Qualys Endpoint Detection and Response v2.x

Release Notes

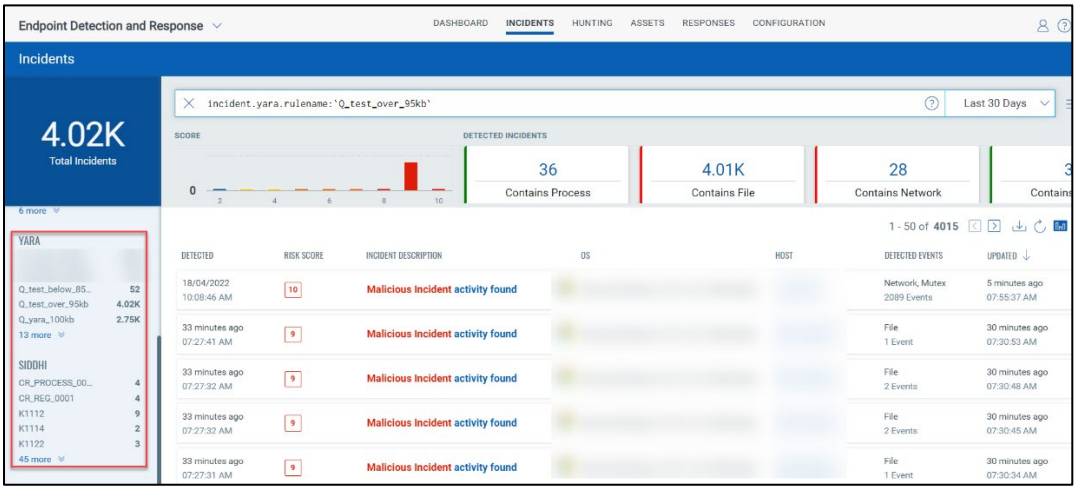
Version 2.0.1
May 23, 2022

Here's what's new in Endpoint Detection and Response 2.0.1!

Endpoint Detection and Response 2.0.1 brings you some improvements and updates! Learn more

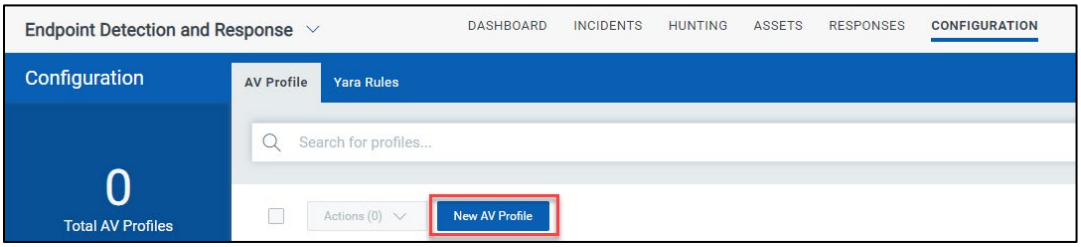
View Yara and Siddhi Filters on Incident Page

You can now view the threat details for an event or incident using the Yara and Siddhi filters on the **Incident** page. You can filter the threats from the left pane of the Incident page.



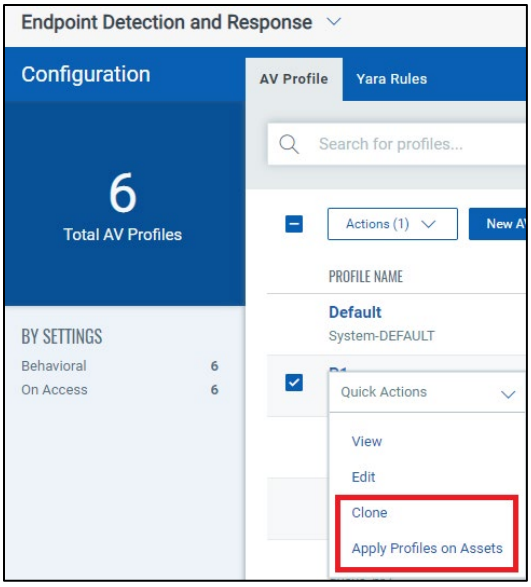
New AV Profile Button in the Configuration Tab

The **New AV Profile** button provides various settings to create a profile. When you click the New AV Profile button, the AV Profile Details window provides you to choose the scans and assets you require for your profile.

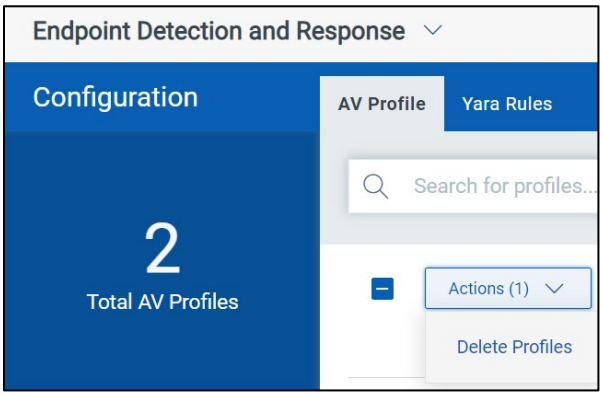


Enhancements to the AV Profile Tab

The **Quick Actions** menu in the Configuration > AV Profile tab now also provides options to Clone and Apply Profiles on Assets options.



The **Actions** button in the Configuration > AV Profile tab now gives the option to Delete your AV profile.



New Tokens Support

We have introduced the following Profile Search tokens and the Incident search tokens to enhance your search results:

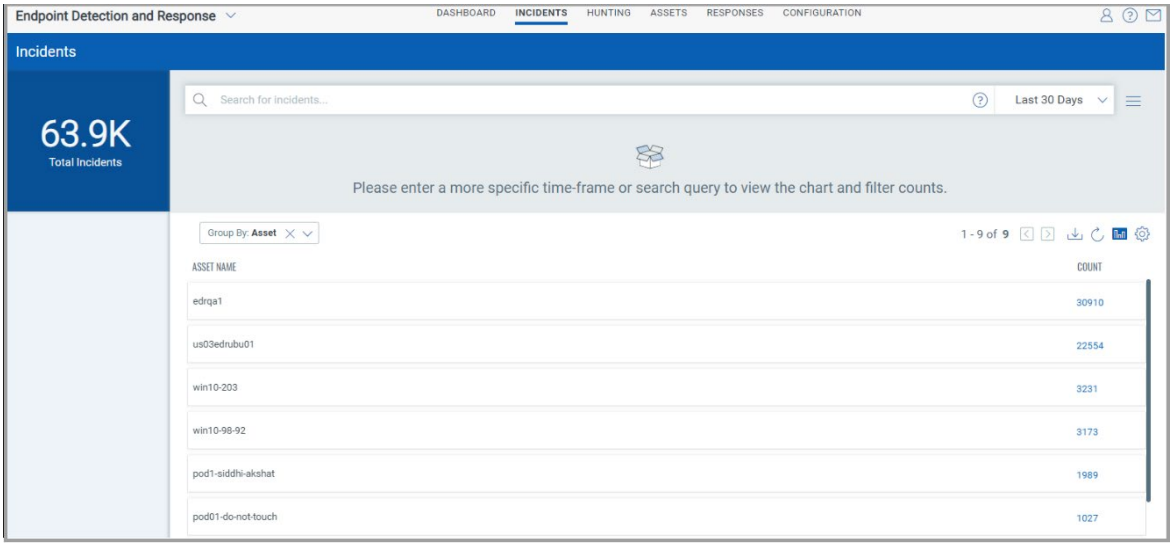
- **assetCount**: This token helps search for profiles with the asset count from the AV Profile tab.
- **behaviour.isEnabled**: This token helps search for profiles with the Behavioural Detection Enabled from the AV Profile tab.
- **fileScan.isEnabled**: This token helps search for profiles with the On Access Enabled from the AV Profile tab.
- **isDefaultProfile**: This token helps search for profiles with the Default from the AV Profile tab.
- **description**: This token helps search for profiles with the description from the AV Profile tab.

- **onDemandScan.isScheduledRunEnabled**: This token helps search for profiles with the On Demand Scan Enabled from the AV Profile tab.
- **name**: This token helps search for profiles with the name from the AV Profile tab.
- **incident.yara.rulename:** Use a string value ##### to detect incident containing specific Yara rules.
- **incident.mite.attack.rule.name:** Use a string value ##### to detect incident containing specific Siddhi rules.

Removal of Active Threats By Host Tab

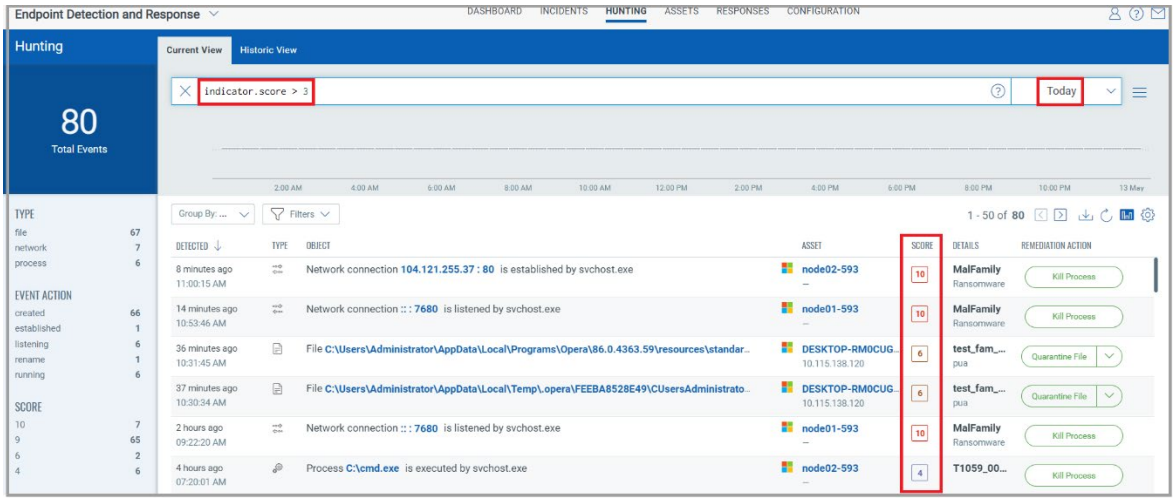
With this release, we have removed the **Active Threats By Host** tab. With the removal of the **Active Threats By Host** tab, the Infected Assets details are now available on the **Incidents** page from the **Incidents** tab.

Note: You can see Infected Assets details by accessing the **Asset AND MALWARE SUMMARY** widget from the **Dashboard** tab.



Updates for New Malicious Events

With the Siddhi revised rule, the new malicious events found for the day are now shown for the risk score greater than 3.



Note: You can see the Malware count by accessing the **Asset AND MALWARE SUMMARY** widget from the **Dashboard** tab.

Changes in Incident Creation Criteria

The incident creation criteria have been modified. With this release, events with an event score greater than or equal to 4 will create an incident. However, its related events with a score between 0 to 10 will be part of an incident.

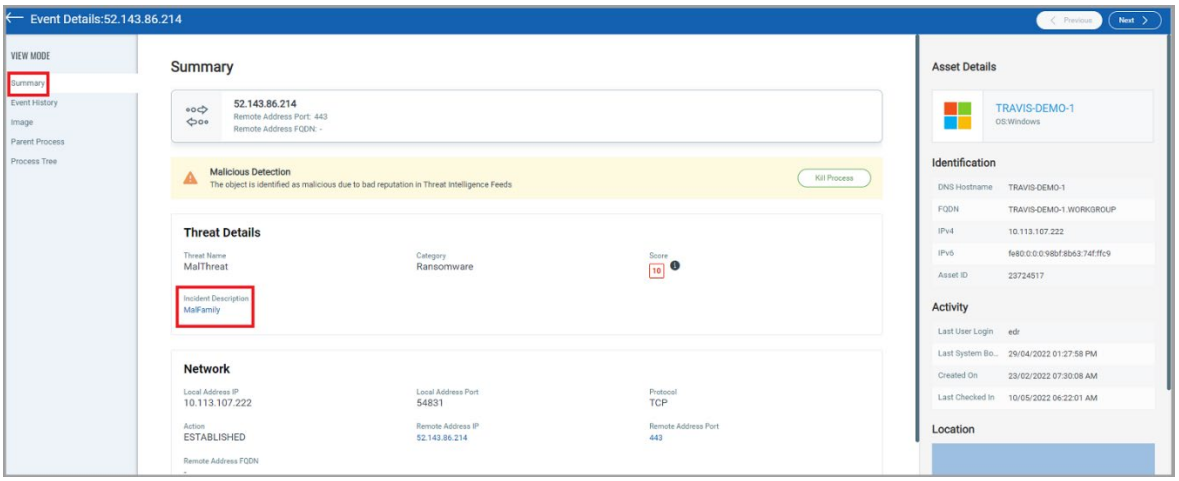
Note: Create alerting rules that are best suited to your business model. For example, 1 to 3 is low, 4 to 6 is medium, 7 to 9 is high, and 10 is critical event severity. As low severity events might be large in volume, you might not want to consider them while creating the alerting rules.

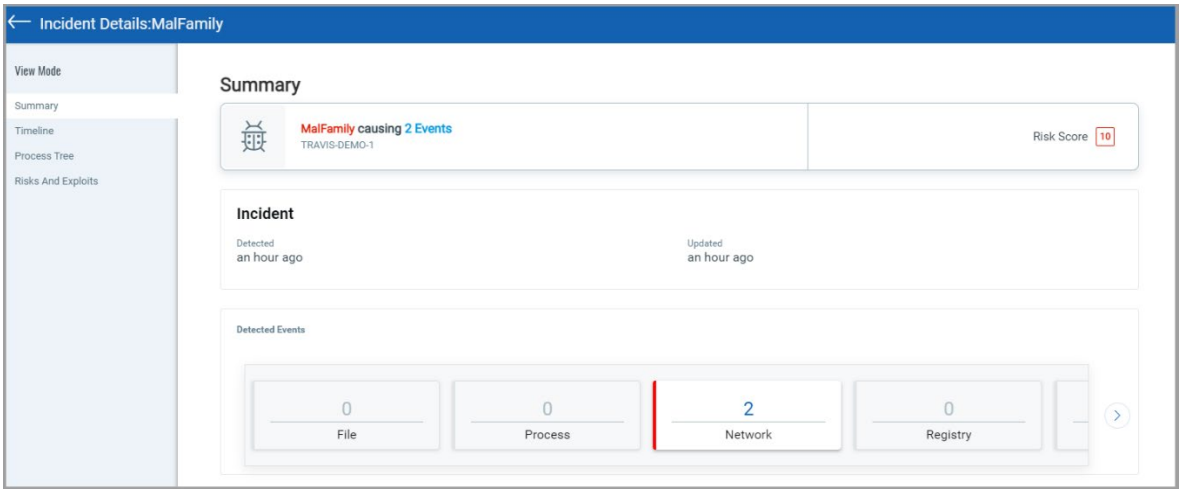
Incident Description for the Malicious Events on the Events Details Page

With this release, a lot of manual effort to identify the incident details for the malicious events has been eliminated. You can now see the **Incident Description** for the malicious events on the **Event Details** page. This is applicable to the malicious events that are shown by clicking the **Current View** and **Historic View** tabs.

Upon clicking the malicious event from the **Current View** and **Historic View** tabs, the **Event Details page** opens. You can see **Incident Description** for the malicious event on the **Event Details** page.

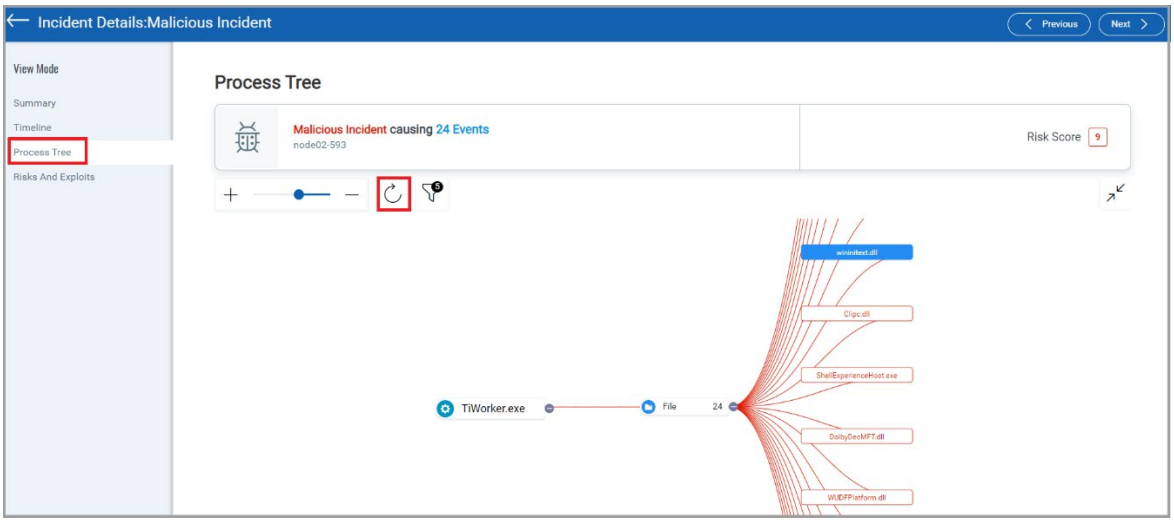
By clicking the **Incident Description**, you can see the Incident Details for the respective malicious event.





Refresh Button added to the Incidents Page

A refresh button is added to the **Incident Details** page that enables you to fetch all the details about the incident.


Incident Details:Malicious Incident
Previous
Next
View Mode
Summary
Timeline
Process Tree
Risks And Exploits
Process Tree
Malicious Incident causing 24 Events
node02-593
Risk Score 9
TiWorker.exe
File
24
wininitext.dll
Clipc.dll
ShellExperienceHost.exe
DolbyDecMFT.dll
WUDFPlatform.dll

Issues Addressed

- We have fixed an issue on the **Assets** tab if you tried to quarantine multiple files; an error message about being unable to quarantine the file was shown.