



CylanceOPTICS

Getting Started Guide

Behavioral Detection Engine

Contents

- Getting started: Behavioral Detection Engine..... 4**
- Behavioral detection policies..... 5**
- Creating a behavioral detection policy..... 6**
 - Detection and response tab: Behavioral detection policy.....6
 - Assigned device policy tab: Behavioral detection policy..... 8
- Importing custom rules..... 10**
- Adding exceptions..... 12**
- Managing detection rule updates..... 15**
- Viewing alerts..... 17**
- Best practice: Tuning your environment..... 18**
- Legal notice..... 19**

Getting started: Behavioral Detection Engine

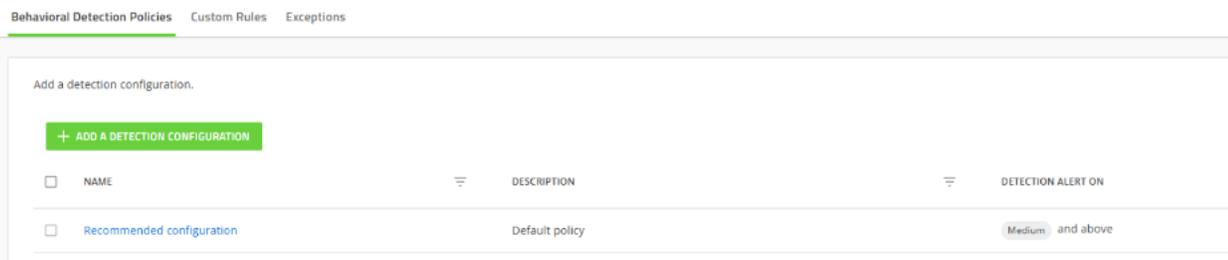
The Behavioral Detection Engine (BDE) uses a behavioral detection policy, which aligned with the MITRE framework, to send detection rules to your users' devices. According to the detection rules, alerts are raised based on the alert threshold and remediation steps automatically take place. The BDE eases the burden of configuring and managing CylanceOPTICS when compared to using the legacy rule sets.

In the Cylance console, you can create the detection policy where you configure the alert threshold and the automated remediation steps according to the response threshold. After you configure the BDE policy, you must link it to a device policy and apply the device policy to devices within your organization. This guide provides an overview of the BDE policy, how to link it with a device policy, manage BDE policy content updates, review alerts, and create exceptions. It also includes guidance and best practices for how start using BDE and recommendations related to automated responses.

If you are an existing CylanceOPTICS customer using legacy rule sets, it is recommended that you migrate from using legacy rule sets to BDE policies. For more information, see the [Behavioral Detection Engine Migration Guide](#).

Behavioral detection policies

CylanceOPTICS > Behavioral detection engine



In the Cylance console, behavioral detection policies are in the **CylanceOPTICS > Behavioral Detection Engine** menu, in the **Behavioral Detection Policies** tab.

The BDE policy defines which MITRE detections to apply to devices, which severity level to alert on, and when to apply automated responses. All tenants have a default policy configured which has all the MITRE detections with Alerts and Observations features enabled. The default policy is configured with an alert threshold of medium and above.

Alert thresholding is a new concept introduced with BDE. It allows easy suppression of alerts that are below a certain level of severity. This means that only alerts at or above the specified threshold level display in the **Alerts** screen and through external interfaces like syslog or the public API. To ensure that there is no loss in information fidelity, the BDE includes support for observations. When **Observations** are enabled, the BDE instructs the CylanceOPTICS agent (version 3.3 or later) to watch for all behaviors that are below the alert threshold, collect any data associated with it, collect any correlated elements along the attack chain, and add the appropriate MITRE TTP tagging to that collected data. Using Alert Thresholds and Observations, the BDE can enact policies with a much lower level of noise without missing important data that may be hiding in low efficacy signal.

Creating a behavioral detection policy

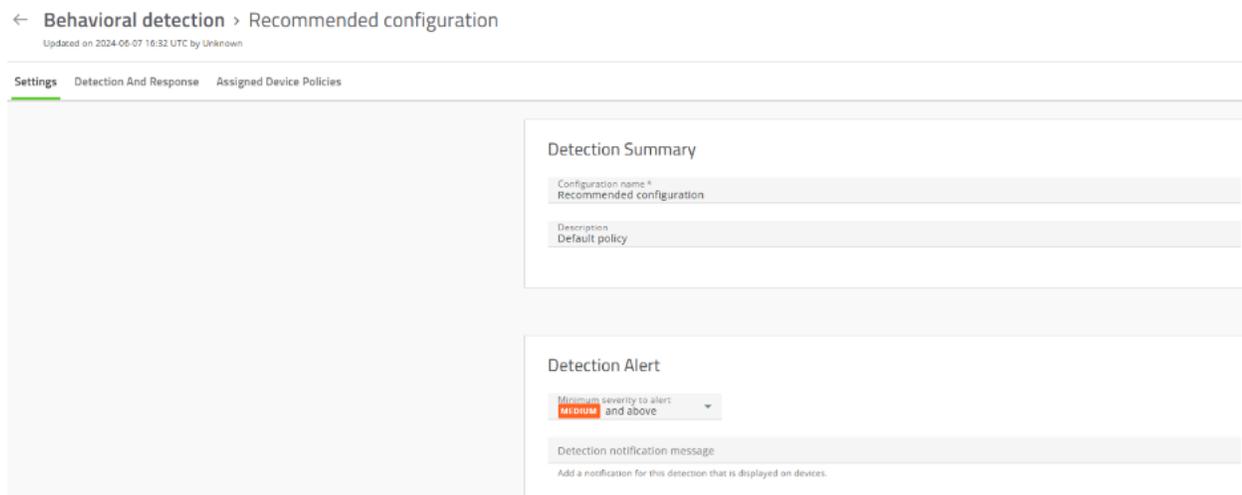
You can create a behavioral detection (BDE) policy from the CylanceOPTICS > Behavioral Detection Engine > Behavioral Detection Policies tab. Click "Add a detection configuration" to create a policy.

Specify this information:

- A name for the configuration.
- A description of the configuration.
- The alert threshold, which is the minimum severity for an alert to be generated and appear in the **Alerts** screen.
- The message to display on the user's device when a detection occurs.

You can configure these settings in the **Settings** tab when you edit a detection policy.

After you create the policy, you need to configure its detection and response settings, and then assign it to device policies.



Detection and response tab: Behavioral detection policy

After you create a detection policy, open the policy and configure the settings in the **Detection and Response** tab.

On the **Detection and Response** tab, on the left side of the screen, you can apply filters to help find the detection rules that you are looking for:

- Alerts (On or Off): Filter detection rules by whether detection alerts are enabled.
- Observations (On or Off): Filter detection rules by whether observations are enabled.
- Notifications (On or Off): Filter detection rules by whether notifications are enabled.
- Automated response action: Filter detection rules by the automated response action.
- Platform: Filter detection rules by operating system platform.



Execution (8)

The image shows three detection rule cards arranged horizontally. Each card has a title, a MITRE technique ID, a 'Rules' count broken down by severity level, and icons for alert, observation, notification, and response configuration. A lightning bolt icon indicates if any are configured.

Rule Name	MITRE ID	Alert	Observation	Notification	Response	Configured
Windows Management Instrumentatio...	T1047	1	2	1	0	None configured
Scheduled Task/Job	T1053	1	1	8	0	None configured
Command and Scripting Interpreter	T1059	14	15	21	10	Medium: 15

On the center of the screen, the detection rules are displayed as cards for specific MITRE techniques aligned from the MITRE framework. Each card includes the rule name, MITRE technique ID, the number of detections rules included at each severity level, and icons that indicate if alerts, observations, notifications and automated responses are configured. Bulk edit options appear above the cards if you use the checkboxes to select them.

You can click on a detection rule card to open a side panel on the right side. The side panel displays a detailed description of the rule as well as controls to enable alerts, observations, notifications, and automated responses.

DETECTION TECHNIQUE
×

Exploit Public-Facing Application

Enable detection alerts

Enable observations

Automated response 0 ^

Minimum severity to respond

HIGH

only
▾

+ ADD ▾

Detection Rules ^

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.

Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device

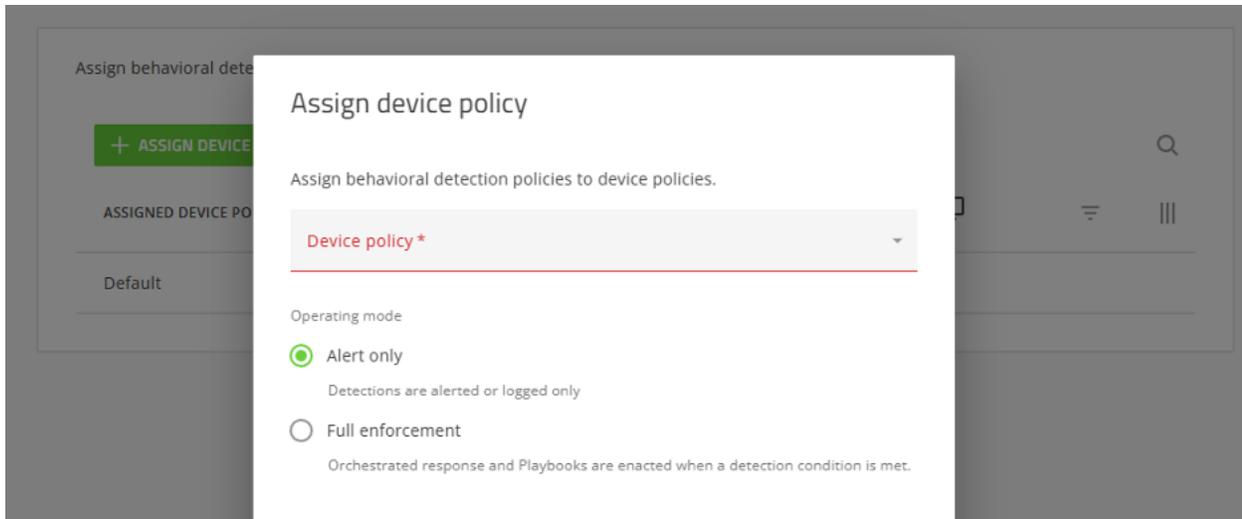
- Display Desktop Notification
- Dump Detection To Disk
- Log Off All Users
- Log Off Interactive Users
- Log Off Remote Users
- Log Off Users
- Suspend Process Trees
- Suspend Processes
- Terminate Process Trees
- Terminate Processes

If you want to configure automated responses for a detection rule, you must specify the minimum severity level for the response to apply. In this example, the default minimum severity is set to **High** because this class of rules are the most precise and the easiest to tune. This ensures minimal impact on business continuity due to the lower false positive rate average. Next, add one or more remediation actions from list of available actions. The CylanceOPTICS agent and BDE will take all applicable response actions that are configured based on the context of the detection.

Assigned device policy tab: Behavioral detection policy

After you create a detection policy, assign the BDE policy to device policies from **Assigned Device Policies** tab. Each device policy associated with a BDE policy will be listed by name and include the number of associated devices.

You can add device policies to associate them with the BDE policy. When adding a device policy, in the **Device policy** list field, you can select from the list the device policies that are available in the tenant. You can also specify the operating mode (**Alert only** or **Full enforcement**) which determines whether an alert triggers the automated responses. The operating mode for each device policy can be changed at any time from the **Policies > Device Policy** menu.



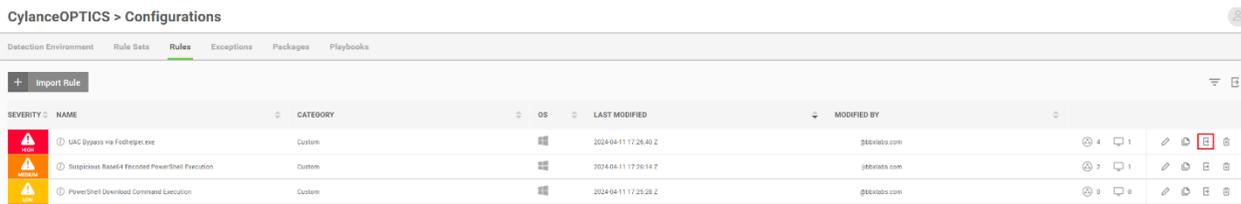
Importing custom rules

The Behavioral Detection Engine supports importing custom detection rules in .json format. In the Cylance console, you can import custom detection rules into custom rule groups from the **CylanceOPTICS > Behavioral Detection Engine > Custom Rules** tab. You can also export legacy rule sets in .json format and import them.

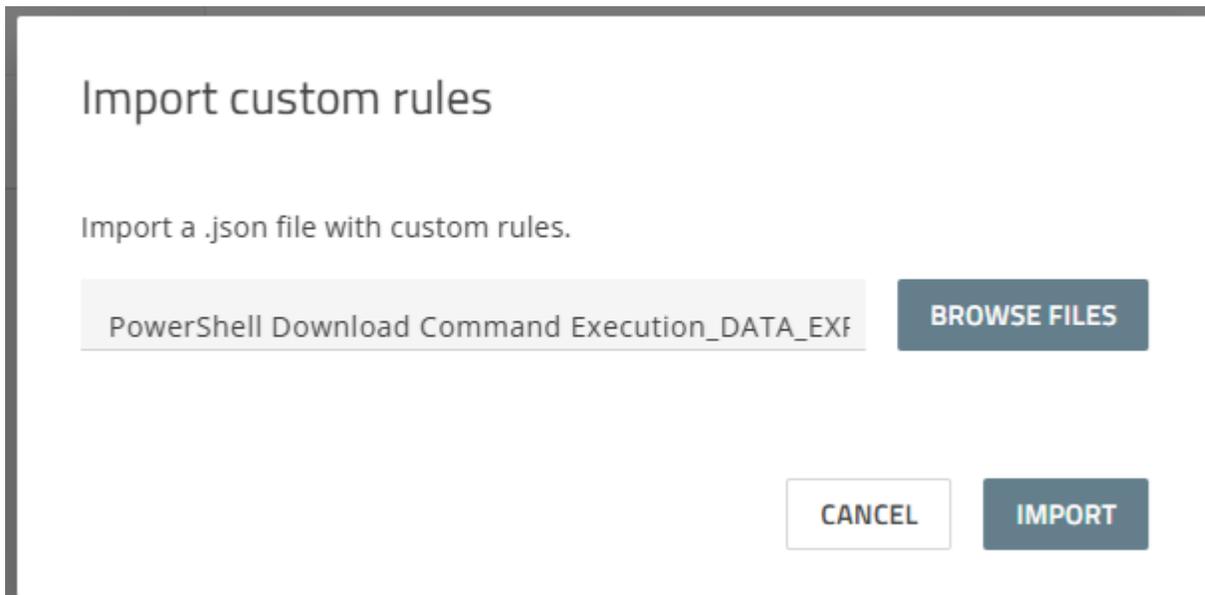
Before you import a custom detection rule, create a custom rule group. The custom rule group that you created appears as a card on the **Custom Rules** screen.

Use these steps to export the legacy rule sets from the Cylance console, create a custom rule group, and then import the legacy rule sets to the custom rule group:

1. Navigate to **CylanceOPTICS > Configurations > Rules**.
2. Beside the rule that you want to export, click **Export** and save the .json file with the rule conditions.



3. Navigate to **CylanceOPTICS > Behavioral Detection Engine > Custom Rules**.
4. In the **Custom Rule** tab, click **Add** and then add a new custom rule group.
5. Click the custom rule group, and then on the right side, click **Add > Import custom rules**, and specify the .json file.



6. Review the imported rule conditions, verify the target custom rule group, and then click **Validate**. After validation, click **Add** to complete the import.

General Information

Priority* **Low** Platform* Windows Custom rule group* imported custom rules

Custom rule name* PowerShell Download Command Execution

Description Detects the usage of native PowerShell download commands/techniques. Threat actors can use these techniques to download malicio

Custom Rule Details

[CONFIGURATION HELP](#)

```

1 {
2   "States": [
3     {
4       "Function": "{&fig}",
5       "HarvestContributingEvent": true,
6       "Name": "Invoke_WebRequest",
7       "Actions": [
8         {
9           "IterName": "InstigatingProcess",
10          "Type": "AOI",
11          "Position": "PostActivation"
12        },
13        {
14          "Type": "AOI",
15          "IterName": "TargetPowerShellTrace",
16          "Position": "PostActivation"
17        }
18      ],
19      "FieldOperators": {
20        "f": {
21          "OperandType": "String",
22          "Type": "ContainsAll",
23          "Options": {
24            "IgnoreCase": true
25          }
26        }
27      }
28    }
29  ]
30 }

```

CANCEL VALIDATE ADD

- On the **Behavioral Detection Engine** screen, open the **BDE policy > Detection And Response** tab where you can enable alerts, observations, and automated responses for your custom rules. The custom rule group will appear as a new card at the bottom of the **Detection And Response** tab when editing a BDE policy, under the **Custom rules** section.

Custom rules (5)

My Custom Rule Group 1

1 rule

Rules: 1 | 0 | 0 | 0

None configured

imported custom rules

1 rule

Rules: 0 | 0 | 1 | 0

None configured

Adding exceptions

In some cases, alerts may be triggered by legitimate business applications installed on your users' devices. If this occurs an exception is required to ensure business continuity and to prevent unnecessary alerts from being reported to the console.

Exceptions can be added in two ways:

- From the **CyalanceOPTICS > Behavioral Detection Engine > Exceptions** tab
- From the **Alerts** view

Regardless of where the exception was created, the **Exceptions** tab displays a list of all exceptions for the tenant, including the name, description, alert description, assignment, and the date the exception was last modified.

Adding exceptions from the Exceptions tab

You can add exceptions from the **CyalanceOPTICS > Behavioral Detection Engine > Exceptions** tab.

NAME	DESCRIPTION	ALERT DESCRIPTION	ASSIGNED TO	MODIFIED
Download Attempt via PowerShell (Windows)		Download Attempt via PowerShell (Windows)	Global	2025-02-10 20:58:22 UTC
Https File Modified (Windows)		Https File Modified (Windows)	Global	2025-01-28 02:01:00 UTC
Exfiltration to Test Storage Sites via Curl (Linux)		Exfiltration to Test Storage Sites via Curl (Linux)	Global	2025-01-28 02:00:49 UTC
Non-HTTPS Connection by script (Windows)		Non-HTTPS Connection by script (Windows)	Global	2024-11-11 20:37:56 UTC

When adding an exception from the **Exceptions** tab, specify the MITRE tactic and technique for which you want to create an exception along with an appropriate alert description.

Add exception

Add exceptions that can be assigned globally, to zones, to devices, or to device policies.

Tactic *
Exfiltration (TA0010)

Technique *
Data Transfer Size Limits (T1030)

Alert description

Search for alert descriptions

Transfer Smaller Files with Split (macOS)

Data Transfer Evasion via Split Command (Linux)

Next, specify one more conditions, including the artifact, facet, operator, and value for each condition.

Add exception

Settings Assigned To

Alert description: Transfer Smaller Files with Split (macOS)

Exception name *
Transfer Smaller Files with Split (macOS)

Description

Conditions

Artifact *
Target File

Facet *
Size

Operator *
Less than

Enter value. *
5

+ ADD

In the **Assigned To** tab, assign the exceptions appropriately using one of the options. For more information, see the next section on "Assigning exceptions globally, to zones, to devices, or to device policies" in this guide.

Adding exceptions from the Alerts view

If you observe an alert for a legitimate business application in the Alerts view, you can use AI to add exceptions. The details of the exception, including the conditions, are automatically defined by AI based on the alert.

To add an exception in the Alerts view, simply open the alert and use the **Actions** menu on the top right of the screen.

← Alerts > Account Manipulation via SSH Authorized Keys

+ ACTIONS

id	status	start	end	operator	exception time (UTC)
946e223-9e76-4829-8622-10c22f295...	NEW	75JAB2204-6219	linux	+	2025-02-28 12:54 UTC
27f196c1-e65e-416e-885c-78d6d043c...	NEW	75JAB2204-6219	linux	+	2025-02-28 12:54 UTC

In the **Add exception** dialog box, review the details of the exception, and then make changes if necessary.

Add exception

Settings Assigned To

Alert description: Account Manipulation via SSH Authorized Keys (Linux)

Exception name *
Account Manipulation via SSH Authorized Keys (Linux)

Description

Conditions

	Artifact * Target File	Facet * Path	Operator * Equals	Enter multiple values. * /etc/ssh/ssh_config...	X
And	Artifact * Instigating Process	Facet * Command Line	Operator * Equals	Enter multiple values. * ./usr/bin/dpkg --statu...	X
And	Artifact * Instigating Process Image File	Facet * Path	Operator * Equals	Enter multiple values. * ./usr/bin/dpkg	X
And	Artifact * Instigating Process Image File	Facet * SHA256 Hash	Operator * Equals	Enter multiple values. * F28D71534FD89C1F...	X

+ ADD

In the **Assigned To** tab, assign the exceptions appropriately using one of the options. For more information, see the next section on "Assigning exceptions globally, to zones, to devices, or to device policies" in this guide.

Assigning exceptions globally, to zones, to devices, or to device policies

Regardless of how you add a detection exception, you must specify how to assign them to devices. When configuring an exception, in the **Assigned To** tab, you can specify whether to assign the exceptions globally, to zones, to devices, or to device policies.

- Global: Applies the exception to your organization's entire tenant
- Zones: Applies the exception to the zones that you select and all devices assigned to those zones.
- Devices: Applies the exception to the selected devices
- Device Policies: Applies the exception to all devices that are assigned to the selected device policies

Add exception

Settings Assigned To

Assigned to *
Global

- Global
- Zones
- Devices
- Device policies

Managing detection rule updates

Cylance continues to develop CylanceOPTICS detection rules for new and emerging threats. To streamline the time to value, and minimize the overhead required to benefit from the new rules, we have automated the deployment process.

When updates are available for detection rules, a notification appears in the Cylance console on the **CylanceOPTICS > Behavioral Detection Engine** screen.



You can click the notification to view the details of each update available. For each update, you can expand it to view the changes, grouped by the detection technique. Knowledge base (KB) articles are available for more information about some of the updates.

A screenshot of a dialog box titled "Detection technique updates". The dialog contains the following text: "Accept updates to the detections for the following techniques. You must accept the updates to enable automated actions for these technique detections." Below this text is a list of four update entries, each with a date and an "ACCEPT" button with a dropdown arrow: "2024-05-16 UPDATES", "2024-06-12 UPDATES", "2024-08-13 UPDATES", and "2024-08-16 UPDATES". At the bottom right of the dialog are two buttons: "CANCEL" and "ACCEPT ALL".

Detection technique updates

Accept updates to the detections for the following techniques. You must accept the updates to enable automated actions for these technique detections.

2024-05-16 UPDATES ACCEPT ^

OS Credential Dumping

- Active Directory Database Snapshot Via ADEplorer (Windows)
- Active Directory Structure Export Via Ldifde.exe (Windows)

Windows Management Instrumentation

- Pass The Hash Toolkit (Linux)
- Application Removed Via Wmic.EXE (Windows)
- Application Terminated Via Wmic.EXE (Windows)

Hide Artifacts

- Hidden Directory or File Created (Linux)
- ADS File Creation (Windows)

As soon as an update is available, the new rules are automatically pushed to devices according to the BDE policy that is already assigned to those devices. Until the rules are accepted, the rules will operate in Alert Only mode. Users and devices will not be impacted due to potentially untuned false positives. This allows administrators to observe the performance and impact of the new rules, and provides an opportunity for any tuning or exception creation prior to accepting the rules and enforcing them. Enforcement means any defined automated responses are applied when the detection rule is triggered.

If business continuity issues arise at any point during enforcement, you can change the BDE policy to Alert Only mode to allow administrators to review alerts and tune their environments without impacting users before enforcing the rules again.

Viewing alerts

Alerts raised from the BDE will appear in the Cylance console on the **Alerts** screen. The initial Alerts view is a summary that groups similar alerts based on criteria such as priority, alert classification, configured responses, and other key alert attributes. Each alert has a priority, status, classification and sub-classification as well as a description and some key indicators. For more information about the data displayed in the **Alerts** screen, see [the Alerts documentation](#).

Alerts

Selected: 1 CHANGE STATUS ASSIGN ALERT CHANGE LABELS DELETE

Product is in CylanceOPTICS

PRIORITY	STATUS	CLASSIFICATION	SUB-CLASSIFICATION	DESCRIPTION	KEY INDICATORS	RESPONSE	COUNT			
HIGH	NEW	TA0003 Persistenc...	T1098 Account Ma...	Account Manipulation...			2	1	1	0
HIGH	NEW	TA0003 Persistenc...	T1098 Account Ma...	Account Manipulation...			1	1	1	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
HIGH	NEW	TA0002 Execution...	T1059 Command ...	Credential Dumping v...			1	1	0	0
MEDIUM	NEW	TA0005 Defense E...	T1070 Indicator R...	Bulk File Deletion via ...			1	1	1	0

On the **Alerts** screen, you can change the status of the alert, assign it for triage, add or edit labels, or delete the alert. You can click an alert group to display second level alert information, such as the individual alerts within the group, and use AI to generate an alert summary. You can use the **Actions** menu within the alert to create exceptions using AI to define the exception conditions automatically.

← Alerts > Account Manipulation via SSH Authorized Keys → ACTIONS

Overview

Alert Summary

Priority: **HIGH**

Account Manipulation via SSH Authorized Keys

Rule ID: 7268b3c-7a00-44f3-8baf-3ce4849d27af

Classification: T1098 Account Manipulation, TA0003 Persistence, TA0004 Privilege Escalation

Subclassification: T1059 Command Manipulation, T1098 Account Manipulation: SSH Authorized Keys

Product: CylanceOPTICS

sshManipulation File updated

target

ID	STATUS	ASSIGNEE	DETECTION TIME
0846f22f-5b19-482d-b...	NEW	T11182204-40f0	2025-02-20 12:54 UTC
37f18b61-e83e-444e-9...	NEW	T11182204-40f0	2025-02-20 12:54 UTC

Alert ID: 0846f22f-5b19-482d-b...-45c37026887

Alert Overview

Detection Time (UTC): 2025-02-20 12:54 UTC

Device: T11182204-40f0

IP address: 127.0.0.1, 127.0.0.1, 10.83.56.152, 4ef0-w79.80b-7745-w32762

Zone: linux

sshManipulation File updated

ID: 56e31657ae2-6c3b-86b6-328231-4937d

Occurred: 2025-02-20T12:54:41.721Z

Path: /etc/ssh/ssh_config.epig.new

Target

Best practice: Tuning your environment

1. As a best practice, start with assigning the default BDE policy to devices and monitor the alerts prior to enabling automated responses. During this observation period, identify any alerts triggered by legitimate business applications and then add exceptions for them so that business continuity can be maintained when you enable automated responses. You can easily add exceptions from the Alerts view using the **Actions** menu.
2. Continue to monitor and review all alerts with **High** severity to determine if additional exceptions are required to remove unwanted alerts. You can apply filters in the **Alerts** screen to quickly find these alerts. For example, click the **Product** column heading, and then filter for **CylanceOPTICS** alerts. By default, the alerts with the highest severity are displayed at the top of the filter results.
3. After the recommended observation period of seven to ten days has passed without any alerts triggered by legitimate business applications and no unwanted alerts, you are ready to enable automated responses and start enforcement.
 - If you want to enable automated responses for a detection technique, set the **Automated response severity** setting to **High only**. For the remediation actions, add **Display Desktop Notification**, **Log Off Remote Users** and **Terminate Process Tree**.
 - To start enforcement, edit the device policy to change the BDE policy operating mode from **Alert only** to **Full enforcement**.

Legal notice

© 2025 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, EMBLEM Design, ATHOC, and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Patents, as applicable, identified at: www.blackberry.com/patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at <https://www.blackberry.com/us/en/legal/third-party-software>

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

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada