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 rev3, 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.
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.
Cylance Extension for QRadar
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
Legal Notice
Legal Notice

©2020 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