le, puis cliquez sur **Envoyer**. • Pour saisir manuellement le hachage de l'application, cliquez sur **Saisir manuellement les informations de hachage de l'application**. Spécifiez les détails de l'application et cliquez sur **Ajouter**. • Pour importer une liste d'applications à partir d'un fichier .csv, cliquez sur **Importer une liste d'applications à partir d'un fichier .csv**. Accédez au fichier et cliquez sur **Charger**. **Remarque :** Si une application contient plusieurs fichiers .apk, vous devez saisir manuellement le hachage de chaque fichier. Sinon, vous pouvez éventuellement ajouter le certificat de signature de l'application.
Ajoutez une application à la liste restreinte de détection des programmes malveillants. (Android uniquement)	**a.** Sous l'onglet **Restreint**, cliquez sur **Applications**. **b.** Cliquez sur **Ajouter une application**. **c.** Effectuez l'une des opérations suivantes : • Pour ajouter un fichier d'application, cliquez sur **Sélectionner un fichier d'application**. Accédez au fichier .apk et sélectionnez-le, puis cliquez sur **Envoyer**. • Pour saisir manuellement le hachage de l'application, cliquez sur **Saisir manuellement les informations de hachage de l'application**. Spécifiez les détails de l'application et cliquez sur **Ajouter**. • Pour importer une liste d'applications à partir d'un fichier .csv, cliquez sur **Importer une liste d'applications à partir d'un fichier .csv**. Accédez au fichier et cliquez sur **Charger**. **Remarque :** Si une application contient plusieurs fichiers .apk, vous devez saisir manuellement le hachage de chaque fichier. Sinon, vous pouvez éventuellement ajouter le certificat de signature de l'application.
Ajoutez une adresse IP à la liste sécurisée d'analyse des messages. (Android uniquement)	**a.** Sous l'onglet **Sécurité**, cliquez sur **Adresses IP**. **b.** Cliquez sur **Ajouter une adresse IP**. **c.** Effectuez l'une des opérations suivantes : • Pour saisir manuellement l'adresse IP, cliquez sur **Saisir manuellement les informations de l'adresse IP**. Spécifiez les détails de l'adresse IP et cliquez sur **Ajouter**. • Pour importer une liste d'adresses IP à partir d'un fichier .csv, cliquez sur **Importer la liste d'adresses IP à partir du fichier .csv**. Accédez au fichier et cliquez sur **Charger**.

Tâche	Étapes
Ajoutez une adresse IP à la liste restreinte d'analyse des messages. (Android uniquement)	**a.** Dans l'onglet **Restreint**, cliquez sur **Adresses IP**. **b.** Cliquez sur **Ajouter une adresse IP**. **c.** Effectuez l'une des opérations suivantes : • Pour saisir manuellement l'adresse IP, cliquez sur **Saisir manuellement les informations de l'adresse IP**. Spécifiez les détails de l'adresse IP et cliquez sur **Ajouter**. • Pour importer une liste d'adresses IP à partir d'un fichier .csv, cliquez sur **Importer la liste d'adresses IP à partir du fichier .csv**. Accédez au fichier et cliquez sur **Charger**.
Ajoutez un domaine à la liste sécurisée d'analyse des messages. (Android uniquement)	**a.** Dans l'onglet **Sécurité**, cliquez sur **Domaines**. **b.** Cliquez sur **Ajouter un domaine**. **c.** Effectuez l'une des opérations suivantes : • Pour saisir manuellement les informations du domaine, cliquez sur **Saisir manuellement les informations de domaine**. Spécifiez les détails du domaine et cliquez sur **Ajouter**. • Pour importer une liste de domaines à partir d'un fichier .csv, cliquez sur **Importer la liste de domaines à partir du fichier .csv**. Accédez au fichier et cliquez sur **Charger**.
Ajoutez un domaine à la liste restreinte d'analyse des messages. (Android uniquement)	**a.** Dans l'onglet **Restreint**, cliquez sur **Domaines**. **b.** Cliquez sur **Ajouter un domaine**. **c.** Effectuez l'une des opérations suivantes : • Pour saisir manuellement les informations du domaine, cliquez sur **Saisir manuellement les informations de domaine**. Spécifiez les détails du domaine et cliquez sur **Ajouter**. • Pour importer une liste de domaines à partir d'un fichier .csv, cliquez sur **Importer la liste de domaines à partir du fichier .csv**. Accédez au fichier et cliquez sur **Charger**.
Ajoutez une source du programme d'installation à la liste sécurisée de détection de charge latérale.	**a.** Sous l'onglet **Sécurisé**, cliquez sur **Sources de programme d'installation**. **b.** Cliquez sur **Ajouter une source de programme d'installation**. **c.** Effectuez l'une des opérations suivantes : • Pour saisir manuellement les informations de la source du programme d'installation, cliquez sur **Saisir manuellement les informations de la source du programme d'installation**. Spécifiez les détails et cliquez sur **Ajouter**. • Pour importer une liste de sources de programme d'installation à partir d'un fichier .csv, cliquez sur **Importer une liste de sources de programme d'installation à partir d'un fichier .csv**. Accédez au fichier et cliquez sur **Charger**.

Tâche	Étapes
Ajoutez une source du programme d'installation à la liste restreinte de détection de charge latérale.	**a.** Sous l'onglet **Restreint**, cliquez sur **Sources de programme d'installation**. **b.** Cliquez sur **Ajouter une source de programme d'installation**. **c.** Effectuez l'une des opérations suivantes : • Pour saisir manuellement les informations de la source du programme d'installation, cliquez sur **Saisir manuellement les informations de la source du programme d'installation**. Spécifiez les détails et cliquez sur **Ajouter**. • Pour importer une liste de sources de programme d'installation à partir d'un fichier .csv, cliquez sur **Importer une liste de sources de programme d'installation à partir d'un fichier .csv**. Accédez au fichier et cliquez sur **Charger**.

À la fin :

- Pour supprimer un élément de l'une des listes sécurisées ou restreintes, sélectionnez-le et cliquez sur **Supprimer**. Lorsque vous y êtes invité, cliquez à nouveau sur **Supprimer**.
- Pour exporter l'une des listes sécurisées ou restreintes, cliquez sur ➔. Cliquez sur **Exporter** pour confirmer.

Analyse des données collectées par CylanceOPTICS

Cette section fournit des informations sur la façon dont vous pouvez afficher, analyser et utiliser les données collectées par CylanceOPTICS.

Capteurs CylanceOPTICS

Les capteurs suivants sont activés par défaut dans l'agent CylanceOPTICS lorsque vous activez CylanceOPTICS dans une stratégie de terminal. Vous ne pouvez pas désactiver ces capteurs. Pour plus d'informations sur les capteurs facultatifs que vous pouvez activer, reportez-vous à la section Capteurs CylanceOPTICS en option.

Pour plus d'informations sur les évènements, les artéfacts et les types d'évènements associés aux capteurs par défaut et facultatifs, reportez-vous à la section Structures de données utilisées par CylanceOPTICS pour identifier les menaces.

Capteur	Plateforme	Description	Types d'évènements
Terminal	macOS Linux	Collecte des informations pertinentes sur le terminal.	Monter
Fichier	Windows macOS Linux	Collecte des informations relatives à des opérations sur fichier.	• Créer • Supprimer • Écraser • Renommer • Écrire
Mémoire	macOS Linux	Collecte des informations relatives à des opérations sur mémoire.	• Mmap • MProtect
Réseau	Windows macOS Linux	Collecte des informations sur les connexions réseau.	Se connecter

Capteur	Plateforme	Description	Types d'évènements
Processus	Windows macOS Linux	Collecte des informations sur des opérations de processus.	Les types d'évènement pris en charge varient en fonction de la plateforme. Reportez-vous à la section Processus de Structures de données utilisées par CylanceOPTICS pour identifier les menaces. • Sortie anormale • Quitter • Sortie forcée • PTrace • Démarrer • Suspendre • Évènement de processus Linux inconnu
Registre	Windows	Collecte des informations sur les opérations de registre.	• KeyCreated • KeyDeleting • ValueChanging • ValueDeleting

Capteurs CylanceOPTICS en option

Vous pouvez activer l'un des capteurs CylanceOPTICS suivants pour collecter des données supplémentaires, outre les évènements de processus, de fichiers, de réseau et des évènements de registre. L'activation de capteurs facultatifs peut avoir un impact sur les performances et l'utilisation des ressources sur les terminaux, ainsi que sur la quantité de données stockées dans la base de données CylanceOPTICS. BlackBerry recommande d'activer les capteurs facultatifs sur un petit nombre de terminaux pour évaluer l'impact.

Les capteurs facultatifs sont pris en charge pour les systèmes d'exploitation 64 bits uniquement, sauf mention contraire.

Capteur	Description	Bonnes pratiques	Notes
Visibilité avancée des scripts	L'agent CylanceOPTICS enregistre les commandes, les arguments, les scripts et le contenu à partir de JScript, PowerShell (console et environnement de script intégré), VBScript et l'exécution de script de macro VBA. Ratio signal/bruit : Élevé Impact potentiel sur la conservation des données et les performances : Faible à modéré	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables • Serveurs Non recommandé pour Microsoft Exchange et les serveurs de messagerie.	• Les outils fournis par Microsoft ou d'autres solutions tierces peuvent considérablement dépendre de PowerShell pour réaliser les opérations. • Pour améliorer la conservation des données, BlackBerry vous recommande de configurer des exceptions de détection pour les outils fiables qui utilisent beaucoup PowerShell.
Visibilité WMI avancée	L'agent CylanceOPTICS enregistre les attributs et paramètres WMI supplémentaires. Ratio signal/bruit : Élevé Impact potentiel sur la conservation des données et les performances : Faible	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables • Serveurs	• Certains processus d'arrière-plan et de maintenance Windows utilisent WMI pour planifier des tâches ou exécuter des commandes, ce qui peut entrainer des pics d'activité WMI élevée. • BlackBerry recommande d'analyser l'utilisation WMI dans votre environnement avant d'activer ce capteur.
Capteur API	L'agent CylanceOPTICS surveille un ensemble identifié d'appels d'API Windows. Ratio signal/bruit : Modéré Impact potentiel sur la rétention des données et les performances : l'activation de ce capteur peut avoir un impact sur les performances du processeur d'un terminal	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables • Serveurs	• Pris en charge sur les systèmes d'exploitation Windows x86 ou x64. • Nécessite l'agent CylancePROTECT Desktop 3.0.1003 ou une version ultérieure. • Nécessite l'agent CylanceOPTICS 3.2 ou une version ultérieure.

Capteur	Description	Bonnes pratiques	Notes
Visibilité de l'objet COM	L'agent CylanceOPTICS surveille les appels d'API et d'interface COM pour détecter les comportements malveillants tels que la création de tâches planifiées. Ratio signal/bruit : Élevé Impact potentiel sur la rétention des données et les performances : l'activation de ce capteur peut avoir un impact sur les performances du processeur.	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables Non recommandé pour les serveurs.	• Windows uniquement. • Nécessite l'agent CylancePROTECT Desktop 3.2 ou une version ultérieure. • Nécessite l'agent CylanceOPTICS 3.3 ou une version ultérieure.
Détection de cryptojacking	L'agent CylanceOPTICS traite l'activité de l'UC Intel à l'aide de registres matériels à la recherche d'activités potentielles de minage de cryptomonnaie et de cryptojacking. Ratio signal/bruit : Modéré Impact potentiel sur la conservation des données et les performances : Faible	Système d'exploitation pris en charge : • Windows 10 x64 • Intel génération 6 à 10	**Remarque :** BlackBerry recommande de désactiver ce capteur, car nous étudions actuellement les problèmes de stabilité que ce capteur peut causer avec le système d'exploitation du terminal. • Non pris en charge pour les machines virtuelles. • Non pris en charge pour les processeurs Intel de génération 11 ou ultérieure. BlackBerry ne recommande pas l'activation de ce capteur pour la génération 11 ou ultérieure.
Visibilité DNS	L'agent CylanceOPTICS enregistre les requêtes DNS, les réponses et les champs de données associés tels que Nom de domaine, Adresses résolues et Type d'enregistrement. Ratio signal/bruit : Modéré Impact potentiel sur la conservation des données et les performances : Modéré	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables Non recommandé pour les serveurs DNS.	• Notez que ce capteur peut collecter une quantité importante de données, mais peut également fournir une visibilité sur les données que d'autres outils peinent à enregistrer. • Pour améliorer la conservation des données, BlackBerry vous recommande de configurer des exceptions de détection pour les outils fiables qui utilisent beaucoup les services cloud.

Capteur	Description	Bonnes pratiques	Notes
Visibilité améliorée de la lecture des fichiers	L'agent CylanceOPTICS surveille les lectures de fichiers dans un ensemble identifié de répertoires. Ratio signal/bruit : Modéré Impact potentiel sur la conservation des données et les performances : Faible	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables • Serveurs	• Certains outils de sécurité tiers peuvent utiliser les API Windows à partir desquelles ce capteur collecte des données. Dans certains cas, CylanceOPTICS peut enregistrer des données non pertinentes ou fiables. • Pour améliorer la conversation des données et obtenir un ratio signal/bruit plus élevé, BlackBerry recommande de configurer des exceptions de détection pour des outils de sécurité fiables.
Analyse améliorée de fichiers exécutables portables	L'agent CylanceOPTICS enregistre les champs de données associés aux fichiers exécutables portables, tels que la version de fichier, les fonctions d'importation et les types d'outils Packer. Ratio signal/bruit : Modéré Impact potentiel sur la conservation des données et les performances : Faible	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables • Serveurs	• Les données collectées par ce capteur sont transmises au moteur d'analyse de contexte pour faciliter l'analyse avancée des fichiers exécutables et ne sont pas stockées dans la base de données CylanceOPTICS. • L'activation de ce capteur aura peu ou pas d'impact sur la conservation des données CylanceOPTICS. • Si vous ajoutez et activez une règle de détection qui analyse les ressources de chaîne, l'agent CylanceOPTICS peut consommer d'importantes ressources de processeur et de mémoire.

Capteur	Description	Bonnes pratiques	Notes
Visibilité Améliorée des processus et de l'accrochage	L'agent CylanceOPTICS enregistre les informations de processus à partir des messages d'API Win32 et d'audit de noyau pour détecter les formes d'accrochage et d'injection de processus. Ratio signal/bruit : Modéré Impact potentiel sur la conservation des données et les performances : Faible	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables • Serveurs	• Certains outils de sécurité tiers peuvent utiliser les API Windows à partir desquelles ce capteur collecte des données. Dans certains cas, CylanceOPTICS peut enregistrer des données non pertinentes ou fiables. • Pour améliorer la conversation des données et obtenir un ratio signal/bruit plus élevé, BlackBerry recommande de configurer des exceptions de détection pour des outils de sécurité fiables.
Visibilité HTTP	L'agent CylanceOPTICS suit les transactions HTTP Windows, y compris le suivi des événements pour Windows, les API WinINet et les API WinHTTP. Ratio signal/bruit : Élevé Impact potentiel sur la rétention des données et les performances : l'activation de ce capteur peut avoir un impact sur les performances du processeur.	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables Non recommandé pour les serveurs.	• Windows uniquement. • Nécessite l'agent CylancePROTECT Desktop 3.2 ou une version ultérieure. • Nécessite l'agent CylanceOPTICS 3.3 ou une version ultérieure.
Visibilité de la charge du module	L'agent CylanceOPTICS surveille les charges du module. Ratio signal/bruit : Élevé Impact potentiel sur la rétention des données et les performances : l'activation de ce capteur peut avoir un impact sur les performances du processeur.	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables • Serveurs	• Windows uniquement. • Nécessite l'agent CylancePROTECT Desktop 3.2 ou une version ultérieure. • Nécessite l'agent CylanceOPTICS 3.3 ou une version ultérieure.

Capteur	Description	Bonnes pratiques	Notes
Visibilité des adresses de réseau privé	L'agent CylanceOPTICS enregistre les connexions réseau comprises dans les espaces d'adresse RFC 1918 et RFC 4193. Ratio signal/bruit : Faible Impact potentiel sur la conservation des données et les performances : Faible	Recommandé pour les ordinateurs de bureau. Déconseillé pour : • Serveurs DNS • Systèmes avec peu ou sans ressources • Systèmes qui utilisent RDP ou un autre logiciel d'accès à distance	• Ce capteur collecte une quantité importante de données et peut avoir un impact sur la durée pendant laquelle les données sont stockées dans la base de données CylanceOPTICS. • BlackBerry recommande d'activer ce capteur uniquement dans les environnements dans lesquelles une visibilité complète de la communication d'adresse de réseau privé est requise.
Visibilité avancée de l'audit sous Windows	L'agent CylanceOPTICS surveille les types et catégories d'événements Windows supplémentaires. Ratio signal/bruit : Modéré Impact potentiel sur la conservation des données et les performances : Faible	—	Ce capteur permet de surveiller les ID d'événement suivants : • 4769 - demande de ticket kerberos • 4662 - opération sur un objet active directory • 4624 connexion réussie • 4702 création de tâches planifiées
Visibilité du journal des événements Windows	L'agent CylanceOPTICS enregistre les événements de sécurité Windows et leurs attributs associés. Ratio signal/bruit : Modéré Impact potentiel sur la conservation des données et les performances : Modéré	Recommandé pour : • Ordinateurs de bureau • Ordinateurs portables • Serveurs Déconseillé pour : • Contrôleurs de domaine • Microsoft Exchange et serveurs de messagerie	• Les journaux d'événements Windows à partir desquels ce capteur collecte des données sont fréquemment générés lors d'une utilisation normale du système. • Pour réduire les doublons et améliorer la conservation des données, déterminez si votre organisation dispose déjà d'outils de collecte des données à partir des journaux d'événements Windows.

Structures de données utilisées par CylanceOPTICS pour identifier les menaces

Les évènements, artefacts et facets sont les trois principales structures de données utilisées par CylanceOPTICS pour analyser, enregistrer et examiner les activités qui se produisent sur les terminaux. Les fonctionnalités CylanceOPTICS s'appuient sur ces structures de données, y compris les requêtes InstaQuery, les données détaillés et le moteur d'analyse de contexte (CAE).

Cette section fournit plus d'informations sur la manière dont CylanceOPTICS interprète et interagit avec les activités sur les terminaux, afin de vous aider à mieux comprendre et utiliser les détections, les requêtes et les données détaillées.

Sources de données en fonction du système d'exploitation

L'agent CylanceOPTICS utilise les sources de données suivantes :

OS	Sources de données
Windows	• Pilote de noyau CyOpticsDrv • Suivi des évènements • Fichier journal d'audit de sécurité
macOS	Pilote de noyau CyOpticsDrvOSX
Linux	ZeroMQ

Pour plus d'informations sur les types de trafic réseau que CylanceOPTICS exclut par défaut, reportez-vous à l'article KB65604.

Évènements

Les évènements sont les composants qui entraînent une modification ou une action observable sur un terminal. Les évènements comportent deux artefacts principaux : l'artefact instigateur qui déclenche une action et l'artefact cible sur lequel des mesures sont prises.

Les tableaux suivants fournissent des détails sur les types d'évènements pouvant être détectés par CylanceOPTICS et avec lesquels il peut interagir.

Évènement : indifférent

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : processus, utilisateur
- Plateforme : Windows, macOS, Linux

Type d'évènement	Description
Indifférent	Tous les évènements enregistrent le processus qui les a générés et l'utilisateur associé à l'action.

Évènement : application

- Option de stratégie de terminal à activer : Visibilité WMI avancée

- Type d'artefact : suivi WMI
- Plateforme : Windows

Type d'évènement	Description
Créer une liaison filtre-client	Un processus a utilisé la persistance WMI.
Créer un client temporaire	Un processus s'est abonné aux évènements WMI.
Exécuter l'opération	Un processus a effectué une opération WMI.

- Option de stratégie de terminal à activer : Visibilité améliorée des accrochages et des processus
- Type d'artefact : fichier
- Plateforme : Windows

Type d'évènement	Description
CBT	L'API SetWindowsHookEx a installé un crochet pour recevoir des notifications utiles à une application CBT.
DebugProc	L'API SetWindowsHookEx a installé un crochet pour déboguer d'autres procédures de crochet.
Obtenir l'état de clé asynchrone	Un processus a appelé l'API Win32 GetAsyncKeyState.
JournalPlayback	L'API SetWindowsHookEx a installé un crochet pour surveiller les messages précédemment enregistrés par une procédure de crochet WH_JOURNALLECORD.
JournalRecord	L'API SetWindowsHookEx a installé un crochet pour surveiller les messages d'entrée publiés dans la file d'attente des messages système.
Clavier	L'API SetWindowsHookEx a installé un crochet pour surveiller les messages de frappe.
Clavier de bas niveau	L'API SetWindowsHookEx a installé un crochet pour surveiller les évènements de saisie clavier de bas niveau.
Souris de bas niveau	L'API SetWindowsHookEx a installé un crochet pour surveiller les évènements d'entrée de souris de bas niveau.
Message	L'API SetWindowsHookEx a installé un crochet pour surveiller les messages publiés dans une file d'attente de messages.
Souris	L'API SetWindowsHookEx a installé un crochet pour surveiller les messages de la souris.
Enregistrer les terminaux d'entrée brute	Un processus a appelé API Win32 RegisterRawInputDevices.

Type d'évènement	Description
Définir le crochet d'événement Windows	Un processus a appelé l'API Win32 SetWinEventHook.
Configurer le crochet Windows	L'API SetWindowsHookEx a installé une valeur de type de crochet non répertoriée.
ShellProc	L'API SetWindowsHookEx a installé un crochet pour recevoir des notifications utiles pour les applications de shell.
SysMsg	L'API SetWindowsHookEx a installé un crochet pour surveiller les messages générés à la suite d'un évènement d'entrée dans une boîte de dialogue, une boîte de message ou une barre de défilement.
WindowProc	L'API SetWindowsHookEx a installé un crochet pour surveiller les messages de procédure Windows.

- Option de stratégie de terminal à activer : Détecteur API
- Type d'artefact : Appel API
- Plateforme : Windows

Type d'évènement	Description
Fonction	Un appel de fonction remarquable a été effectué.

- Option de stratégie de terminal à activer : Visibilité charge de module
- Type d'artefact : fichier
- Plateforme : Windows

Type d'évènement	Description
Charger	Une application a chargé un module.

- Option de stratégie de terminal à activer : Visibilité objet COM
- Plateforme : Windows

Type d'évènement	Description
Créé	Un objet COM a été créé.

Évènement : terminal

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : fichier
- Plateforme : macOS, Linux

Type d'évènement	Description
Monter	Le terminal est connecté à une machine ou les dossiers sont montés sur des emplacements réseau spécifiques.

Évènement : fichier

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : fichier
- Plateforme : Windows, macOS, Linux

Type d'évènement	Description
Créer	Un fichier a été créé.
Supprimer	Un fichier a été supprimé.
Écraser	Un fichier a été écrasé.
Renommer	Un fichier a été renommé.
Écrire	Un fichier a été modifié.

- Option de stratégie de terminal à activer : Visibilité améliorée de lecture de fichier
- Type d'artefact : fichier
- Plateforme : Windows

Type d'évènement	Description
Ouvrir	Un fichier a été ouvert.

Évènement : mémoire

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : processus
- Plateforme : macOS, Linux

Type d'évènement	Description
Mmap	Une région de mémoire a été mappée dans un but spécifique, généralement allouée à un processus.
MProtect	Les métadonnées ont été modifiées pour une région de mémoire, généralement pour modifier son état (par exemple, pour le rendre exécutable).

Évènement : réseau

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : réseau
- Plateforme : Windows, macOS, Linux

Type d'évènement	Description
Se connecter	Une connexion réseau a été établie. Par défaut, le trafic local n'est pas collecté.

- Option de stratégie de terminal à activer : Visibilité des adresses réseau privées
- Type d'artefact : réseau
- Plateforme : Windows

Type d'évènement	Description
Se connecter	Les évènements de connexion incluent le trafic local.

- Option de stratégie de terminal à activer : Visibilité DNS
- Type d'artefact : requête DNS
- Plateforme : Windows, Linux

Type d'évènement	Description
Demande	Un processus a effectué une requête DNS réseau qui n'était pas mise en cache.
Réponse	Un processus a reçu une réponse DNS.

- Option de stratégie de terminal à activer : Visibilité HTTP
- Type d'artefact : HTTP
- Plateforme : Windows

Type d'évènement	Description
Get	Windows a utilisé WinINet ou WinHTTP pour créer une requête HTTP.
Post	Windows a utilisé WinINet ou WinHTTP pour envoyer des données.

Évènement : processus

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : processus

Type d'évènement	Plateforme	Description
Sortie anormale	macOS Linux	Surveillé par le capteur de présélection, un processus s'est arrêté sans être terminé (par exemple, une exception a provoqué la fermeture d'un processus).
Quitter	Windows macOS Linux	Un processus a été arrêté.
Sortie forcée	macOS Linux	Surveillé par le capteur de présélection, un processus a été forcé de quitter le système par un autre processus.

Type d'évènement	Plateforme	Description
PTrace	macOS Linux	Il s'agit d'un outil système Unix qui permet à un processus de surveiller et de contrôler un autre processus.
Démarrer	Windows macOS Linux	Un processus a démarré.
Suspendre	Linux	Surveillé par le capteur de présélection, un processus a été suspendu.
Évènement de processus Linux inconnu	macOS Linux	Surveillé par le capteur de présélection, un évènement inconnu s'est produit avec le processus comme cible. Cela peut indiquer qu'un logiciel malveillant masque son activité.

- Option de stratégie de terminal à activer : Visibilité améliorée des accrochages et des processus
- Type d'artefact : processus
- Plateforme : Windows

Type d'évènement	Description
SetThreadContext	Un processus a appelé l'API SetThreadContext.
Terminer	Un processus instigateur a mis fin à un autre processus cible.

Évènement : registre

- Option de stratégie de terminal à activer : case à cocher CylanceOPTICS
- Type d'artefact : registre, fichier (si la clé de registre fait référence à un fichier spécifique)
- Plateforme : Windows

Type d'évènement	Description
KeyCreated	Une clé de registre a été créée.
KeyDeleting	Une clé de registre a été supprimée.
ValueChanging	La valeur de clé de registre a été modifiée.
ValueDeleting	Une valeur de clé de registre a été supprimée.

Évènement : scripts

- Option de stratégie de terminal à activer : Visibilité avancée des scripts
- Type d'artefact : suivi PowerShell
- Plateforme : Windows

Type d'évènement	Description
Exécuter la commande	Windows PowerShell a exécuté une commande. Les paramètres sont inconnus.
Exécuter le script	Windows PowerShell a exécuté un script.
Exécuter le bloc de script	Windows PowerShell a exécuté un bloc de script.
Appeler la commande	Windows PowerShell a appelé une commande avec des paramètres liés.
Empêcher le script	Un résultat de ScanBuffer AMSI indique qu'un script a été détecté ou bloqué par un administrateur.

Évènement : utilisateur

- Option de stratégie de terminal à activer : Visibilité avancée des scripts
- Type d'artefact : événement Windows
- Plateforme : Windows

Type d'évènement	Description
Déconnexion du lot	L'ID d'évènement Windows suivant s'est produit : 4634 (type 4).
Connexion au lot	L'ID d'évènement Windows suivant s'est produit : 4624 (type 4).
Déconnexion interactive en cache	L'ID d'évènement Windows suivant s'est produit : 4634 (type 11).
Connexion interactive en cache	L'ID d'évènement Windows suivant s'est produit : 4624 (type 11).
Déconnexion interactive	L'ID d'évènement Windows suivant s'est produit : 4634 (type 2).
Connexion interactive	L'ID d'évènement Windows suivant s'est produit : 4624 (type 2).
Déconnexion du réseau	L'ID d'évènement Windows suivant s'est produit : 4634 (type 3).
Connexion réseau	L'ID d'évènement Windows suivant s'est produit : 4624 (type 3).
Déconnexion au réseau en texte clair	L'ID d'évènement Windows suivant s'est produit : 4634 (type 8).

Type d'évènement	Description
Connexion au réseau en texte clair	L'ID d'évènement Windows suivant s'est produit : 4624 (type 8).
Déconnexion des nouveaux identifiants	L'ID d'évènement Windows suivant s'est produit : 4634 (type 9).
Connexion aux nouveaux identifiants	L'ID d'évènement Windows suivant s'est produit : 4624 (type 9).
Déconnexion interactive à distance	L'ID d'évènement Windows suivant s'est produit : 4634 (type 10).
Connexion interactive à distance	L'ID d'évènement Windows suivant s'est produit : 4624 (type 10).
Déconnexion du service	L'ID d'évènement Windows suivant s'est produit : 4634 (type 5).
Connexion au service	L'ID d'évènement Windows suivant s'est produit : 4624 (type 5).
Déverrouiller la déconnexion	L'ID d'évènement Windows suivant s'est produit : 4634 (type 7).
Déverrouiller la connexion	L'ID d'évènement Windows suivant s'est produit : 4624 (type 7).
Déconnexion utilisateur	L'ID d'évènement Windows suivant s'est produit : 4634 (valeur de type non répertoriée).
Connexion utilisateur	L'ID d'évènement Windows suivant s'est produit : 4624 (valeur de type non répertoriée).

Artefacts et facets

Les artefacts sont des éléments d'information complexes pouvant être utilisés par CylanceOPTICS. Le moteur d'analyse de contexte (CAE) peut identifier les artefacts sur les terminaux et les utiliser pour déclencher une réponse automatique aux incidents et des actions correctives. Les requêtes InstaQueries utilisent des artefacts comme base d'une requête.

Les facets sont les attributs d'un artefact qui peuvent être utilisés pour identifier les traits d'un artefact associé à un évènement. Les facets sont corrélés et combinés pendant l'analyse pour identifier les activités potentiellement malveillantes. Par exemple, un fichier nommé « explorer.exe » peut ne pas être intrinsèquement suspect, mais si le fichier n'est pas signé par Microsoft et qu'il réside dans un répertoire temporaire, il peut être identifié comme suspect dans certains environnements.

CylanceOPTICS utilise les artefacts et facets suivants :

Artefact	Facets
Appel d'API	• Fonction • DLL • Paramètres
DNS	• Connexion • IsRecursionDesired • IsUnsolicitedResponse • Opcode • RequestId • Résolution • ResponseOriginatedFromThisDevice • Questions
Évènement	• Heure d'occurrence • Heure d'enregistrement
Fichier	• Enregistrement de fichier exécutable (fichiers binaires uniquement) • Heure de création du fichier (signalée par le système d'exploitation) • Chemin du fichier • Signature de fichier (fichiers binaires uniquement) • Taille du fichier • Heure de la dernière modification (signalée par le système d'exploitation) • Hachage md5 (fichiers binaires uniquement) • Emplacement d'écriture récent • Hachage sha256 (fichiers binaires uniquement) • Type de fichier suspecté • Utilisateur
Réseau	• Adresse locale • Port local • Protocole • Adresse distante • Port distant
Suivi PowerShell	• EventId • Charge utile • PayloadAnalysis • ScriptBlockText • ScriptBlockTextAnalysis

Artefact	Facets
Processus	• Ligne de commande • Fichier à partir duquel l'exécutable a été exécuté • Processus parent • ID de processus • Heure de début • Utilisateur
Registre	• Si la valeur fait référence à un fichier sur le système • Chemin de registre • Valeur
Utilisateurs	• Domaine • Identifiant spécifique au système d'exploitation (par exemple, SID) • Nom d'utilisateur Les artefacts utilisateur peuvent contenir l'une des valeurs suivantes. Cependant, les données ne sont pas disponibles sur la plupart des terminaux. • AccountType • BadPasswordCount • Commentaire • CountryCode • FullName • HasPasswordExpired • HomeDirectory • IsAccountDisabled • IsLocalAccount • IsLockedOut • IsPasswordRequired • LanguageCodePage • LogonServer • PasswordAge • PasswordDoesNotExpire • ProfilePath • ScriptPath • UserPrivilege • Workstations

Artefact	Facets
Évènement Windows	• Classe • ID d'évènement • Serveur objet • Liste de privilèges • ID de processus • Nom du processus • Nom du fournisseur • Service • Nom du domaine objet • ID de connexion objet • Nom d'utilisateur objet • Sid d'utilisateur objet
Suivi WMI	• ConsumerText • ConsumerTextAnalysis • EventId • Espace de noms • Opération • OperationAnalysis • OriginatingMachineName

Valeurs et clés de registre

CylanceOPTICS surveille les valeurs et les clés communes de persistance, de démarrage de processus et d'escalade des privilèges, ainsi que les valeurs indiquées dans l'article KB 66266.

Pour en savoir plus sur la manière dont CylanceOPTICS surveille les points de persistance dans le registre, consultez l'article KB 66357.

Afficher les terminaux activés pour CylanceOPTICS

Vous pouvez afficher les détails et les informations sur l'état de tous les terminaux activés pour CylanceOPTICS, y compris la version de l'agent CylanceOPTICS installée sur le terminal, l'adresse IP du terminal et les zones attribuées. Vous pouvez utiliser la vue du terminal pour prendre des mesures et gérer les menaces potentielles.

Si un terminal est hors ligne pendant au moins 90 jours, il ne s'affiche pas sur la console.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Terminaux**.
2. Cliquez sur pour filtrer les résultats et afficher un terminal ou un groupe de terminaux spécifique.
3. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Afficher le résumé des détails d'un terminal	Cliquez sur le nom du terminal.

Tâche	Étapes
Afficher les détails complet d'un terminal et modifier ses propriétés et ses attributions	**a.** Dans la colonne **Détails**, cliquez sur **Afficher**. **b.** Sous **Modifier les propriétés du terminal**, vous pouvez modifier le nom du terminal, la stratégie de terminal attribuée, les zones attribuées, le niveau de journal de l'agent CylanceOPTICS et le niveau de protection. Cliquez sur **Enregistrer**. **c.** Dans la section **Menaces et activités**, vous pouvez afficher les détails des menaces que l'agent CylanceOPTICS a détectées.
Verrouiller un terminal	Reportez-vous à la section Verrouiller un terminal.
Déployer un package pour collecter des données à partir du terminal	**a.** Cliquez sur le nom du terminal. **b.** Dans la liste déroulante **Sélectionner une action**, cliquez sur **Déploiement du package**. **c.** Suivez les instructions de la page Déployer un package pour collecter des données à partir de terminaux.
Démarrer une session de réponse à distance pour envoyer des commandes au terminal	**a.** Cliquez sur le nom du terminal. **b.** Dans la liste déroulante **Sélectionner une action**, cliquez sur **Réponse distante**. **c.** Saisissez des commandes dans la fenêtre de session de réponse distante. Pour plus d'informations, reportez-vous à Envoi d'actions vers un terminal.
Exporter un fichier .csv de tous les terminaux	Cliquez sur .

Utilisation des requêtes InstaQuery et avancées pour analyser les données d'artefact

Les requêtes InstaQuery et avancées sont des fonctionnalités d'CylanceOPTICS qui vous permettent d'analyser les données d' artefact pour découvrir les indicateurs de compromis et déterminer leur prévalence sur les terminaux de votre entreprise. Les résultats d'une requête ne vous indiqueront pas comment ou quand un artefact a été utilisé, mais ils indiqueront si un artefact a déjà été observé en termes techniques significatifs pouvant signaler une menace pour les terminaux et les données de votre organisation.

InstaQuery vous permet d'interroger un ensemble de terminaux sur un type spécifique d'artefact médico-légal et de déterminer si un artefact existe sur les terminaux et à quel point cet artefact est commun. La requête avancée est une évolution d'InstaQuery qui fournit des fonctionnalités de recherche plus granulaires à l'aide de la syntaxe EQL pour améliorer votre capacité à identifier les menaces.

Une fois l'agent CylanceOPTICS installé et activé sur un terminal, il collecte les artefacts et les stocke dans la base de données CylanceOPTICS. Avec l'agent CylanceOPTICS 2.x et versions antérieures, la base de données est stockée localement sur le terminal. Avec l'agent CylanceOPTICS 3.0 et versions ultérieures, l'agent charge et stocke automatiquement les données dans la base de données cloud CylanceOPTICS. Lorsque vous créez une requête, les données importantes au niveau technique sont récupérées de la base de données CylanceOPTICS. Vous pouvez afficher et examiner les résultats dans la console de gestion.

Pour les terminaux dotés de l'agent CylanceOPTICS 2.x et versions antérieures, une requête ne peut s'exécuter correctement que lorsqu'un terminal est en ligne. Pour les terminaux dotés de l'agent 3.0 et versions ultérieures, il n'est pas nécessaire que le terminal soit en ligne, car la requête utilisera les données les plus récentes disponibles dans la base de données cloud CylanceOPTICS.

Une seule requête affiche et conserve un maximum de 10 000 résultats. Les résultats d'une requête sont conservés pendant 60 jours.

Notez les détails suivants sur les artefacts spécifiques que vous pouvez interroger :

Artefact	Détails
Fichiers	Vous pouvez interroger des fichiers spécifiques qui ont été créés, modifiés ou supprimés après l'installation de l'agent CylanceOPTICS sur le terminal. CylanceOPTICS se concentre sur les fichiers qui peuvent être utilisés pour exécuter du contenu (par exemple, des fichiers exécutables, des documents Microsoft Office, des PDF, etc.).
Connexions réseau	Vous pouvez effectuer des requêtes sur les adresses IP de destination IPv4 et IPv6. CylanceOPTICS ignore le trafic réseau privé, non routable, multicast, link-local et de bouclage.
Processus	Tous les processus sont indexés dans la base de données CylanceOPTICS, avec les restrictions suivantes : • Les lignes de commande sont limitées à 1 Kio de données • Les noms de processus ne doivent pas contenir plus de 256 caractères • Les chemins d'accès aux fichiers d'image de processus ne doivent pas contenir plus de 512 caractères • Les lignes de commande modifiées après le démarrage du processus ne sont pas surveillées
Clés de registre	CylanceOPTICS surveille uniquement les points de persistance et les points de suppression de fichiers. Il s'agit de zones généralement exploitées par des programmes malveillants. Pour obtenir la liste détaillée des clés de Registre et des valeurs surveillées par CylanceOPTICS, consultez l'article KB66266. Pour en savoir plus sur la manière dont CylanceOPTICS surveille les points de persistance dans le registre, consultez KB66357.

Créer une requête InstaQuery

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > InstaQuery**.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Créez une requête InstaQuery.	Si vous souhaitez cloner une requête précédente, développez la section **Requêtes précédentes**, recherchez la requête de votre choix, puis cliquez sur **Cloner la requête**. **a.** Dans le champ **Terme de recherche**, saisissez la valeur que vous souhaitez rechercher (par exemple, un nom de fichier, un hachage, un processus, une valeur de registre, etc.). Si vous souhaitez rechercher une correspondance exacte, cochez la case **Correspondance exacte**. **b.** Dans la liste déroulante **Artefact**, cliquez sur un type d'artefact. **c.** Dans la liste déroulante **Facette**, cliquez sur la facette appropriée. **d.** Dans la liste déroulante **Zone**, sélectionnez une ou plusieurs zones. **e.** Saisissez le nom et la description de la requête. **f.** Cliquez sur **Soumettre la requête**. **g.** L'état actuel de la requête s'affiche dans la section **Requêtes précédentes**. Une fois la requête terminée, cliquez sur **Afficher les résultats**.
Afficher une requête InstaQuery précédente.	**a.** Développez la section **Requêtes précédentes**. **b.** Pour la requête que vous souhaitez afficher, cliquez sur **Afficher les résultats**.

3. Dans la section **Résultats InstaQuery**, vous pouvez développer le menu **Actions** pour accéder aux actions disponibles pour chaque résultat. En fonction du type de résultat, les actions suivantes peuvent être disponibles :
   - Demander et afficher les données détaillées
   - Mettre le fichier en quarantaine globale ; le fichier s'affiche sous **Paramètres > Liste globale > Quarantaine globale**, dans **Protection > Menaces** et dans la section **Menaces** la des détails du terminal.
   - Demander et télécharger un fichier; si des informations de chemin sont disponibles pour des fichiers associés à d'autres types d'artefacts, vous pouvez également télécharger ces fichiers. Le fichier est compressé et protégé par un mot de passe afin d'éviter toute exécution par erreur. Le mot de passe est « infecté ».

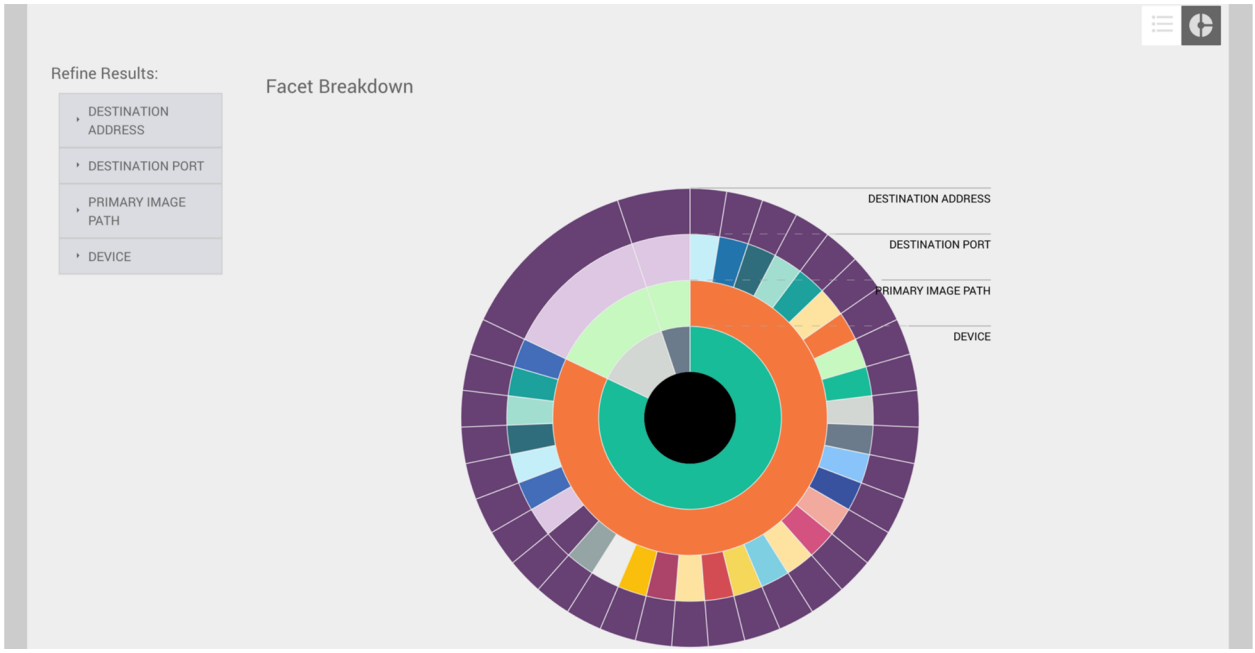
     La taille maximum pour la récupération de fichiers est de 50 Mo. Les artefacts et les fichiers sont conservés par CylanceOPTICS pendant 30 jours (cette période peut être prolongée en fonction des licences de votre organisation).
4. Pour afficher la répartition des facettes InstaQuery, dans la section **Résultats InstaQuery**, cliquez sur l'icône de répartition des facettes.

Utilisation de la répartition des facettes InstaQuery

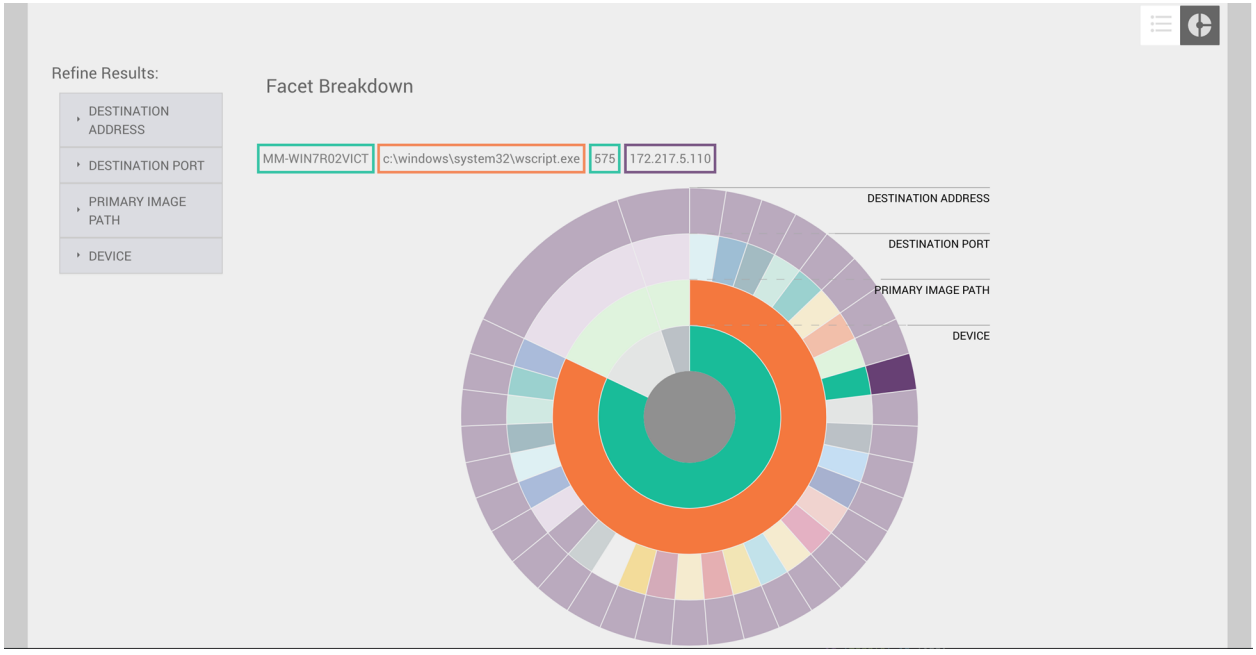
La répartition des facets de requête InstaQuery fournit un affichage visuel interactif des différents facets impliqués dans une requête afin que vous puissiez identifier et suivre leurs chemins relationnels.

Le modèle en rayons de soleil de la répartition des facets est utile pour identifier les activités suspectes dans un ensemble de données spécifique. Par exemple, si vous tentez de détecter des connexions réseau suspectes dans un environnement ou plusieurs zones, les modèles de données et les anomalies peuvent être difficiles à identifier en raison du volume et de la complexité des données. Les images suivantes montrent comment vous pouvez afficher et filtrer les données dans la répartition des facets pour localiser rapidement les activités suspectes.

Les images suivantes ont été générées en créant une requête InstaQuery pour rechercher des connexions à une adresse IP spécifique. Les résultats de la requête sont représentés dans un diagramme en rayons de soleil avec les facets suivants : terminal, chemin de l'image principale, port de destination et adresse de destination.

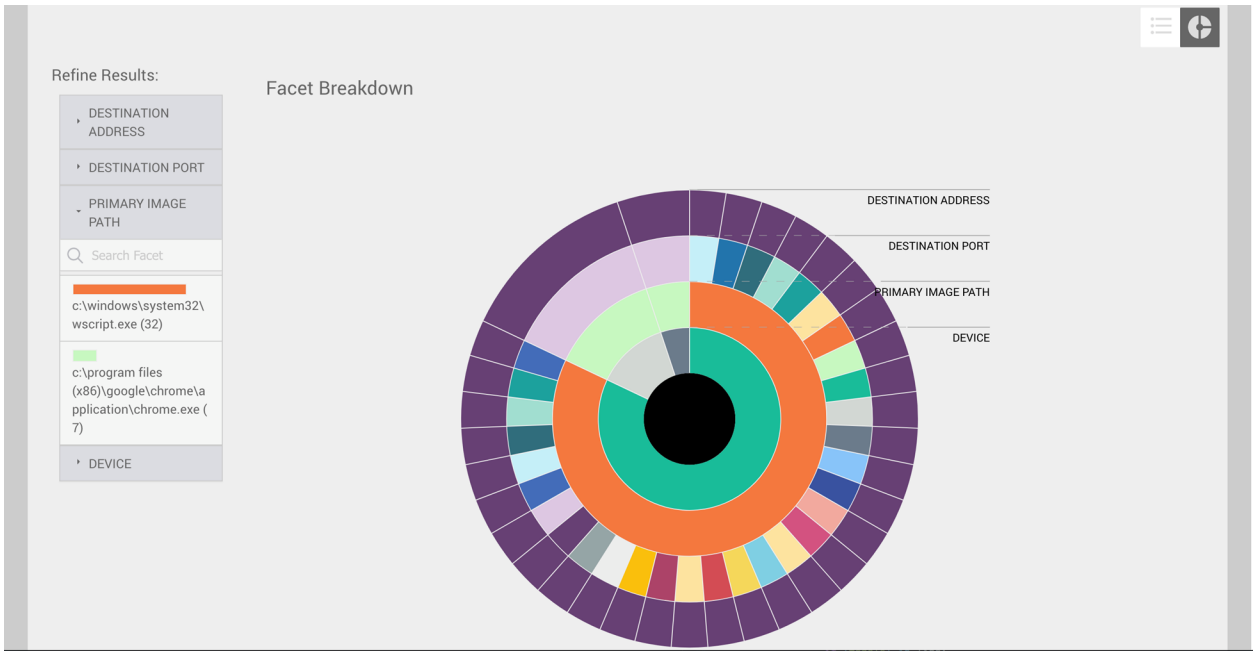


Vous pouvez passer la souris sur n'importe quel facet pour afficher les valeurs associées. Dans l'image suivante, l'administrateur a sélectionné le facet le plus à l'extérieur pour afficher le nom du terminal, le chemin d'accès au fichier qui a initié la connexion réseau, le numéro de port utilisé pour la connexion et l'adresse IP du système distant.



Lorsque vous passez le curseur sur un facet, les facets parent associés sont également mis en surbrillance pour vous aider à établir une relation visuelle entre les points de données. Dans l'exemple ci-dessus, vous pouvez voir qu'un terminal et un processus parent étaient responsables de la plupart des connexions à l'adresse IP. Le diagramme illustre également que de nombreux ports réseau différents ont été utilisés pour se connecter à cette adresse IP à partir de l'hôte associé, ce qui diffère des deux autres facets de l'hôte dans le diagramme.

Vous pouvez également obtenir des informations utiles à partir des menus d'affinement des résultats. Chaque menu de facet contient les valeurs uniques et le nombre d'occurrences pour chaque facet. Dans l'exemple ci-dessous, vous pouvez voir que deux processus étaient responsables des connexions à cette adresse IP : Google Chrome et Wscript.



Lorsque vous cliquez sur une valeur de facet dans le menu d'affinement des résultats, le diagramme change de façon à afficher les facets directement liés. Cette fonction est utile pour filtrer les données non pertinentes et permettre une analyse plus ciblée.

Créer une requête avancée

La fonction de requête avancée vous permet de créer des requêtes personnalisées pour améliorer vos activités de recherche de menaces. Les requêtes avancées offrent une visibilité approfondie de votre environnement CylanceOPTICS, des options de requêtes étendues et des flux de travail optimisés qui vous permettent de combiner des recherches connexes pour révéler de nouvelles informations. La requête avancée est prise en charge pour les terminaux dotés de l'agent CylanceOPTICS version 3.0 ou ultérieure.

La requête avancée repose sur l'utilisation de la syntaxe EQL. Vous utilisez EQL pour construire des requêtes pour les évènements, et les résultats fournissent des informations sur les artefacts qui ont été impliqués dans ces évènements. L'interface utilisateur de requête avancée inclut des informations sur la syntaxe pour vous aider à créer des requêtes EQL.

Avant de commencer : Consultez les sections Syntaxe EQL prise en charge pour les requêtes avancées et Exemples de requêtes EQL CylanceOPTICS.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Requête avancée**.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Créer une nouvelle requête avancée	Si vous souhaitez utiliser un modèle de requête existant pour créer une requête, cliquez sur **Afficher la liste des modèles** et sélectionnez un modèle, puis ignorez la première étape ci-dessous. **a.** Dans le champ de requête, saisissez ou collez la syntaxe EQL de la requête. À mesure de la saisie, des options de syntaxe et des messages de validation s'affichent pour vous aider à créer votre requête. Si vous souhaitez enregistrer la requête actuelle en tant que modèle, cliquez sur **Enregistrer comme modèle**. Saisissez un nom et une description, puis indiquez si vous souhaitez que le modèle soit privé ou disponible pour tous les administrateurs. Cliquez sur **Enregistrer**. Vous pouvez épingler, modifier et supprimer des requêtes de la liste des modèles. **b.** Pour définir le champ d'application de la requête, sous **Rechercher des terminaux**, cliquez sur **Par zone** ou **Par terminal** (une icône en regard de chaque terminal indique si le terminal est en ligne). Sélectionnez au moins une zone ou un terminal, puis cliquez sur **Enregistrer**. Si vous ne définissez pas la portée, la requête s'applique à toutes les zones et tous les terminaux. **c.** Pour définir une plage de dates et d'heures pour la requête, cliquez sur et configurez la plage. Cliquez sur **Apply** (Appliquer). Si vous ne définissez pas de plage, la requête s'applique à toutes les données disponibles. **d.** Effectuez l'une des opérations suivantes : • Si vous souhaitez exécuter la requête, cliquez sur **Exécuter la requête**. • Si vous souhaitez planifier l'exécution de la requête à une date et une heure spécifiques ou à intervalles réguliers, cliquez sur **Planifier une requête**. Saisissez un nom et une description, indiquez si vous souhaitez que la requête soit privée ou visible pour tous les utilisateurs, et définissez les paramètres de date, d'heure et de récurrence facultative. Si vous souhaitez restreindre la requête aux données collectées depuis l'exécution précédente, cochez la case **Interroger uniquement les nouvelles données**. Cliquez sur **Planifier une requête**. Vous pouvez afficher et modifier les requêtes planifiées, mais aussi visualiser et exporter les résultats dans l'onglet **Requêtes planifiées**. Vous pouvez exécuter au maximum 25 requêtes ou en planifier l'exécution. Les requêtes arrêtées ou les requêtes exécutées une seule fois mais terminées ne sont pas prises en compte dans cette limite. Si vous souhaitez enregistrer les résultats de la requête pour les afficher ultérieurement à partir de l'onglet **Instantanés de requête**, dans la section des résultats, cliquez sur . Saisissez un nom et une description, puis indiquez si vous souhaitez que les résultats soient privés ou visibles par tous les utilisateurs.
Afficher un instantané de requête	Dans l'onglet **Instantanés de requête**, cliquez sur un instantané de requête. Notez que cela affiche les résultats d'origine de la requête lorsqu'elle a été enregistrée et qu'il ne s'agit pas d'une nouvelle requête.

3. Pour filtrer les résultats de la requête, effectuez l'une des opérations suivantes :

- Pour filtrer les résultats de la requête par date et horodatage, cliquez sur une ou plusieurs barres de l'histogramme. Cliquez sur n'importe quelle barre de la plage sélectionnée pour supprimer le filtre de date et d'heure.
- Pour filtrer les résultats de la requête par colonne, cliquez sur en regard de cette colonne (par exemple, Terminal) et sélectionnez les critères de filtre.
- Pour filtrer les résultats de la requête en fonction d'une valeur que vous spécifiez, cliquez sur au-dessus des résultats de la requête, puis saisissez ou collez la valeur dans le champ de recherche (par exemple, un horodatage spécifique, une valeur de détail d'évènement, etc.).

4. Développez un résultat pour afficher les détails correspondants. Cliquez sur » pour ouvrir un panneau contenant les détails de l'évènement et des informations sur les alertes associées (vous devrez peut-être faire défiler la fenêtre des résultats vers la droite). Pour filtrer les résultats de la requête en vue d'afficher les correspondances d'un ou de plusieurs facets spécifiques, cliquez sur en regard de ces facets. Cliquez à nouveau sur l'icône pour supprimer le filtre.
5. Dans les résultats de la requête, développez le menu ⋮ pour afficher les actions disponibles pour chaque résultat. En fonction du type de résultat, les actions suivantes peuvent être disponibles :
   - Demander et afficher les données détaillées
   - Mettre le fichier en quarantaine globale ; Le fichier apparaît dans **Paramètres > Liste globale > Quarantaine globale**, dans **Protection > Menaces** et dans la section **Menaces** des détails du terminal.
   - Demander et télécharger un fichier; si des informations de chemin sont disponibles pour des fichiers associés à d'autres types d'artefacts, vous pouvez également télécharger ces fichiers. Le fichier est compressé et protégé par un mot de passe afin d'éviter toute exécution par erreur. Le mot de passe est « infecté ». La taille maximum pour la récupération de fichiers est de 50 Mo. CylanceOPTICS conserve les artéfacts et les fichiers pendant 30 jours.
6. Si vous souhaitez épingler un résultat de sorte à l'afficher avec un marqueur visuel s'il apparait dans les requêtes suivantes, cliquez sur .

À la fin :

- Pour exporter les résultats de requête dans un fichier .csv, cliquez sur . Saisissez un nom et une description, indiquez si vous souhaitez que les résultats exportés soient privés ou visibles par tous les administrateurs, puis cliquez sur **Exporter**. Vous pouvez télécharger le fichier à partir de l'onglet **Résultats exportés** lorsqu'il est prêt.
- Pour ajouter une nouvelle requête, cliquez sur en regard de l'onglet de la requête en cours.
- Pour copier une requête existante, placez le pointeur de la souris sur l'onglet correspondant et cliquez sur .

Syntaxe EQL prise en charge pour les requêtes avancées

Aide sur la syntaxe

Le volet d'aide sur la syntaxe sous CylanceOPTICS > Recherche avancée répertorie les classes d'évènements CylanceOPTICS disponibles et leurs artéfacts, types, catégories et sous-catégories associés. À mesure de la saisie, des options de syntaxe et des messages de validation s'affichent pour vous aider à créer votre requête.

Format de requête EQL

Les requêtes EQL CylanceOPTICS utilisent le format suivant pour une requête de base :

```
<event class> where <event/artifact>.<facet> == <value>
```

Une requête recherche les événements liés à des artefacts. Vous devez donc utiliser la classe d'événements appropriée dans votre requête.

La clause WHERE peut filtrer les résultats en fonction des valeurs event.type, event.category, event.subcategory ou artifact.facet.

Vous pouvez utiliser `or` ou `and` pour combiner plusieurs clauses de filtre.

Faire correspondre n'importe quelle classe d'événement

Vous pouvez utiliser `any` pour la classe d'évènements, qui correspond à toutes les classes d'évènements disponibles.

Échapper une classe d'événements

Pour échapper aux classes d'événements qui contiennent un caractère spécial (par exemple, un tiret ou un point), contiennent un espace ou commencent par un chiffre, utilisez des guillemets (") ou trois guillemets (""").

Échapper un nom de champ

Pour échapper des noms de champ contenant un trait d'union, un espace ou commençant par un chiffre, utilisez les coches arrière (`). Utilisez des coches doubles (``) pour échapper tout coche (`) dans le nom du champ.

Échapper une valeur

Si vous utilisez un caractère spécial dans une valeur, y compris un guillemet ou une barre oblique inverse, elle doit être précédée d'une barre oblique inverse (par exemple, \" pour un guillemet et \\ pour une barre oblique inverse).

Conditions

Une condition consiste en un ou plusieurs critères auxquels un événement doit correspondre. Vous pouvez spécifier et combiner des critères avec les opérateurs décrits dans les sections suivantes.

Opérateurs de comparaison

Opérateur	Description
<	Cet opérateur renvoie vrai si la valeur à gauche de l'opérateur est inférieure à la valeur à droite. Sinon, il renvoie faux.
<=	Cet opérateur renvoie vrai si la valeur à gauche de l'opérateur est inférieure ou égale à la valeur à droite. Sinon, il renvoie faux.
==	Cet opérateur renvoie vrai si les valeurs à gauche et à droite de l'opérateur sont égales. Sinon, il renvoie faux. Les caractères génériques ne sont pas pris en charge.
:	Cet opérateur renvoie vrai si les chaînes à gauche et à droite de l'opérateur sont égales. Sinon, il renvoie faux. Peut être utilisé pour comparer des chaînes uniquement.

Opérateur	Description
!=	Cet opérateur renvoie la vrai si les valeurs à gauche et à droite de l'opérateur ne sont pas égales. Sinon, il renvoie faux. Les caractères génériques ne sont pas pris en charge. Notez que les valeurs NULL sont également filtrées à partir des résultats (vous pouvez utiliser == NULL pour afficher les résultats NULL).
>=	Cet opérateur renvoie vrai si la valeur à gauche de l'opérateur est supérieure ou égale à la valeur à droite. Sinon, il renvoie faux. Lors de la comparaison de chaînes, l'opérateur utilise un ordre lexicographique sensible à la casse.
>	Cet opérateur renvoie vrai si la valeur à gauche de l'opérateur est supérieure à la valeur à droite. Sinon, il renvoie faux. Lors de la comparaison de chaînes, l'opérateur utilise un ordre lexicographique sensible à la casse.

= n'est pas pris en charge en tant qu'opérateur égal. Utilisez plutôt == ou :

Mots-clés de comparaison de modèles

Opérateur	Description
like	Cet opérateur renvoie vrai si la chaîne à gauche du mot-clé correspond à la chaîne à droite (sensible à la casse). Il prend en charge les recherches de liste (voir les opérateurs de recherche ci-dessous) et peut être utilisé pour comparer des chaînes uniquement. Pour une correspondance non sensible à la casse, utilisez like~.
regex	Cet opérateur renvoie vrai si la chaîne à gauche du mot-clé correspond à une expression régulière à droite (reportez-vous à la section Syntaxe d'expression régulière). Il prend en charge les recherches de liste et peut être utilisé pour comparer des chaînes uniquement. Pour une correspondance non sensible à la casse, utilisez regex~.

```
my_field like  "VALUE*"         // case-sensitive wildcard matching
my_field like~ "value*"         // case-insensitive wildcard matching

my_field regex  "VALUE[^Z].?"   // case-sensitive regex matching
my_field regex~ "value[^z].?"   // case-insensitive regex matching
```

Limites des comparaisons

Vous ne pouvez pas les comparer en chaîne. Utilisez plutôt un opérateur logique entre les comparaisons (reportez-vous à la section opérateurs logiques ci-dessous).

Par exemple, `foo < bar <= baz` n'est pas prise en charge, alors que `foo < bar and bar <= baz` l'est.

Vous ne pouvez pas comparer un champ à un autre, même si les champs sont modifiés à l'aide d'une fonction.

La requête suivante n'est pas valide car elle compare la valeur du champ process.parent.name au champ process.name :

```
process where process.parent.name == "foo" and process.parent.name == process.name
```

La requête suivante est valide car elle compare les champs process.parent.name et process.name aux valeurs statiques :

```
process where process.parent.name == "foo" and process.name == "foo"
```

Opérateurs logiques

Opérateur	Description
and	Cet opérateur renvoie vrai uniquement si la condition à gauche et à droite renvoient toutes les deux la valeur vrai. Sinon, il renvoie faux.
ou	Cet opérateur renvoie vrai si l'une des conditions à gauche ou à droite est vraie. Sinon, il renvoie faux.
non	Cet opérateur renvoie vrai si la condition à droite est faux.

Opérateurs de recherche

Opérateur	Description
in	Cet opérateur renvoie vrai si la valeur figure dans la liste fournie (sensible à la casse). Pour une correspondance non sensible à la casse, utilisez in~.
not in	Cet opérateur renvoie vrai si la valeur ne figure pas dans la liste fournie (sensible à la casse). Pour une correspondance non sensible à la casse, utilisez not in~.
:	Cet opérateur renvoie vrai si la chaîne est contenue dans la liste fournie. Il ne peut être utilisé que pour comparer des chaînes.
like	Cet opérateur renvoie vrai si la chaîne correspond à une chaîne de la liste fournie (sensible à la casse). Il ne peut être utilisé que pour comparer des chaînes. Pour une correspondance non sensible à la casse, utilisez like~.
regex	Cet opérateur renvoie vrai si la chaîne correspond à un modèle d'expression régulière dans la liste fournie (reportez-vous à la section Syntaxe des expressions régulières). Il ne peut être utilisé que pour comparer des chaînes. Pour une correspondance non sensible à la casse, utilisez regex~.

```
my_field in ("Value-1", "VALUE2", "VAL3")                 // case-sensitive
my_field in~ ("value-1", "value2", "val3")                // case-insensitive

my_field not in ("Value-1", "VALUE2", "VAL3")             // case-sensitive
my_field not in~ ("value-1", "value2", "val3")            // case-insensitive
```

```
my_field : ("value-1", "value2", "val3")                  // case-insensitive

my_field like  ("Value-*", "VALUE2", "VAL?")              // case-sensitive
my_field like~ ("value-*", "value2", "val?")              // case-insensitive

my_field regex  ("[vV]alue-[0-9]", "VALUE[^2].?", "VAL3") // case-sensitive
my_field regex~  ("value-[0-9]", "value[^2].?", "val3")   // case-insensitive
```

Correspond à n'importe quelle condition

Utilisez la condition `where true` pour mettre en correspondance les évènements uniquement sur la catégorie d'évènement. Par exemple, la requête suivante correspond à n'importe quel événement de fichier :

```
file where true
```

Pour faire correspondre n'importe quel événement, vous pouvez combiner le mot-clé any avec la condition where true :

```
any where true
```

Exemples d'interrogations

Reportez-vous à la section Exemples de requêtes EQL CylanceOPTICS.

Exemples de requêtes EQL CylanceOPTICS

Interroger les recherches DNS pour une URL spécifiée :

```
network where dns.questions.question_name == "<URL>"
```

Interroger un espace de noms WMI spécifié :

```
application where event.subcategory == "wmi" and wmi_trace.namespace == "<espace
 de noms>"
```

Interroger les fichiers avec l'une des valeurs SHA256 spécifiées :

```
file where file.sha256 in ("<valeur>", "<valeur>", "<valeur>")
```

Interroger les processus portant le nom de processus spécifié :

```
process where process.name == "<nom>"
```

Interroger les processus dans lesquels la ligne de commande contient une chaîne spécifiée :

```
process where process.command_line like "<chaîne>"
```

Interroger les informations sur les connexions réseau à une adresse IP spécifiée sur un port spécifié :

```
network where network.destination.ip_address == "<IP>" and
 network.destination.port == "<port>"
```

Afficher les données détaillées

Focus Data vous permet de visualiser et d'analyser la chaîne d'événements, ainsi que les artefacts et facettes associés de ces événements, qui ont entraîné la création d'un logiciel malveillant ou d'une autre menace de sécurité sur un terminal. Les données détaillées conservées pendant 30 jours.

Pour les terminaux dotés de l'agent CylanceOPTICS 2.x ou versions antérieures, la console ne peut récupérer les données détaillées que s'ils sont en ligne. Pour les terminaux dotés de l'agent 3.0 ou versions ultérieures, il n'est pas nécessaire que les terminaux soient en ligne, car la console peut récupérer les dernières données disponibles dans la base de données cloud de CylanceOPTICS.

Avant de commencer : Pour activer le chargement automatique des données détaillées des terminaux vers la console de gestion, activez ces options dans la stratégie de terminal. Si vous ne sélectionnez pas cette option, vous devez utiliser la console pour demander manuellement des données détaillées.

Effectuez l'une des opérations suivantes :

Tâche	Étapes
Affichez les données détaillées à partir des détails du terminal.	**a.** Dans la barre de menus de la console de gestion , cliquez sur **Actifs > Terminaux**. **b.** Cliquez sur un terminal et consultez la section **Menaces et activités**. **c.** Si vous n'avez pas activé le chargement automatique des données détaillées pour une menace ou un événement, cliquez sur **Demander des données**. **d.** Cliquez sur **Afficher les données**.
Afficher les données détaillées à partir d'une requête InstaQuery.	Pour créer une requête InstaQuery, reportez-vous à la page Créer une requête InstaQuery. **a.** Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > InstaQuery > Requêtes précédentes**. **b.** Pour une requête InstaQuery, cliquez sur **Afficher les résultats**. **c.** Pour obtenir un résultat, cliquez sur **Actions > Demander des données détaillées**. **d.** Cliquez sur **Afficher les données détaillées**.
Affichez les données données détaillées à partir d'une liste principale.	**a.** Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Données détaillées**. La liste inclut les données détaillées précédemment demandées par un administrateur ou chargées automatiquement dans la console. **b.** Pour un artefact ou un événement, cliquez sur **Afficher les données**.

À la fin :

- Certains artefacts ou certaines facettes dans les données détaillées peuvent inclure une option **Créer une requête InstaQuery** pour récupérer d'autres informations. Ce type de requête est appelé pivot. Les propriétés d'artefact ou de facette sont préremplies, vous devez uniquement spécifier les zones appropriées. Les résultats de la requête pivot sont alors disponibles avec les données détaillées associées.
- Pour exporter les données de mise au point dans un fichier .csv, cliquez sur , puis sur .

Afficher et télécharger les fichiers récupérés par CylanceOPTICS

Lorsque CylanceOPTICS identifie un fichier comme une menace potentielle, vous pouvez le récupérer à partir du terminal (par exemple, lorsque vous examinez les détails de détection ou les résultats InstaQuery). Vous pouvez afficher la liste de tous les fichiers récupérés par CylanceOPTICS, et vous pouvez télécharger des fichiers à partir de cette vue pour une analyse plus approfondie.

1. Sur la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Historique des actions**.
2. Cliquez sur l'onglet **Historique des téléchargements de fichiers**.
3. Si vous souhaitez filtrer les résultats, cliquez sur .
4. Si vous souhaitez télécharger un fichier, cliquez sur **Télécharger le fichier**. Lisez l'avertissement et cliquez sur **Confirmer le téléchargement**.

Utilisation de CylanceOPTICS pour détecter les évènements et y répondre

CylanceOPTICS utilise le moteur d'analyse de contexte (CAE) pour analyser et corréler les évènements qui se produisent sur les terminaux en temps quasi réel. La logique du CAE est stockée localement sur le terminal, ce qui permet à l'agent CylanceOPTICS de surveiller et de suivre les activités malveillantes ou suspectes, même si le terminal n'est pas connecté aux services cloud CylanceOPTICS. Vous pouvez configurer CylanceOPTICS pour prendre des mesures de réponse automatisées lorsque le CAE identifie certains artefacts d'intérêt, fournissant ainsi une couche supplémentaire de détection et de prévention des menaces pour compléter les fonctionnalités de CylancePROTECT Desktop.

Vous pouvez personnaliser les capacités de détection de CylanceOPTICS pour répondre aux besoins de votre entreprise. Vous pouvez créer des jeux de règles de détection avec la configuration souhaitée des réponses et des règles de détection, cloner et modifier des règles de détection existantes ou créer vos propres règles personnalisées, et créer des exceptions de détection pour exclure des artefacts spécifiques de la détection.

Créer un jeu de règles de détection

Créez et appliquez un jeu de règles de détection pour configurer les types d'évènements CylanceOPTICS à détecter et comment CylanceOPTICS répond à ces évènements. Un jeu de règles de détection par défaut est disponible pour vous aider à tester et à évaluer la manière dont vous souhaitez utiliser les règles de détection. Dans le jeu de règles par défaut, toutes les règles de détection sont activées, et les réponses automatisées et les notifications utilisateur sont désactivées.

Lorsque vous créez un jeu de règles de détection, il est recommandé d'activer d'abord les règles de détection souhaitées sans action de réponse ni notifications sur le bureau. Après avoir évalué les données de détection, vous pouvez configurer les actions de réponse appropriées et les notifications utilisateur pour chaque règle.

Avant de commencer :

- Pour afficher un jeu de règles, vous devez disposer d'un rôle d'administrateur avec les autorisations Afficher le jeu de règles et Modifier un jeu de règles dans la section Réponse de détection de point de terminaison.
- Pour plus d'informations sur les règles CylanceOPTICS facultatives que vous pouvez importer pour l'environnement de votre organisation, consultez l'article KB76816.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Configurations**.
2. Dans l'onglet **Jeux de règles**, cliquez sur **Créer**.
3. Saisissez un nom et une description.
4. Si vous souhaitez que l'agent CylanceOPTICS affiche un message lorsqu'une règle est déclenchée sur le terminal, saisissez le message dans le champ **Message de notification de détection**.
5. Passez en revue les règles disponibles. Pour chaque règle, vous pouvez passer la souris sur l'icône d'informations pour afficher une description. Cliquez sur **Activer** pour activer un groupe de règles entier ou une règle spécifique.
6. Si vous souhaitez afficher une notification de bureau lorsqu'une règle est déclenchée sur un terminal, cochez la case **Afficher la notification de détection sur le terminal** correspondant à la règle.
7. Si vous souhaitez que l'agent CylanceOPTICS exécute une action de réponse lorsqu'une règle est déclenchée sur un terminal, sélectionnez une ou plusieurs actions dans la liste déroulante de la règle **Réponse**. Passez le curseur de la souris sur l'icône d'informations de chaque action pour en afficher la description.
8. Dans la liste déroulante **Stratégie de terminal**, cliquez sur une ou plusieurs stratégies de terminal auxquelles vous souhaitez attribuer le jeu de règles de détection.

Vous pouvez également attribuer un jeu de règles de détection à une stratégie de terminal lorsque vous créez ou modifiez une stratégie de terminal.

9. Cliquez sur **Confirmer**. Vérifiez le résumé, puis cliquez de nouveau sur **Confirmer**.

À la fin : Après avoir attribué le jeu de règles de détection à une stratégie de terminal, vous pouvez afficher et gérer les détections. Vous pouvez également effectuer l'une des tâches facultatives suivantes :

- Pour réduire les faux positifs ou les évènements en double, vous pouvez créer des exceptions de détection.
- Créez des règles de détection personnalisées.
- Créer un playbook de package pour répondre à des événements.

Réponses aux événements

L'agent CylanceOPTICS peut exécuter les actions de réponse suivantes lorsqu'un événement de détection est déclenché :

Réponse	Description
Journal d'application	L'agent consigne les événements de détection dans le journal d'application Windows.
Supprimer des fichiers	L'agent supprime définitivement tous les artefacts de fichier identifiés comme artefacts d'intérêt (AOI).
Supprimer des clés de registre	L'agent supprime définitivement la clé de registre complète des AOI identifiés comme artefacts de registre.
Supprimer des valeurs de registre	L'agent supprime définitivement la valeur de registre des AOI identifiés comme artefacts de registre.
Détection de vidage sur disque	L'agent crée un fichier de données de détection dans le répertoire de données de l'application CylanceOPTICS.
Déconnecter tous les utilisateurs	L'agent déconnecte tous les utilisateurs interactifs et distants.
Déconnecter les utilisateurs	L'agent déconnecte les utilisateurs spécifiés.
Déconnecter les utilisateurs inactifs	L'agent déconnecte tous les utilisateurs qui sont actuellement en interaction physique avec le terminal.
Déconnecter les utilisateurs à distance	L'agent déconnecte tous les utilisateurs dont la session est actuellement établie à distance sur le système.
Fenêtre de notification	L'agent affiche une fenêtre de notification avec le message de notification de détection que vous avez spécifié, en utilisant la zone de notification native du système d'exploitation au lieu de l'agent CylancePROTECT.
Suspendre les processus	L'agent suspend les artefacts de processus identifiés comme AOI.

Réponse	Description
Suspendre les arborescences de processus	L'agent suspend l'ensemble de l'arborescence de processus des artefacts de processus identifiés comme AOI. L'AOI est traité comme la racine de l'arborescence.
Arrêter les processus	L'agent arrête les artefacts de processus identifiés comme AOI.
Arrêter les arborescences de processus	L'agent arrête l'ensemble de l'arborescence de processus des artefacts de processus identifiés comme AOI. L'AOI est traité comme la racine de l'arborescence.
Mettre les processus sur liste blanche	Cette option exclut les processus spécifiés de l'observation par CylanceOPTICS.

Afficher et gérer les détections

Vous pouvez utiliser la console de gestion pour afficher et analyser les évènements détectés par le CAE. Le tableau de bord des détections vous permet d'afficher les tendances des évènements sur différentes périodes et la sévérité des différentes détections, et d'accéder à des informations détaillées pour chaque détection.

Avant de commencer : Créer un jeu de règles de détection.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Détections**.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Modifiez la portée des données de détection.	Dans la liste déroulante **Détections au fil du temps**, sélectionnez la portée souhaitée.
Incluez ou excluez les détections de différents niveaux de priorité.	Le graphique indique le nombre d'évènements de priorité faible, moyenne et élevée, à titre informatif. Cliquez sur l'un des nombres pour exclure ces évènements des données de détection. Cliquez à nouveau sur le même élément pour l'inclure dans les données.
Affichez les détails et les artefacts d'intérêt pour une détection.	Cliquez sur **Afficher**. En fonction des artefacts associés à la détection, vous pouvez sélectionner différentes actions (par exemple, vous pouvez télécharger un fichier, mettre un fichier en quarantaine, afficher les données détaillées, créer une exception de détection, etc.). Vous pouvez cliquer sur la section **Notes de détection** pour ajouter des notes pertinentes à votre analyse.
Verrouillez le terminal associé à une détection.	**a.** Cliquez sur **Afficher**. **b.** Dans la liste déroulante **Actions**, cliquez sur **Verrouiller le terminal**. **c.** Reportez-vous à la section Verrouiller un terminal.
Exportez les détails de détection dans un fichier JSON.	**a.** Cliquez sur **Afficher**. **b.** Dans la liste déroulante **Actions**, cliquez sur **Exporter des données**.

Tâche	Étapes
Définissez l'état d'un évènement de détection.	Effectuez l'une des opérations suivantes : • Cliquez sur la liste déroulante **État** pour une détection et sélectionnez l'état approprié. Si vous sélectionnez **Faux positif**, vous êtes invité à indiquer comment vous souhaitez gérer les détections de doublons. Sélectionnez l'option appropriée et cliquez sur **Enregistrer**. • Sélectionnez une ou plusieurs détections et cliquez sur **Sélectionner une action > Modifier l'état**. Sélectionnez l'état approprié et cliquez sur **Confirmer**.
Supprimez au moins une détection.	Sélectionnez les détections et cliquez sur **Sélectionner une action > Supprimer la détection**. Cliquez sur **Confirmer la suppression**.

Création de règles de détection personnalisées

Pour répondre aux besoins et exigences de sécurité de votre organisation, vous pouvez utiliser l'éditeur de règles CylanceOPTICS pour cloner et modifier les règles de détection disponibles dans la console de gestion, ou vous pouvez créer vos propres règles de détection personnalisées. Vous pouvez utiliser la flexibilité et la logique du moteur d'analyse de contexte (CAE) pour détecter les activités suspectes ou malveillantes, y compris pour surveiller des caractéristiques de comportement générales (par exemple, des fichiers qui utilisent certains modèles de dénomination) ou une série d'événements ciblée (par exemple, un processus avec une empreinte de signature de fichier spécifique qui crée des fichiers et initie des connexions réseau). Les règles de détection personnalisées utilisent le même flux de travail que les règles de détection fournies par BlackBerry et vous pouvez configurer des actions de réponse automatisées, des notifications utilisateur et des Playbooks de package pour vos règles personnalisées.

L'éditeur de règles utilise JSON et fournit des outils de validation intégrés. Lorsque vous validez une règle, l'éditeur vérifie la syntaxe pour identifier les éventuels problèmes. Si la règle réussit la vérification de la syntaxe, CylanceOPTICS utilise un service CAE pour vérifier qu'elle pourra être compilée et s'exécuter sur un terminal. Si l'un des processus de validation détecte un problème, il fournit des informations sur les erreurs à corriger. Lorsqu'une règle réussit les deux vérifications de validation, vous pouvez la publier et l'ajouter aux jeux de règles de détection.

Cette section fournit des conseils et des informations de référence pour créer vos propres règles CAE. Les règles CAE prennent en charge les données et les filtres suivants :

Élément	Description
États	Les états définissent le flux d'une règle CAE, ce qui permet à CylanceOPTICS d'observer en termes d'état une série d'événements pouvant se produire sur un terminal. Ces états représentent un scénario de type « 1, puis 2, puis 3 » qui peut se produire.
Fonctions	Les fonctions définissent la logique requise pour remplir un état. Cette logique s'applique directement aux opérateurs de champ définis et représente les attributs d'un événement qui se produit sur un terminal (par exemple, « A, et B, et C » ou « A, et B, mais pas C »).

Élément	Description
Opérateurs de champ	Les opérateurs de champ définissent la méthode d'évaluation des opérandes (extracteurs de valeur de facette). Les opérateurs de champ incluent des actions telles que Égal à, Contient et Est vrai.
Opérandes (Extracteurs de valeur de facette)	Les opérandes sont les valeurs que CylanceOPTICS compare. Les opérandes permettent d'extraire des données spécifiques concernant un événement (par exemple, chemins d'accès aux fichiers, hachage des fichiers et noms de processus) et de les comparer à des valeurs littérales (par exemple, chaines, nombres décimaux, valeurs booléennes et nombres entiers).
Artefacts d'intérêt	Les artefacts d'intérêt définissent les artefacts que CylanceOPTICS peut cibler lorsqu'il exécute des actions de réponse automatisées (par exemple, l'arrêt de processus, la déconnexion d'utilisateurs ou la suppression de fichiers).
Chemins d'accès	Les chemins d'accès définissent la façon dont le CAE interprète le flux de plusieurs objets d'état dans une règle.
Filtres	Les filtres réduisent ou étendent la portée d'un état avec un nombre plus ou moins important d'événements à analyser.

Pour résoudre les problèmes de performances dans les environnements qui génèrent un nombre anormalement élevé d'événements (par exemple, des systèmes de serveurs ou des systèmes d'ingénierie logicielle), le CAE prend en charge des règles d'exclusion que vous pouvez utiliser pour exclure certains événements du pipeline de données CylanceOPTICS. CylanceOPTICS n'analyse pas les événements exclus et ne les enregistre pas. Vous pouvez utiliser les règles d'exclusion préconfigurées disponibles dans la console de gestion, ou utiliser l'éditeur de règles pour créer vos propres règles d'exclusion à l'aide de la même structure JSON que les règles de détection. L'objectif d'une règle d'exclusion est de la satisfaire en fonction des processus que vous souhaitez exclure.

Après avoir publié une règle d'exclusion, vous pouvez l'associer à l'action de réponse aux processus autorisés dans un jeu de règles de détection. Avec cette action de réponse, le CAE exclut automatiquement tous les événements et processus qui correspondent à la logique de la règle associée. Faites preuve de prudence lorsque vous utilisez des règles d'exclusion, car elles peuvent réduire la sécurité globale des terminaux CylanceOPTICS.

Exemple de règle de détection

Consultez les rubriques suivantes pour comprendre le format et les options des règles CAE :

- États
- Fonctions
- Opérateurs de champ
- Opérandes (Extracteurs de valeur de facette)
- Artefacts d'intérêt
- Chemins d'accès
- Filtres

```
{
    "States": [
    {
        "Name": "TestFile",
        "Scope": "Global",
        "Function": "(a)",
        "FieldOperators": {
```

```
            "a": {
                "Type": "Contains",
                "Operands": [
                    {
                        "Source": "TargetFile",
                        "Data": "Path"
                    },
                    {
                        "Source": "Literal",
                        "Data": "my_test_file"
                    }
                ],
                "OperandType": "String"
                }
            },
            "ActivationTimeLimit": "-0:00:00.001",
            "Actions": [
                {
                    "Type": "AOI",
                    "ItemName": "InstigatingProcess",
                    "Position": "PostActivation"
                },
                {
                    "Type": "AOI",
                    "ItemName": "TargetProcess",
                    "Position": "PostActivation"
                },
                {
                    "Type": "AOI",
                    "ItemName": "TargetFile",
                    "Position": "PostActivation"
                }
            ],
            "HarvestContributingEvent": true,
            "Filters": [
                {
                    "Type": "Event",
                    "Data": {
                        "Category": "File",
                        "SubCategory": "",
                        "Type": "Create"
                    }
                }
            ]
        }
    ],
     "Paths": [
        {
            "StateNames": [
            "NewSuspiciousFile",
            "CertUtilDecode"
            ]
        }
    ],
    "Tags": [
        "CylanceOPTICS"
    ]
}
```

Pour consulter un autre exemple de règle de détection personnalisée, reportez-vous à l'article KB66651.

Créer et gérer des règles et des exclusions de détection

Avant de commencer : Si vous souhaitez cloner et modifier une règle de détection existante ou créer votre propre règle personnalisée, consultez les rubriques suivantes et la règle de détection d'échantillon pour comprendre le format et les options des règles CAE :

- États
- Fonctions
- Opérateurs de champ
- Opérandes (Extracteurs de valeur de facette)
- Artefacts d'intérêt
- Chemins d'accès
- Filtres

1. Dans le menu de la console de gestion, cliquez sur **CylanceOPTICS > Configurations**, puis cliquez sur l'onglet **Règles**.

   Vous pouvez trier et filtrer les règles de détection disponibles et afficher les informations de chaque règle.
2. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Exporter une règle vers un fichier .json.	Vous pouvez exporter des règles de détection à partir de l'une des catégories de règles suivantes : personnalisé, Cylance Experimental, Cylance Exclusion, Cylance macOS Official, Cylance Windows Official. Cliquez sur pour une règle.
Importer une règle de détection personnalisée à partir d'un fichier .json.	**a.** Cliquez sur **Importer une règle**. **b.** Accédez au fichier .json et sélectionnez-le ou faites-le glisser-déposer. Cliquez sur **Importer**. **c.** Modifiez la configuration et la syntaxe des règles selon vos besoins. **d.** Cliquez sur **Valider**. **e.** Cliquez sur **Publier**. Pour modifier une règle personnalisée après sa publication, cliquez sur pour la règle.
Cloner et modifier une règle de détection.	Vous pouvez cloner des règles de détection à partir de l'une des catégories de règles suivantes : personnalisé, Cylance Experimental, Cylance Exclusion, Cylance macOS Official, Cylance Windows Official. **a.** Cliquez sur pour une règle. **b.** Modifiez la configuration et la syntaxe des règles selon vos besoins. **c.** Cliquez sur **Valider**. **d.** Cliquez sur **Publier**.
Supprimer une règle personnalisée.	Vous pouvez supprimer des règles de la catégorie personnalisé uniquement. **a.** Cliquez sur pour une règle. **b.** Cliquez sur **Confirmer la suppression**.

États

Les états sont le niveau logique le plus élevé d'une règle CAE et ont un plus grand nombre de champs obligatoires.

Nom du champ	Description
Actions	Ce champ contient une liste des objets utilisés pour définir des artefacts d'intérêt dans un état. Pour plus d'informations, reportez-vous à Artefacts d'intérêt.
Durée limite d'activation	Ce champ définit la durée d'attente d'CylanceOPTICS avant que des évènements déclenchent l'évènement. La valeur par défaut recommandée est -0:00:00:001.
Opérateurs de champ	Ce champ contient les opérateurs de champ et les opérandes qui doivent être inspectés pour remplir la fonction définie dans l'état. Pour plus d'informations, reportez-vous à Opérateurs de champ.
Filtres	Ce champ définit les catégories, sous-catégories et types d'évènements que CylanceOPTICS doit inspecter lors de la tentative de traitement d'un état. Pour plus d'informations, reportez-vous à Filtres.
Fonction	Ce champ contient la fonction logique devant être observée par CylanceOPTICS pour considérer qu'un état est satisfait. Pour plus d'informations, reportez-vous à Fonctions.
Évènements de contribution de collecte	Ce champ définit si CylanceOPTICS doit enregistrer les évènements qui satisfont un état. La valeur recommandée est 3.
Nom	Ce champ définit le nom de l'état qui sera affiché dans l'interface utilisateur si la règle est satisfaite.
Portée	Ce champ définit la portée dans laquelle CylanceOPTICS recherche les évènements pertinents. Dans la plupart des cas, la valeur recommandée est globale.
États	Ce champ contient une liste d'un ou de plusieurs objets d'état. Ces objets peuvent être chaînés.

Fonctions

Les fonctions définissent la logique requise pour remplir l'état d'une règle CAE. Cette logique s'applique directement aux opérateurs de champ définis et est utilisée pour représenter les attributs « A et B, et C » ou « A et B, mais pas C » d'un événement qui se produit sur un terminal. Cette logique s'applique directement aux opérateurs de champ définis dans un état.

Fonction	Description	Exemple
AND - &	Au moins deux opérateurs de champ doivent être mis en correspondance pour satisfaire l'état.	a & b & c
OR - |	Un ou plusieurs opérateurs de champ doivent être mis en correspondance pour satisfaire l'état.	a | b | c

Fonction	Description	Exemple
NOT - !	Un opérateur de champ défini doit être défini sur false ou ne pas correspondre pour satisfaire l'état.	a & b & !c
GROUP - ()	Les opérateurs de terrain sont regroupés pour répondre à des exigences logiques plus complexes.	(a & b) | (c & !d)

Opérateurs de champ

Les opérateurs de champ sont les parties logiques d'une règle qui permettent à CylanceOPTICS de comparer deux valeurs. Si au moins deux opérandes correspondent aux critères de comparaison, CylanceOPTICS considère que cette partie de la fonction définie a été exécutée. Lorsque toutes les parties de la fonction sont exécutées, l'état est satisfait.

Le champ Opérateurs de champ est un objet qui comprend un ou plusieurs objets conditionnels. Ces objets conditionnels peuvent être définis sur une valeur quelconque ; cependant, ils doivent correspondre aux mêmes valeurs conditionnelles référencées dans le champ de fonction. BlackBerry recommande de définir ces noms sur des valeurs simples et logiques, telles que des chiffres ou des lettres.

Opérateur de champ	Description
Base64Encoding Base64	Cet opérateur de champ tokenise une chaîne et détermine si l'un des jetons correspond à un opérande. Il tente également de déterminer le type de codage de chaîne (ASCII, UTF-7, UTF-8, UTF-16-LE, UTF-16-BE, UTF-32-LE OU UTF-32-BE). Sans nomenclature, l'opérateur peut détecter de manière fiable uniquement UTF-8, UTF-16-LE et UTF-16-BE. Si toutes les détections échouent, l'opérateur se règle par défaut sur la page de codes par défaut du système. Positif : `powershell.exe -ex bypass -e "ZwBlAHQALQBwAHIAbwBjAGUAcwBzAA==" equals ("get-process", )` Négatif : `powershell.exe -ex bypass "ZwBlAHQALQBhAGwAaQBhAHMA" does not contain ("get-process", )`
ContainsAll	Cet opérateur de champ détermine si l'opérande spécifié contient tous les opérandes d'un jeu. Positif : « hello, I am a string » contient tous les éléments (« ello », « ng ») Négatif : « hello, I am a string » ne contient pas tous les éléments (« hi », « ng »)

Opérateur de champ	Description
ContainsAllWords	Cet opérateur de champ détermine si l'opérande spécifié contient tous les opérandes d'un jeu, dans lequel chaque opérande défini doit apparaitre comme un mot entier entouré d'espace blanc, de ponctuation ou de marqueurs de chaine de fin ou de début. Positif : « hello, I am a string » contient tous les mots (« hello », « a », « string ») Négatif : « hello, I am a string » ne contient pas tous les mots (« ello », « ng »)
ContainsAny Contient	Cet opérateur de champ détermine si l'opérande spécifié contient l'un des opérandes d'un jeu. Positif : « hello, I am a string » contient l'un des éléments (« ello », « banana ») Négatif : « hello, I am a string » ne contient aucun des éléments (« hi », « ng »)
ContainsAnyWord ContainsWord	Cet opérateur de champ détermine si l'opérande spécifié contient l'un des opérandes d'un jeu, dans lequel chaque opérande défini doit apparaitre comme un mot entier entouré d'espace blanc, de ponctuation ou de marqueurs de chaine de fin ou de début. Positif : « hello, I am a string » contient l'un des mots (« hello », « banana ») Négatif : « hello, I am a string » ne contient aucun des mots (« ello », « ng »)
DamerauLevenshteinDistance DLDistance	Cet opérateur de champ détermine si la distance, le nombre de modifications nécessaires pour convertir un opérande en un autre opérande, se situe dans une plage acceptable, mais permet la transposition de symboles adjacents. Positif : « cat » est à une distance Damerau-Levenshtein de 1 de « bat » Positif : « hello » est à une distance Damerau-Levenshtein de 2 de « bell » Positif : « ca » est à une distance Damerau-Levenshtein de 3 de « abc » Négatif : « cart » n'est pas à une distance Damerau-Levenshtein de 1 de « act »

Opérateur de champ	Description
Coefficient de Dice Dice	Cet opérateur de champ détermine la similarité entre deux ensembles ou chaînes en fonction du nombre de bigrammes communs (une paire de lettres adjacentes dans la chaîne). Il détermine si le résultat de la comparaison se situe entre le « mincoefficient » et le « maxcoefficient ». Par exemple, la comparaison du nom de processus « Test.exe » avec « Tes.exe » renvoie 0,76923076923076927. Avec « Arrondi » réglé sur 2 : Positif : min. : 0,5 < 0,77 < 0,8 max. ; non inclusif Positif : min. : 0,77 < = 0,77 < = 0,77 max. ; inclusif Négatif : min. : 0,8 < 0,77 < 0,85 max. ; non inclusif L'option « Arrondi » arrondit la décimale à l'entier spécifié. Par exemple, si « Arrondi » est défini sur 2, 0,6666666667 devient 0,67.
EndsWithAny EndsWith	Cet opérateur de champ détermine si l'opérande de gauche spécifié se termine par l'opérande de droite spécifié. Positif : « hello, I am a string » se termine par « ring » Négatif : « hello, I am a string » ne se termine pas par « bring »
EqualsAny Est égal à	Cet opérateur de champ détermine si l'opérande spécifié est exactement égal à l'un des opérandes d'un jeu, dans lequel chaque opérande défini doit apparaitre sous forme de nombre ou de mot entier entouré d'espace blanc, de ponctuation ou de marqueurs de chaine de fin ou de début. Positif : 10 est égal à l'un des éléments (10, 20, 30) Positif : « hello » est égal à l'un des éléments (« hello », « banana ») Négatif : 100 n'est égal à aucun des éléments (10, 20, 30) Négatif : « hello » n'est égal à aucun des éléments « ello », « ng »)
GreaterThan	Cet opérateur de champ détermine si l'opérande de gauche spécifié est supérieur à l'opérande de droite spécifié. Positif : 14,4 est supérieur à 10,1 Négatif : 1 n'est pas supérieur à 1000
GreaterThanOrEquals	Cet opérateur de champ détermine si l'opérande de gauche spécifié est supérieur ou égal à l'opérande de droite spécifié. Positif : 14,4 est supérieur ou égal à 10,1 Négatif : 1 n'est pas supérieur ou égal à 1000

Opérateur de champ	Description
HammingDistance	Cet opérateur de champ détermine la distance entre deux chaînes de longueur égale, c'est-à-dire le nombre de positions auxquelles les symboles correspondants sont différents. Il mesure le nombre minimal de substitutions requises pour changer une chaîne en une autre. Positif : « cat » est à une distance Hamming de 1 de « bat » • cat → bat(1) Positif : « hello » est à une distance Hamming de 2 de « bell » • hello → bello(1) → bell(2) Positif : « ca » est à une distance Hamming de 3 de « abc » • ca → aa(1) → ab(2) → abc(3) Négatif : « cart » n'est pas à une distance Hamming de 4 de « act » • cart → aart(1) → acrt(2) → actt(3) → act(4)
HexEncoding	Cet opérateur de champ tokenise une chaîne et détermine si l'un des jetons correspond à un opérande. Il tente également de déterminer le type de codage de chaîne (ASCII, UTF-7, UTF-8, UTF-16-LE, UTF-16-BE, UTF-32-LE, UTF-32-BE). Sans nomenclature, il peut détecter de manière fiable uniquement UTF-8, UTF-16-LE et UTF-16-BE. Si toutes les détections échouent, l'opérande est défini par défaut sur la page de codes par défaut du système. Positif : « 74657374 » contient « test » Négatif : « 696e76616c6964 » ne contient pas « test »
InRange	Cet opérateur de champ détermine si l'opérande du milieu spécifié est placé entre les opérandes de gauche et de droite. Positif : 10 est entre 1 et 20 Positif : 5,3 est entre 5,3 et 20,1 (inclus) Négatif : 4 n'est pas entre 5 et 10 Négatif : 20 n'est pas entre 20 et 40 (exclus)

Opérateur de champ	Description

IpIsInRange
IpRange
	Cet opérateur de champ détermine si l'adresse TargetNetworkConnection (SourceAddress, DestinationAddress) figure dans les options « min » et « max » spécifiées.
	Les opérandes suivants sont autorisés :
	`{ "Source": "TargetNetworkConnection", "Data": "SourceAddress" }`
	And:
	`{ "Source": "TargetNetworkConnection", "Data": "DestinationAddress" }`
	Exemple :
	`"FieldOperators": { "a": { "Type": "IpIsInRange", "OperandType": "IPAddres", "Options": { "min": "123.45.67.89", "max": "123.45.67.255" }, "Operands": [ { "Source": "TargetNetworkConnection", "Data": "DestAddr" } ] } }`
	Incluez l'objet de filtres suivant dans l'exemple ci-dessus pour générer le trafic réseau :
	`"Filters": [ { "Type": "Event", "Data": { "Category": "Network", "SubCategory": "*", "Type": "Connect" } } ]`

Opérateur de champ	Description
IsFlagSet	Cet opérateur de champ vérifie si un ou plusieurs bits d'un masque binaire sont définis. Il peut utiliser base-10 ou base-16 (en utilisant le préfixe « 0x ») pour la valeur de comparaison. Positif : 0x10 est défini pour 0x4111 Positif : 3 est défini pour 0x7 Négatif : 0x3 n'est pas défini pour 0x4 Négatif : 2 n'est pas défini pour 0x5
IsHomoglyph	Cet opérateur de champ détermine si l'opérande de gauche est un homoglyphe de l'opérande de droite. Par exemple, le caractère US Latin 1 « e » et le caractère « e » français semblent être identiques et avoir la même signification, mais leurs valeurs sont différentes. Positif : « 3xplor3 » est un homoglyphe de « explore » avec 100 % de certitude Positif : « 3xplord » est un homoglyphe de « explore » avec 90 % de certitude Négatif : « temp » n'est pas un homoglyphe de « temp », car il s'agit de la même chaine Négatif : « 431 » n'est pas un homoglyphe de « big », car ils ne présentent aucune caractéristique transitive
IsNullOrEmpty	Cet opérateur de champ détermine si l'opérande spécifié est nul ou vide. Positif : <null> est nul ou vide Positif : "" est nul ou vide Positif : " " est nul ou vide Négatif : « Hello » n'est pas nul ou vide
IsPopulated Exists HasContent	Cet opérateur de champ détermine si l'opérande spécifié n'est pas nul ni vide. Positif : « Hello » n'est pas nul ni vide Négatif : <null> est nul ou vide Négatif : "" est nul ou vide Négatif : " " est nul ou vide
IsTrue	Cet opérateur de champ détermine si la valeur spécifiée est vraie. Positif : TriState.True Négatif : TriState.False Négative : TriState.Unknown

Opérateur de champ	Description
LessThan	Cet opérateur de champ détermine si l'opérande de gauche spécifié est inférieur à l'opérande de droite spécifié. Positif : 4,4 est inférieur à 10,1 Négatif : 1000 n'est pas inférieur à 1
LessThanOrEquals	Cet opérateur de champ détermine si l'opérande de gauche spécifié est inférieur ou égal à l'opérande de droite spécifié. Positif : 4,4 est inférieur ou égal à 10,1 Positif : 14 est inférieur ou égal à 14 Négatif : 1000 n'est pas inférieur ou égal à 1
LevenshteinDistance	Cet opérateur de champ détermine si la distance, le nombre de modifications nécessaires pour convertir un opérande en un autre opérande, se situe dans une plage acceptable. Positif : « cat » est à une distance Levenshtein de 1 de « bat » Positif : « hello » est à une distance Levenshtein de 3 de « bell » Négatif : « cart » n'est pas à une distance Levenshtein de 1 de « act »
LongestCommonSubsequence	Cet opérateur de champ compare un opérande gauche fixe avec un ensemble d'opérandes droits et détermine la sous-séquence la plus longue dans chaque comparaison. Il compare le nombre de résultats aux valeurs min et max pour déterminer si le résultat se situe dans une plage acceptable. Comparaison de « aggtab » et « gxtxayb » : Positif : « gtab » est la séquence la plus longue. Si le min est 1 et le max est 10, cela se situe dans une plage acceptable. Négatif : dans l'exemple précédent, si le min était de 5 et le max de 10, cela ne se situerait pas dans une plage acceptable.
LongestCommonSubstring	Cet opérateur de champ compare les opérandes gauche et droit et renvoie le nombre de la plus longue sous-chaîne trouvée. Comparaison entre « abababc » et « abcdaba » : Positif : « aba » et « abc » sont deux résultats de la même taille dans « abcdaba » et renvoient la sous-chaîne la plus longue définie sur 3. Négatif : si la distance minimale et la distance maximale étaient définies sur 4, cela serait supérieur à la plus longue sous-chaîne trouvée. Comparaison entre « ababcd » et « abcdaba » : Positif : « abcd » est la plus longue sous-chaîne trouvée.
MatchOnFilter NoOp	Cet opérateur de champ indique qu'aucune opération n'est en cours d'exécution et que l'état correspond simplement si le filtre trouve un événement correspondant.

Opérateur de champ	Description
RegexMatches	Cet opérateur de champ détermine si l'opérande spécifié est conforme à une expression régulière. Positif : « hello, I am a string » est conforme à « ^hello, [Ii] am [aA] string $ » Négatif : « hello, I am a string » n'est pas conforme à « ^[hi|hey], I am a string$ »
ShannonEntropy	Cet opérateur de champ détermine la mesure de l'imprévisibilité de l'état, ou son contenu d'information moyen lors de la comparaison d'un seul opérande. Positif : « abc » est calculé à 1,5849625007211561 et se situe dans la plage entre 1,55 et 1,6. Négatif : « Z2V0LXByb2NIc3M=" est calculé à 3,875 et ne se situe pas dans la plage entre 1,55 et 1,6.
StartsWithAny StartsWith	Cet opérateur de champ détermine si l'opérande de gauche spécifié commence par l'opérande de droite spécifié. Positif : « hello, I am a string » commence par « hello, I » Négatif : « hello, I am a string » ne commence pas par « help »

Opérandes (Extracteurs de valeur de facette)

Le CAE d'CylanceOPTICS utilise des extracteurs de valeurs de facet pour identifier une propriété individuelle (facet) d'un seul artefact associé à un évènement CylanceOPTICS observé. Bien que les extracteurs de valeurs de facet soient eux-mêmes limités, ils peuvent être regroupés de manière logique pour analyser les comportements complexes qui se produisent sur un terminal et déclencher un évènement de détection.

Nom de l'extracteur	Description	Facets pris en charge
InstigatingProcess	Cet extracteur extrait un facet du processus instigateur d'un évènement et est couramment utilisé pour inspecter les arguments de nom ou de ligne de commande d'un processus qui déclenche une action (par exemple, démarrer un autre processus, initier une connexion réseau ou écrire un fichier).	Nom (sous forme de chaîne) CommandLine (sous forme de chaîne)

Nom de l'extracteur	Description	Facets pris en charge	
InstigatingProcessImageFile	Cet extracteur extrait un facet du fichier image qui est associé au processus instigateur d'un évènement. Il est couramment utilisé pour inspecter divers attributs du fichier image (par exemple, nom, chemin, hachage ou état de signature).	Chemin (sous forme de chaîne) Taille (sous forme d'entier) Md5Hash (sous forme de chaîne) Sha256Hash (sous forme de chaîne) IsHidden (sous forme de valeur booléenne) IsReadOnly (sous forme de valeur booléenne) Répertoire (sous forme de chaîne) SuspectedFileType (sous forme de chaîne) SignatureStatus (sous forme de chaîne) IsSelfSigned (sous forme de valeur booléenne) LeafDNSString (sous forme de chaîne) LeafThumbprint (sous forme de chaîne) LeafSignatureAlgorith (sous forme de chaîne) LeafCN (sous forme de chaîne) LeafDN (sous forme de chaîne) LeafOU (sous forme de chaîne) LeafO (sous forme de chaîne) LeafL (sous forme de chaîne) LeafC (sous forme de chaîne)	IssuerDNString (sous forme de chaîne) IssuerThumbprint (sous forme de chaîne) IssuerSignatureAlgorithm (sous forme de chaîne) IssuerCN (sous forme de chaîne) IssuerDN (sous forme de chaîne) IssuerOU (sous forme de chaîne) IssuerO (sous forme de chaîne) IssuerL (sous forme de chaîne) IssuerC (sous forme de chaîne) RootDNString (sous forme de chaîne) RootThumbprint (sous forme de chaîne) RootSignatureAlgorithm (sous forme de chaîne) RootCN (sous forme de chaîne) RootDN (sous forme de chaîne) RootOU (sous forme de chaîne) RootO (sous forme de chaîne) RootL (sous forme de chaîne) RootC (sous forme de chaîne)

Nom de l'extracteur	Description	Facets pris en charge
InstigatingProcessOwner	Cet extracteur extrait un facet du propriétaire associé au processus instigateur d'un évènement. Il est couramment utilisé pour inspecter l'utilisateur propriétaire du processus.	Nom (sous forme de chaîne) Domaine (sous forme de chaîne)
TargetFile	Cet extracteur extrait un facet d'un fichier sur lequel un évènement s'est produit. Il est couramment utilisé pour inspecter divers attributs du fichier (par exemple, nom, chemin, hachage ou état de signature).	Voir InstigatingProcessImageFile ci-dessus.
TargetFileOwner	Cet extracteur extrait un facet du propriétaire associé au fichier sur lequel un évènement s'est produit. Il est couramment utilisé pour inspecter l'utilisateur propriétaire du fichier.	Voir InstigatingProcessOwner ci-dessus.
TargetNetworkConnection	Cet extracteur extrait un facet de la connexion réseau sur laquelle un évènement s'est produit. Il est couramment utilisé pour inspecter l'adresse IP du réseau ou le port sur lequel des mesures sont prises.	SourceAddress (sous forme d'adresse IP) SourcePort (sous forme d'entier) DestinationAddress (sous forme d'adresse IP) DestinationPort (sous forme d'entier)
TargetProcess	Cet extracteur extrait un facet du processus sur lequel un évènement s'est produit. Il est couramment utilisé pour inspecter les arguments de nom ou de ligne de commande d'un processus sur lequel des mesures sont prises.	Voir InstigatingProcess ci-dessus.

Nom de l'extracteur	Description	Facets pris en charge
TargetProcessImageFile	Cet extracteur extrait un facet du fichier image associé un processus sur lequel un évènement s'est produit. Il est couramment utilisé pour inspecter les attributs du fichier image (par exemple, nom, chemin, hachage ou état de signature).	Voir InstigatingProcessImageFile ci-dessus.
TargetProcessOwner	Cet extracteur extrait un facet du propriétaire associé un processus sur lequel un évènement s'est produit. Il est couramment utilisé pour inspecter l'utilisateur propriétaire du processus sur lequel des mesures sont prises.	Voir InstigatingProcessOwner ci-dessus.
TargetRegistryKey	Cet extracteur extrait un facet de la clé de registre sur laquelle un évènement s'est produit. Il est couramment utilisé pour inspecter la valeur ou la clé de registre sur laquelle des mesures sont prises.	Chemin (sous forme de chaîne) ValueName (sous forme de chaîne)

Extracteurs de valeurs de chemin

Nom de l'extracteur	Description
EnvVar	EnvVar extrait une variable d'environnement du système d'exploitation.
LiteralWithEnvVar	LiteralWithEnvVar développe un chemin contenant une variable d'environnement.
Literal	Literal, qui représente une valeur littérale, est l'extracteur et l'opérande les plus courants.

Artefacts d'intérêt

Vous pouvez utiliser les artefacts d'intérêt (AOI) dans le champ des actions pour définir une liste d'artefacts pour lesquels CylanceOPTICS peut effectuer des actions de réponse automatisées. L'AOI suit la même syntaxe que les opérandes. Tout artefact associé à un évènement ou à un ensemble d'évènements satisfaisant à un état peut être marqué comme un AOI. L'AOI n'a pas besoin d'être défini comme opérande pour être considéré comme AOI.

Si un filtre est appliqué à un état, notez que certains AOI ne seront pas disponibles pour prendre des mesures de réponse automatiques. Par exemple, si un filtre de création de fichier est appliqué à un état, l'AOI lié au fichier et au processus est disponible, mais n'a pas d'AOI lié au registre ou au réseau. Si un AOI non pertinent est fourni dans un état, l'agent CylanceOPTICS se charge de son exclusion de la manière appropriée. Le tableau ci-dessous décrit le filtre applicable aux relations d'AOI.

Catégorie	Sous-catégorie	Type	AOI applicable
Fichier	—	Créer	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
Fichier	—	Supprimer	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
Fichier	—	Renommer	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
Fichier	—	Écrire	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetFile TargetFileOwner
Réseau	IPv4	Se connecter	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
Réseau	IPv6	Se connecter	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection

Catégorie	Sous-catégorie	Type	AOI applicable
Réseau	TCP	Se connecter	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
Réseau	UDP	Se connecter	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetNetworkConnection
Processus	—	Quitter	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
Processus	—	Démarrer	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
Processus	CylancePROTECT Desktop	AbnormalExit	TargetProcess TargetProcessImageFile TargetProcessOwner
Registre	—	PersistencePoint KeyCreating	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registre	—	PersistencePoint : KeyCreated	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey

Catégorie	Sous-catégorie	Type	AOI applicable
Registre	—	PersistencePoint KeyDeleting	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registre	—	PersistencePoint : KeyDeleted	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registre	—	PersistencePoint KeyRenaming	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registre	—	PersistencePoint : KeyRenamed	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registre	—	PersistencePoint ValueChanging	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registre	—	PersistencePoint : ValueChanged	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Registre	—	PersistencePoint ValueDeleting	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey

Catégorie	Sous-catégorie	Type	AOI applicable
Registre	—	PersistencePoint : ValueDeleted	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetRegistryKey
Thread	—	Créer	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner
Thread	—	Injecter	InstigatingProcess InstigatingProcessImageFile InstigatingProcessOwner TargetProcess TargetProcessImageFile TargetProcessOwner

Exemple :

```
"Actions": [
    {
        "Type": "AOI",
        "ItemName": "InstigatingProcess",
        "Position": "PostActivation"
    },
    {
        "Type": "AOI",
        "ItemName": "TargetProcess",
        "Position": "PostActivation"
    },
    {
        "Type": "AOI",
        "ItemName": "InstigatingProcessOwner",
        "Position": "PostActivation"
    }
],
```

Chemins d'accès

Les chemins d'accès définissent la façon dont le CAE interprète le flux de plusieurs objets d' état au sein d'une règle. Vous utilisez les chemins d'accès lors de la création d'une règle composée de plusieurs objets d'état (également appelée règle à états multiples). Les états définissent le flux d'une règle CAE et permettent

à CylanceOPTICS d'observer avec état une série d'évènements se produisant sur un terminal. Ces éléments représentent un scénario « 1, puis 2, puis 3 » qui peut se produire.

Si une règle possède un seul objet d'état, vous n'avez pas besoin d'utiliser un objet de chemins. Les règles se composent d'un seul objet d'état et ne nécessitent pas explicitement l'utilisation de l'objet de chemins. Les règles qui utilisent l'objet de chemins le font uniquement pour la définition explicite (pas pour la fonctionnalité de règle).

Dans les exemples suivants, deux objets d'état sont utilisés : NewSuspiciousFile et CertUtilDecode. Chaque état possède son propre ensemble logique.

Exemple 1 : dans la configuration suivante, le CAE recherche un évènement qui satisfait l'état NewSuspiciousFile. Lorsque cet état est satisfait, le CAE recherche un évènement qui satisfait l'état CertUtilDecode.

```
"Paths": [
    {
        "StateNames": [
            "NewSuspiciousFile",
            "CertUtilDecode"
        ]
    }
],
```

Exemple 2 : dans la configuration suivante, le CAE recherche un évènement qui satisfait l'état CertUtilDecode, puis l'état NewSuspiciousFile.

```
"Paths": [
    {
        "StateNames": [
            "CertUtilDecode",
            "NewSuspiciousFile"
        ]
    }
],
```

Exemple 3 : dans la configuration suivante, le CAE recherche un évènement qui satisfait l'état NewSuspiciousFile ou CertUtilDecode. Cela est utile lorsque les états ont des ensembles d'objets de filtre différents. Dans cet exemple, NewSuspiciousFile utilise un filtre d'écriture de fichier et CertUtilDecode utilise un filtre de démarrage de processus.

```
"Paths": [
    {
        "StateNames": [
            "CertUtilDecode"
        ]
    },
    {
        "StateNames": [
            "NewSuspiciousFile"
        ]
    }
],
```

Filtres

Vous pouvez utiliser des filtres pour réduire ou étendre la portée d'un état afin de prendre en compte un nombre plus ou moins important d'événements à analyser. Les filtres d'événements utilisent les mêmes catégories,

sous-catégories et types d'événements que ceux décrits dans la section Structures de données utilisées par CylanceOPTICS pour identifier les menaces.

Exemple 1 : l'exemple suivant limite les événements inspectés pour traiter les événements de démarrage.

```
"Filters": [
    {
        "Type": "Event",
        "Data": {
            "Category": "Process",
            "SubCategory": "",
            "Type": "Start"
        }
    }
]
```

Exemple 2 : l'exemple suivant examine tous les types d'événements de fichier (créer, écrire, supprimer).

```
"Filters": [
    {
        "Type": "Event",
        "Data": {
            "Category": "File",
            "SubCategory": "",
            "Type": "*"
        }
    }
]
```

Créer une exception de détection

Pour réduire les faux positifs ou les événements en double dans vos résultats de détection, vous pouvez créer des exceptions pour les règles de détection. Lorsque vous créez une exception de détection, les processus spécifiés ne sont pas évalués par le moteur de détection CylanceOPTICS. Soyez prudent lorsque vous créez des exceptions de détection, car elles peuvent réduire la sécurité globale des terminaux.

Remarque : Si vous créez et activez une exception de règle qui utilise uniquement des correspondances regex pour des conditions, cela peut entraîner une utilisation du CPU plus élevée que la normale sur certains systèmes avec un nombre d'événements constamment élevé, en raison de l'exception de règle exécutée sur chaque événement. Si vous rencontrez ce problème, BlackBerry recommande de désactiver l'exception de règle qui utilise les correspondances regex pour les conditions.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Configurations**.
2. Dans l'onglet **Exceptions**, cliquez sur **Créer une exception**.
3. Saisissez un nom pour l'exception de détection.
4. Dans la section **Conditions**, configurez les conditions d'exception. Cliquez sur **Ajouter une autre condition** pour configurer des exceptions supplémentaires.

   Dans une exception de détection, une instruction AND est appliquée à toutes les conditions. Toutes les conditions doivent être remplies pour que l'exception soit vraie. Lorsque vous spécifiez une valeur pour une condition, elle est traitée comme une instruction ANY. Lorsque deux valeurs ou plus sont ajoutées, si l'une de ces valeurs existe, la condition est vraie.
5. Cliquez sur **Enregistrer**.

À la fin : Dans la barre de menus, cliquez sur **CylanceOPTICS > Configurations**, puis cliquez sur l'onglet **Jeux de règles**. Modifiez un jeu de règles de détection et attribuez l'exception de détection aux règles souhaitées. Cliquez sur **Confirmer**.

Déployer un package pour collecter des données à partir de terminaux

Vous pouvez utiliser la fonction de déploiement de package CylanceOPTICS pour exécuter un processus à distance et en toute sécurité (par exemple, un script Python) sur les terminaux CylanceOPTICS afin de collecter et de stocker les données souhaitées dans un emplacement spécifié pour une analyse plus approfondie par les administrateurs de sécurité. Par exemple, vous pouvez exécuter un processus de collecte des données du navigateur. Vous pouvez utiliser les packages de collecte de données CylanceOPTICS disponibles dans la console de gestion ou créer les vôtres.

Lorsque vous déployez un package sur des terminaux hors ligne, le déploiement attend pendant une période spécifiée qu'ils soient mis en ligne.

Avant de commencer :

- Si vous le souhaitez, créez un package qui s'exécutera sur un terminal, collectez des points de données spécifiques et générez ces données vers un emplacement local ou de serveur que vous spécifierez dans les étapes ci-dessous. Pour plus d'informations sur la création d'un package personnalisé, rendez-vous sur support.blackberry.com/community pour consulter l'article 66563.
- Si vous créez votre propre package, vous devez le charger sur la console de gestion. Dans la console, accédez à **CylanceOPTICS > Configurations > Packages** et cliquez sur **Télécharger le fichier**.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Packages**.
2. Cliquez sur **Déployer des packages**.
3. Dans la liste déroulante **Package**, cliquez sur le package à envoyer aux terminaux. Cliquez sur **Ajouter un autre package** pour ajouter des packages supplémentaires.
4. Dans la liste déroulante **Type de collecte**, cliquez sur l'emplacement où vous souhaitez stocker les données que le package collectera.
   - Le type **Local** enregistre les données à l'emplacement indiqué sur le terminal.
   - Si vous sélectionnez **SFTP**, **SMB**, ou **S3**, spécifiez les informations requises.
5. Cliquez sur **Suivant**.
6. Sélectionnez **Terminal** ou **Zone**, puis sélectionnez les terminaux ou les zones auxquels livrer le package.
7. Pour spécifier un délai d'expiration et une priorité pour le déploiement du package, cliquez sur **Afficher les options avancées** et effectuez l'une des opérations suivantes :
   - Dans la liste déroulante **Valide pour**, cliquez sur le délai d'expiration souhaité. Si un terminal n'est pas en ligne pendant cette période, le déploiement du package est annulé pour ce terminal.
   - Réglez le curseur de **priorité** pour définir une priorité supérieure ou inférieure. La priorité est prise en compte lorsque d'autres tâches CylanceOPTICS sont mises en file d'attente pour le même terminal.
8. Saisissez le nom et la description du déploiement du package.
9. Cliquez sur **Déployer**.

À la fin :

- Accédez à **CylanceOPTICS > Packages** pour afficher l'état actuel et la progression du déploiement du package.
- Vous pouvez cliquer sur l'état de déploiement d'un package pour afficher des détails sur le déploiement. Pour afficher l'état individuel de chaque terminal, développez la section Cibles. Si vous souhaitez arrêter un déploiement de package en cours, dans la liste déroulante **Sélectionner une action**, cliquez sur **Arrêter la tâche**.

Créer un playbook de package pour répondre à des événements

Lorsqu'un incident de sécurité se produit sur un terminal, vous pouvez réduire le temps de réponse en créant un playbook de package. Un playbook de package vous permet d'automatiser l'exécution de packages refract lorsqu'un événement déclenche une règle de moteur d'analyse de contexte (CAE) que vous avez configurée dans un jeu de règles de détection.

Les playbooks de package prennent uniquement en charge les packages refract Python. Vous pouvez utiliser des packages refract prêts à l'emploi disponibles dans la console de gestion, ou vous pouvez ajouter vos propres packages refract personnalisés. Le contenu d'un playbook de package est stocké sur le terminal, pour être exécuté même si le terminal est hors ligne. Vous pouvez créer 100 playbooks de package maximum.

Avant de commencer :

- Créer un jeu de règles de détection.
- Si vous le souhaitez, créez un package refract Python qui peut s'exécuter sur un terminal lorsqu'une règle de détection est déclenchée. Pour plus d'informations sur la création d'un package personnalisé, consultez l'article KB 66563.
- Si vous créez votre propre package, vous devez le charger sur la console de gestion. Dans la console, accédez à **CylanceOPTICS > Configurations > Packages** et cliquez sur **Télécharger le fichier**.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Configurations**, puis cliquez sur l'onglet **Playbooks**.
2. Cliquez sur **Créer un playbook**.

   Si vous souhaitez cloner un playbook de package existant, filtrez la liste des playbooks pour obtenir le playbook de votre choix et cliquer sur .
3. Saisissez un nom et une description.
4. Dans la liste déroulante **Type de collecte**, cliquez sur l'emplacement où vous souhaitez stocker les données que le package collectera.
   - Le type **Local** enregistre les données à l'emplacement indiqué sur le terminal.
   - Si vous sélectionnez **SFTP**, **SMB**, ou **S3**, spécifiez les informations requises.
5. Cliquez sur **Suivant**.
6. Dans la liste déroulante **Package**, cliquez sur un package que vous souhaitez inclure dans le playbook de package. Si nécessaire, spécifiez des arguments de ligne de commande facultatifs.
7. Cliquez sur **Ajouter un autre package** pour ajouter des packages supplémentaires. Vous pouvez ajouter 20 playbooks maximum à un playbook de package.
8. Cliquez sur **Enregistrer**.

À la fin : Dans la barre de menus, cliquez sur **CylanceOPTICS > Configurations > Jeux de règles**. Modifiez un jeu de règles de détection et attribuez le playbook de package aux règles de votre choix. Cliquez sur **Confirmer**. Vous pouvez associer jusqu'à 10 playbooks de package à chaque règle de détection.

Verrouiller un terminal

Vous pouvez verrouiller un terminal infecté ou potentiellement infecté pour arrêter l'activité de commande et de contrôle, l'exfiltration des données et le mouvement latéral des logiciels malveillants. Vous disposez des options de verrouillage suivantes :

Type de verrouillage	Description
Verrouillage complet (toutes les plateformes)	Empêchez toute communication réseau à partir du terminal. Vous pouvez verrouiller un terminal pendant une durée maximale de 96 heures. Pour déverrouiller le terminal avant la fin de la période de verrouillage, utilisez une clé de déverrouillage.
Verrouillage partiel (agent CylanceOPTICS 3.1 ou versions ultérieures pour Windows uniquement)	Désactivez les capacités de réseau LAN et Wi-Fi du terminal et conservez la communication avec les services cloud CylanceOPTICS ce qui permet à CylanceOPTICS de continuer à recevoir les détections et les données du capteur. Le verrouillage partiel dure indéfiniment. Vous pouvez déverrouiller le terminal à tout moment à l'aide d'une clé de déverrouillage ou de la fonction de déverrouillage à distance.
Verrouillage partiel personnalisé (agent CylanceOPTICS 3.2.1140 ou versions ultérieures pour Windows uniquement)	Cette option est identique au verrouillage partiel, mais vous permet également de spécifier des canaux de communication supplémentaires que vous souhaitez autoriser lors d'un verrouillage partiel.

Avant de commencer :

- Pour connaitre les conditions requises pour la prise en charge de la fonction de verrouillage pour Linux, consultez Configuration requise de CylanceOPTICS.
- Si vous souhaitez utiliser un verrouillage partiel personnalisé, dans la barre de menus, cliquez sur **Paramètres > Détection et réponse > Ajouter une nouvelle configuration**. Spécifiez un nom, une description et l'adresse IP, le port et les opérations (entrantes, sortantes, bidirectionnelles) pour les canaux de communication que vous souhaitez autoriser pendant le verrouillage partiel. Cliquez sur **Enregistrer**.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Terminaux**.
2. Cliquez sur le nom du terminal.
3. Effectuez l'une des opérations suivantes :

Tâche	Étapes
Verrouiller complètement un terminal (toutes les plateformes)	**a.** Dans la liste déroulante **Sélectionner une action**, cliquez sur **Verrouiller**. **b.** S'il s'agit d'un terminal Windows, cliquez sur **Verrouillage complet** dans la liste déroulante. **c.** Sélectionnez une période de verrouillage. **d.** Cliquez sur **Confirmer le verrouillage**.

Tâche	Étapes
Verrouiller partiellement un terminal (agent CylanceOPTICS 3.1 ou version ultérieure pour Windows uniquement)	**a.** Dans la liste déroulante **Sélectionner une action**, cliquez sur **Verrouiller**. **b.** Dans la liste déroulante, effectuez l'une des opérations suivantes : • Pour utiliser la configuration de verrouillage partiel par défaut, cliquez sur **Verrouillage partiel**. • Pour utiliser l'une de vos configurations de verrouillage partiel personnalisées, cliquez sur la configuration. **c.** Si vous souhaitez autoriser les sessions de réponse à distance sur le terminal alors qu'il est partiellement verrouillé, activez **Réponse à distance**. **d.** Cliquez sur **Confirmer le verrouillage**. Pour déverrouiller le terminal à distance, cliquez sur le terminal et, dans la liste déroulante **Sélectionner une action**, sélectionnez **Déverrouiller le terminal**. Confirmez le déverrouillage à distance.

4. Si vous souhaitez déverrouiller manuellement un terminal complètement ou partiellement verrouillé, cliquez sur **Actions > Afficher la clé de déverrouillage**. Copiez la clé de déverrouillage unique et exécutez les commandes suivantes sur le terminal :

OS	Commandes
Windows	**a.** Accédez au dossier exécutable CylanceOPTICS (par défaut, C:\Program Files \Cylance\Optics). **b.** Exécuter `CyOptics.exe control --password "<unlock_key>" unlock -a`
macOS	**a.** Exécuter `cd /Library/Application\ Support/Cylance/Optics/CyOptics.app/Contents/Resources` **b.** Exécuter `sudo ../MacOS/CyOptics control --password <unlock_key> unlock -net`
Linux	Exécuter `./CyOptics control --password "password" unlock -net`

Envoi d'actions vers un terminal

Vous pouvez utiliser la fonction de réponse à distance pour exécuter en toute sécurité des scripts et des commandes sur un terminal CylanceOPTICS directement à partir de la console de gestion, à l'aide d'une interface de ligne de commande connue.

Lorsque vous démarrez une session de réponse distante, l'agent CylanceOPTICS crée une instance du shell natif du terminal (cmd pour Windows, bash pour macOS et Linux) et gère le transfert des commandes vers et depuis le shell. Vous avez ainsi accès aux fonctions du shell natif et aux applications et scripts disponibles sur le terminal. CylanceOPTICS fournit également des commandes réservées que vous pouvez utiliser pour transférer des fichiers vers et depuis le terminal.

Une session de réponse distante ne peut être lancée qu'avec un terminal en ligne et expire au bout de 25 minutes d'inactivité. Plusieurs sessions peuvent être ouvertes simultanément pour le même terminal (50 maximum).

La réponse distante fournit un haut niveau d'accès à un terminal. Soyez donc prudent lorsque vous émettez des commandes et respectez les stratégies de sécurité de votre organisation. Lorsque vous utilisez la réponse

distante, les détails de la session, y compris les commandes envoyées, les informations sur les transferts de fichiers et les réponses reçues, sont enregistrés dans le journal du terminal auquel vous pouvez accéder à partir de la console de gestion. Le fichier journal est conservé pendant 30 jours.

Démarrer une session de réponse à distance

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceOPTICS > Terminaux**.
2. Recherchez le terminal et cliquez sur son nom.
3. Dans la liste déroulante **Sélectionner une action**, cliquez sur **Réponse distante**.
4. Entrez des commandes dans la fenêtre de session de réponse distante.

   Pour plus d'informations sur les commandes réservées pour CylanceOPTICS, reportez-vous à la section Commandes réservées pour la réponse à distance.

À la fin : Pour télécharger le journal du terminal avec l'enregistrement de la session de réponse distante, cliquez sur **CylanceOPTICS > Historique des actions** dans la barre de menus. Recherchez le terminal et cliquez sur **Télécharger le journal**.

Commandes réservées pour la réponse à distance

Les commandes réservées suivantes, communes aux plateformes de système d'exploitation prises en charge, n'interagissent pas directement avec le shell natif sur le terminal.

Élément	Description
`rr-clear`	Cette commande efface la fenêtre du terminal de réponse distante.
`rr-get <absolute_path_to_file>`	Cette commande copie le fichier spécifié (qui doit inclure le nom du fichier) depuis le terminal et le télécharge dans votre navigateur Web pour que vous puissiez l'enregistrer sur votre système local. Si la taille du fichier est supérieure à 70 Mo, la commande échoue avec une erreur. Exemple : `rr-get C:\Program Files\Cylance\Desktop \2021-03-26.log`
`rr-help`	Cette commande affiche la liste des commandes réservées.
`rr-put <destination_directory>`	Cette commande ouvre une fenêtre de navigateur de fichiers qui vous permet de sélectionner un fichier de votre système local qui sera envoyé au répertoire spécifié sur le terminal (par exemple, le dossier de téléchargements de l'utilisateur). Si la taille du fichier est supérieure à 70 Mo, la commande échoue avec une erreur. Exemple : `rr-put C:\Users\username\Downloads`
`rr-quit`	Cette commande met fin à la session de réponse distante. La fenêtre du terminal reste ouverte pour que vous puissiez afficher l'historique des sessions, mais les commandes ne sont plus envoyées ou reçues.

Surveillance des connexions réseau avec CylanceGATEWAY

Vous pouvez surveiller l'activité et les évènements associés aux connexions réseau des utilisateurs. CylanceGATEWAY consigne toutes les activités réseau de chaque utilisateur ayant le mode travail CylanceGATEWAY activé sur son terminal. Par défaut, les données d'activité réseau CylanceGATEWAY sont conservées pendant 30 jours. Vous pouvez effectuer une recherche sur 30 jours d'évènements réseau consignés.

Remarque : Si CylanceGATEWAY n'est pas activé pour votre locataire, les options de menu permettant de le configurer ne s'affichent pas dans la console de gestion.

Affichage de l'activité réseau

CylanceGATEWAY consigne toutes les activités réseau pour les terminaux sur lesquels le mode de travail et le mode sans échec sont activés. Le journal des activités réseau enregistre l'utilisateur, le modèle du terminal et son système d'exploitation, le nom d'hôte, la destination, la date et l'heure, ainsi que d'autres détails sur chaque événement de tentative de connexion. Si la confidentialité du trafic est activée dans une règle ACL, les tentatives d'accès au réseau auxquelles la règle s'applique ne sont pas consignées sur l'écran Évènements réseau ou envoyées à la solution SIEM ou au serveur syslog, si elle est configurée.

Si une connexion est identifiée comme une menace, la colonne **Détections** spécifie le type de menace détectée.

- Les détections **Tunnellisation DNS** sont des menaces basées sur l'analyse du trafic DNS entre le client et le serveur DNS de l'utilisateur malveillant (par exemple, lorsqu'un hôte est infecté, le logiciel malveillant peut lancer un canal de commande et de contrôle (C2) avec son créateur pour tenter d'exfiltrer des données).
- Les détections **Réputation** sont des menaces provenant d'adresses figurant sur la liste BlackBerry des destinations Internet dangereuses et sont détectées par l'option de réputation de destination. Une valeur de risque est attribuée à chaque destination. Vous pouvez configurer le niveau de risque des réputations de destination à bloquer.
- Les détections **Détection de signatures** font référence aux menaces détectées par les détections de signature. La détection basée sur la signature est une méthodologie utilisée pour détecter les logiciels malveillants connus qui sont stockés dans une base de données. Lorsqu'une nouvelle signature de logiciel malveillant est identifiée, les experts en cybersécurité ajoutent la signature à une base de données.
- Les détections de type **Du jour zéro** font référence aux nouvelles destinations malveillantes identifiées (par exemple, algorithme de génération de domaine (DGA) et hameçonnage), c'est-à-dire qui n'ont pas été précédemment découvertes. Une fois identifiées, une valeur de risque est attribuée à ces destinations. Elles sont ensuite bloquées ou envoient une alerte en fonction du niveau de risque que vous avez défini pour la protection de votre réseau. Pour plus d'informations, consultez la section Configurer les paramètres de protection réseau dans le contenu relatif à la configuration de Cylance Endpoint Security.

Pour afficher le journal des activités réseau dans la console de gestion, dans la barre de menus, cliquez sur **CylanceGATEWAY > Évènements**.

Pour afficher les détails d'un évènement réseau, cliquez sur la ligne du journal d'activité. Pour en savoir plus sur les détails des évènements, consultez Afficher la page Détails de l'évènement.

Pour filtrer n'importe quelle colonne, cliquez sur ⏷ en haut de la colonne.

Pour effectuer une recherche de formulaire libre, cliquez sur 🔍 et saisissez la requête de recherche. Lorsque vous saisissez les caractères dans le champ de recherche, vous pouvez sélectionner l'une des options de correspondance affichées.

Pour modifier les colonnes à afficher, cliquez sur ||| à droite des en-têtes de colonne.

Pour modifier l'ordre des colonnes d'évènements, faites glisser la colonne à l'endroit où vous souhaitez qu'elle apparaisse.

Pour exporter les informations relatives à l'activité du réseau dans un fichier .csv, cliquez sur . Sélectionnez cette option pour exporter tout ou uniquement l'activité réseau filtrée et cliquez sur **Exporter**.

Pour savoir comment CylanceGATEWAY peut classer une destination réseau à laquelle un utilisateur tente d'accéder, reportez-vous à la section Évaluer le niveau de risque d'une destination réseau.

Afficher la page Détails de l'évènement

Vous pouvez afficher des métadonnées et des détails supplémentaires pour un évènement réseau qui a été consigné sur la page Évènements. Les métadonnées affichées dépendent de plusieurs facteurs, tels que le type de demande réseau effectuée et la manière dont vous avez configuré les règles ACL. Par exemple, les évènements DNS affichent des détails spécifiques au DNS et les évènements TLS affichent des détails spécifiques au TLS. De même, si la protection réseau est activée dans une règle ACL, des métadonnées supplémentaires s'affichent. Vous pouvez partager l'évènement réseau avec d'autres utilisateurs de la console pour auditer ou examiner les destinations auxquelles l'utilisateur a tenté d'accéder. Les utilisateurs de la console doivent disposer des autorisations appropriées pour afficher l'évènement partagé. Cliquez sur pour copier le lien vers l'évènement.

Vous pouvez filtrer les évènements réseau consignés à l'aide des filtres de données suivants :

Filtre	Description
Présentation de l'évènement	
ID d'évènement	Il s'agit d'un identifiant unique pour l'évènement réseau de votre locataire.
Adresse IP source	Il s'agit de l'adresse IP de la passerelle privée qui a été attribuée au tunnel du point de terminaison pendant l'évènement.
Port source	Il s'agit du numéro de port de la destination.
Nom de la requête DNS	Il s'agit du nom de ressource demandée (RR) du serveur DNS que l'agent CylanceGATEWAY a interrogé.
Type de requête DNS	Il s'agit du type de requête DNS (par exemple, un enregistrement A, AAAA ou SRV) qui a été envoyé au serveur DNS.
Destination	Il s'agit de la destination de l'évènement. L'adresse IP de destination est toujours incluse. L'évènement peut également afficher le nom du service réseau ou le nom d'hôte, le cas échéant.
Port de destination	Il s'agit du port de la destination à laquelle vous avez accédé.

Filtre	Description
Adresse IP source de la NAT privée	Il s'agit de l'adresse IP source de cet évènement lorsqu'il a quitté le CylanceGATEWAY Connector pour l'un de vos réseaux privés. Si l'adresse IP source n'est pas disponible ou si cette fonctionnalité n'a pas été activée, le filtre indique « Inconnu ». **Important :** Vous devez vous assurer que l'heure du système CylanceGATEWAY Connector est exacte. Si l'heure du système CylanceGATEWAY Connector manque de précision, les détails de la NAT signalés par le connecteur peuvent ne pas correspondre à l'évènement réseau dans le BlackBerry Infrastructure. Par défaut, le système CylanceGATEWAY Connector utilise le serveur de temps Ubuntu (serveur ntp.ubuntu.com) pour la synchronisation de l'heure ; vous pouvez également spécifier un serveur NTP personnalisé. Si vous utilisez le serveur de temps Ubuntu, assurez-vous qu'il est accessible depuis votre réseau privé. Pour en savoir plus, consultez la section Configurer le système CylanceGATEWAY Connector. Le système CylanceGATEWAY Connector envoie les détails de la NAT mis à jour à l'écran Détails de l'évènement toutes les minutes. Cette fonctionnalité est activée par défaut. Si les détails de la source de la NAT privée ne s'affichent pas dans la page Détails de l'évènement de la console Cylance, vérifiez que vous avez installé la dernière version CylanceGATEWAY Connector et redémarré le connecteur.
Port source de la NAT privée	Il s'agit du port IP source de cet évènement lorsqu'il a quitté le système CylanceGATEWAY Connector pour l'un de vos réseaux privés. Si le numéro de port n'est pas disponible ou si cette fonctionnalité n'a pas été activée, le filtre indique « Inconnu ». Cette fonctionnalité est activée par défaut. Si les détails de la source de la NAT privée ne s'affichent pas dans la page Détails de l'évènement de la console Cylance, vérifiez que vous avez installé la dernière version CylanceGATEWAY Connector et redémarré le connecteur.
Adresse IP source BlackBerry	Il s'agit de l'adresse IP de cet évènement lorsqu'il a quitté le BlackBerry Infrastructure. Cette adresse IP source BlackBerry n'est pas disponible pour les flux qui n'utilisent pas le tunnel CylanceGATEWAY (par exemple, mode sans échec).
Adresse IP source du tunnel	Il s'agit de l'adresse IP du point de terminaison telle qu'elle est détectée par l'BlackBerry Infrastructure lors de son accès au tunnel CylanceGATEWAY.
Protocole	Il s'agit du protocole (couche 4) utilisé par l'évènement réseau pour accéder à la destination. Le protocole peut être UDP ou TCP.
Protocole d'application	Il s'agit du protocole (couche 6 ou 7), tel que TLS, DNS ou HTTP, utilisé pour la communication.
Type d'accès	Il s'agit du type d'accès (par exemple, mode sans échec ou tunnel de passerelle) utilisé par l'évènement réseau pour accéder à la destination.
Routage réseau	Le trafic est ainsi fourni en tant que connexions publiques ou privées qui ont été utilisées pour acheminer le trafic. En ce qui concerne les connexions privées, vous pouvez filtrer par nom de groupe de connecteurs et par CylanceGATEWAY Connector.

Filtre	Description
Connecteur	Il s'agit du système CylanceGATEWAY Connector auquel l'évènement réseau est associé. Pour afficher plus d'informations sur le connecteur, cliquez sur le nom du connecteur.
Catégorie	Il s'agit de la catégorie appliquée à l'évènement. Par exemple, si CylanceGATEWAY a déterminé que la destination contient des menaces potentiellement malveillantes, la catégorie affichée peut être Risque dynamique. Pour plus d'informations sur la catégorie Risque dynamique, reportez-vous à la section Configuration de la protection réseau dans le contenu relatif à la configuration. La destination peut également être classée en fonction de son contenu, par exemple « Informatique et technologies de l'information ». Pour plus d'informations sur les catégories de contenu de destination, reportez-vous à la section Catégories de contenu de destination dans le contenu relatif à la configuration.
Sous-catégorie	Il s'agit de la description de la sous-catégorie de trafic réseau liée à la catégorie associée à la destination. Pour plus d'informations sur les sous-catégories qui peuvent s'afficher lorsque la catégorie est Risque dynamique, reportez-vous à la section Configuration de la protection réseau dans le contenu relatif à la configuration. Pour plus d'informations sur les sous-catégories qui peuvent s'afficher lorsque la catégorie est une catégorie de contenu de destination, reportez-vous à la section Catégories de contenu de destination dans le contenu relatif à la configuration.
Heure de début (UTC)	Il s'agit de l'heure à laquelle la communication de l'activité réseau a commencé. L'heure est affichée en UTC.
Heure de fin (UTC)	Il s'agit de l'heure à laquelle la communication de l'activité réseau s'est terminée. L'heure est affichée en UTC.
PID	Il s'agit de l'ID numérique du processus qui a déclenché la demande DNS. Le PID est signalé par le terminal Windows ou macOS lorsque l'agent est activé avec le mode sans échec.
Chemin d'accès	Indique le chemin d'accès à l'exécutable à partir duquel le processus a été exécuté. Il s'agit généralement du chemin d'accès au fichier svchost.exe. Le chemin est tronqué à 1 024 caractères. Le chemin est signalé par le terminal Windows ou macOS lorsqu'il est activé avec le mode sans échec.
Transféré(e)(s)	Cela indique le nombre d'octets échangés entre la destination et l'agent CylanceGATEWAY. Il s'affiche sous la forme du nombre total d'octets chargés et téléchargés sur le serveur et l'agent CylanceGATEWAY.
Flux de paquets	Il s'agit du nombre de paquets envoyés entre la destination et l'agent CylanceGATEWAY.
Utilisateur	Il s'agit du nom d'utilisateur auquel l'évènement réseau est associé. Vous pouvez filtrer les évènements réseau en fonction du nom d'utilisateur et du nom d'affichage d'un utilisateur Active Directory. Lorsque vous exportez la page Évènements, seul le nom d'utilisateur est exporté. Vous pouvez cliquer sur le nom d'utilisateur pour afficher les évènements associés à l'utilisateur.

Filtre	Description
OS	Il s'agit du terminal utilisé pour lancer l'activité réseau (par exemple,Android, iOS, macOS ou Windows).
Modèle	Il s'agit du modèle du terminal (par exemple iPhone, Samsung Galaxy, Google Pixel).
Terminal	Il s'agit du nom d'hôte de l'utilisateur macOS ou du terminal Windows (exemple.com).
Action	Cela permet d'identifier si l'évènement réseau est autorisé ou bloqué en fonction de vos paramètres de protection réseau et des règles ACL que vous avez spécifiées pour l'environnement. Des informations supplémentaires sur l'action sont incluses dans la section Action.
Action	
Phase de connexion	Il s'agit de la phase d'évaluation au cours de laquelle les propriétés de tentative d'accès ont été comparées aux destinations et conditions de chaque règle ACL. Une ou plusieurs des phases (par exemple, lors de la recherche DNS, de la tentative de connexion et de l'établissement d'une liaison TLS) qui ont été évaluées par rapport aux règles ACL s'affichent.
Heure (UTC)	Il s'agit de l'heure à laquelle l'activité réseau a été évaluée à l'aide d'une règle ACL. L'heure est affichée en UTC.
Règle appliquée	Il s'agit du nom de la règle ACL qui a été appliquée au moment de l'évaluation au cours des différentes phases des règles ACL.
Action	Indique si l'action a été autorisée ou bloquée pour les phases évaluées.
Alertes	
Type	Permet d'identifier l'anomalie déclenchée par l'activité réseau avec le niveau de protection réseau associé. Pour en savoir plus sur les anomalies prises en charge, consultez la section Affichage de l'activité réseau.
Heure (UTC)	Il s'agit de l'heure à laquelle l'activité réseau a déclenché l'alerte. L'heure est affichée en UTC.
Catégorie	C'est l'anomalie qui a déclenché l'alerte. Pour en savoir plus les anomalies, consultez la section Affichage de l'activité réseau.
Signature	Il s'agit de l'anomalie de signature déclenchée par l'évènement réseau.
Transféré(e)(s)	
Téléchargé	Il s'agit du nombre total d'octets de données envoyés de la destination à l'agent CylanceGATEWAY.
Chargé	Il s'agit du nombre total d'octets de données qui ont été envoyés de la destination du serveur à l'agent CylanceGATEWAY.

Filtre	Description
TLS	
Version de TLS	Il s'agit de la version du protocole TLS qui a été utilisée pour se connecter à la destination.
ALPN client	Il s'agit des informations d'entête ALPN qui ont été envoyées à l'agent CylanceGATEWAY depuis la destination.
ALPN du serveur	Il s'agit des informations d'entête qui ont été envoyées de la destination à l'agent CylanceGATEWAY.
SNI	Il s'agit du nom d'hôte de la destination à laquelle l'agent CylanceGATEWAY a tenté de se connecter.
Émetteur	Il s'agit du certificat présenté par la destination.
Objet	Il s'agit du nom de la règle qui a été appliquée au moment de l'évaluation au cours des différentes phases (par exemple, recherche DNS, établissement de la connexion et liaison TLS) en relation avec les règles ACL.
Non valide avant	Il s'agit de la date avant laquelle le certificat n'est pas valide.
Non valide après	Il s'agit de la date après laquelle le certificat n'est pas valide.
Évènements HTTP	Ce paramètre indique les flux HTTP d'origine non chiffrés en texte brut à des fins d'analyse et de recherche des menaces. Notez que les flux HTTP ne sont pas déchiffrés. Un résumé des détails de la demande et de la réponse comprend les détails de la demande et de la réponse suivants : • Méthode HTTP et URL de la demande (URI) • Agent utilisateur • entêtes de type contenu • Codes d'état HTTP Les trois premiers évènements HTTP du nombre total d'évènements s'affichent. Un badge affiche le nombre total d'évènements qui ont été consignés pour l'évènement. Cliquez sur **Tous les évènements HTTP** pour afficher tous les évènements sur la page Aperçu des évènements. Cliquez sur chaque évènement pour afficher plus de détails, tels que des informations d'entête. Vous ne pouvez pas effectuer de recherche ou de filtrage dans les évènements HTTP pour le moment. Les détails HTTP présentent les limites suivantes : • Le nom de l'entête affiche jusqu'à 64 octets. • La valeur d'entête affiche jusqu'à 512 octets. • La taille totale de l'entête par direction (par exemple, nom et corps) affiche jusqu'à 4 096 octets. • Le corps de la demande et de la réponse affiche jusqu'à 512 octets. • La demande et la réponse utilisent le codage Base64 par défaut. Vous pouvez afficher le corps décodé.

Filtre	Description

DNS	Indique la requête DNS et tous les détails de réponse associés à l'évènement. Un résumé des détails de la demande et de la réponse comprend les détails de la demande et de la réponse suivants :
	• Détails de la demande
	  • Nom de la requête : il s'agit du nom de ressource demandée (RR) du serveur DNS que l'agent CylanceGATEWAY a interrogé.
	  • Type de requête : il s'agit du type de requête DNS (par exemple, un enregistrement A, AAAA ou SRV) qui a été envoyé au serveur DNS.
	• Détails de la réponse
	  • Nom de l'enregistrement de la ressource : nom du serveur DNS qui répond à la requête de l'agent CylanceGATEWAY.
	  • Type d'enregistrement de la ressource : il s'agit du type de la réponse DNS (par exemple, A) qui a été envoyé au serveur DNS.
	  • Données de la ressource : adresse du serveur DNS qui renvoie la réponse.
	  • TTL : durée en secondes pendant laquelle les données de la ressource demandées restent valides.
	Un badge affiche le nombre total de réponses pour la requête DNS.

Surveiller les fichiers sensibles avec CylanceAVERT

Vous pouvez surveiller l'activité et les évènements associés aux fichiers sensibles, à la fois au repos et en transit. Tous les fichiers sensibles de votre organisation s'affichent dans l'inventaire des fichiers. Les fichiers qui ont été impliqués dans un évènement d'exfiltration s'affichent dans la vue Évènements de CylanceAVERT et dans le casier de preuves.

Remarque : Si CylanceAVERT n'est pas activé pour votre locataire, les options de menu permettant de le configurer ne s'affichent pas dans la console de gestion.

Évènements CylanceAVERT

Les évènements d'exfiltration de données sont enregistrés et répertoriés sur la page des évènements CylanceAVERT. Les évènements CylanceAVERT sont stockés dans la liste des évènements pendant 30 jours. Lorsqu'un évènement d'exfiltration de données se produit, un nouvel élément de liste est ajouté à la liste des évènements et affiche les informations suivantes :

Élément	Description
Heure de détection	Il s'agit de la date et de l'heure auxquelles l'évènement d'exfiltration s'est produit.
Terminal	Il s'agit du nom du terminal sur lequel l'évènement d'exfiltration a été détecté.
Utilisateur	Il s'agit du prénom, du nom, de l'adresse e-mail, du service et du titre de l'utilisateur qui a validé l'évènement d'exfiltration. Vous pouvez cliquer sur le lien pour afficher la page des détails de l'utilisateur.
Activité	Il s'agit du type d'activité CylanceAVERT marqué comme évènement d'exfiltration de données. Les valeurs possibles sont Web, e-mail et USB.
Emplacement	Il s'agit de l'emplacement vers lequel les données sensibles ont été téléchargées. La valeur dépend du type de téléchargement effectué (domaine racine du site Web, domaines et destinataires de l'e-mail, emplacement des fichiers USB copiés).
Fichiers	Il s'agit du nombre de fichiers impliqués dans l'évènement. Vous pouvez cliquer sur le lien pour afficher la page des détails du fichier. Plusieurs fichiers peuvent être associés à un évènement d'exfiltration.
Stratégie	Il s'agit du nombre de stratégies utilisateur CylanceAVERT qui ont été enfreintes. Plusieurs stratégies peuvent être associées à un évènement d'exfiltration.
Type de données	Il s'agit du nombre de mots-clés ou d'expressions régulières qui ont été satisfaits pour déclencher l'évènement CylanceAVERT.

Afficher les détails de l'évènement CylanceAVERT

Lorsqu'un évènement d'exfiltration de données se produit, les détails de l'évènement sont répertoriés sur la page des évènements CylanceAVERT. Vous pouvez cliquer sur la ligne de chaque évènement pour afficher plus de détails sur l'évènement d'exfiltration, y compris le nombre de types de données sensibles impliqués dans l'évènement, un extrait de l'évènement et télécharger le fichier concerné. Les étapes suivantes décrivent comment

trouver la page des évènements et les actions que vous pouvez effectuer pour afficher plus de détails. Pour les fichiers chiffrés ou protégés par mot de passe, le texte « fichier chiffré » s'affiche à la place des types de données sensibles.

Avant de commencer :

Les paramètres de collecte de données suivants doivent être activés pour afficher les fragments de fichier et télécharger le fichier complet. Pour plus d'informations, consultez Configurer les paramètres de collecte de données.

- Générer des extraits de fichier
- Activer la collecte des fichiers de preuve

Les autorisations suivantes sont requises pour afficher les informations sur l'évènement :

- Afficher la liste des évènements généraux
- Afficher le nom des terminaux
- Afficher le nom des utilisateurs
- Afficher les noms des stratégies
- Lier aux détails de la stratégie
- Afficher les entités de données
- Afficher les détails du fichier
- Télécharger le fichier complet

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceAVERT > Évènements**.
2. Cliquez sur une ligne pour afficher plus de détails sur un évènement.
3. Dans le panneau **Détails de l'évènement**, effectuez l'une des opérations suivantes :
   - Sous **Détails de l'utilisateur**, cliquez sur le nom de l'utilisateur pour être redirigé vers la page d'informations de l'utilisateur où vous pouvez afficher les stratégies, les évènements ou les terminaux associés à l'utilisateur.
   - Sous **Violations de stratégie**, cliquez sur une stratégie pour afficher plus d'informations sur la stratégie qui a été enfreinte.
   - Sous **Détails du fichier**, cliquez sur l'icône d'informations pour afficher des détails sur le fichier, y compris le type de fichier, les types de données sensibles qui ont été analysés et le nombre d'occurrences de ces types de données. Vous pouvez cliquer sur pour afficher des informations sur l'évènement d'exfiltration. Vous pouvez également cliquer sur pour télécharger le fichier impliqué dans l'évènement d'exfiltration. Les fichiers de preuves sont téléchargés sous forme de fichier .gz compressé. Vous aurez besoin d'un outil utilitaire, tel que 7zip, pour décompresser les fichiers et les afficher.

Afficher l'inventaire des fichiers pour identifier les fichiers sensibles

Lorsque CylanceAVERT est installé sur votre terminal, le processus de recherche de point de terminaison commence automatiquement à découvrir tous les fichiers du terminal qui contiennent les types de données sensibles, comme spécifié dans les stratégies de protection des informations. Les fichiers marqués comme contenant des documents organisationnels sensibles sont ajoutés à l'inventaire des fichiers. L'inventaire des fichiers vous permet de voir le nombre et le type de documents sensibles dans votre environnement, ainsi que les utilisateurs et les terminaux qui ont accès aux données sensibles à des fins d'évaluation des risques. Vous pouvez également regrouper la liste Inventaire des fichiers par utilisateurs, terminaux et types de données.

Remarque : Le processus de suivi peut prendre plusieurs heures après l'installation de CylanceAVERT.

Avant de commencer :

Les autorisations suivantes sont requises pour afficher l'inventaire des fichiers :

- Lire le résumé du fichier
- Répertorier et lire les règles

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceAVERT > Inventaire des fichiers**.

   L'inventaire des fichiers de CylanceAVERT est une liste de tous les fichiers contenant des types de données sensibles, comme spécifié dans les règles de protection des informations, qui ont été découverts pendant le processus de collecte des fichiers. Les types de fichiers pris en charge sont .PDF, .ooxml (Microsoft Word, Excel et PowerPoint), .txt, .rtf, .zip et .csv. Le tableau suivant explique les informations affichées dans la liste d'inventaire des fichiers.

Élément	Description
Nom de fichier	Il s'agit du nom du fichier.
Taille du fichier	Il s'agit de la taille du fichier en Ko.
Types d'informations	Il s'agit du type d'information auquel le fichier appartient.
Types de données	Il s'agit du nombre de types de données sensibles trouvés dans le fichier.
Utilisateurs	Il s'agit du nombre d'utilisateurs ayant accès au fichier.
Terminaux	Il s'agit du nombre de terminaux ayant accès au fichier.
Stratégies	Il s'agit de la ou des stratégies dont ce fichier fait partie.
Type	Il s'agit du type de fichier. Les types de fichiers pris en charge sont .PDF, .ooxml (Microsoft Word, Excel et PowerPoint), .txt, .rtf, .zip et .csv.

   Remarque : Il n'y a pas de pagination pour cette liste, vous pouvez faire défiler pour charger plus de résultats ou utiliser les options de filtre.

   Une fois le processus de chalutage initial terminé, CylanceAVERT interroge régulièrement pour vérifier la présence de nouvelles données sensibles. Si un fichier est partiellement évalué et que des informations sensibles ont été détectées, une icône s'affiche en regard du fichier dans le tableau et les vues détaillées avec une alerte indiquant que le fichier n'a été que partiellement analysé.
2. Effectuez l'une des opérations suivantes :
   - Pour filtrer les colonnes Nom de fichier ou Types d'informations, cliquez sur ⩒ dans l'entête de colonne.
   - Pour modifier les colonnes à afficher, cliquez sur ||| à droite des entêtes de colonne.
   - Pour regrouper les données par utilisateurs, terminaux ou types de données, sélectionnez le regroupement dans le menu déroulant. Dans la vue Inventaire des fichiers du groupe, vous pouvez cliquer sur un élément pour afficher des informations détaillées sur ce groupe.

   Remarque : Vous pouvez afficher le nom et les attributs du fichier dans l'inventaire des fichiers, mais les extraits de fichier et l'accès complet aux fichiers ne sont pas pris en charge.
3. Vous pouvez cliquer sur un élément dans l'inventaire des fichiers pour afficher le menu des détails du fichier. Ce menu vous permet d'afficher les détails du fichier, les utilisateurs ayant accès au fichier, les terminaux ayant accès au fichier, les types de données trouvés dans le fichier et les stratégies que le fichier enfreint.

Afficher des fichiers partiellement analysés

CylanceAVERT fournit une visibilité sur les fichiers partiellement analysés. Si CylanceAVERT ne parvient pas à déterminer entièrement la sensibilité d'un fichier, ce dernier figure dans la liste Fichiers partiellement analysés. Il est possible qu'un fichier ne soit analysé que partiellement dans les cas suivants :

- Le fichier est tellement volumineux que le moteur d'évaluation n'a pas pu terminer son analyse avant son exfiltration.
- Le fichier est un fichier compressé (zip) doté de plusieurs niveaux de hiérarchie, dont seuls les niveaux initiaux ont été analysés.

En fonction des indices de sensibilité d'un fichier partiellement analysé, deux résultats sont possibles. Soit le fichier est partiellement évalué et des données sensibles sont trouvées, soit le fichier est partiellement évalué et aucune donnée sensible n'est détectée.

Si un fichier est partiellement évalué et qu'aucune information sensible n'est détectée, le fichier figure dans la liste Fichiers partiellement analysés avec une alerte indiquant qu'il n'a été que partiellement analysé.

Si un fichier est partiellement évalué et que des informations sensibles sont détectées, il est traité comme un fichier entièrement évalué et figure dans l'inventaire des fichiers, la vue Évènements et le casier de preuves. Une icône apparait néanmoins en regard du fichier dans les tableaux et les vues détaillées avec une alerte indiquant qu'il n'a été que partiellement analysé.

Vous pouvez afficher la liste des fichiers qui n'ont pas été entièrement évalués par CylanceAVERT dans la vue Fichiers partiellement analysés.

1. Dans la barre de menus de la console de gestion, cliquez sur **CylanceAVERT > Fichiers partiellement analysés**.

Colonne	Description
Nom de fichier	Il s'agit du nom du fichier partiellement analysé.
Date d'ajout	Il s'agit de l'heure à laquelle le fichier partiellement analysé a été ajouté à la liste.
Taille du fichier	Il s'agit de la taille du fichier partiellement analysé.
Extension	Il s'agit du type d'extension du fichier partiellement analysé.

   Remarque : Il n'existe aucune pagination pour cette liste. Vous pouvez parcourir la liste pour charger des résultats supplémentaires ou utiliser les options de filtre.
2. Effectuez l'une des opérations suivantes :
   - Pour filtrer les colonnes Nom de fichier ou Extension, cliquez sur ⏷ dans l'entête de colonne.
   - Pour modifier les colonnes à afficher, cliquez sur ||| à droite des entêtes de colonne.
3. Vous pouvez cliquer sur un élément dans la liste Fichiers partiellement analysés pour afficher le menu des détails du fichier. Ce menu vous permet d'afficher les détails du fichier, les utilisateurs ayant accès au fichier, les terminaux ayant accès au fichier ainsi que les types de données trouvés dans le fichier.

Utiliser le casier de preuves pour afficher les détails d'évènement d'exfiltration

Lorsqu'un fichier de votre inventaire de fichiers est impliqué dans un évènement d'exfiltration de données, il est stocké et chiffré dans l'instance AWS gérée par BlackBerry à l'aide des clés différentes pour chaque locataire, et est ajouté au casier de preuves. Vous pouvez afficher ou télécharger les fichiers impliqués dans les évènements d'exfiltration à partir du casier de preuves.

Avant de commencer :

La collecte des fichiers de preuve doit être activée dans les paramètres de protection des informations. Pour plus d'informations, consultez Configurer les paramètres de collecte de données.

1. Dans la barre de menus de la console de gestion, cliquez sur **Avert > Casier de preuves**.

   Le casier de preuves affiche une liste de tous les fichiers de votre organisation qui ont été impliqués dans un évènement d'exfiltration de données. Le tableau suivant explique les informations figurant dans la liste du casier de preuves :

Élément	Description
Date d'ajout	Il s'agit de l'heure à laquelle le fichier a été ajouté au casier de preuves.
Nom de fichier	Il s'agit du nom du fichier impliqué dans un évènement d'exfiltration.
Taille du fichier	Il s'agit de la taille du fichier impliqué dans un évènement d'exfiltration.
Évènements associés	Il s'agit des évènements d'exfiltration auxquels le fichier est associé. Vous pouvez cliquer sur le numéro pour en savoir plus.
Télécharger	Vous pouvez cliquer sur ce bouton pour télécharger le fichier complet impliqué dans l'évènement d'exfiltration. Les fichiers de preuves sont téléchargés sous forme de fichier .gz compressé. Vous aurez besoin d'un outil utilitaire, tel que 7zip, pour décompresser les fichiers et les afficher.

2. Cliquez sur le numéro dans la colonne évènements associés pour afficher les évènements CylanceAVERT.
3. Pour filtrer les colonnes Date d'ajout, Nom de fichier ou Taille du fichier, cliquez sur ⏷ dans l'entête de colonne.

Afficher les vulnérabilités du SE mobile

Vous pouvez utiliser la console de gestion pour afficher une liste collective des CVE (vulnérabilités et expositions courantes), telles qu'identifiées, définies et suivies par la National Vulnerability Database (base de données nationale sur les vulnérabilités), pour tout système d'exploitation mobile de l'environnement de votre organisation où l'application CylancePROTECT Mobile est installée. Pour chaque version du système d'exploitation, vous pouvez afficher le nombre de terminaux qui utilisent cette version, le nombre total de CVE pour cette version du système d'exploitation, la classification des risques et une brève description de chaque CVE, ainsi qu'un lien pour afficher tous les détails dans la base de données nationale des vulnérabilités.

1. Sur la barre de menus de la console de gestion, cliquez sur **Protection > Vulnérabilités**.
2. Cliquez sur l'onglet **OS mobile**. Effectuez l'une des opérations suivantes :
   - Pour trier les vulnérabilités dans l'ordre croissant ou décroissant par colonne, cliquez sur le nom de la colonne.
   - Pour filtrer les vulnérabilités, cliquez sur sur une colonne, et saisissez ou sélectionnez les critères de filtre.
3. Pour afficher la liste des vulnérabilités pour une version du système d'exploitation, cliquez sur le lien dans la colonne **Nombre total de CVE**. Cliquez sur un lien de CVE pour afficher les détails dans la base de données nationale des vulnérabilités.

Audit des actions de l'administrateur

Vous pouvez utiliser le journal d'audit pour afficher et exporter des informations sur les actions effectuées par les administrateurs de votre organisation.

Afficher le journal d'audit

1. Dans la console de gestion , cliquez sur > **Journal d'audit**.
2. Dans les champs de filtre, spécifiez les critères que vous souhaitez utiliser pour filtrer les informations du journal d'audit.
3. Pour exporter les résultats dans un fichier .csv, cliquez sur  . Sélectionnez la portée de l'exportation et cliquez sur **Exporter**.

   Vous pouvez exporter 50 000 enregistrements maximum à la fois. Le nombre de résultats s'affiche en bas de l'écran. Pour exporter plus de 50 000 enregistrements, vous pouvez filtrer les résultats (par date, par exemple) et les exporter, puis appliquer un filtre et une exportation différents, etc.

Informations du journal d'audit : administration générale

Le tableau suivant répertorie les informations qui sont ajoutées au journal d'audit pour les actions administratives qui affectent plusieurs fonctionnalités Cylance Endpoint Security. Vous pouvez utiliser les options de filtrage dans la console pour filtrer les résultats du journal d'audit.

Catégorie	Action	Détails
Mise à jour de l'agent	Modifier	Règle : *<nom de règle>* ; zones : *<zones>* ; version de l'agent : *<version>* ; version Optics : *<version>*
Mise à jour de l'agent	Modifier	Niveau : *<nom de niveau>* ; zones : N/A ; version de l'agent : *<version>* ; version Optics : *<version>*
Règle de mise à jour personnalisée	Ajouter	Règle de mise à jour personnalisée : *<nom de la règle>* ; zones : *<zones>* ; version de l'agent : *<version>* ; version Optics : *<version>*
Règle de mise à jour personnalisée	Supprimer	La règle de mise à jour personnalisée *<ID règle>* est supprimée.
Terminal	Ajouter	Terminal : *<nom du terminal>* ; zone : *<nom de la zone>*
Terminal	Modifier	Renommé : *<nom d'origine>* en *<nouveau nom>* ; Stratégie modifiée : *<ancienne stratégie>* en *<nouvelle stratégie>* ; Zones supprimées : *<noms de zone>* ; Zones ajoutées : *<noms de zone>* ; niveau de journalisation de l'agent modifié : *<valeur d'origine>* en *<nouvelle valeur>* ; niveau d'autoprotection de l'agent modifié : *<valeur d'origine>* en *<nouvelle valeur>*
Terminal	Supprimer	Terminaux : *<noms des terminaux>*

Catégorie	Action	Détails
Connexion	Réussite	Fournisseur : CylancePROTECT, IP source : *<adresse IP>*
Connexion	Échec	—
Stratégie	Ajouter	Stratégie : *<nom de la stratégie>*, Paramètres de détection modifiés de *<détails de la modification>*
Stratégie	Modifier	Stratégie : *<nom de la stratégie>* : *<détails de la modification>*
Stratégie	Supprimer	Stratégie : *<nom de la stratégie>*
Syslog	Désactivé	Syslog désactivé.
Syslog	Enregistrement des paramètres	{*<configuration_settings>*}
Configuration de locataire	Mettre à jour	Nom de domaine personnalisé mis à jour vers *<nom>*.
Rôle de locataire	Ajouter	Rôle : *<nom du rôle personnalisé>*
Rôle de locataire	Modifier	Rôle : *<nom du rôle personnalisé>*
Rôle de locataire	Supprimer	Rôle : *<nom du rôle personnalisé>*
Utilisateur	Ajouter	Utilisateur : *<nom d'utilisateur>* ; Rôle : *<type de rôle>*
Utilisateur	Modifier	Utilisateur : *<nom d'utilisateur>* ; e-mail : *<e-mail de l'utilisateur>*
Utilisateur	Supprimer	Utilisateurs : *<noms des utilisateurs>*
Zone	Ajouter	Zone : *<nom de la zone>* ; Stratégie : *<nom de la stratégie>* ; Valeur : *<« élevée » / « faible » / « normal »>*
Zone	Modifier	Renommé : *<nom d'origine>* en *<nouveau nom>* ; Stratégie actuelle : *<nom de la stratégie>* ; Stratégie appliquée à tous les terminaux de la zone : *<VRAI / FAUX>* ; Valeurs affectées : *<« élevé » / « faible » / « normal »>*
Zone	Supprimer	Zones : *<noms de zones>*

Informations du journal d'audit : CylancePROTECT Desktop

Le tableau suivant répertorie les informations qui sont ajoutées au journal d'audit pour les actions administratives CylancePROTECT Desktop. Vous pouvez utiliser les options de filtrage dans la console pour filtrer les résultats du journal d'audit.

Catégorie	Action	Détails
Paramètre de l'application	Désactivation de l'authentification personnalisée	Authentification personnalisée désactivée.
Paramètre de l'application	Enregistrement de l'authentification personnalisée	Authentification personnalisée enregistrée : {*<configuration_settings>*}
Paramètre de l'application	Enregistrer le mot de passe requis pour désinstaller l'agent	Mot de passe de désinstallation de l'agent enregistré.
Paramètre de l'application	Désactiver le mot de passe requis pour désinstaller l'agent	Mot de passe requis pour désinstaller l'agent désactivé.
Paramètre de l'application	Supprimer le jeton d'installation	Le jeton d'installation a été supprimé.
Paramètre de l'application	Régénérer le jeton d'installation	Le jeton d'installation a été généré.
Liste globale	Ajouter	Source : CylancePROTECT ; SHA256 : *<file hash>* ; Nom de fichier : *<name>* ; Motif : *<value>* ; Ajouté à : Quarantaine globale *ou* Liste sécurisée ; Catégorie : *<value>*
Liste globale	Supprimer	SHA256 : *<file hash>*
Liste globale de scripts	Ajouter	Source : CylancePROTECT ; SHA256 : *<file hash>* ; Nom de fichier : *<name>* ; Motif : *<value>* ; Ajouté à : Liste d'exclusions de contrôle de script
Liste globale de scripts	Supprimer	SHA256 : *<file hash>*
Menace	Liste sécurisée	SHA256 : *<file hash>* ; Catégorie : *<value>* ; Motif : *<value>*
Menace	Quarantaine globale	Source : CylancePROTECT; SHA256 : *<file hash>* ; Motif : *<value>*
Rapport de données sur les menaces	Générer un jeton	—
Rapport de données sur les menaces	Supprimer le jeton	—

Informations du journal d'audit : CylancePROTECT Mobile

Le tableau suivant répertorie les informations qui sont ajoutées au journal d'audit pour les actions administratives CylancePROTECT Mobile. Vous pouvez utiliser les options de filtrage dans la console pour filtrer les résultats du journal d'audit.

Catégorie	Action	Détails
Utilisateur final	Ajouter	Utilisateur : <*e-mail*>, Type : local
Utilisateur final	Importer	Nombre de réussites : <*nombre*>, nombre d'échecs : <*nombre*>
Utilisateur final	Supprimer	Utilisateur : <*e-mail*> Une entrée de journal est générée pour chaque utilisateur qui a été supprimé.
Utilisateur final	Attribuer la stratégie	Stratégie : <*nom de la stratégie*>, Utilisateurs : <*adresses e-mail*>
Utilisateur final	Envoyer une invitation	Utilisateurs : <*adresses e-mail*>, Nombre de réussites : <*nombre*>, Nombre d'échecs : <*nombre*>
Terminaux mobiles	Supprimer	Utilisateur : <*e-mail*>, Terminal : <*nom du terminal*>, Système d'exploitation : <*famille de système d'exploitation*>, Version du système d'exploitation : <*version*> Une entrée de journal est générée pour chaque terminal qui a été supprimé.
Terminaux mobiles	Exporter	Filtre : <*champs et valeurs de filtre*> Si « Tout » a été sélectionné, la valeur de filtre est Aucun. Si « Filtre actuel » a été sélectionné, le nom et la valeur de chaque champ sont répertoriés.
Stratégie mobile	Ajouter	Source : Protect Mobile, Stratégie : <*nom de la stratégie*>, <*valeurs et noms des paramètres*>
Stratégie mobile	Modifier	Source : Protect Mobile, Stratégie : <*nom de la stratégie*>, <*valeurs et noms des paramètres modifiés*>
Stratégie mobile	Supprimer	Source : Protect Mobile, Stratégie : <*nom de la stratégie*> Une entrée de journal est générée pour chaque règle qui a été supprimée.
Exclusions Mobile	Ajouter	Source : Protect Mobile, Type : <*App / Développeur / domaine / IP*>, Catégorie : <*Approuvé / Restreint*>, Nom : <*nom*>, Plateforme : <*plateforme*>, Identifiant : <*identifiant*>, Émetteur : <*émetteur*>

Catégorie	Action	Détails
Exclusions Mobile	Supprimer	Source : Protect Mobile, Type : *<App / Développeur / domaine / IP>*, Nom : *<nom>* Une entrée de journal est générée pour chaque exclusion qui a été supprimée.
Alertes mobiles	Ignorer	Source : Protect Mobile, ID : *<ID>*, Type : *<type_alerte>*, Nom : *<nom_alerte>*, Description : *<OS_terminal>* Une entrée de journal est générée pour chaque alerte qui a été ignorée.
Alertes mobiles	Exporter	Source : Protect Mobile, Filtre : *<champs et valeurs de filtre>* Si « Tout » a été sélectionné, la valeur de filtre est Aucun. Si « Filtre actuel » a été sélectionné, le nom et la valeur de chaque champ sont répertoriés.

Informations du journal d'audit : CylanceOPTICS

Le tableau suivant répertorie les informations qui sont ajoutées au journal d'audit pour les actions administratives CylanceOPTICS. Vous pouvez utiliser les options de filtrage disponibles dans la console pour filtrer les résultats du journal d'audit.

Catégorie	Action	Détails
Requête avancée	Exécuter	Requête : *<EQL_query>*
Export de requête avancée	Ajouter	Nom : *<name>* ; Description : *<description>* ; Partagé : *<isShared>*
Export de requête avancée	Télécharger	Nom : *<name>* ; Description : *<description>*
Export de requête avancée	Supprimer	Nom : *<name>* ; Description : *<description>* ; Partagé : *<isShared>*
Instantané de requête avancée	Ajouter	Nom : *<name>* ; Description : *<description>* ; Partagé : *<isShared>*
Instantané de requête avancée	Modifier	Nom : *<name>* ; Description : *<description>* ; Partagé : *<isShared>*
Instantané de requête avancée	Supprimer	Nom : *<name>* ; Description : *<description>* ; Partagé : *<isShared>*
Modèle de requête avancée	Ajouter	Nom : *<name>* ; Description : *<description>* ; Partagé : *<isShared>* ; Requête : *<EQL_query>*

Catégorie	Action	Détails
Modèle de requête avancée	Modifier	Nom : <*name*> ; Description : <*description*> ; Partagé : <*isShared*> ; Requête : <*EQL_query*>
Modèle de requête avancée	Supprimer	Nom : <*name*> ; Description : <*description*> ; Partagé : <*isShared*>
Détections	Modifier l'état	Détection : <*detection label*> ; ID de détection : <*detection id*> ; Terminal : <*device name*> ; État précédent : <*previous detection status*> ; Nouvel état : <*new detection status*>
Détections	Supprimer	Détection : <*detection label*> ; ID de détection : <*detection id*> ; Terminal : <*device name*>
Exception de détection	Ajouter	Nom : <*name*>
Exception de détection	Modifier	Nom : <*name*>
Exception de détection	Supprimer	Nom : <*name*>
Règle de détection	Ajouter	Nom : <*name*> ; Description : <*description*> ; Sévérité : <*severity*> ; SE : <*OS list*>
Règle de détection	Modifier	Nom : <*name*> ; Description : <*description*> ; Sévérité : <*severity*> ; SE : <*OS list*>
Règle de détection	Supprimer	Nom : <*name*> ; Description : <*description*> ; Sévérité : <*severity*> ; SE : <*OS list*>
Jeu de règles de détection	Ajouter	Nom : <*name*> ; Description : <*description*> ; Stratégie de terminal : <*device policy name*>
Jeu de règles de détection	Modifier	Nom : <*name*> ; Description : <*description*> ; Stratégie de terminal : <*device policy name*>
Jeu de règles de détection	Supprimer	Nom : <*name*> ; Description : <*description*> ; Stratégie de terminal : <*device policy name*>
Terminal	Télécharger le fichier	Terminal : <*device name*> ; Fichier : <*file path and name*>
Terminal	Verrouiller	Terminal : <*device name*> ; Profil de configuration : <*profile name*> ; Période de verrouillage : <*lockdown period*>
Terminal	Déverrouiller	Terminal : <*device name*>

Catégorie	Action	Détails
Terminal	Modifier le verrouillage du profil	Terminal : <*device name*> ; Profil de configuration : <*profile name*>
Terminal	Afficher la clé de déverrouillage	Terminal : <*device name*>
Données détaillés	Ajouter	Terminal : <*device name*> ; Type : <*focus view type*> ; Artéfact : <*focus view artifact*>
Requête InstaQuery	Ajouter	Nom : <*IQ name*>, Artéfact : <*IQ artifact*>, Facet : <*IQ facet*>, Terme : <*IQ term*>
Requête InstaQuery	Supprimer	Nom : <*IQ name*>, Artéfact : <*IQ artifact*>, Facet : <*IQ facet*>, Terme : <*IQ term*>
Réseau de la tâche	Arrêter	Nom : <*name*> ; Service : <*parent service type*>
Configuration du verrouillage	Ajouter	Profil de configuration : <*configuration profile*> ; Description : <*description*> ; Définitions de la liste blanche : <*allowed_connections*>
Configuration du verrouillage	Supprimer	Profil de configuration <*configuration profile*>
Configuration du verrouillage	Modifier	Profil de configuration : <*configuration profile*> ; Description : <*description*> ; Définitions de la liste blanche : <*allowed_connections*>
Déploiement du package	Ajouter	Nom : <*name*> ; Packages : <*packages*>
Déploiement du package	Supprimer	Nom : <*name*>
Playbook de package	Ajouter	Nom : <*name*> ; Packages : <*packages*>
Playbook de package	Modifier	Nom : <*name*> ; Packages : <*packages*>
Playbook de package	Supprimer	Nom : <*name*> ; Packages : <*packages*>
Résultat du playbook	Supprimer	Terminal : <*device name*> ; Nom du playbook : <*playbook name*> ; ID de détection : <*detection id*> ; État : <*status*>
Réponse distante	Se connecter	Terminal : <*device name*>
Réponse distante	Se déconnecter	Terminal : <*device name*>

Catégorie	Action	Détails
Requête avancée programmée	Ajouter	Nom : <*name*> ; Description : <*description*> ; Partagé : <*isShared*> ; Planning : <*schedule_details*>
Requête avancée programmée	Modifier	Nom : <*name*> ; Description : <*description*> ; Partagé : <*isShared*> ; Planning : <*schedule_details*>
Requête avancée programmée	Supprimer	Nom : <*name*> ; Description : <*description*> ; Partagé : <*isShared*>
Requête avancée programmée	Supprimer le résultat	Nom : <*name*> ; Description : <*description*> ; Horodatage du résultat : <*result_timestamp*> ; Résultats : <*result_count*>
Requête avancée programmée	Démarrer	Nom : <*name*> ; Description : <*description*> ; Partagé : <*isShared*> ; Planning : <*schedule_details*>
Requête avancée programmée	Arrêter	Nom : <*name*> ; Description : <*description*> ; Partagé : <*isShared*> ; Planning : <*schedule_details*>

Informations du journal d'audit : CylanceAVERT

Le tableau suivant répertorie les informations qui sont ajoutées au journal d'audit pour les actions administratives CylanceAVERT. Vous pouvez utiliser les options de filtrage dans la console pour filtrer les résultats du journal d'audit.

Catégorie	Action	Détails

Entité de données	Ajouter	{
		"id": "<*Identifiant*>",
		"tenantId": "<*Identifiant du locataire*>",
		"occurred": "<*Date/Heure*>",
		"traceId": "<*Identifiant de la trace*>",
		"spanId": "<*Identifiant de la couverture*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "Entité",
		"subcategory": "créé",
		"message": "L'administrateur a créé une entité de données nommée <*Nom de la stratégie*>"
		},
		"admin": {
		"ecoId": "<*Identifiant Eco*>"
		},
		"entity": {
		"id": "<*Identifiant*>",
		"type": "ENTITÉ DE DONNÉES",
		"displayName": "<*Nom affiché de l'entité*>"
		},
		"changes": {
		"regions": {
		"new": "<*Région*>"
		},
		"name":{
		"new": "<*Nom de l'entité de données*>"
		"description": {
		"new": "<*Description*>"
		},
		"infoTypes": {
		"new": "<*Types d'informations*>"
		},
		"Type": {
		"new": "<*Type de données*>"
		},
		"Parameters": {
		"new": "<*Paramètres*>"
		},
		"algorithm":{
		"new":<*Algorithme*>
		}
		}

Catégorie	Action	Détails

Entité de données	Modifier	{
		"id": "<*Identifiant*>",
		"tenantId": "<*Identifiant du locataire*>",
		"occurred": "<*Date/Heure*>",
		"traceId": "<*Identifiant de la trace*>",
		"spanId": "<*Identifiant de la couverture*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITÉ",
		"subcategory": "MIS À JOUR",
		"message": "L'administrateur a mis à jour une entité de données nommée <*Nom de l'entité de données*>",
		"crud": {
		"admin": {
		"ecoId": "<*Identifiant Eco*>"
		},
		"entity": {
		"id": "<*ID*>",
		"type": "ENTITÉ DE DONNÉES",
		"displayName": "<*Nom affiche de l'entité de données*>"
		},
		"changes": {
		"description": {
		"new": "<*Nouvelle description*>",
		"old": "<*Ancienne description*>"
		}
		}
		}
		}

Catégorie	Action	Détails

Entité de données	Supprimer	{
		"id": "<*Identifiant*>",
		"tenantId": "<*Identifiant du locataire*>",
		"occurred": "<*Date/Heure*>",
		"traceId": "<*Identifiant de la trace*>",
		"spanId": "<*Identifiant de la couverture*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITÉ",
		"subcategory": "SUPPRIMÉ",
		"message": "L'administrateur a supprimé une entité de données nommée <*Nom de l'entité de données*>",
		"crud": {
		"admin": {
		"ecoId": "<*Identifiant Eco*>"
		},
		"entity": {
		"id": "<*Identifiant*>",
		"type": "ENTITÉ DE DONNÉES",
		"displayName": "<*Nom affiche de l'entité de données*>"
		}
		}
		}

Fichier de preuve	Télécharger	{
		"id": "<*Identifiant*>",
		"tenantId": "<*Identifiant du locataire*>",
		"occurred": "<*Date/Heure*>",
		"traceId": "<*Identifiant de la trace*>",
		"spanId": "<*Identifiant de la couverture*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITÉ",
		"subcategory": "LECTURE",
		"message": "Le fichier de preuve a été téléchargé",
		"crud": {
		"admin": {
		"ecoId": "<*Identifiant Eco*>"
		},
		"entity": {
		"id": "<*Identifiant*>",
		"type": "<*Type d'entité*>"
		}
		}
		}

Catégorie	Action	Détails

Fichier de preuve	Supprimer	<pre>{
		    "id": "<*Identifiant*>",
		    "tenantId": "<*Identifiant du locataire*>",
		    "occurred": "<*Date/Heure*>",
		    "traceId": "<*Identifiant de la trace*>",
		    "spanId": "<*Identifiant de la couverture*>",
		    "source": "com.blackberry.dlp",
		    "type": "AUDIT",
		    "category": "ENTITÉ",
		    "subcategory": "SUPPRIMÉ",
		    "message": "Le fichier de preuve a été
		SUPPRIMÉ",
		    "crud": {
		        "admin": {
		            "ecoId": "<*Identifiant Eco*>"
		        },
		        "entity": {
		            "id": "<*Identifiant*>",
		            "type": "<*Type d'entité*>"
		        }
		    }
		}</pre>

Catégorie	Action	Détails

Stratégie	Ajouter	{
		"common": {
		"id": "<*Identifiant*>",
		"tenantId": "<*Identifiant du locataire*>",
		"occurred": "<*Date/Heure*>",
		"traceId": "<*Identifiant de la trace*>",
		"spanId": "<*Identifiant de la couverture*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "Entité",
		"subcategory": "créé",
		"message": "L'administrateur a créé une Stratégie nommée <*Nom de la stratégie*>"
		},
		"admin": {
		"ecoId": "<*Identifiant Eco*>"
		},
		"entity": {
		"id": "<*Identifiant*>",
		"type": "PROFIL",
		"displayName": "<*Nom affiché de l'entité*>"
		},
		"changes": {
		"emailDomainsRule": {
		"new": "<*Règle du domaine*>"
		},
		"condition": {
		"new": "<*Condition*>"
		},
		"policyName": {
		"new": "<*Nom de la stratégie*>"
		},
		"policyType": {
		"new": "<*Type de stratégie*>"
		},
		"description": {
		"new": "<*Description*>"
		},
		"policyRules": {
		"new": "<*Règles de la stratégie*>"
		},
		"classification": {
		"new": "<*Classification*>"
		},
		"browserDomains": {
		"new": "<*Domaines du navigateur*>"
		}
		}
		}

Catégorie	Action	Détails
Stratégie	Modifier	

```
{
    "common": {
        "id": "<Identifiant>",
        "tenantId": "<Identifiant du locataire>",
        "occurred": "<Date/Heure>",
        "traceId": "<Identifiant de la trace>",
        "spanId": "<Identifiant de la couverture>",
        "source": "com.blackberry.dlp",
        "type": "AUDIT",
        "category": "Entité",
        "subcategory": "Mis à jour",
        "message": "L'administrateur a créé une
 Stratégie nommée <Nom de la stratégie>"
    },
    "admin": {
        "ecoId": " "
    },
    "entity": {
        "id": "fbfa8366-
e58c-4018-925f-2a536dce4c2d",
        "type": "PROFIL",
        "displayName": "nom-stratégie-créée-par-
auto-test"
    },
    "changes":
{
    "policyName":{
              "old": "HIPAA",
              "new": "Conformité HIPAA"
        },

    "condition": {
          "old": "<Ancienne condition>",
          "new": "<Nouvelle condition>"
      },

    "policyRules": {
            "old": [{<Anciennes règles de la
 stratégie>}],
            "new": [{<Nouvelles règles de la
 stratégie>}]
      },

    "policyConfigs": {
            "old": [{<Anciennes règles de la
 stratégie>}],
            "new": [{<Nouvelles règles de la
 stratégie>}]
      },

    "browserDomains":{
            "old":<Anciens domaines du navigateur>,
            "new":<Nouveaux domaines du navigateur>
      },

    "emailDomainsRule": {
            "old":<Ancienne règle du domaine>,
            "new":<Nouvelle règle du domaine>
      }
    }
}
```

Catégorie	Action	Détails
Stratégie	Supprimer	{ "id": "<*Identifiant*>", "tenantId": "<*Identifiant du locataire*>", "occurred": "<*Date/Heure*>", "traceId": "<*Identifiant de la trace*>", "spanId": "<*Identifiant de la couverture*>", "source": "com.blackberry.dlp", "type": "AUDIT", "category": "ENTITÉ", "subcategory": "SUPPRIMÉ", "Message": "L'administrateur a SUPPRIMÉ la stratégie nommée <*Nom de la stratégie*>", "crud": { "admin": { "ecoId": "<*Identifiant Eco*>" }, "entity": { "id": "<*Identifiant*>", "type": "PROFIL", "displayName": "<*Nom affiché de l'entité*>" } }}
Paramètre	Mettre à jour	{ "id": "<*Identifiant*>", "tenantId": "<*Identifiant du locataire*>", "occurred": "<*Date/Heure*>", "traceId": "<*Identifiant de la trace*>", "spanId": "<*Identifiant de la couverture*>", "source": "com.blackberry.dlp", "type": "AUDIT", "category": "PARAMÈTRE", "subcategory": "MIS À JOUR", "message": "L'administrateur a MIS À JOUR les paramètres DLP", "crud": { "admin": { "ecoId": "<*Identifiant Eco*>" }, "changes": { "ui.tenant.setting.emailRecipients": { "new": "<*Nouveaux destinataires de l'e-mail*>", "old": "<*Anciens destinataires de l'e-mail*>" } } } }

Catégorie	Action	Détails

Modèle	Supprimer	{
		"id": "<*Identifiant*>",
		"tenantId": "<*Identifiant du locataire*>",
		"occurred": "<*Date/Heure*>",
		"traceId": "<*Identifiant de la trace*>",
		"spanId": "<*Identifiant de la couverture*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITÉ",
		"subcategory": "SUPPRIMÉ",
		"message": "Le modèle <*Nom du modèle*> a été supprimé",
		"crud": {
		"admin": {
		"ecoId": "<*Identifiant Eco*>"
		},
		"entity": {
		"id": "<*Identifiant*>",
		"type": "MODÈLE",
		"displayName": "<*Nom du modèle*>"
		}
		}
		}

Catégorie	Action	Détails

Modèle	Ajouter	{
		"id": "<*Identifiant*>",
		"tenantId": "<*Identifiant du locataire*>",
		"occurred": "<*Date/Heure*>",
		"traceId": "<*Identifiant de la trace*>",
		"spanId": "<*Identifiant de la couverture*>",
		"source": "com.blackberry.dlp",
		"type": "AUDIT",
		"category": "ENTITÉ",
		"subcategory": "CRÉÉ",
		"message": "Le modèle <*Nom du modèle*> a été créé",
		"crud": {
		"admin": {
		"ecoId": "<*Identifiant Eco*>"
		},
		"entity": {
		"id": "<*Identifiant*>",
		"type": "MODÈLE",
		"displayName": "<*Nom du modèle*>"
		},
		"changes": {
		"condition": {
		"new": "<*Condition*>"
		},
		"regions": {
		"new": "<*Région*>"
		},
		"name":{
		"new": "<*Nom du modèle*>"
		},
		"description": {
		"new": "<*Description*>"
		},
		"infoTypes": {
		"new": "*Types d'informations*>"
		},
		"type": {
		"new": "<*Type de modèle*>"
		}
		}
		}
		}

Gestion des journaux

Cette section fournit des informations sur la modification des paramètres de journal pour les différents fonctions et services Cylance Endpoint Security.

Configurer la journalisation BlackBerry Connectivity Node

Le système BlackBerry Connectivity Node vous permet d'effectuer une synchronisation avec un annuaire Microsoft Active Directory local ou LDAP pour ajouter des utilisateurs et des groupes d'utilisateurs activés pour l'application CylancePROTECT Mobile et pour CylanceGATEWAY.

Vous pouvez définir le niveau de journalisation, les informations syslog et les informations de fichier local pour les évènements BlackBerry Connectivity Node.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions à l'annuaire**.
2. Dans l'onglet **Nœud de connectivité**, cliquez sur **Paramètres**.
3. Dans le menu déroulant **Niveaux de débogage du serveur**, sélectionnez le niveau d'événement que vous souhaitez consigner.
4. Pour envoyer les journaux à SysLog, cliquez sur le bouton près de **SysLog** et renseignez les champs **Hôte** et **Port**.
5. Pour envoyer les journaux à l'ordinateur sur lequel BlackBerry Connectivity Node est installé, cliquez sur le bouton près d'**Activer la destination du fichier local**.
6. Renseignez les champs **taille maximale du fichier journal** en Mo et **Ancienneté maximale des fichiers journaux** (en jours).
7. Pour compresser le dossier des journaux, cliquez sur le bouton près d'**Activer la compression du dossier de consignation**.
8. Cliquez sur **Enregistrer**.

Gérer les journaux de l'agent CylancePROTECT Desktop

Les fichiers journaux de l'agent CylancePROTECT Desktop fournissent des informations utiles pour résoudre les problèmes. Lors du dépannage, activez la journalisation détaillée et reproduisez le problème pour capturer les informations pertinentes indiquées dans le fichier journal. La journalisation détaillée crée un fichier journal plus volumineux. Elle doit donc être utilisée à des fins de dépannage uniquement. Les fichiers journaux de l'agent sont conservés pendant 30 jours dans la console de gestion.

1. Dans la barre de menus de la console de gestion , cliquez sur **Actifs > Terminaux**.
2. Cliquez sur un terminal.
3. Effectuez l'une des opérations suivantes :
   - Si vous souhaitez modifier le niveau de journalisation, dans la liste déroulante **Niveau de journalisation de l'agent**, cliquez sur le niveau de journalisation.

     Si vous modifiez le niveau de journalisation sur Détaillé, reportez-vous à la page Activer la journalisation détaillée sur un terminal CylancePROTECT Desktop.
   - Pour obtenir le fichier journal de l'agent CylancePROTECT Desktop, sous **Menaces et activités** dans l'onglet **Journaux de l'agent**, cliquez sur **Charger le fichier journal actuel**. Cette option est uniquement disponible si votre terminal est géré en ligne.

Activer la journalisation détaillée sur un terminal CylancePROTECT Desktop

Avant de commencer : Dans la console de gestion, définissez le niveau de journalisation de l'agent CylancePROTECT Desktop sur Détaillé.

Suivez les étapes pour le système d'exploitation du terminal :

OS	Étapes

Windows	**a.** Cliquez avec le bouton droit de la souris sur l'icône de l'agent dans la barre d'état système, puis cliquez sur **Quitter**.
	b. Ouvrez la ligne de commande en tant qu'administrateur.
	c. Exécutez la commande suivante :
	`cd C:\Program Files\Cylance\Desktop`
	d. Exécutez la commande suivante :
	`CylanceUI.exe -a`
	e. Cliquez avec le bouton droit de la souris sur l'icône de l'agent dans la barre d'état système, puis cliquez sur **Journalisation > Tout**.

macOS	**a.** Quittez l'interface utilisateur en cours d'exécution. **b.** Exécutez la commande suivante à partir du terminal : `sudo /Applications/Cylance/CylancePROTECTUI.app/Contents/MacOS/CylancePROTECTUI.-a` **c.** Cliquez avec le bouton droit de la souris sur l'icône de l'agent dans la barre d'état système, puis sélectionnez **Journalisation > Tout**.

Journalisation Linux

Consultez les sections suivantes pour en savoir plus sur la définition du niveau de journalisation et la collecte des fichiers journaux de l'agent.

Définir le niveau de journalisation

Le niveau de journalisation défini détermine le niveau de détail dans les journaux de l'agent. Notez que plus le niveau de journalisation est élevé, plus la taille du fichier journal augmente.

Avant de commencer : Vous pouvez utiliser la commande suivante pour afficher le niveau de journalisation actuel défini pour l'agent Linux :

```
/opt/cylance/desktop/cylance -l
```

Pour définir le niveau de journalisation, utilisez la commande suivante :

```
/opt/cylance/desktop/cylance -L <level>
```

Remplacez la valeur de *<level>* par l'un des éléments suivants :

- `0` : Erreur
- `1` : Avertissement
- `2` : Information

- 3 : Détaillé

Par exemple, la commande suivante définit le niveau de journalisation sur Détaillé.

```
/opt/cylance/desktop/cylance -L 3
```

Collecter les fichiers journaux de l'agent à partir des terminaux Linux

Utilisez les commandes suivantes pour collecter les fichiers journaux de l'agent à partir d'un terminal Linux. Les fichiers journaux sont stockés sur le terminal pendant 30 jours. Vous devez disposer des autorisations root pour collecter les fichiers journaux.

Red Hat et CentOS :

```
ps aux > ~/ps.txtph product="Cylance">sudo pmap -x $(ps -e | grep cylancesvc | cut
 -d ‘ ‘ -f 1) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339=’date’).tgz /var/log/messages* /opt/
cylance/desktop/log ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt ~/ps.txt ~/
mem.txt ~/slabinfo.txt
```

Ubuntu:

```
ps aux > ~/ps.txt
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ‘ ‘ -f 2) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339=’date’).tgz /var/log/syslog* /opt/
cylance/desktop/log ~/ps.txt ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt   ~/
slabinfo.txt  ~/mem.txt
```

Amazon et SUSE Linux :

```
ps aux > ~/ps.txt
sudo pmap -x $(ps -e | grep cylancesvc | cut -d ' ' -f 2) > ~/maps.txt
cat /proc/cpuinfo > ~/cpu.txt
cat /proc/meminfo > ~/mem.txt
cat /proc/mounts > ~/mounts.txt
cat /proc/modules > ~/modules.txt
cat /proc/slabinfo > ~/slabinfo.txt
tar -cvzf cylancelogs-$(date --rfc-3339='date').tgz /var/log/messages* /opt/
cylance/desktop/log ~/ps.txt ~/maps.txt ~/cpu.txt ~/mounts.txt ~/modules.txt ~/
slabinfo.txt
```

Envoyer les événements à une solution SIEM ou à un serveur syslog

Le logiciel SIEM (Security information and Event Management) collecte, analyse et regroupe les données de sécurité provenant de plusieurs sources afin de détecter les menaces de sécurité potentielles. Vous pouvez envoyer les événements détectés par les solutions Cylance Endpoint Security au serveur syslog ou logiciel SIEM de votre organisation. Les données d'alerte envoyées à un serveur SIEM ou syslog sont les mêmes que celles affichées dans la console de gestion. Pour plus d'informations sur les événements spécifiques signalés par les solutions Cylance Endpoint Security, reportez-vous au Guide Syslog.

1. Sur la barre de menus de la console de gestion, cliquez sur **Paramètres > Application**.
2. Cochez la case **Syslog/SIEM**.
3. Sélectionnez les événements que vous souhaitez envoyer à l'intégration SIEM ou syslog de votre organisation. Pour en savoir plus sur chaque type d'évènement, consultez le Guide Syslog.
4. Spécifiez les informations de votre intégration SIEM ou syslog. Pour plus d'informations, consultez le Guide Syslog.
5. Cliquez sur **Tester la connexion** pour vérifier les paramètres.
6. Cliquez sur **Enregistrer**.

Activer l'accès à l'API utilisateur Cylance

Cylance Endpoint Security prend en charge l'intégration à des programmes tiers à l'aide de l'API utilisateur Cylance, un ensemble d'API RESTful. Cela permet à votre entreprise de gérer les paramètres et configurations Cylance Endpoint Security à l'aide d'un programme. Les administrateurs peuvent personnaliser les paramètres d'intégration pour contrôler les privilèges d'API dont dispose un utilisateur. Pour des raisons de sécurité, un utilisateur d'API a besoin d'un ID d'application et d'un secret d'application générés lorsque vous ajoutez une application personnalisée dans la console de gestion. Un locataire peut compter jusqu'à 10 intégrations personnalisées.

Pour plus d'informations, consultez le Guide d'API utilisateur Cylance.

Remarque : En juillet 2022, une amélioration de la sécurité a été introduite pour les locataires Cylance Endpoint Security existants. Les utilisateurs ayant le rôle Administrateur peuvent activer une nouvelle fonctionnalité qui supprime définitivement les secrets d'application de la console de gestion après leur génération, en veillant à ce qu'ils ne puissent pas être consultés par les utilisateurs ayant accès à la console Cylance. Si vous activez cette fonctionnalité dans Paramètres > Intégrations, lorsqu'un administrateur génère ou régénère un secret d'application, elle s'affiche uniquement jusqu'à ce que l'administrateur ferme la boite de dialogue ou quitte l'écran. Le secret d'application ne s'affiche pas dans la liste. Pour supprimer vos secrets d'application existants et activer ce comportement, vous pouvez développer **Sécurité améliorée disponible** et cliquer sur **Supprimer le secret**. Une fois la fonction activée, tous les secrets d'application générés précédemment ne seront plus disponibles à l'affichage. Vous devez enregistrer les secrets d'application existants avant d'activer cette fonction. Vous ne pouvez pas revenir au comportement précédent qui expose les secrets d'application dans la console. Vous pouvez générer de nouveaux ID et secrets d'application, le cas échéant.

Pour les nouveaux locataires Cylance Endpoint Security créés après juillet 2022, cette fonction est activée par défaut.

1. Dans la console de gestion, cliquez sur **Paramètres > Intégrations**.
2. Cliquez sur **Ajouter une application**.
3. Donnez un nom à l'application.
4. Sélectionnez les privilèges API auxquels autoriser l'accès.
5. Cliquez sur **Enregistrer**.
   L'ID d'application et le secret d'application s'affichent.
6. Cliquez sur **OK**.

Résolution des problèmes Cylance Endpoint Security

Cette section fournit des conseils pour le dépannage des services et des fonctionnalités Cylance Endpoint Security.

Utilisation de l'outil de collecte de l'assistance BlackBerry

Si vous travaillez avec l'assistance BlackBerry pour résoudre un problème, vous pouvez télécharger l'outil de collecte de l'assistance BlackBerry pour collecter des données produit et des informations système. Pour en savoir plus, rendez-vous sur le site support.blackberry.com et consultez l'article 66596.

Utilisation de la fonction Signaler un problème

L'agent CylanceGATEWAY et l'application CylancePROTECT Mobile incluent l'option Signaler un problème que les utilisateurs peuvent utiliser pour envoyer un rapport de problème et les fichiers journaux de l'agent à BlackBerry sans contacter leur administrateur informatique pour obtenir de l'aide au dépannage. BlackBerry recommande de demander aux utilisateurs de contacter leur administrateur informatique pour obtenir de l'aide au dépannage avant de soumettre le rapport et les fichiers journaux de l'agent à BlackBerry. Pour plus d'informations, reportez-vous aux paramètres de l'agent CylanceGATEWAY et la section Signaler un problème à BlackBerry,

Supprimer BlackBerry Connectivity Node de Cylance Endpoint Security

Vous pouvez utiliser l'application de désinstallation pour supprimer BlackBerry Connectivity Node du serveur sur lequel il est installé. La désinstallation du BlackBerry Connectivity Node ne le supprime pas de la console de gestion Cylance Endpoint Security. Par conséquent, si vous souhaitez réinstaller BlackBerry Connectivity Node ultérieurement, vous devez d'abord supprimer l'instance de la console de gestion BlackBerry Connectivity Node.

Pour supprimer BlackBerry Connectivity Node, effectuez les actions suivantes :

Étape	Action
1	Supprimez le logiciel BlackBerry Connectivity Node du serveur local.
2	Supprimez tous les utilisateurs Active Directory associés à toutes les connexions d'annuaire que vous souhaitez supprimer.
3	Supprimez les groupes d'utilisateurs associés à toutes les connexions de répertoire que vous souhaitez supprimer.
4	Supprimez l'instance BlackBerry Connectivity Node de la console de gestion de Cylance Endpoint Security.

Supprimer BlackBerry Connectivity Node du serveur local

Si vous effectuez un dépannage, sauvegardez `\Program Files\BlackBerry\BlackBerry Connectivity Node - UES\Logs` avant de désinstaller le logiciel.

1. Dans la barre des tâches, cliquez sur **Démarrer > Panneau de configuration > Programmes > Programmes et fonctionnalités**.
2. Cliquez sur **BlackBerry Connectivity Node - UES**.
3. Cliquez sur **Désinstaller**.
4. Cliquez sur **Suivant**.
5. Cliquez sur **Fermer**.
6. Redémarrez l'ordinateur pour terminer la suppression de BlackBerry Connectivity Node.

Supprimer une instance BlackBerry Connectivity Node de la console de gestion de Cylance Endpoint Security

Si vous désinstallez une instance de BlackBerry Connectivity Node, vous devez suivre les étapes ci-dessous pour supprimer les données de cette instance de la base de données Cylance Endpoint Security. Si ce n'est pas le cas, la saisie de BlackBerry Connectivity Node dans la console de gestion de Cylance Endpoint Security restera et son état sera « En pause ».

Avant de commencer :

- Supprimez BlackBerry Connectivity Node du serveur local.
- Assurez-vous d'être connecté en tant qu'utilisateur autorisé à supprimer l'instance. Par défaut, le rôle Administrateur de sécurité ou Administrateur d'entreprise.

1. Dans la barre de menus de la console de gestion, cliquez sur **Paramètres > Connexions au répertoire > Nœud de connectivité**.
2. Cliquez sur l'onglet **Connectivity Node**.
3. Cliquez sur en regard du BlackBerry Connectivity Node que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**.

Résolution des problèmes CylancePROTECT Desktop

Cette section fournit des informations pour vous aider à résoudre les problèmes liés à CylancePROTECT Desktop.

Supprimer l'agent CylancePROTECT Desktop d'un terminal

Avant de commencer :

- Pour les terminaux desquels vous souhaitez supprimer l'agent CylancePROTECT Desktop, affectez une stratégie de terminal sans aucun paramètre activé. Vérifiez que **Paramètres de protection > Empêcher l'arrêt du service à partir du terminal** et **Contrôle de l'application** sont désactivés dans la stratégie.
- Si vous demandez aux utilisateurs de fournir un mot de passe pour supprimer l'agent CylancePROTECT Desktop, notez le mot de passe.

1. Utilisez l'une des méthodes suivantes pour supprimer l'agent d'un terminal :

   Windows

   - Pour supprimer manuellement CylancePROTECT Desktop, utilisez Ajouter/Supprimer des programmes. Si un mot de passe de désinstallation est requis, vous devez utiliser la méthode de ligne de commande ci-dessous avec la commande de protection par mot de passe.

- Exécutez l'invite de commande en tant qu'administrateur et utilisez l'une des commandes suivantes :
  - CylancePROTECTSetup.exe :

    ```
    CylancePROTECTSetup.exe /uninstall
    ```
  - CylancePROTECT_x64.msi standard :

    ```
    msiexec /uninstall CylancePROTECT_x64.msi
    ```
  - Programme d'installation Windows CylancePROTECT_x64.msi :

    ```
    msiexec /x CylancePROTECT_x64.msi
    ```
  - CylancePROTECT_x86.msi standard :

    ```
    msiexec /uninstall CylancePROTECT_x86.msi
    ```
  - Programme d'installation Windows CylancePROTECT_x86.msi :

    ```
    msiexec /x CylancePROTECT_x86.msi
    ```
  - GUID d'ID produit standard :

    ```
    msiexec /uninstall {2E64FC5C-9286-4A31-916B-0D8AE4B22954}
    ```
  - Programme d'installation GUID d'ID produit Windows :

    ```
    msiexec /x {2E64FC5C-9286-4A31-916B-0D8AE4B22954}
    ```

Commandes facultatives :

- Désinstallation silencieuse :

  ```
  /quiet
  ```
- Silencieuse et masquée :

  ```
  /qn
  ```
- Protection par mot de passe :

  ```
  UNINSTALLKEY="<password>"
  ```
- Fichiers mis en quarantaine automatiquement :

  ```
  QUARANTINEDISPOSETYPE=<0_or_1>
  ```
  - 0 supprime tous les fichiers
  - 1 restaure tous les fichiers
- Générer le fichier journal de désinstallation :

  ```
  /Lxv* <path_including_file_name>
  ```

macOS

Exécutez la commande suivante :

```
sudo /Applications/Cylance/Uninstall\ CylancePROTECT.app/Contents/MacOS/
Uninstall\ CylancePROTECT
```

Si un mot de passe de désinstallation est requis, ajoutez le paramètre suivant :

```
--password=<password>
```

Linux

a. Utilisez l'une des commandes suivantes pour désinstaller l'agent :

- RHEL/CentOS :

  ```
  rpm -e $(rpm -qa | grep -i cylance)
  ```

- Ubuntu/Debian :

  ```
  dpkg -P cylance-protect cylance-protect-ui cylance-protect-driver cylance-
  protect-open-driver
  ```

- Amazon Linux 2/SUSE :

  ```
  rpm -e $(rpm -qa | grep -i cylance)
  ```

b. Utilisez l'une des commandes suivantes pour désinstaller les pilotes de l'agent Linux :

- RHEL/CentOS :

  ```
  rpm -e CylancePROTECTDriver CylancePROTECTOpenDriver
  ```

- Ubuntu/Debian :

  ```
  dpkg -P cylance-protect-driver cylance-protect-open-driver
  ```

- Amazon Linux 2 :

  ```
  rpm -e CylancePROTECTDriver-<package_version>.amzn2.x86_64
  rpm -e CylancePROTECTOpenDriver-<package_version>.amzn2.86_64
  ```

2. Dans la console de gestion, dans **Actifs > Terminaux**, sélectionnez le terminal et cliquez sur **Supprimer**. Cliquez sur **Oui** pour confirmer.

Réenregistrer un agent Linux

Si un agent n'est plus enregistré dans la console, pour quelque raison que ce soit, l'utilisateur doit réenregistrer le terminal à l'aide d'un jeton. Utilisez l'une des commandes suivantes pour réenregistrer le terminal, en remplaçant `token` par le jeton d'installation du locataire :

Red Hat, CentOS et Ubuntu :

```
/opt/cylance/desktop/cylance --register=token
```

Pour CentOS, vous pouvez également utiliser la commande suivante :

```
/opt/cylance/desktop/cylance --r=token
```

Amazon et SUSE Linux :

```
/opt/cylance/desktop/cylance -r token
```

Résolution des problèmes de mise à jour, d'état et de connectivité avec CylancePROTECT Desktop

Tenez compte des éléments suivants lors de la résolution des problèmes de mise à jour, d'état et de connectivité avec CylancePROTECT Desktop :

- Examinez les icônes d'état de l'agent CylancePROTECT Desktop.
- Vérifiez que le port 443 du pare-feu est ouvert, et que le terminal peut résoudre le problème et se connecter aux sites BlackBerry.
- Vérifiez les informations du terminal dans la console de gestion. Vérifiez si le terminal est en ligne ou hors ligne, et l'heure de sa dernière connexion.
- Vérifiez si le terminal utilise un proxy pour se connecter à Internet et si les informations d'identification sont correctement configurées sur le proxy.
- Redémarrez le service Cylance afin qu'il tente de se connecter à la console.
- Collectez les journaux de débogage. Reportez-vous à la section Gérer les journaux de l'agent CylancePROTECT Desktop.
- Collectez les données de sortie des informations système lorsque le problème se produit.
  - Windows : msinfo32 ou winmsd
  - macOS : informations système

Un grand nombre de violations de l'injection DYLD sont signalées par les terminaux Linux

Cause possible

Certaines applications tierces, telles que Splunk, Dynatrace, AppDynamics et DataDog, essaient de précharger les modules (variable d'environnement LD_PRECHARGE pour un processus), provoquant des évènements de violation d'injection DYLD pour tout processus surveillé par l'application.

Solution possible

Procédez comme suit :

1. Si vous utilisez une version de l'agent CylancePROTECT Desktop antérieure à la version 2.1.1574, effectuez une mise à niveau vers la version 2.1.1574 ou ultérieure. BlackBerry recommande vivement d'effectuer une mise à niveau vers la dernière version disponible de l'agent pour bénéficier des dernières améliorations.
2. Ajoutez des exclusions de protection de la mémoire pour les composants .so qu'une application tierce tente d'injecter. Inspectez la variable LD_PRECHARGE afin de déterminer les composants pour lesquels vous devez ajouter des exclusions (« man ld.so » peut fournir des conseils). Il est recommandé de contacter l'assistance de l'application tierce pour identifier les fichiers .so applicables.

Variations de fuseau horaire pour CylancePROTECT Desktop

Selon l'endroit où vous affichez les informations de date et d'heure pour CylancePROTECT Desktop, le fuseau horaire utilisé peut varier.

Date et heure affichées dans cette interface utilisateur	Fuseau horaire utilisé
Agent CylancePROTECT Desktop (y compris les notifications d'évènements et les journaux d'agent)	Fuseau horaire de la machine locale.
Console de gestion (à l'exception de l'onglet Rapports et des données exportées)	Fuseau horaire de l'administrateur utilisant la console.
Onglet Rapports de la console de gestion	Fuseau horaire de l'administrateur utilisant la console. Lorsque vous exportez un rapport, le fuseau horaire UTC est utilisé dans l'exportation.
Évènements syslog	Fuseau horaire UTC.
Rapport de données sur les menaces et données exportées depuis la console de gestion	Fuseau horaire UTC.

Exclusions de dossiers lors de l'utilisation de CylancePROTECT Desktop avec des produits de sécurité tiers

Si vous utilisez des produits de sécurité tiers avec CylancePROTECT Desktop, vous devrez les configurer pour exclure Cylance des répertoires afin de vous assurer que CylancePROTECT Desktop peut s'exécuter simultanément avec eux sans problème.

Répertoires, fichiers ou processus CylancePROTECT à exclure dans Windows

Version Windows	Chemin d'accès

Windows (toutes les versions)	`C:\Program Files\Cylance`
	`C:\ProgramData\Cylance`
	`C:\Documents and Settings\All Users\Application Data\Cylance\Desktop\q`
	`C:\Windows\System32\Drivers\CyProtectDrv*.sys`
	`C:\Windows\System32\Drivers\CyDevFlt*.sys`
	`C:\Windows\System32\Drivers\CylanceDrv*.sys`
	`C:\Windows\CyProtect.cache`
	`C:\Windows\CylanceUD.cache`
	`C:\Windows\Temp\CylanceDesktopArchive`
	`C:\Windows\Temp\CylanceDesktopRemoteFile`
	`C:\Program Files\Cylance\Desktop\CylanceSvc.exe`
	`C:\Program Files\Cylance\Desktop\CylanceUI.exe`
	`C:\Program Files\Cylance\Desktop\CyUpdate.exe`
	`C:\Program Files\Cylance\Desktop\LocalePkg.exe`

Répertoires CylancePROTECT à exclure dans macOS

macOS Version	Chemin d'accès

macOS X (10.9-10.11), macOS 10.12 et versions ultérieures	`/Library/Application Support/Cylance/Desktop/q`
	`/Library/Application Support/Cylance/`
	`/System/Library/Extensions/CyProtectDrvOSX.kext/`
	`/private/tmp/CylanceDesktopArchive`
	`/private/tmp/CylanceDesktopRemoteFile`

Répertoires CylancePROTECT à exclure dans Linux

Les chemins liés à la configuration du proxy sont des exclusions facultatives. Ils ne sont requis que si vous avez configuré un remplacement de proxy pour CylancePROTECT.

Version Linux	Chemin d'accès

Amazon Linux	CylancePROTECT :
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init/cylancesvc.conf`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Configuration du proxy (uniquement si nécessaire) :
	`/etc/init/cylancesvc.override`
	CylanceUI :
	Non disponible sur Amazon Linux.

Version Linux	Chemin d'accès

Amazon Linux 2
Amazon Linux 2023
	CylancePROTECT :
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/usr/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Configuration du proxy (uniquement si nécessaire) :
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI :
	Non disponible sur Amazon Linux 2 ou Amazon 2023.

RHEL/CentOS 6.x	CylancePROTECT :
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init/cylancesvc.conf`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Configuration du proxy (uniquement si nécessaire) :
	`/etc/init/cylancesvc.override`
	CylanceUI :
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`

Version Linux	Chemin d'accès

RHEL/CentOS 7.x, 8.x
Oracle Linux 7, 8, 9
	CylancePROTECT :
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/usr/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Configuration du proxy (uniquement si nécessaire) :
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI :
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`
	`/usr/share/gnome-shell/extensions/cylance-protect@cylance.com`

SUSE (SLES) 11.x	CylancePROTECT :
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init.d/cylancesvc`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	CylanceUI :
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`

Version Linux	Chemin d'accès

SUSE (SLES) 12 SP1, SP2, SP3, SP4
SUSE (SLES) 15
	CylancePROTECT :
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/sysconfig/modules/cylance.modules`
	`/etc/modprobe.d/cylance.conf`
	`/usr/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Configuration du proxy (uniquement si nécessaire) :
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI :
	`/etc/xdg/autostart/cylance-protect.desktop`
	`/usr/share/applications/cylance-protect.desktop`
	`/usr/share/gnome-shell/extensions/cylance-protect@cylance.com`

Ubuntu LTS/Xubuntu 14.04	CylancePROTECT :
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/modprobe.d/cylance.conf`
	`/etc/init/cylancesvc.conf`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Configuration du proxy (uniquement si nécessaire) :
	`/etc/init/cylancesvc.override`
	CylanceUI :
	`/usr/share/applications/cylance-protect.desktop`
	`/etc/xdg/autostart/cylance-protect.desktop`

Version Linux	Chemin d'accès

Ubuntu LTS/Xubuntu 16.04, 18.04, 20.04
Debian 10, 11
	CylancePROTECT :
	`/opt/cylance`
	`/usr/src/CyProtectDrv-1.2`
	`/tmp/CylanceDesktopArchive`
	`/tmp/CylanceDesktopRemoteFile`
	`/lib/modules/*/extra/CyProtectDrv.ko`
	`/etc/modprobe.d/cylance.conf`
	`/lib/systemd/system/cylancesvc.service`
	`/etc/dbus-1/system.d/com.cylance.agent_server.conf`
	`/var/run/cylancesvc.pid`
	Configuration du proxy (uniquement si nécessaire) :
	`/etc/systemd/system/cylancesvc.service.d/proxy.conf`
	CylanceUI :
	`/usr/share/applications/cylance-protect.desktop`
	`/etc/xdg/autostart/cylance-protect.desktop`

Le pilote Linux n'est pas chargé. Mettre à niveau le package du pilote.

Cause

Le pilote CylancePROTECT Desktop du terminal n'est pas compatible avec le kernel Linux.

Solution

Mettez à jour le pilote Linux en fonction de l'un des scénarios suivants :

Élément	Description
Le terminal exécute la version 3.1 de l'agent ou une version ultérieure.	Effectuez l'une des opérations suivantes : • Définissez la règle de mise à jour de zone pour mettre à jour automatiquement le pilote Linux. • Mettez à jour manuellement le pilote Linux.
Le terminal exécute l'agent 2.1.1590 ou une version ultérieure (jusqu'à 3.0)	• Mettez à jour manuellement le pilote Linux.

Résolution des problèmes CylanceOPTICS

Cette section fournit des informations pour vous aider à résoudre les problèmes liés à CylanceOPTICS.

Résolution des problèmes avec l'agent CylanceOPTICS sur Linux

Problème	Solution possible

Les packages kernel-header et kernel-devel ne correspondent pas au noyau.	Utilisez le noyau de mise à jour yum et redémarrez le terminal.
	Si un redémarrage n'est pas possible, utilisez l'une des commandes suivantes :
	• RHEL/CentOS ou Amazon Linux 2 : `yum install kernel-headers-`
	`uname -r` `kernel-devel-`
	`uname -r`
	• Ubuntu : `sudo apt-get install linux-headers -$(uname -r)`

Si vous activez la journalisation du débogage, un message indiquant que l'outil de corroboration a trouvé une correspondance pour PID apparaît dans les journaux.	Ce message est attendu, et n'indique pas un bogue ou un autre problème.

Suppression de l'agent CylanceOPTICS d'un terminal

Lorsque vous désinstallez l'agent CylanceOPTICS d'un terminal, toutes les données locales stockées par CylanceOPTICS et les fichiers journaux sont également supprimés. Vous devez désinstaller l'agent CylanceOPTICS avant CylancePROTECT.

Pour désinstaller l'agent, utilisez les options de désinstallation standard disponibles sur le système d'exploitation (par exemple, Ajout/Suppression de programmes sous Windows ou désinstallation à partir de Finder > Applications sous macOS), ou désinstallez l'agent CylanceOPTICS à l'aide des commandes du système d'exploitation décrites sur la page Contenu de configuration Cylance Endpoint Security.

Sous Windows, si vous souhaitez désinstaller l'agent à l'aide des commandes du système d'exploitation, l'utilisateur doit être propriétaire des fichiers et répertoires appartenant au système local. Si vous avez activé la fonction de prévention de l'arrêt du service de l'agent CylanceOPTICS pour Windows (sous les paramètres de protection de la stratégie de terminal), vous devez la désactiver (ou attribuer une autre stratégie de terminal dans laquelle cette fonction n'est pas activée) avant de tenter de supprimer l'agent CylanceOPTICS.

Il est recommandé de redémarrer le terminal une fois l'agent désinstallé.

Suppression de l'agent CylanceOPTICS d'un terminal macOS

Vérifier que l'agent CylanceOPTICS a été supprimé

Exécutez la commande suivante :

```
kextstat | grep -i cyoptic
```

Pour macOS Big Sur (11.x), exécutez également la commande ci-dessous :

```
systemextensionsctl list | grep -i cyoptics
```

Les commandes ne doivent renvoyer aucune sortie.

Vérifiez que les fichiers et les chemins suivants ne sont plus présents sur le système :

- /Library/Application Support/Cylance/Optics
- /Library/Application Support/OpticsUninstall
- /Applications/Cylance/Optics
- /Library/LaunchDaemons/com.cylance.cyoptics_service.plist
- /Library/LaunchDaemons/com.cylance.optics.postuninstall.plist
- /Library/LaunchDaemons/com.cylance.cyopticsesfservice.plist

Sur un terminal macOS Big Sur (11.x), après avoir utilisé une session ssh pour effectuer la désinstallation silencieuse de l'agent CylanceOPTICS, /Applications/Cylance/Optics/CyOpticsESFLoader.app demeure et l'extension système est toujours active

Ce problème se produit car Apple ne dispose d'aucun mécanisme pour désinstaller silencieusement les extensions système sans confirmation explicite de l'utilisateur final.

Pour résoudre ce problème, utilisez l'utilitaire de recherche pour localiser CyOpticsESFLoader.app et faites-le glisser vers la corbeille, puis confirmez l'invite de l'interface utilisateur pour désactiver et supprimer l'extension système.

Si vous obtenez une erreur d'autorisation lorsque vous faites glisser le fichier vers la corbeille, exécutez la commande suivante pour désactiver temporairement CylancePROTECT Desktop :

```
sudo launchctl unload /Library/LaunchDaemons/com.cylance.agent_service.plist
```

Après avoir exécuté la commande, vous pouvez faire glisser le fichier vers la corbeille et confirmer l'invite de l'interface utilisateur. Si vous souhaitez que CylancePROTECT Desktop reste actif, redémarrez le terminal.

Remarque : Vous devez supprimer CyOpticsESFLoader.app de cette manière avant de supprimer l'agent CylancePROTECT Desktop du terminal. Si vous supprimez l'agent CylancePROTECT Desktop avant d'effectuer cette tâche, /Applications/Cylance est supprimé du terminal, y compris CyOpticsESFLoader.app, de sorte que vous ne pourrez pas le supprimer manuellement et désactiver l'extension système.

Informations juridiques

Cette documentation, y compris la documentation incluse pour référence telle que celle fournie ou mise à disposition sur le site Web BlackBerry, est fournie ou mise à disposition « EN L'ÉTAT » et « TELLE QUELLE », sans condition ni garantie en tout genre de la part de BlackBerry Limited et de ses filiales (« BlackBerry »), et BlackBerry décline toute responsabilité en cas d'erreur ou d'oubli typographique, technique ou autre inexactitude contenue dans ce document. Pour des raisons de protection des informations confidentielles et/ou des secrets commerciaux de BlackBerry, cette documentation peut décrire certains aspects de la technologie BlackBerry en termes généraux. BlackBerry se réserve le droit de modifier périodiquement les informations contenues dans cette documentation. Cependant, BlackBerry ne s'engage en aucune manière à vous communiquer les modifications, mises à jour, améliorations ou autres ajouts apportés à cette documentation.

La présente documentation peut contenir des références à des sources d'informations, du matériel ou des logiciels, des produits ou des services tiers, y compris des composants et du contenu tel que du contenu protégé par copyright et/ou des sites Web tiers (ci-après dénommés collectivement « Produits et Services tiers »). BlackBerry ne contrôle pas et décline toute responsabilité concernant les Produits et Services tiers, y compris, sans s'y limiter, le contenu, la précision, le respect du code de la propriété intellectuelle, la compatibilité, les performances, la fiabilité, la légalité, l'éthique, les liens ou tout autre aspect desdits Produits et Services tiers. La présence d'une référence aux Produits et Services tiers dans cette documentation ne suppose aucunement que BlackBerry se porte garant des Produits et Services tiers ou de la tierce partie concernée.

SAUF DANS LA MESURE SPÉCIFIQUEMENT INTERDITE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, TOUTES LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE TOUTE NATURE, EXPRESSES OU TACITES, NOTAMMENT (SANS LIMITATIONS) LES CONDITIONS, GARANTIES OU REPRÉSENTATIONS DE DURABILITÉ, D'ADÉQUATION À UNE UTILISATION OU À UN BUT PARTICULIER, DE COMMERCIALISATION, DE QUALITÉ MARCHANDE, DE NON-INFRACTION, DE SATISFACTION DE LA QUALITÉ OU DE TITRE, OU RÉSULTANT D'UNE LOI, D'UNE COUTUME, D'UNE PRATIQUE OU D'UN USAGE COMMERCIAL, OU EN RELATION AVEC LA DOCUMENTATION OU SON UTILISATION, OU LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICE OU DES PRODUITS ET SERVICES TIERS CITÉS, SONT EXCLUES. VOUS POUVEZ JOUIR D'AUTRES DROITS QUI VARIENT SELON L'ÉTAT OU LA PROVINCE. CERTAINES JURIDICTIONS N'AUTORISENT PAS L'EXCLUSION OU LA LIMITATION DES GARANTIES ET CONDITIONS IMPLICITES. DANS LA MESURE AUTORISÉE PAR LES LOIS, TOUTE GARANTIE OU CONDITION IMPLICITE RELATIVE À LA DOCUMENTATION, DANS LA MESURE OÙ ELLES NE PEUVENT PAS ÊTRE EXCLUES EN VERTU DES CLAUSES PRÉCÉDENTES, MAIS PEUVENT ÊTRE LIMITÉES, SONT PAR LES PRÉSENTES LIMITÉES À QUATRE-VINGT-DIX (90) JOURS À COMPTER DE LA DATE DE LA PREMIÈRE ACQUISITION DE LA DOCUMENTATION OU DE L'ARTICLE QUI FAIT L'OBJET D'UNE RÉCLAMATION.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS EN VIGUEUR DANS VOTRE JURIDICTION, EN AUCUN CAS BLACKBERRY N'EST RESPONSABLE DES DOMMAGES LIÉS À LA PRÉSENTE DOCUMENTATION OU À SON UTILISATION, OU À LA PERFORMANCE OU NON-PERFORMANCE DES LOGICIELS, DU MATÉRIEL, DES SERVICES OU DES PRODUITS ET SERVICES TIERS MENTIONNÉS DANS LES PRÉSENTES, ET NOTAMMENT, SANS S'Y LIMITER, DES DOMMAGES DIRECTS, EXEMPLAIRES, ACCIDENTELS, INDIRECTS, SPÉCIAUX, PUNITIFS OU AGGRAVÉS, DES DOMMAGES LIÉS À UNE PERTE DE PROFITS OU DE REVENUS, UN MANQUE À GAGNER, UNE INTERRUPTION D'ACTIVITÉ, UNE PERTE D'INFORMATIONS COMMERCIALES, UNE PERTE D'OPPORTUNITÉS COMMERCIALES, LA CORRUPTION OU LA PERTE DE DONNÉES, LE NON-ENVOI OU LA NON-RÉCEPTION DE DONNÉES, DES PROBLÈMES LIÉS À DES APPLICATIONS UTILISÉES AVEC DES PRODUITS OU SERVICES BLACKBERRY, DES COUTS D'INDISPONIBILITÉ, LA PERTE D'UTILISATION DES PRODUITS OU SERVICES BLACKBERRY EN TOUT OU EN PARTIE, OU DE TOUT SERVICE DE COMMUNICATION, DU COUT DE BIENS DE

SUBSTITUTION, DES FRAIS DE GARANTIE, DES ÉQUIPEMENTS OU SERVICES, DES COUTS DE CAPITAL, OU AUTRES PERTES FINANCIÈRES SIMILAIRES, PRÉVISIBLES OU NON, MÊME SI BLACKBERRY A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

DANS LA MESURE MAXIMALE PERMISE PAR LES LOIS APPLICABLES DANS VOTRE JURIDICTION, BLACKBERRY N'EST NULLEMENT TENU PAR DES OBLIGATIONS, DEVOIRS OU RESPONSABILITÉS, CONTRACTUELS, DÉLICTUELS OU AUTRES, PAS MÊME PAR UNE RESPONSABILITÉ EN CAS DE NÉGLIGENCE OU RESPONSABILITÉ STRICTE ET NE VOUS EST REDEVABLE EN RIEN.

LES LIMITATIONS, EXCLUSIONS ET CLAUSES DE NON-RESPONSABILITÉ CONTENUES DANS LES PRÉSENTES S'APPLIQUENT : (A) INDÉPENDAMMENT DE LA NATURE DE LA CAUSE D'ACTION, DE DEMANDE OU D'ACTION ENTREPRISE PAR VOUS, NOTAMMENT, SANS S'Y LIMITER, POUR RUPTURE DE CONTRAT, NÉGLIGENCE, FAUTE, RESPONSABILITÉ STRICTE OU TOUTE AUTRE THÉORIE LÉGALE, ET RESTENT APPLICABLES EN CAS DE RUPTURES SUBSTANTIELLES OU DE MANQUEMENT AU BUT ESSENTIEL DU PRÉSENT CONTRAT OU DE TOUT RECOURS ENVISAGEABLE PAR LES PRÉSENTES ; ET (B) À BLACKBERRY ET À SES FILIALES, LEURS AYANTS DROIT, REPRÉSENTANTS, AGENTS, FOURNISSEURS (NOTAMMENT LES FOURNISSEURS DE SERVICES), REVENDEURS AGRÉÉS BLACKBERRY (NOTAMMENT LES FOURNISSEURS DE SERVICES) ET LEURS DIRECTEURS, EMPLOYÉS ET SOUS-TRAITANTS RESPECTIFS.

OUTRE LES LIMITATIONS ET EXCLUSIONS SUSMENTIONNÉES, EN AUCUN CAS, LES DIRECTEURS, EMPLOYÉS, AGENTS, REVENDEURS, FOURNISSEURS, SOUS-TRAITANTS DE BLACKBERRY OU DE SES FILIALES N'ONT UNE RESPONSABILITÉ CONSÉCUTIVE OU RELATIVE À LA PRÉSENTE DOCUMENTATION.

Avant de vous abonner, d'installer ou d'utiliser des Produits et Services tiers, il est de votre responsabilité de vérifier que votre fournisseur de services prend en charge toutes les fonctionnalités. Certains fournisseurs de services peuvent ne pas proposer de fonctionnalités de navigation Internet avec un abonnement à BlackBerry® Internet Service. Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance, les plans de service et les fonctionnalités. L'installation ou l'utilisation de Produits et Services tiers avec des produits et services BlackBerry peuvent nécessiter un ou plusieurs brevets, marques commerciales, licences de copyright ou autres licences à des fins de protection des droits d'autrui. Vous êtes seul responsable de votre décision d'utiliser ou non les Produits et Services tiers et si cela nécessite l'obtention de licences tierces. Si de telles licences sont requises, vous êtes seul responsable de leur acquisition. Vous ne devez pas installer ou utiliser de Produits et Services tiers avant d'avoir acquis la totalité des licences nécessaires. Les Produits et Services tiers fournis avec les produits et services BlackBerry vous sont fournis à toutes fins utiles « EN L'ÉTAT » sans conditions, garanties ou représentations expresses ou tacites d'aucune sorte par BlackBerry, et BlackBerry n'engage aucune responsabilité sur les Produits et Services tiers à cet égard. L'utilisation que vous faites des Produits et Services tiers est régie par et dépendante de votre acceptation des termes des licences et autres accords distincts applicables à cet égard avec d'autres parties, sauf dans la limite couverte expressément par une licence ou autre accord conclu avec BlackBerry.

Les conditions d'utilisation de tout produit ou service BlackBerry sont stipulées dans une licence ou autre accord distinct conclu avec BlackBerry à cet égard. LE CONTENU DE CETTE DOCUMENTATION N'EST PAS DESTINÉ À REMPLACER LES ACCORDS OU GARANTIES EXPRÈS ET ÉCRITS FOURNIS PAR BLACKBERRY POUR UNE PARTIE DES PRODUITS OU SERVICES BLACKBERRY AUTRES QUE CETTE DOCUMENTATION.

BlackBerry Enterprise Software incorpore des éléments logiciels tiers. La licence et les informations de copyright associées à ce logiciel sont disponibles à l'adresse http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue Est
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,

Maidenhead, Berkshire SL6 1RL
Royaume-Uni

Publié au Canada