Cylance Extension for QRadar
Install Guide
**Product:** Cylance Extension for QRadar

**Document:** This guide is a succinct resource for analysts, administrators, and customers who are reviewing or evaluating the product.

**Document Release Date:** v1.0 rev2, February 2020

**About BlackBerry Cylance®:** BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees’ home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.

**Copyright:** © 2020 BlackBerry Cylance Inc. All Rights Reserved.

**Global Headquarters**
400 Irvine Spectrum Drive, Irvine, CA 92618

**Professional Services Hotline**
+1-877-97DEFEND • +1-877-973-3336

**Corporate Contact**
+1-914-CYLANCE • +1-914-295-2623

**Email**
sales@cylance.com

**Website**
https://www.cylance.com

**To Open a Support Ticket**
https://support.cylance.com — Click on Submit a Ticket

**To View Knowledge Base and Announcements**
Login to https://support.cylance.com

**To Request a Callback from BlackBerry Cylance Support**
+1-866-699-9689
Notice

The Cylance Extension for QRadar is provided "as is," and its use is solely at the user's own risk. Cylance does not warrant that the Cylance Extension for QRadar will meet the user's requirements or that its operation will be uninterrupted or error free or secure. To the extent permitted under applicable law, Cylance disclaims all representations and warranties, express, implied, and statutory, concerning the application, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, and any statutory warranties of non-infringement. In no event shall Cylance be liable to the user for any loss or damage for lost profits or revenues, or lost data or similar economic loss, regardless of how such loss or damages are characterized, or for any consequential, special, incidental, indirect or punitive damages, arising out of use of the Cylance Extension for QRadar. To the maximum extent permitted under applicable law, in no event will Cylance's total, aggregate liability to the user, related to use of the application, exceed the amount of direct damages actually incurred by the user up to the total amounts paid by user to Cylance; or if no amounts are paid to Cylance, one hundred dollars ($100). Any statements regarding adherence to the Common Information Model are provisionary.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>3</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>4</td>
</tr>
<tr>
<td>Cylance Extension for QRadar</td>
<td>6</td>
</tr>
<tr>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Requirements</td>
<td>7</td>
</tr>
<tr>
<td>Contents</td>
<td>7</td>
</tr>
<tr>
<td>Installation</td>
<td>8</td>
</tr>
<tr>
<td>Log Source</td>
<td>8</td>
</tr>
<tr>
<td>Dashboard</td>
<td>8</td>
</tr>
<tr>
<td>Appendix</td>
<td>10</td>
</tr>
<tr>
<td>Appendix</td>
<td>11</td>
</tr>
</tbody>
</table>
Introduction

The Cylance Extension for QRadar enables SIEM administrators to parse SYSLOG events from both CylancePROTECT and CylanceOPTICS. The extension includes custom fields and event mapping. It supports SYSLOG and TLS SYSLOG protocols.

Requirements

The Cylance Extension for QRadar has been tested on QRadar version 7.3.1 only. Cylance cannot guarantee the extension will work on other versions of QRadar.

Contents

The Cylance Extension for QRadar contains the following custom content:

- Reports (1)
- Logos (1)
- Saved Searches (12)
- Accumulator References (12)
- Dashboards (1)
- Regex Properties (44)
- Property Expressions (48)
- Log Source Extensions (1)
- Log Sources (1)
- Log Source Categories (1)
- Log Source/Protocol Mappings (34)
- Log Source Types (1)
- QID Records (86)
- DSM Event Mappings (86)
Installation

To install the Cylance Extension for QRadar:

1. In QRadar, navigate to the Admin tab.
2. Open Extension Management.
3. In the Extension Management window, click Add.
4. Click Browse, choose the downloaded extension file, then click Open.
5. Select the Install Immediately option.
6. Click Add.
7. When the install screen displays, select Replace existing items, then click Install.
8. When the install completes, click OK.

Log Source

This extension comes with a log source for Cylance. It is configured for a SYSLOG (non-TLS) feed. To use this log source, you must enable it and configure the Log Source Identifier.

Dashboard

After installation is complete, you may need to add the Cylance dashboard to the appropriate User Roles so users who are not in the Admin role can see the dashboard.

Note: There is a known bug that may cause some of the saved searches to lose their accumulated data settings. If you find that some of the dashboards are not populating, try the following to correct the problem.

1. Find the dashboard item that is not loading and click the Settings button.
2. Select Capture Time Series Data, then click Save.
3. Refresh the browser page.
   Note: The browser cache might need to be cleared.
No results were returned for this item.
Appendix

The following is a list of the custom properties that are included in this extension.

- Agent Version
- Auto Run
- Cylance Score
- Detected By
- Device ID
- External Device Name
- External Device Product ID
- External Device Serial Number
- External Device Type
- External Device Vendor ID
- File Name
- File Type
- Found Date
- Host IP Address(es)
- Host MAC Address(es)
- Host Zone Name(s)
- Hostname
- Instigating Process ImageFileSha256
- Instigating Process Name
- Instigating Process Owner
- Interpreter
- Interpreter Version
- Is Malware
- Is Running
- Is Unique to Cylance
- Optics Event ID
- Optics Severity
- Path of File
- Policy Name
- Process ID
- Process Name
- SHA256
- Status
- Target File Owner
- Target File Sha256
- Target Process ImageFileSha256
- Target Process Name
- Target Process Owner
- Target Registry KeyPath
- Target Registry ValueName
- Threat Classification
- Threat Subclass
- Violation Type