

Alert Handling Quick Reference Guide

1 67 533 Total levis Total Lic cardio Open Econations 1 Intel Lic cardio Open Econations 2 Intel Lic cardio Artifact of Interest Hold Device name Priority Severity Trigger Product Assigned to Timestamp 2 SIG02467 G3001484 OpticsDerivmitivent Midowsferre 2K19 FS High Protect 20210911120730 2 SIG02467 G3001061 OpticsDerivmitivent AB0014SRVER High Protect 2010911120730 2 SIG022634 G3001061 OpticsDerivmitivent AB0014SRVER FS Optics Joe Macboneld 2021093153430 2 SIG022634 G3001051 OpticsDerivent on MILE-2K19 FST High										scalations
Alert ID Case Number Artifact of interest Host/ Device name Pilority Severity Trigger Product Assigned to Timestamp C 05007467 050001464 OpticsCaeVinitEvent WindowaServer 2K19 F5 High Protect 2021 09:11 12:07:30 C 050007583 OpticsCaeVinitEvent LAB011:SERVER Medium Control 2001 09:15 15:40:40 SIR0072834 050001061 OpticsCaeVinitEvent LAB011:SERVER P5 Optics Joe MacDonald 2021 09:15 15:40:40 SIR0072834 050001061 OpticsCaeVinitEvent ESTATION-78653 P5 Optics Joe MacDonald 2021 09:15 15:40:40 C 050001582 SenetDearbol on MILE-2K'9 TESTLAB097 High 2021 09:15 15:40:40										-
Aller ID Case Number Artifact of interest Host/ Device name Priority Severity Trigger Product Assigned to Timestamp 2 05007467 050001484 OpticiDaeWmiEvent WindowsServer 2K19 PS High Protect 2021 09:1112:07:20 1 050001583 OpticiDaeWmiEvent LAB001+SBRVER Medium Medium 2001 09:15 15:40:40 5880072834 050001061 OpticiDaeWieleVent BSTATION-78653 PS Optics Joe MacDonald 2021 09:31 15:34:53 1 050001061 OpticsDeatEleEVent BSTATION-78653 PS High Levent 2021 09:31 15:34:53 1 050001061 OpticsDeatEleEVent BSTATION-78653 PS High Levent 2021 09:31 15:34:53 1 050001061 Selex0cented on MLE-20:9 TESTLABU07 High Levent 2021 09:31 15:34:53	٩	calations	Search for e							
SRR0024607 DSD001484 OpticsCaevMmEVent WindowsServer 2K19 F5 High Protect 2021 09-11 12:07:30 L DSD001583 OpticsCaevMeEVent LA3001587VER Medium 2001 09-15 15:40-00 2001 09-15 15:40-00 SR0022834 DSD001061 OpticsCaevFletVent BSTATION-78653 P5 Optics Joe Macboneld 2021 09-31 13:45:3 L DSD001061 OpticsCaevFletVent BSTATION-78653 P5 Optics Joe Macboneld 2021 09-31 13:45:3 L DSD001061 OpticsCaevFletVent BSTATION-78653 P5 Optics Joe Macboneld 2021 09-31 13:45:3	Status	Timestamp	Assigned to	Trigger Product	Severity	Priority	Host/ Device name	Artifact of interest	Case Number	Alert ID
DS00072834 DS0001061 Optics/CavRogithyFvent LAS001458/VER Medium 2001491511540-00 S880072834 DS0001061 Optics/CavRogithyFvent BSTATION-78653 P5 Optics Jace MacDonald 20214931153453 C30001582 Selebothedion MLE-2019 TESTLAB007 High 202149451992431	New	2021-09-11 12:07:30		Protect	High	P5	WindowsServer 2K19	OpticsCaeWmiEvent	CS0001484	
C30001582 ScriptControl on MILE-2K19 TESTLA8007 High 2021-09-15 09:24:21	New	2001-09-15 15:40:40			Medium		LAB001-SERVER	OpticsCaeRegistryEvent	CS0001583	
	New	2021-08-30 15:34:53	Joe MacDonald	Optics		P5	BSTATION-78653	OpticsDaeFileEvent	CS0001061	SIR0022834
CSD001581 Threat on PWI John W2K19-01 PWILSON-2K19 Medium Protect Exan M 2021-09-15 09:23:51	New	2021-09-15 09:24:31			High		TESTLAB007	ScriptControl on MILE-2K19	CS0001582	
	New	2021-09-15 09:23:51	Evan M	Protect	Medium		PWILSON-2K19	Threat on PWilson-W2K19-01	C\$0001581	
Ro	Rows 16 - 20 of 596									< >

- 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.

쓰										
Θ										
Ŭ	State: New			Category:	CAT 0 - Exercise/Network Defense Testing (Stop TTR/TTD)			Organization:	Always Good Inc	
5	Priority: P5 🥜			3 Assignee:	1			Alert ID:	SIRDD10019	
e	Severity: HIGH	Severity: HIGH		Assigned group: Priority - High				Created:	2021-08-31 08:46:12	
A	Triggered Events (15) Obser	vations (0) Whitelisted Eve	ents (0)							
Ê										
	Description:	(OPTICSCAEREGISTRY) GUAR	D: Registry Run Key Persisten	cc (V2)						
₽	Instigating Process Artifact Type:	Process					Activity (2)	Attachments		
	Instigating Process End Date:	1970-01-01T00:00:00.000Z					6			_
	Instigating Process Name: svchostTest.exe Created: 2021-08-23 14:03:03						Type your message here			Send
										Ø
		2021-08-23T20:47:48Z					8			
	Instigating Process Integrity Level:	-1						Evan M		16d ago
	Received Time:	2021-08-23T20:47-49Z				4		itional comment	5	
	Instigating Process Owner Name:	SYSTEM				5		test		
	Guard Platform Region ID:	US				ి				
	Detection Rule Policy Group:	CylanceOfficialDetectionRules	et					Evan M		16d ago
	Target Registry Key Referenced File Type:	File					EG	Work notes		200 0 <u>0</u> 0
		3a00dd22-75fd-40ef-aa3c-9a9 New	4990501e1					Added as a child	of SIR0010019	
_	Statuo	NICSA								

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 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.blackborn.com/logal/thirdparty.software.isp

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