Qualys Endpoint Detection and Response v2.x

Release Notes

Version 2.4

April 5, 2023

Here's what's new in Endpoint Detection and Response 2.4!

What's New

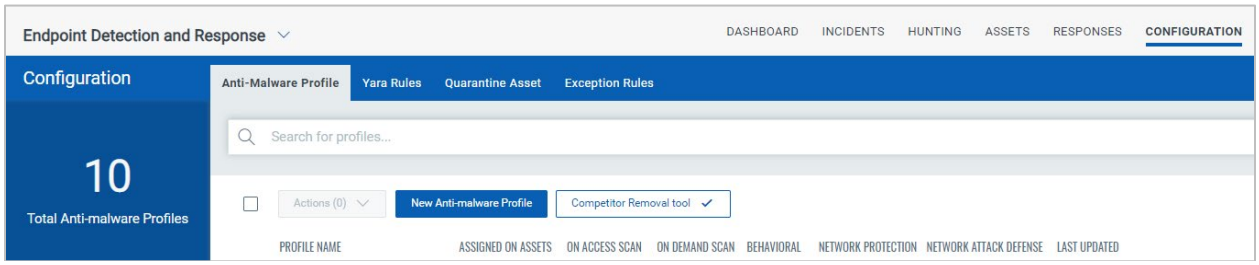
Endpoint Detection and Response 2.4 brings you some improvements and updates!

Competitor Removal Tool

With this release, we have introduced the **Competitor Removal tool** that removes the third-party anti-virus and its traces from the applications. The minimum requirement for the Windows Agent version is 5.1.0 and OPSWAT-supported applications to enable the Competitor Removal tool.

To enable the Current Removal tool, from the **Configuration** tab, under **Anti-malware Profile**, and click **Competitor Removal tool**.

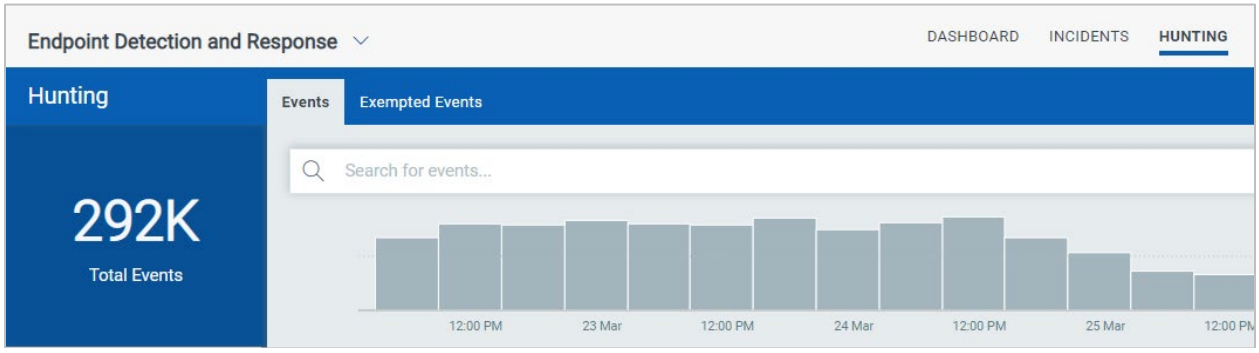
See the *EDR Online Help* for more information.



Removed Current View and Historic View

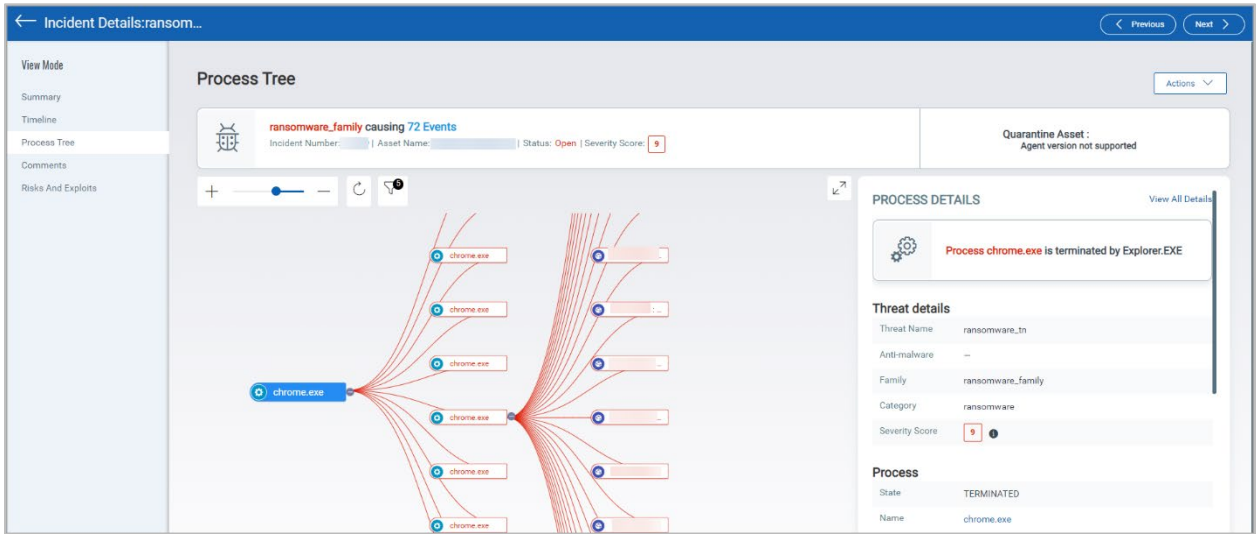
We removed the **Current View** and **Historic View** tabs from the **Hunting** tabs with this release. The **Event** tab replaces these tabs. The Events tab lists all available events with remediation functionality, registered and executed on the assets. The remediation functionality is now available only for File and Process. To perform remediation functionality for Network or Mutex event, you can remediate the parent process of that Network or Mutex event.

See the *EDR Online Help* or *EDR Getting Started Guide* for more information.



Removed Type Node from the Process Tree

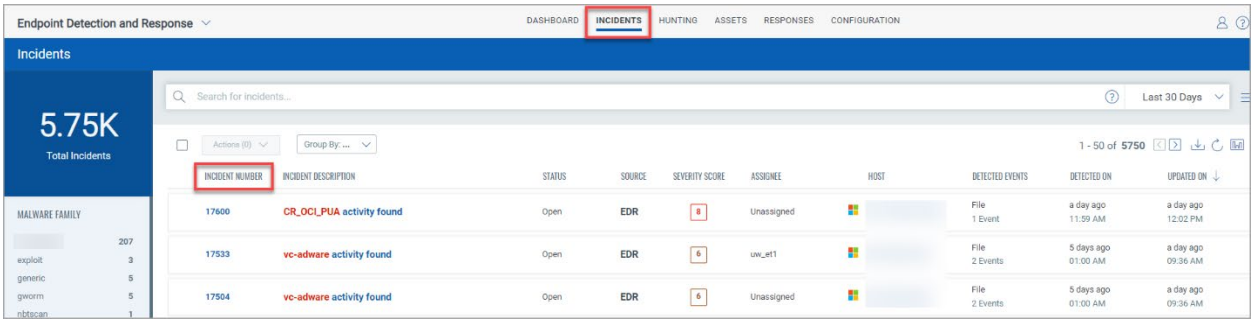
The type node is no more available in the **Process Tree** of the **Incidents** tab. You can continue to perform the remediation action from the Process tree. An event of the "Process" type will show its parent and child processes.



See the *EDR Online Help* for more information.

Incident Data Cleanup based on the Incident Number

With this release, we have introduced Incident Data Cleanup based on the Incident Number. The Incident Number is displayed in the Incidents tab, Incident Details page, and CSV download file. Incidents with Open, In-Progress, and Closed Status for more than 60 days are included in this cleanup activity.



Introduced New Tokens

- **exception.reason**: This token selects a reason to flag the unwanted events generated by the non-malicious program.
- **exception.status**: This token selects the rules actively supporting the events.
- **exception.title**: This token mentions the exception title used while creating the exception.

See *EDR Online Help* for more information.