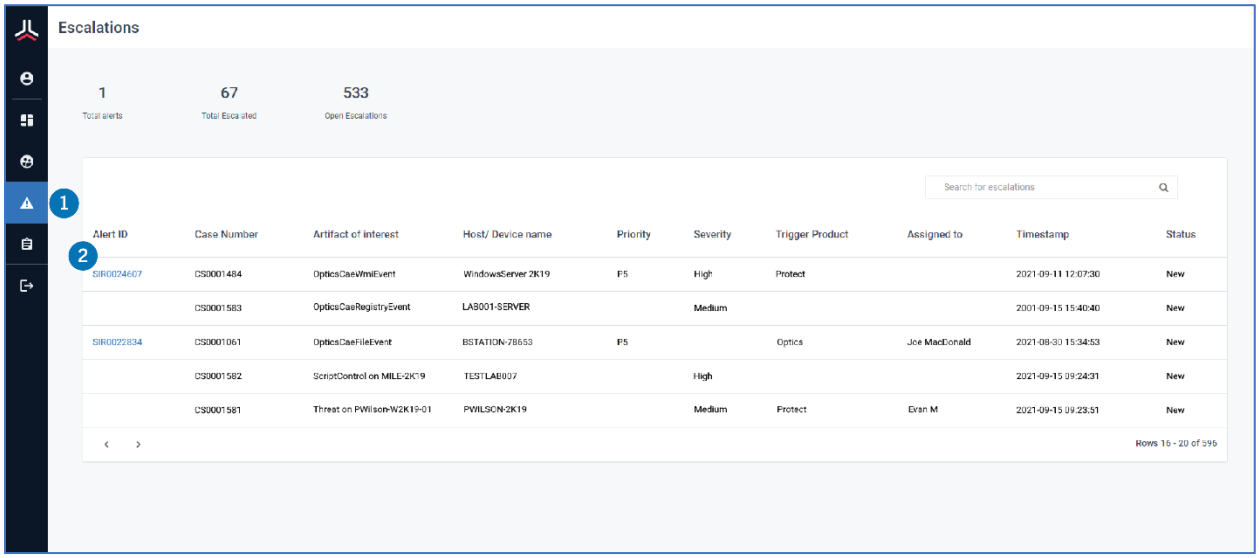
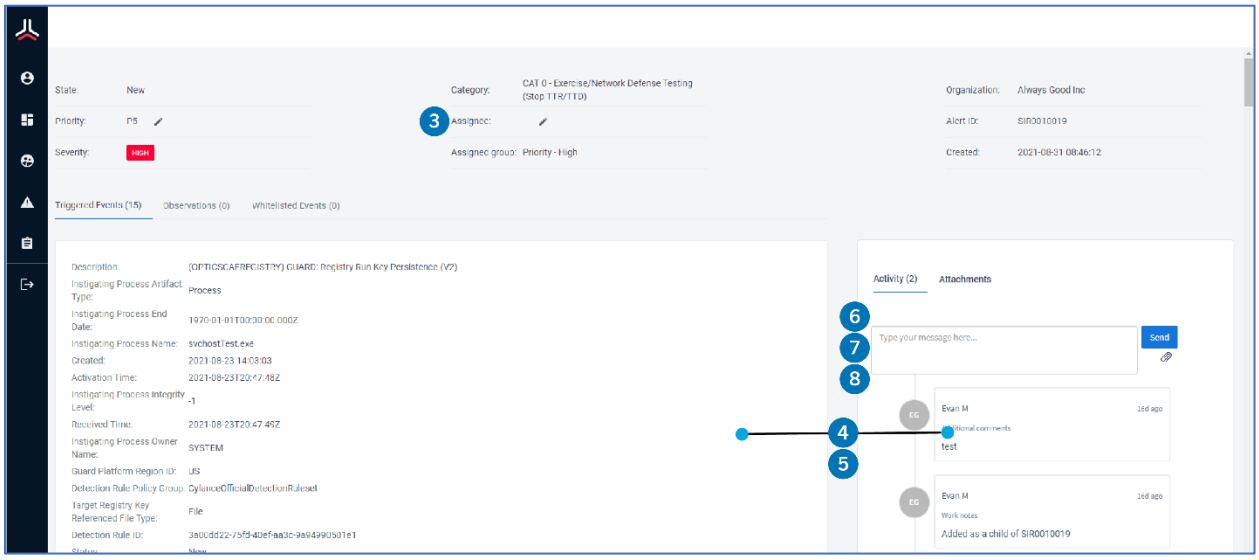
BlackBerry Guard

Alert Handling Quick Reference Guide



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.



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

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