



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!

[View Yara and Siddhi Filters on Incident Page](#)

[New AV Profile Button in the Configuration Tab](#)

[Enhancements to the AV Profile Tab](#)

[New Tokens Support](#)

[Removal of Active Threats By Host Tab](#)

[Updates for New Malicious Events](#)

[Changes in Incident Creation Criteria](#)

[Incident Description for the Malicious Events on the Events Details Page](#)

[Refresh Button added to the Incidents Page](#)

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.

The screenshot shows the Incident page in the Endpoint Detection and Response interface. The top navigation bar includes DASHBOARD, INCIDENTS, HUNTING, ASSETS, RESPONSES, and CONFIGURATION. The main header is 'Incidents' with a search bar containing 'Incident.yara.rulename: 'Q_test_over_95kb'' and a 'Last 30 Days' filter. A summary card shows '4.02K Total Incidents'. Below this, a bar chart shows 'DETECTED INCIDENTS' with a score of 36. A table below the chart shows incident details: 'Contains Process' (4.01K), 'Contains File' (28), and 'Contains Network'. The main table lists detected incidents with columns for 'DETECTED', 'RISK SCORE', 'INCIDENT DESCRIPTION', 'OS', 'HOST', 'DETECTED EVENTS', and 'UPDATED'. The left sidebar shows filters for 'YARA' and 'SIDDHI' rules, with a red box highlighting the filter list.

DETECTED	RISK SCORE	INCIDENT DESCRIPTION	OS	HOST	DETECTED EVENTS	UPDATED
18/04/2022 10:08:46 AM	10	Malicious Incident activity found			Network, Mutex 2089 Events	5 minutes ago 07:55:37 AM
33 minutes ago 07:27:41 AM	9	Malicious Incident activity found			File 1 Event	30 minutes ago 07:30:53 AM
33 minutes ago 07:27:32 AM	9	Malicious Incident activity found			File 2 Events	30 minutes ago 07:30:48 AM
33 minutes ago 07:27:32 AM	9	Malicious Incident activity found			File 2 Events	30 minutes ago 07:30:45 AM
33 minutes ago 07:27:31 AM	9	Malicious Incident activity found			File 1 Event	30 minutes ago 07:30:34 AM

New AV Profile Button in the Configuration Tab

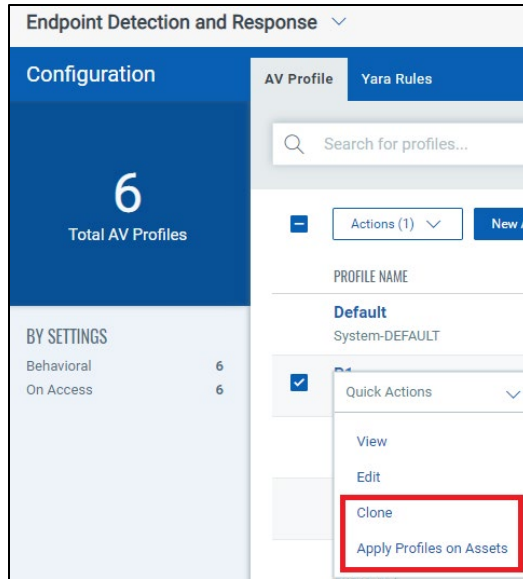
The **New AV Profile** button provides various settings to create a profile. When you click the New AV Profile button, the AV Profile Details window provides you to choose the scans and assets you require for your profile.

The screenshot shows the Configuration page in the Endpoint Detection and Response interface. The top navigation bar includes DASHBOARD, INCIDENTS, HUNTING, ASSETS, RESPONSES, and CONFIGURATION. The main header is 'Configuration' with a search bar containing 'Search for profiles...'. A summary card shows '0 Total AV Profiles'. Below this, a table lists 'AV Profile' and 'Yara Rules'. A red box highlights the 'New AV Profile' button.

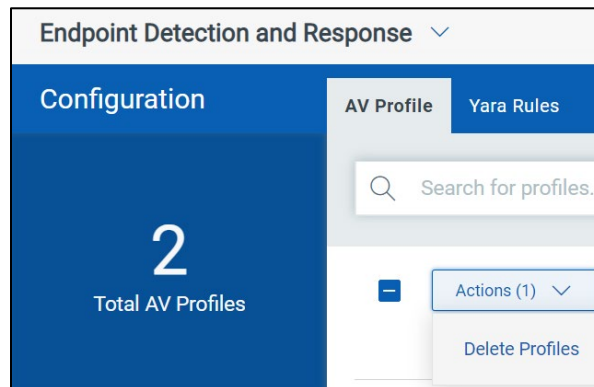
AV Profile	Yara Rules
<input type="checkbox"/>	Actions (0) New AV Profile

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.rule.name:** 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

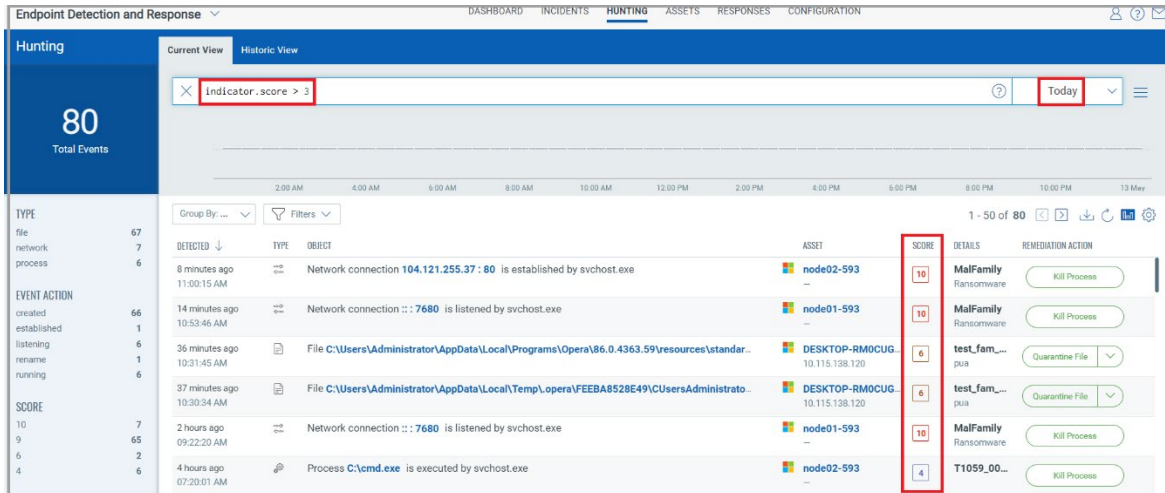
With this release, we have removed the **Active Threats By Host** tab. With the removal of the **Active Threats By Host** tab, the Infected Assets details are now available on the **Incidents** page from the **Incidents** tab.

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

ASSET NAME	COUNT
edrgs1	30910
us03edrubu01	22554
win10-203	3231
win10-98-92	3173
pod1-siddhi-akshat	1989
pod01-do-not-touch	1027

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.

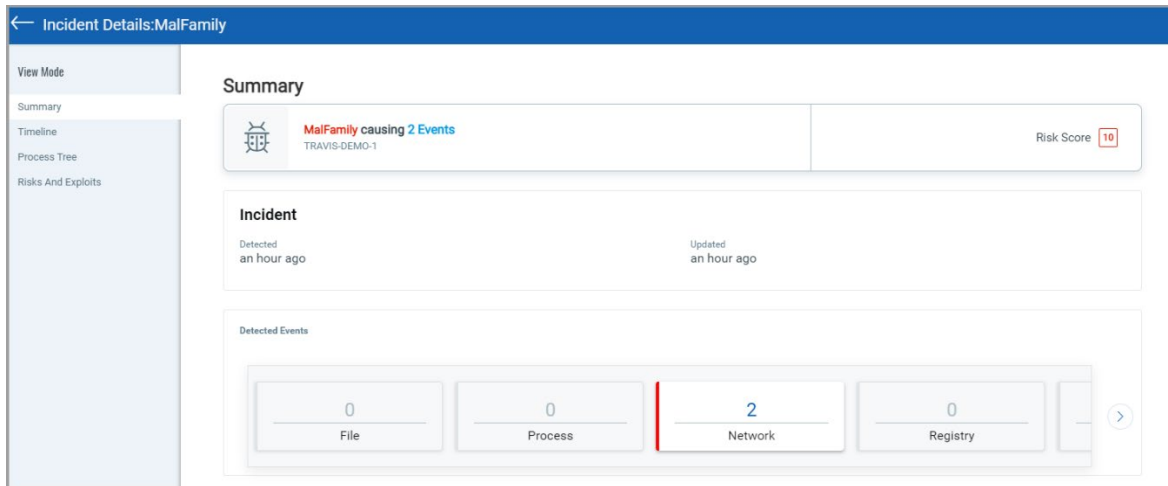
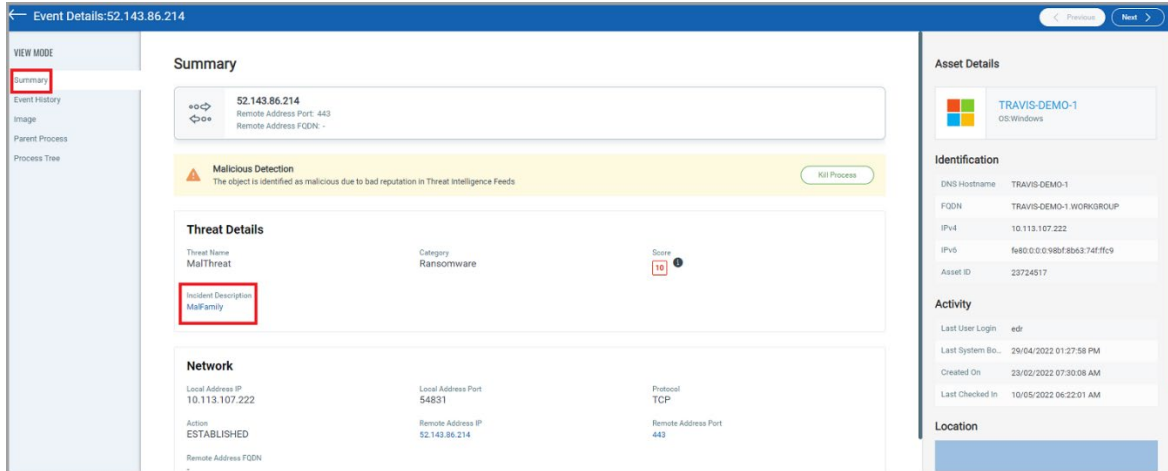
Note: Create alerting rules that are best suited to your business model. For example, 1 to 3 is low, 4 to 6 is medium, 7 to 9 is high, and 10 is critical event severity. As low severity events might be large in volume, you might not want to consider them while creating the alerting rules.

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.

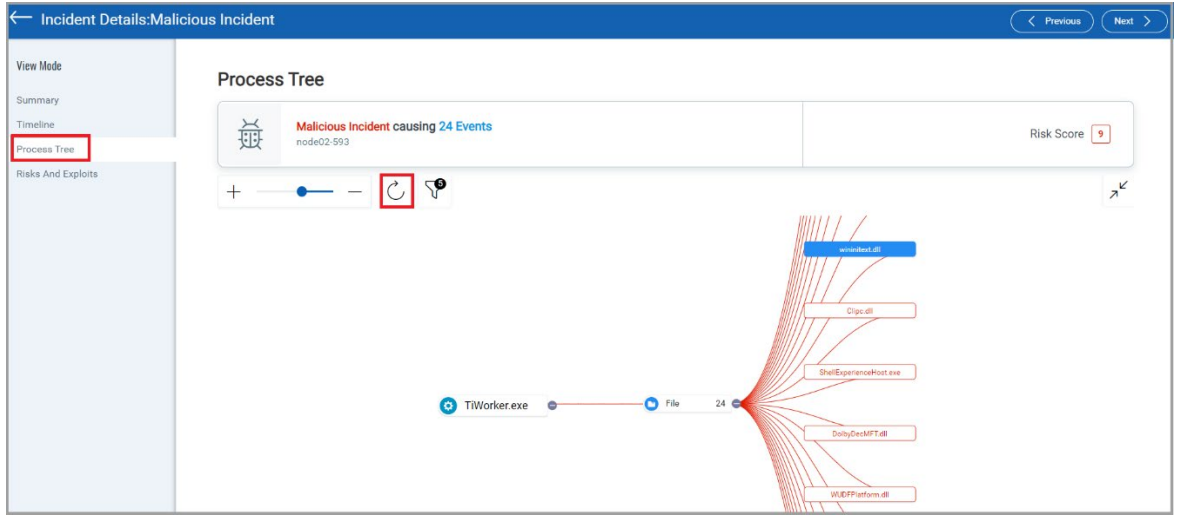
Upon clicking the malicious event from the **Current View** and **Historic View** tabs, the **Event Details** page opens. You can see **Incident Description** for the malicious event on the **Event Details** page.

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.



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.