Introduction

The CylancePROTECT Desktop Application for Splunk allows security professionals and administrators to monitor their organization for high-risk threats by consuming Cylance console data in their Splunk environment. This application allows users to effectively monitor, track, and analyze threat data and activity across their environment using preconfigured, but customizable, dashboard views and reports for Threat and Device Management. This application can be configured using real-time data and/or the once-daily Cylance Threat Data Report (TDR).

Index, Eventtypes, and Sourcetypes

The most important data classifiers are outlined below:

Index

• Following Splunk best practices, this application is no longer bundled with a pre-specified index, however, we strongly recommend sending data to index=cylance_protect. If the index was previously specified as index=protect, this will also work as the dashboards are populated using an eventtype that will accept either. If a custom index name is used, then the eventtype=cylance_index must be modified to accept the custom index name.

Eventtypes

• eventtype=cylance_index – eventtypes allows the index to either be protect or cylance_protect. If a custom index name is used, the eventtype must be modified for the dashboards to populate properly.

Sourcetypes

• syslog sourcetypes
  • syslog_protect
    • syslog_app_control
    • syslog_audit_log
    • syslog_device
    • syslog_device_control
    • syslog_exploit
    • syslog_optics
    • syslog_script_control
    • syslog_threat
    • syslog_threat_classification

  Note: Syslog events will enter the app as syslog_protect and will be sorted into one of the other “syslog_” source types, based on content.

• TDR sourcetypes
  • threat
  • device
  • threat_indicator
  • event
## Dashboards

Dashboards and panels within the application are populated using syslog and TDR data.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Heads up display using real-time syslog data</td>
</tr>
<tr>
<td>Threat Center</td>
<td>Contains real-time syslog and once-daily TDR dashboards for analyzing threats</td>
</tr>
<tr>
<td>Protection Center</td>
<td>Contains real-time dashboards for investigating exploits, script, app, and device control events</td>
</tr>
<tr>
<td>Operation Center</td>
<td>Contains real-time syslog and once-daily TDR dashboards for examining agent information</td>
</tr>
<tr>
<td>Optics</td>
<td>Contains real-time dashboards to display CylanceOPTICS syslog data</td>
</tr>
<tr>
<td>Searches and Reports</td>
<td>Preconfigured reports for issues such as duplicate devices, infected hosts, offline/online devices, and more</td>
</tr>
<tr>
<td>Tools</td>
<td>Indicator correlation and BlackBerry specific searching</td>
</tr>
<tr>
<td>Help</td>
<td>Threat Data Report (TDR) Configuration, data sources overview, and tenant login auditing</td>
</tr>
</tbody>
</table>
## System requirements

Please ensure your system meets the requirements listed below before installing the application.

<table>
<thead>
<tr>
<th>OS</th>
<th>This application has been tested with at least 4GB RAM and two or more CPU cores on the following x64 platforms:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Ubuntu 14.04</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 7.2 Server</td>
</tr>
<tr>
<td></td>
<td>• CentOS 7</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Splunk</th>
<th>This application has been tested with the following Splunk versions:</th>
</tr>
</thead>
</table>

Tip for Splunk Version / Installation:

• Not all Splunk versions interact with the app the same way. Using different browsers may help increase setup and navigation compatibility. For example, use Chrome for configuring TDR and Firefox to view menus:


| Network | Once-per day scripted inputs, such as threats.py, poll the Threat Data Report by connecting to the Threat Data Report URLs over port 443. Syslog event forwarding from your Cylance Tenant to your Splunk deployment requires network configuration in the management console and a firewall rule on the Splunk deployment or a log forwarder. Please refer to the SIEM and Syslog integration information at [https://support.blackberry.com/community/s/article/66572](https://support.blackberry.com/community/s/article/66572) |

## Installation

BlackBerry provides both an application and a technology add-on (TA). If the Splunk environment is an all-in-one, only the application needs to be installed since it contains both the visual and the data ingest components. If the Splunk environment is distributed, then the application should be installed on the search heads and the TA should be installed on the indexers and forwarders.

**Note:** If the once-per-day Threat Data Report data source is desired, the full app is required on at least one Heavy Forwarder because it uses inputs.

Application Download:

• [CylancePROTECT Application for Splunk](#)
• [CylancePROTECT TA for Splunk](#)

If this is the first time you are installing the app in this Splunk instance, then follow the steps below. In most cases, an application upgrade will work. However, if you run into issues upgrading the CylancePROTECT Desktop Application for Splunk, then follow the uninstall steps (outlined in the Uninstallation section) before installing the latest version of the app.
After you have downloaded CylancePROTECT Desktop Application for Splunk via Splunkbase, the installation of this app follows the normal app install procedure of either manually unpacking the package (.tar.gz) or using Splunk Web Manage Apps.

**Note:** If you run Splunk in a distributed setup, you must install the CylancePROTECT Desktop Application for Splunk on a single Heavy Forwarder in addition to the search heads. The search heads should only have the Splunk Web enabled (GUI visible) and do not require the inputs because the Heavy Forwarder should have the inputs enabled.

**Tip for Splunk Version / Installation:**
- Not all Splunk versions interact with the app the same way. Using different browsers may help increase setup and navigation compatibility. For example, use Chrome for configuring TDR and use Firefox to view menus:

**Installing using Splunk Web**

Use the Splunk Web App Manager and Install app from the Splunk app Store or download .spl file.

1. In the Splunk Web App Manager, Click the Splunk app Store.
2. Install the Splunk app.

  **Note:** You can also download the .spl file.

**Installing Manually**

**Manually Unpacking the Package (.spl == .tar.gz)**

**Linux Package**

**Note:** By default, $SPLUNK_HOME is located at: /opt/splunk

- Copy the cylance_protect-<version>.spl to $SPLUNK_HOME/etc/apps
- $ tar xvf cylance_protect-<version>.spl
  - A cylance_protect folder is created in $SPLUNK_HOME/etc/apps
  - Verify that the app files and folders have the appropriate owner and permissions e.g. Splunk user and group, and read/write/execute where applicable

**Windows Package**

**Note:** By default, $SPLUNK_HOME is located at: c:\program files\splunk

- Copy the cylance_protect-<version>.spl to $SPLUNK_HOME\etc\apps
- Use a program such as 7zip to unpack cylance_protect-<version>.spl
  - A cylance_protect folder is created in #SPLUNK_HOME\etc\apps

**Configure the index**

In accordance with Splunk best practices, this application does not create an index by default (the app is not distributed with a ./default/indexes.conf file).

After installing this app, the Splunk administrator should make sure the index is set up correctly. There are two scenarios:

**Installing for the First Time**

Immediately after installation, there will be no app-specific index, so you should create one using Splunk Web > Settings > Indexes. It is recommended to use the index name: cylance_protect.
Next, you should confirm in **Splunk Web > Settings > Event Types** that the entry cylance_index search string is search = index=protect OR index=cylance_protect.

**Note:** This app uses eventtypes to drive the dashboard searches and a macro to define the index. Both can be checked using the Splunk UI with the following: In **Splunk Web > Settings > Event Types**, the entry cylance_index search string is: cylance_index and the macro under **Splunk Web > Advanced Search > Search Macros** that search string is: search = index=protect OR index=cylance_protect.

**Upgrading**

In the case of an upgrade, there should be an existing index, and the existing config files in local should contain the correct name, and therefore no specific steps need to be taken.

It is recommended to check for any local files that may have been created for previous installations, as they will override defaults.

For example, the following local (default.xml) file will override any menus provided in new releases. Delete this file and restart the Splunk search head to see any new menus and dashboards.

```
$SPLUNK_HOME/etc/apps/cylance_protect/local/data/ui/nav/default.xml
$SPLUNK_HOME/bin/splunk restart
```

**Data sources**

This application can simultaneously consume data from the management console via real-time syslog and/or once per day Threat Data Reports (TDR). The preference for you will most likely be to consume real-time data so they can act upon it in a timely fashion. TDR is intended to be a backup for those that cannot consume syslog or wish to have backward compatibility with previous versions of this application. The sections below will explain how to forward syslog and TDR data.
Configure Syslog

The CylancePROTECT Desktop Application for Splunk has the ability to consume real-time syslog data from the management console. To get these events flowing into Splunk, Syslog forwarding needs to be enabled and configured within Splunk and the management console.

Architecture

Your architecture may vary depending on the location of Splunk, but these are common scenarios:

Management Console To Cloud (including Splunk Cloud)

Note: When you deploy the app to an On-Premises Splunk instance, you have the option to send data directly from the management console to indexers on the Internal network. However, from a security perspective, it is often not advisable to allow traffic from the Internet into the internal network without first going through the DMZ.
**Splunk settings**

**Note Regarding Syslog Over SSL**

Sending data over encrypted protocols is recommended, when possible. Cylance and Splunk can communicate syslog data using plain-text and over SSL. For more information about how to configure forwarding, see the Splunk documentation at: [https://docs.splunk.com/Documentation/Splunk/6.6.1/Security/ConfigureSplunkforwardingtousesignedcertificates](https://docs.splunk.com/Documentation/Splunk/6.6.1/Security/ConfigureSplunkforwardingtusesignedcertificates)

To see instructions that work in BlackBerry’s development environment, please see Appendix: configure Syslog over SSL in Splunk in Appendix A.

Unencrypted syslog input is not recommended; however, for troubleshooting purposes, it can be enabled on a port other than 6514. You can enable Syslog in Splunk Web in Settings > Data Inputs > Local Inputs > TCP. Enable TCP Port 6515.

**Note on Multi-Tenant Configurations and Syslog**

Each tenant will require its own stanza in inputs.conf, and each tenant requires its own port. For example, if there are two tenants, CompanyOne and CompanyTwo, inputs.conf should contain:

```plaintext
[tcp-ssl://6514]
disabled = false
sourcetype = syslog_protect
source = CompanyOne
index = cylance_protect
```

```plaintext
[tcp-ssl://6515]
disabled = false
sourcetype = syslog_protect
source = CompanyTwo
index = cylance_protect
```

**BlackBerry tenant settings**

1. In the console, go to Settings and Scroll down to Syslog/SIEM.
2. Check the box for Syslog/SIEM.
3. Check all boxes for Event Types.
4. Select Splunk from the SIEM drop-down.
5. Select TCP for the Protocol.
6. Check the TLS/SSL box if setting up Splunk to receive syslog data over SSL.
7. Enter the IP/FQDN of your forwarder or Splunk instance for IP/Domain.
8. Select the Port.
9. Click Save.
Verify configuration of Syslog

You can now perform a basic test to verify that CylancePROTECT Desktop is forwarding syslog messages to the Splunk app:

- In the Splunk Search bar, with the time set to the Real-time one-minute Window, run the following query:
  `eventtype=cylance_index sourcetype=syslog`
- In the console, go to Settings > Application
- Under Syslog/SIEM, in the Integrations section, click the Test Connection button. You should see a green popup with a message: Connection was successful
- In Splunk, below the search bar in the results part of the page, an event should appear which contains the text: CylancePROTECT---Test Connection Message

All of the provided syslog dashboards should begin populating as events occur.

In addition, by adhering to the Common Information Model, the CylancePROTECT Desktop Application for Splunk provides the console syslog data that is ready for integration with other Splunk apps such as the Splunk for Enterprise Security app.
Configure threat data report

This section is optional and provides insight into retrieving CylancePROTECT Desktop data only once per day, as opposed to the syslog data feed, which is real-time. For those that cannot consume syslog data (or want both data sources), the CylancePROTECT Desktop Application for Splunk provides the Threat Data Report-based sourcetypes, such as threats and devices.

To enable data of these sourcetypes, you will need to configure your app to match your Cylance console settings, such as the Threat Data Report download URL and the current Threat Data Report token.

To configure tenants, go to the application’s Help menu and select Configure TDR, which should take you to the following URL: http://<IP>:<PORT>/en-US/app/cylance_protect/ConfigureTDR

Tenant information is available in the console on the Settings/Application page, using the information below.

Cylance Console Settings/Application page

For Tenant Name, use the text to the right of Company: shown in the Cylance console.

For token, look in the Integrations section, check the Threat Data Report checkbox (if it is not already checked), and copy or generate/copy the token.
Note on Token Regeneration

If an administrator deletes or regenerates the Threat Data Report token after you have set the above token, you must update the TDR configuration page with the new token.

Note on Tenant Removal

When a tenant is deleted in the Configure Tenants page, all the data associated with the tenant is permanently removed from the app. This data includes entries in password.conf, indexed data, and files (.csv and .sha) in the local directory for the app. If this tenant were to be added back to the app in the future, then all the Threat Data would be restored (Threat Data Reports include a tenant’s complete history). In a distributed configuration, ensure that the .csv and .sha files (in the local directory for the app) have been deleted before you add the same tenant name back into the app.

Note: In contrast, syslog data would only start accumulating data in the app from the point at which the newly configured tenant’s syslog is enabled in the app.

For your specific download URL value, please refer to New Threat Report which has URLs for threats, devices, events, indicators, and cleared. All you need is the base URL, which is common to each of the URLs (for example, https://protect.cylance.com/Reports/ThreatDataReportV1)

Note: The base URL should not end with a slash (/), and the Chrome web browser seems to work best in the TDR setup screen. The SPLUNK_HOME Environment variable must be set to the Splunk installation location.

Enable threat data report

After you restart Splunk, the CylancePROTECT Desktop Application for Splunk will now appear in your Splunk instance.

In a single-instance Splunk installation or on a Heavy Forwarder, you will need to enable inputs, which are disabled by default:

1. In the Splunk menu, click Settings > Data inputs.
2. In the Data section, in Local inputs, click Section > Scripts.
3. For each of the scripts (devices, events, indicators, and threats), in the Status column, click the Enable link.

   Note: When you click on the Enable link, Splunk will invoke the associated script, and thereafter Splunk will repeatedly invoke the script according to the interval setting for that script, which is 24 hours by default.
Configure adaptive response

The CylancePROTECT Desktop Application for Splunk is part of Splunk’s Adaptive Response (AR) program. This means users with sufficient Splunk privileges can act on Cylance-protected hosts from the Splunk console. While this capability provides fast and convenient response actions, there is also some risk when operated by uninformed, but well-meaning, security personnel. This capability should be restricted using Splunk’s included Role-Based Access Controls (RBAC).

Functionality and usage

The API Connector dashboard default functionality is shown below, along with the required argument. The Global Whitelist and Blacklist will have a profound effect on CylancePROTECT Desktop Agents, since any hash and corresponding binary found on the Global Blacklist will be acted upon, even if the policy for the Agents are alert-only.

<table>
<thead>
<tr>
<th>Function</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Global Whitelist</td>
<td>N/A</td>
</tr>
<tr>
<td>Get Global Blacklist</td>
<td>N/A</td>
</tr>
<tr>
<td>Add to Global Whitelist</td>
<td>SHA256</td>
</tr>
<tr>
<td>Add to Global Blacklist</td>
<td>SHA256</td>
</tr>
<tr>
<td>Delete from Global Whitelist</td>
<td>SHA256</td>
</tr>
<tr>
<td>Delete from Global Blacklist</td>
<td>SHA256</td>
</tr>
</tbody>
</table>

HTTP responses

If the task from the API Connector reaches the BlackBerry cloud tenant, it will always display confirmation in the form of an HTTP response. The most common response codes, and their meanings, are shown in the table below.

<table>
<thead>
<tr>
<th>Response</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request – Check configuration and try again</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized – Check setup file for proper credentials</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden – Check the BlackBerry Tenant integration application for proper permissions</td>
</tr>
<tr>
<td>404</td>
<td>Not Found – Resource does not exist</td>
</tr>
<tr>
<td>500</td>
<td>Internet Server Error – Check configuration and try again</td>
</tr>
</tbody>
</table>
If an error occurs that is outside the normal response codes, it should be accompanied by a descriptive error message, such as the one shown below.

<table>
<thead>
<tr>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP STATUS CODE: 409</td>
</tr>
<tr>
<td>HTTP RESPONSE: &quot;There's already an entry for this threat.&quot;</td>
</tr>
</tbody>
</table>

Set up the Cylance Console

The Adaptive Response features within the CylancePROTECT Desktop Application for Splunk rely on sufficient access to the BlackBerry Cloud API.

1. Log in to the console as an administrator.
2. Click **Settings > Integrations**.
3. Click **Add Application**, then type and select the following:
   - Application Name: Splunk API Connector
   - Global List: Select Read, Write, and Delete
4. Click **Save**.
5. Copy and save the Application ID, the Application Secret, and the Tenant ID. These will be used later.

Set up the CylancePROTECT Desktop Application for Splunk

Setup in Splunk requires command-line access due to the need to edit the api.py configuration file.

1. On the desired search head, edit the api.py configuration file found here: `$SPLUNK_HOME/etc/apps/cylance_protect/bin/api.py`
2. Line 9-12 must be populated with the Cylance console information (obtained in the Cylance Console Setup steps).
3. In the CylancePROTECT Desktop Application for Splunk, select **Tools > API Connector**.
4. Select a Function using the drop-down menu. Example: Add to Global Blacklist.
5. Enter the file hash as the Parameter.
6. Click Submit. Check the Result information to see the HTTP responses from the Cylance console.

Note: If API calls fail after editing the api.py configuration file, the *.pyc files may need to be deleted in the following directory: $SPLUNK_HOME/etc/apps/cylance_protect/bin/

Restrict access to the API connector

To restrict access to the API connector, you can create a role in the console and set permissions in Splunk. If an SOC or IR role exists within Splunk, you can skip this section.

1. Under Users and Authentication, click Settings > Access Controls.
2. Next to Roles, click Add New.
3. For the Role Name, type CylanceAPI.
4. With the proper role created, you can set permissions for the role. On the Dashboard, click Settings > All Configurations
5. In the search field, type api_connector, then click Search.
6. Under Sharing, click Permissions. The role permissions display.
7. For the Everyone role, make sure Read and Write are not selected.
8. For the CylanceAPI role, make sure Read is selected. If the role name is different, make sure Read is selected for that role.
9. Click Save.
Removing the CylancePROTECT Desktop Application for Splunk

To remove an installed CylancePROTECT Desktop Application for Splunk from your Splunk instance, follow the steps below. In each of the cases below, you need to restart Splunk to complete the removal.

**Note:** You may choose to either delete or retain the existing log files for the application. The log files are stored at <opt/splunk/var/log/splunk/cylance.log>

### Remove application only and leave data intact

Use the commands below to remove the application but leave the log files intact. If you reinstall the application, the previously indexed data is accessible.

**Linux**

```
./splunk remove app [appname]
```

**Windows**

```
splunk remove app [appname]
```

**Note:** If you reinstall the application, the previously indexed data is available again.

### Remove application and data

**Note:** Index names below will most likely be protect or cylance_protect.

| Linux | 1. Remove data: ./splunk remove index <Your Index Name>  
2. Remove app: ./splunk remove app [appname] |
|-------|------------------------------------------------------|
| Windows | 1. Remove data: splunk remove index <Your Index Name>  
2. Remove app: splunk remove app [appname] |

**Note:** If you reinstall the application, the previously indexed data is available again.

### Disable application

Instead of removing the application, you can temporarily deactivate it. In the commands below, use `cylance_protect` for appname.

To disable the application:

```
./splunk disable app [app_name] -auth <username>:<password>
```

To re-enable the application, use the above command, but replace `disable` with `enable`. 
Data source types

Syslog Events
The Syslog-based source types for the CylancePROTECT Desktop Application for Splunk provide real time information on threats, devices, threat classifications, memory protection, application control, and audit log (script control events are not yet supported). The Syslog source types below for this application adhere to the Splunk CIM and provide the ability to integrate with other Splunk enterprise applications.

<table>
<thead>
<tr>
<th>Application Control</th>
<th>Syslog will report any events detected on devices with Application Control enabled, including denied attempts to create or modify applications, or to execute files from a network or external location.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Log</td>
<td>Syslog will report all user actions performed on the Cylance console by administrators, zone managers, and users.</td>
</tr>
<tr>
<td>Devices</td>
<td>Syslog will report devices that have been registered, modified, or removed.</td>
</tr>
<tr>
<td>Device Control</td>
<td>Syslog will report device control events like the device type, vendor ID, and product ID.</td>
</tr>
<tr>
<td>Memory Protection</td>
<td>Syslog will report any malicious processes and exploits that were detected and/or blocked by Memory Protection.</td>
</tr>
<tr>
<td>Script Control</td>
<td>Syslog will report all scripts that ran or attempted to run.</td>
</tr>
<tr>
<td>Threats</td>
<td>Syslog will report any newly found threats in your environment as well as any changes observed for existing threats.</td>
</tr>
<tr>
<td>Threat Classifications</td>
<td>Syslog will report any newly classified threats or changes to existing threat classifications (as made by the Threat Analysis Team).</td>
</tr>
</tbody>
</table>

Threat Data Report
The Threat Data source types for the CylancePROTECT Desktop Application for Splunk are extracted from the CylancePROTECT Desktop Threat Data Report, which provides all details and information pertaining to threats and devices in your environments. The Threat Data source types below adhere to the Splunk Common Information Model (CIM).

<table>
<thead>
<tr>
<th>Threats</th>
<th>The Threats script reports all threats that have been detected in your environment, along with relevant information such as file name, file hashes, file status, Cylance Score, classification, file path, device it was detected on, first and last found date, etc. Fields conform to the Malware data model in Splunk’s CIM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices</td>
<td>The Devices script reports all CylancePROTECT Desktop registered devices in your organization, along with each device’s operating system, agent version, device policy, zones it belongs to, MAC address, IP address, last reported user, date it was added, status (online or offline), total files analyzed, etc. Fields conform to the Inventory data model in Splunk’s CIM.</td>
</tr>
<tr>
<td>Indicators</td>
<td>The Indicators script reports each threat (with a unique SHA256 hash) and all associated threat indicators that characterize the file. See <a href="https://support.blackberry.com/community/s/article/66181">https://support.blackberry.com/community/s/article/66181</a> for more information on threat indicators.</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Events</td>
<td>The Events script will report all threat events that occurred in your organization for the last 30 days. This information includes the file hash, the device name, file path, the date and time it was found, the threat status, and Cylance Score.</td>
</tr>
</tbody>
</table>
Troubleshooting

The following are recommendations for troubleshooting the CylancePROTECT Desktop Application for Splunk.

**Troubleshoot Syslog consumption**

Troubleshoot the Cylance Splunk Syslog data if the dashboards do not populate.

1. If in a distributed Splunk environment, ensure that you are configuring syslog consumption on the Forwarder and that the Splunk environment is running version 6.2 or higher.
2. Ensure the latest version of the app is installed on the Splunk Search Head. Ensure the matching version of the TA is installed on Indexers and Forwarder.
   
   **Note:** If the Threat Data Report (TDR) is desired, a Heavy Forwarder will be required due to scripted inputs.
3. Ensure the index name is either `cylance_protect` (preferred) or `protect` to match the inputs.conf file.
4. Ensure the incoming sourcetype defined in inputs.conf is `syslog_protect`.
5. Ensure eventtypes.conf has not been altered since this populates the dashboards. Then ensure that the macro `cylance_index` has not been altered as this needs to search the index that contains Cylance data – usually `cylance_protect` or `protect`.
6. Go to Splunk search box, select All Time, then type: `eventtype=cylance_index sourcetype=syslog*`
   
   **If no data is returned (example: no results found for this particular query):**
   a) Click Test Connection hyperlink in the BlackBerry tenant. You should see Test Connection Successful.
   b) Ensure port is open to receive syslog data. For example, assuming 6514 is being used, `netstat -an | grep 6514`.
   c) Ensure no network or host firewalls are blocking traffic. Layer 7 firewalls may need to be told to expect TLS/SSL traffic.
      • Use a packet sniffer such as Wireshark to verify the connection is made and data is passed.
      • If using a syslog daemon to write the data to a file first, ensure data is being written to the file.
      • Go to Splunk search box select All Time, then type: `eventtype=cylance_index sourcetype=syslog*`
   
   **If data is returned but is illegible (example: boxes instead of text):**
   a) Ensure TLS matches in tenant and Splunk. For example: TLS/SSL checkbox is checked in the BlackBerry tenant and `tcp-ssl` is used in the Splunk inputs.conf file.

   **If only syslog_protect data is returned and no other sourcetype (examples: syslog_app_control, syslog_audit_log, or syslog_devices):**
   a) Ensure the app is installed on the forwarder and search head so the props.conf and transforms.conf take effect and properly rename `sourcetype=syslog_protect` to another sourcetype name, based on the content of the event.

**Troubleshoot threat data report (TDR) consumption**

If the TDR (non-syslog) dashboards do not populate

1. If in a distributed Splunk environment, ensure that you are configuring TDR consumption on a Heavy Forwarder that is running the full CylancePROTECT Desktop Splunk application (not just the TA), and that the Splunk environment is running 6.2 or higher.
2. Ensure the latest version of the application is installed on the Splunk Search Head. Ensure the matching version of the TA is installed on Indexers.

3. Ensure the index name is either cylance_protect (preferred) or protect to match the inputs.conf file.

4. Ensure eventtypes.conf has not been altered since this populates the dashboards. Then ensure that the macro cylance_index has not been altered as this needs to search the index that contains BlackBerry data – usually cylance_protect or protect.

5. Go to Splunk search box, select All Time, then type: `eventtype=cylance_index sourcetype=syslog*`

6. You should see JSON data, possibly with a sourcetype of device, threat_indicator, etc.

   **If no data is returned (example: No results found for this particular query):**
   
   a) From the command line: check the cylance_protect/ local directory for the presence of CSV and SHA files. For example: `<TenantName>-event.csv` or `<TenantName>-indicators.sha`.

   **If the CSV and SHA files are present:**
   
   a) Check defaults/inputs.conf for the index name that the scripted inputs are using.
   b) Ensure that index exists and search on just that index name from the Splunk search bar.

   **If the CSV and SHA files are not present:**
   
   a) Is the Splunk instance behind a proxy or firewall that could be blocking connectivity?
   b) If so, can you whitelist this host to the BlackBerry Tenant URL?
   c) Run the test.py script using the instructions below.

**Log examination**

In case of issues, such as when the post install test does not result in observable output, then you will need to examine splunkd.log and cylance.log files in the `$SPLUNK_HOME/var/logs/splunk` directory.

To generate more detailed log data, edit the log level in the config.py file (about line 54) in the bin directory (requires command-line access). For example, change:

```python
self.log_level = 'WARNING'
```

to

```python
self.log_level = 'DEBUG'
```

**Available Log Levels**

- DEBUG
- INFO
- WARNING
- ERROR
- CRITICAL, FATAL

The default is WARNING. DEBUG will report on most events (generates many log messages) and CRITICAL (same as the level FATAL) will report only the most severe of events (generates few log messages).

To control various aspects of log file generation, you can configure parameters in the config.py:

- Filename – Default is cylance.log
- Level – Described above
- Size – Default is 1000000 (i.e. one million bytes or one megabyte). When the file size exceeds this number, a new log file is created (i.e. logging rotates to a new log file).
- Rotations – How many log files will be created before the oldest is overwritten.
Support

BlackBerry supports the CylancePROTECT Desktop Application for Splunk, but does not support Splunk-specific troubleshooting. An existing, healthy Splunk environment is assumed. For more information about the CylancePROTECT Desktop Application for Splunk, visit support.blackberry.com/community to read article 66726.

You can open a BlackBerry Support ticket for assistance. For information about how to create a BlackBerry Support ticket using the BlackBerry myAccount Support portal, visit support.blackberry.com/community to read article 68846.

Request guidelines

To expedite handling of your email (feature enhancement, feature request, bug), please supply the following information:

1. Splunk App version (look in app.conf)
2. Splunk version (e.g. Splunk Enterprise 6.3.3)
3. OS and version
4. Company name
5. Description of the feature, feature enhancement (and how to invoke it, e.g. the menu items clicked to arrive at a dashboard), or the bug (how to reproduce the issue and describe the expected behavior versus the actual suspected erroneous behavior)
6. Supporting information: screenshot(s), log file(s)
7. Results of the Troubleshooting section.
Appendix: configure Syslog over SSL in Splunk

Configure syslog over SSL in the Splunk app.

Linux Splunk 6.5.0 and newer

Note: sslRootCAPath was moved to server.conf.
The following instructions work for generating our own certs.

Generate certs

```
mkdir /opt/splunk/etc/certs
export OPENSSL_CONF=/opt/splunk/openssl/openssl.cnf
/opt/splunk/bin/genRootCA.sh -d /opt/splunk/etc/certs
/opt/splunk/bin/genSignedServerCert.sh -d /opt/splunk/etc/certs -n splunk -c
  splunk -p
```

Modify configuration files

```
$SPLUNK_HOME/etc/apps/cylance_protect/local/inputs.conf:
[tcp-ssl://6514]
disabled = false
sourcetype = syslog_protect
index = cylance_protect
source = <YourTenantNameHere>

[SSL]
serverCert = /opt/splunk/etc/certs/splunk.pem
sslPassword = <The password that was used in the genSignedServerCert command above>
requireClientCert = false
```

Restart Splunk and verify open port

```
$SPLUNK_HOME/bin/splunk restart splunkd
netstat -an | grep :6514
```

Linux Splunk versions prior to 6.5.0

Note: RootCA was specified in inputs.conf and not server.conf.

Generate certs

```
mkdir /opt/splunk/etc/certs
export OPENSSL_CONF=/opt/splunk/openssl/openssl.cnf
/opt/splunk/bin/genRootCA.sh -d /opt/splunk/etc/certs
```

| Appendix: configure Syslog over SSL in Splunk | 24 |
/opt/splunk/bin/genSignedServerCert.sh -d /opt/splunk/etc/certs -n splunk -c splunk -p

Modify configuration files

$SPLUNK_HOME/etc/apps/cylance_protect/local/inputs.conf:
[tcp-ssl://6514]
disabled = false
sourcetype = syslog_protect
index = cylance_protect
source = <tenant name>

[SSL]
rootCA = $SPLUNK_HOME/etc/certs/cacert.pem
serverCert = $SPLUNK_HOME/etc/certs/splunk.pem
password = <The password that was used in the genSignedServerCert command above>

Restart Splunk and verify open port

$SPLUNK_HOME/bin/splunk restart splunkd
netstat -an | grep :6514

Windows Splunk 6.5.0 and newer

Note: sslRootCAPath is ignored in Windows. Instead use: caCertFile.
The following instructions work for generating our own certs:

Generate certs

mkdir c:\progra~1\Splunk\etc\certs
C:\progra~1\Splunk\bin\splunk.exe cmd cmd.exe /c c:\progra~1\Splunk\bin
\genRootCA.bat -d c:\progra~1\Splunk\etc\certs
C:\progra~1\Splunk\bin\splunk.exe cmd python c:\progra~1\Splunk\bin
\genSignedServerCert.py -d c:\progra~1\Splunk\etc\certs -n splunk -c splunk -p

Add the following to C:\Program Files\Splunk\etc\apps\cylance_protect\local\inputs.conf

[tcp-ssl://6514]
disabled = false
sourcetype = <syslog_protect>
index = cylance_protect
source = <YourTenantNameHere>
[SSL]
sslPassword = <The password that was used in the genSignedServerCert command above>
requireClientCert = false
serverCert = c:\progra~1\Splunk\etc\certs\splunk.pem

Restart Splunk and verify open port

c:\progra~1\Splunk\bin\splunk.exe restart
netstat -an | findstr :6514
Legal notice

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE 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.

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 QUALITY, 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 http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

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