



## Alert Handling Quick Reference Guide

Alert ID	Case Number	Artifact of Interest	Host/ Device name	Priority	Severity	Trigger Product	Assigned to	Timestamp	Status
SIR0024607	CS0001484	OpticsCaeVmlEvent	WindowsServer 2K19	P5	High	Protect		2021-09-11 12:07:30	New
	CS0001583	OpticsCaeRegistryEvent	LAB001-SERVER		Medium			2001-09-15 15:40:40	New
SIR0022834	CS0001061	OpticsCaeFileEvent	BSTATION-78653	P5		Optics	Joe MacDonald	2021-08-30 15:34:53	New
	CS0001582	ScriptControl on MILE-2K19	TESTLAB007		High			2021-09-15 09:24:31	New
	CS0001581	Threat on PWLSON-W2K19-01	PWLSON-2K19		Medium	Protect	Evan M	2021-09-15 09:23:51	New

1. On the **Escalations** page, view the list of alerts that were escalated to your organization. The appropriate team in your organization is also notified through email when an analyst escalates an alert.
2. Open a case that you want to investigate.

State: New

Priority: P5

Severity: High

Category: CAT 0 - Exercise/Network Defense Testing (Stop T1R/T1D)

Organization: Always Good Inc

Alert ID: SIR0010019

Created: 2021-08-31 08:46:12

Assigned: [User]

Assigned group: Priority - High

Triggered Events (15) | Observations (0) | Whitelisted Events (0)

Description: (OPTICSCAFRREGISTRY) GIARD: Registry Run Key Persistence (V2)

Investigating Process Artifact: process

Investigating Process End Date: 1970-01-01T00:00:00.000Z

Investigating Process Name: svchostTest.exe

Created: 2021-08-31 14:09:03

Activation Time: 2021-08-23T20:47:48Z

Investigating Process Integrity Level: -1

Received Time: 2021-08-23T20:47:48Z

Investigating Process Owner Name: SYSTEM

Guard Platform Region ID: US

Detection Rule Policy Group: CylanceOfficial\DetectionRuleSet

Target Registry Key: File

Referenced File Type: File

Detection Rule ID: 3800dd22-75fd-40efaa3c-9894990307e1

Activity (2)

Attachments

Type your message here... [Send]

cc: Evan M (Personal comments) test

cc: Evan M (Work notes) Added as a child of SIR0010019

3. If you can respond to the escalation, assign it to yourself to take ownership.

4. Review the trigger events and comments.
  - For example, an analyst may have left a comment asking you to verify suspicious activity. "We have seen a PowerShell script running on System A that is connecting to the following IP address, is this behavior expected on this system?"
5. Investigate the issue and gather any relevant information.
  - For example, identify the host computer, users, and application owner and investigate whether there is unusual or unexpected system behavior.
6. If you require more information from a Guard analyst and want to escalate back to them, add a comment to notify them of your request. You can continue to use the comment box to communicate with analysts.
7. Once you have gathered enough information about the alert and determined whether it is expected behavior, leave a comment for the Guard analyst to inform them about the next steps.
  - **Example 1:** If this is expected behavior, or you can resolve the issue through the IT department in your organization, add a comment to inform the Guard analyst so that they can take appropriate action in the console to exclude this alert in the future.
  - **Example 2:** If this is unexpected behavior, review any recommendations provided in the comments. Add a comment to the alert and state that this is not expected behavior and communicate any actions, next steps, and if incident response is needed. If needed, initiate an incident response plan which might involve engaging with an incident response team (such as BlackBerry Security Services).
  - **Example 3:** If no action is required, add a comment to the alert to notify the Guard team and confirm the case can be closed with no action required.
8. When you consider an alert to be resolved or when no further action is required, leave a comment to confirm that no further action is required and that the issue can be closed.

# Legal notice

©2021 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU 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.

Use of this BlackBerry product and/or service is governed by a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY SUCH WRITTEN AGREEMENTS OR OTHER WARRANTIES PROVIDED BY BLACKBERRY.

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