Qualys Endpoint Detection and Response v2.x

Release Notes

Version 2.1.1

September 12, 2022

Here's what's new in Endpoint Detection and Response 2.1.1!

Bulk Remediation Action

AV renamed to Anti-Malware Profile

Integration with AMSI

New Tokens Support

Endpoint Detection and Response 2.1.1 brings you some improvements and updates!

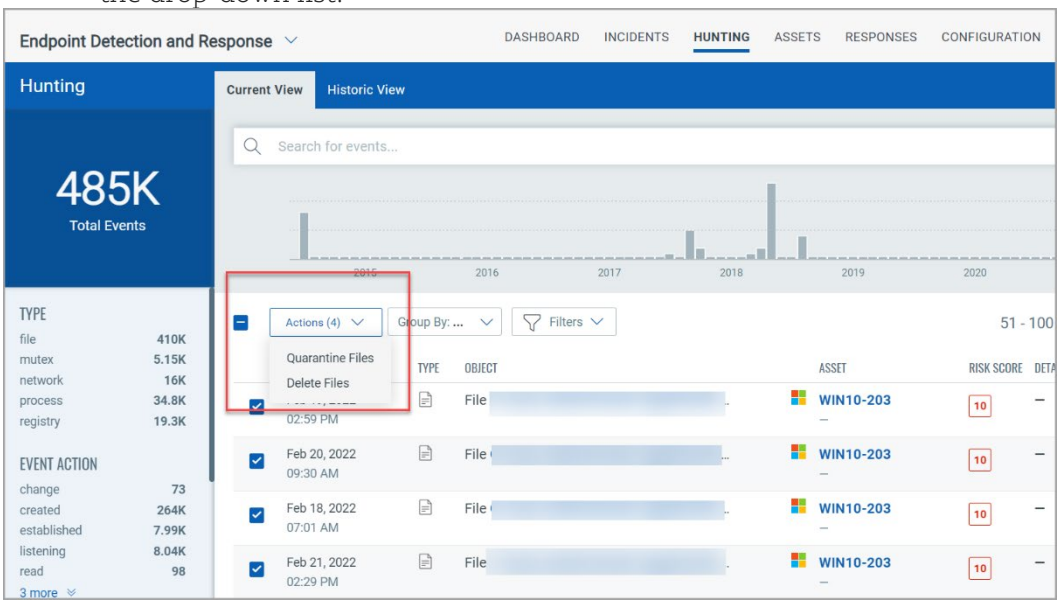
Bulk Remediation Action

With this release, we have introduced bulk remediation action. This option will allow you to perform remediation actions to Quarantine File, Delete File, and Kill Process options. Bulk remediation can happen only for a similar type of event on the same page of the **Current View** tab. You cannot apply bulk remediation action if you select a file from page 1 and another from page 2 of the **Current View** tab. At a time, you can use bulk remediation for 200 events. Remediation action is not available for Registry events.

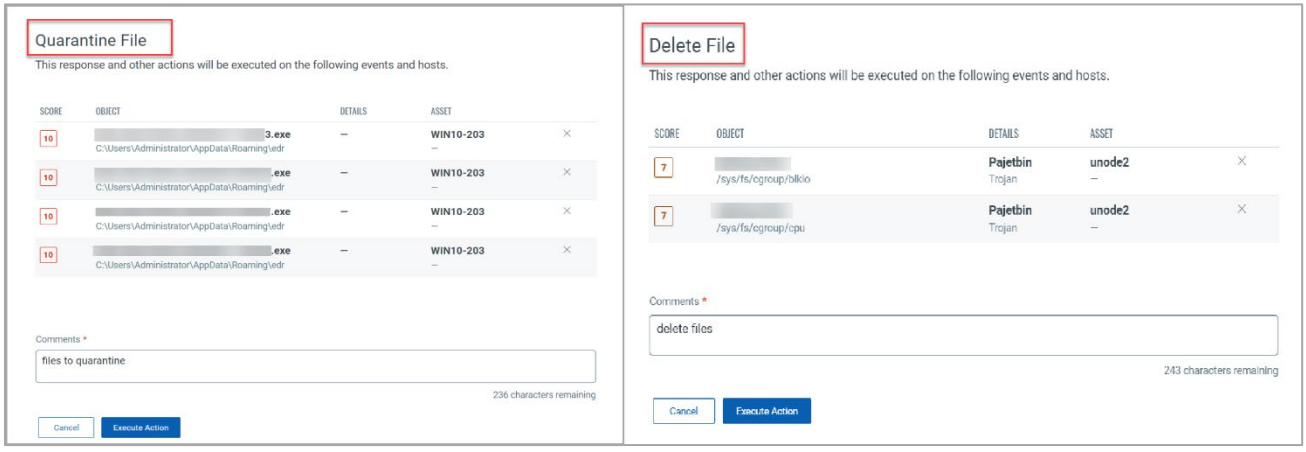
For more information, see Qualys Endpoint Detection and Response online help.

Perform the following steps for File events to perform bulk remediation action:

1. Select mulitple file events and click **Actions**. Select **Quarantine Files** or **Delete Files** from the drop-down list.



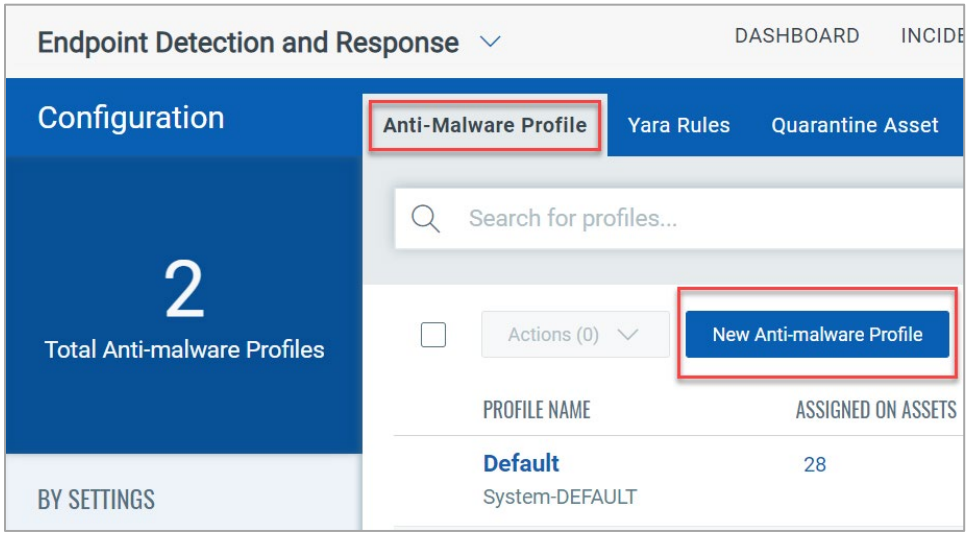
2. Based on your selection (Quarantine File/Delete File), one of the following window is displayed. Enter the required comment and click **Execute Action**.



3. A pop-up message indicating the status of submission request is displayed on the top-right corner of screen. You can click **View Request Status** from the pop-up message, to view the status (In Progress, Success, Failed) of the remediation request.
4. You can also view the status for the remediation request from the Status column on the **Responses** tab.

AV renamed to Anti-Malware Profile

With this release, we have renamed the occurrences of AV to **Anti-malware** across Endpoint Detection and Response module. For example, in the **Configuration** tab, you will now have **Anti-Malware Profile** instead of AV Profile.

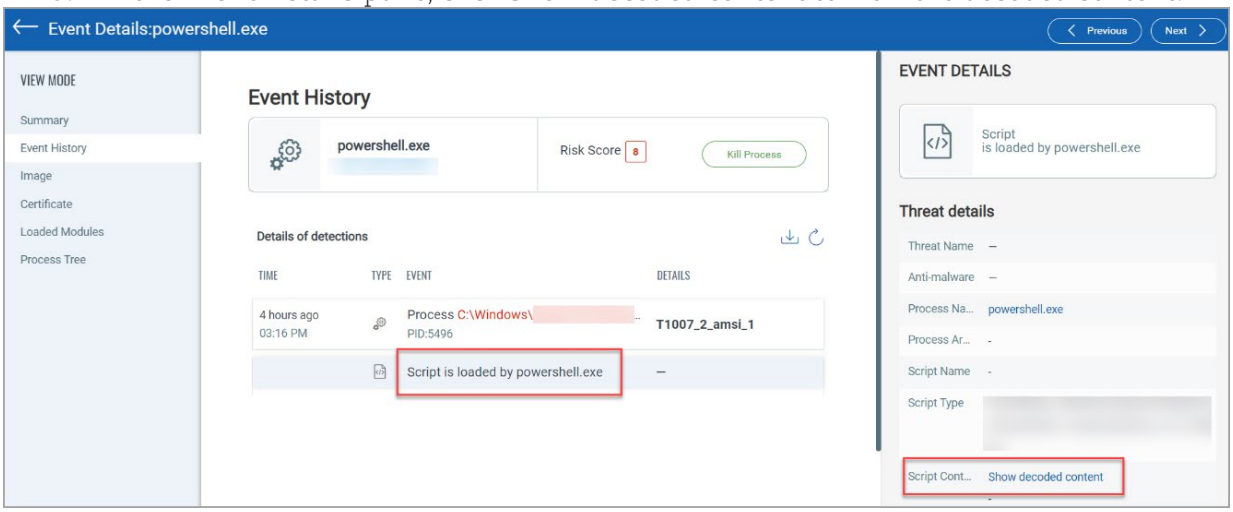


Integration with AMSI

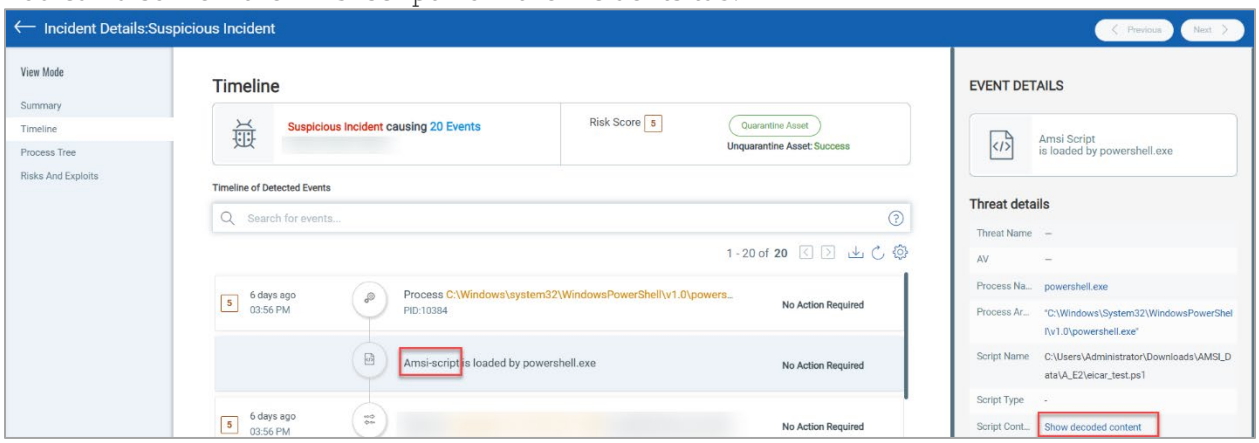
With this release, we have introduced integration with Antimalware Scan Interface (AMSI). This integration will help you detect malicious scripts or commands. The encoded scripts or arguments are decoded in a human-readable format by the AMSI engine. You must log in to the Antimalware Scan Interface on Windows 10.

Perform the following steps to view AMSI script from the **Hunting** tab:

1. Select a process from the **Hunting** tab to verify if the AMSI script is loaded. For example, you can run any of the AMSI token queries mentioned in New Tokens Support.
2. Click **Event History** and from the **Event** coulmn, click **Script is loaded by**. The details of the script is displayed in the **Event Details**.
3. In the **Event Details** pane, click **Show decoded content** to view the decoded content.



You can also view the AMSI script from the Incidents tab.



For more information, see Qualys Endpoint Detection and Response online help.

New Tokens Support

We have introduced the following search tokens to enhance your search results:

- **amsi.type**: This token helps you to filter events by the loaded script type.
- **amsi.filename**: This token helps you to filter events by the loaded script name.
- **amsi.arguments**: This token helps you to filter events by the loaded script arguments.
- **amsi.commandline**: This token helps you to filter events by loaded script content.
- **amsi.commandline.length**: This token helps you filter events by the loaded script length.
- **event.hasAmsi**: This token helps you to filter events that have loaded script.
- **isAntiMalwareInstalled**: This token helps you to list assets that have Anti-malware installed.