Qualys Endpoint Detection and Response v1.x

Release Notes

Version 2.0

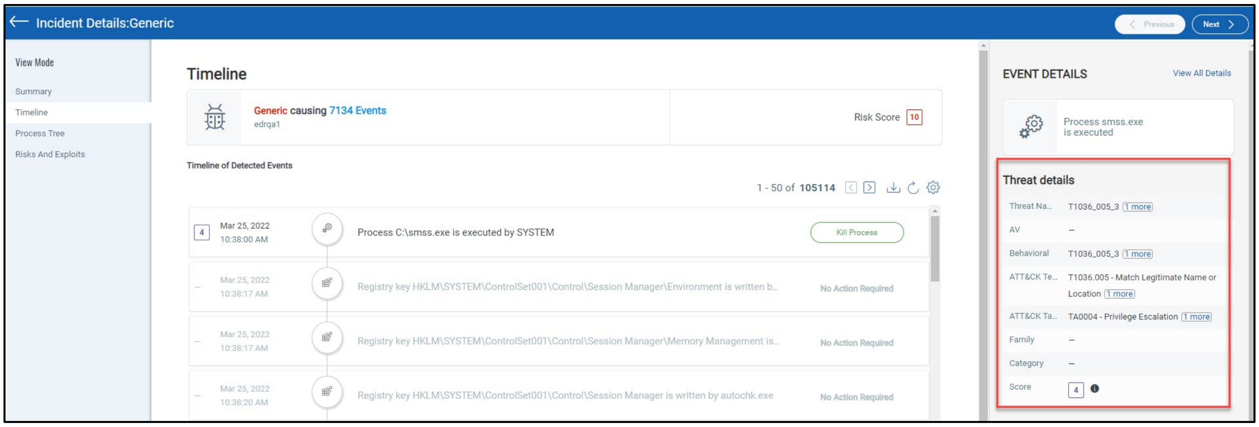
April 8, 2022

Here's what's new in Endpoint Detection and Response 2.0!

Endpoint Detection and Response 2.0 brings you some improvements and updates! Learn more

View the Threat Details for an Incident or Event

You can now view the threat details for an event or incident. The threat details include the risk score for the incident. The risk score is the assigned score based on the detection engine that detected the event or incident.



Timeline

Generic causing 7134 Events
edrqa1

Risk Score 10

Timeline of Detected Events

1 - 50 of 105114

4	Mar 25, 2022 10:38:00 AM	Process C:\smss.exe is executed by SYSTEM	Kill Process
–	Mar 25, 2022 10:38:17 AM	Registry key HKLM\SYSTEM\ControlSet001\Control\Session Manager\Environment is written b...	No Action Required
–	Mar 25, 2022 10:38:17 AM	Registry key HKLM\SYSTEM\ControlSet001\Control\Session Manager\Memory Management is...	No Action Required
–	Mar 25, 2022 10:38:20 AM	Registry key HKLM\SYSTEM\ControlSet001\Control\Session Manager is written by autochk.exe	No Action Required

EVENT DETAILS View All Details

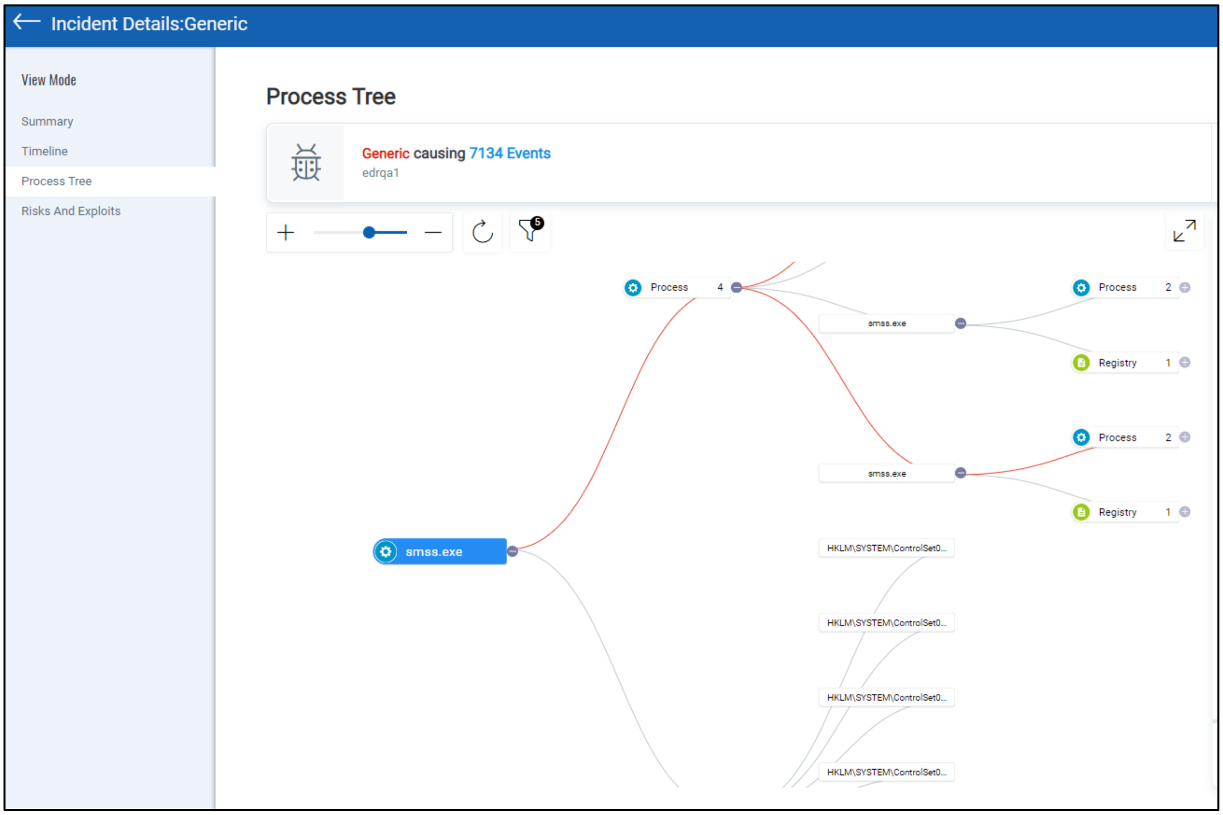
Process smss.exe is executed

Threat details

Threat Na...	T1036_005_3 1 more
AV	–
Behavioral	T1036_005_3 1 more
ATT&CK Te...	T1036.005 - Match Legitimate Name or Location 1 more
ATT&CK Ta...	TA0004 - Privilege Escalation 1 more
Family	–
Category	–
Score	4

Enhancements to the Incident Process Tree

In Incident details, the path is highlighted from the root node to any suspicious or malicious node in the process tree. You can filter the events to show or hide a specific node type in the process tree. The Root node and the Process type nodes are always visible and cannot be hidden.

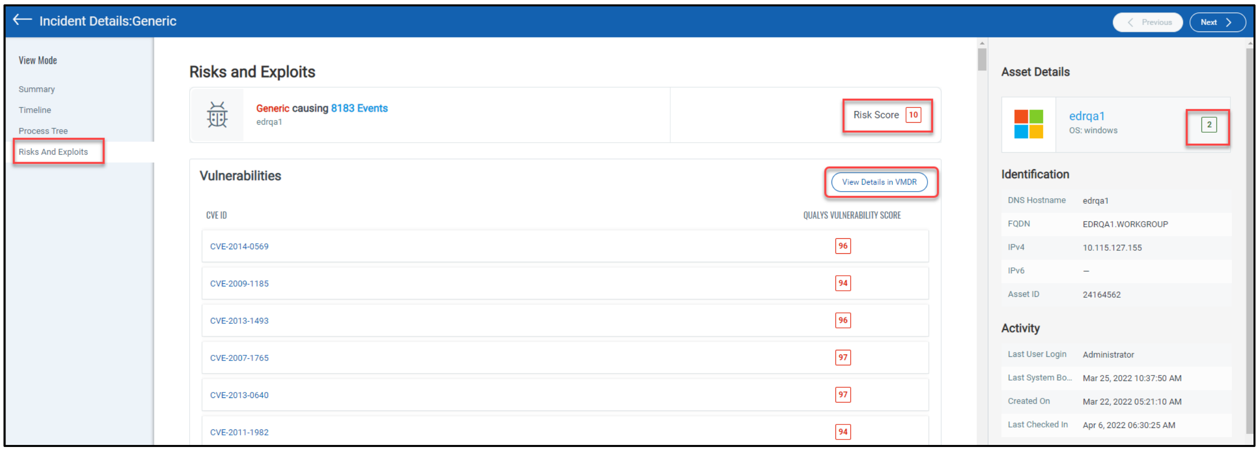

← Incident Details:Generic
View Mode
Summary
Timeline
Process Tree
Risks And Exploits
5
Process 4
smss.exe
Process 2
Registry 1
smss.exe
Process 2
Registry 1
smss.exe
HKLM\SYSTEM\ControlSet0...
HKLM\SYSTEM\ControlSet0...
HKLM\SYSTEM\ControlSet0...
HKLM\SYSTEM\ControlSet0...

Process Tree

Generic causing 7134 Events
edrqa1

New Risks and Exploits tab for Incident Details

The new Risks and Exploits tab for Incident shows the vulnerabilities details such as CVE ID for the incident and the Qualys Vulnerability Score for the CVEs linked to the incident.
If you have a subscription to the VMDR application, you can click the View Details in VMDR to view detailed information about the vulnerabilities linked to the incident.



Risks and Exploits

Generic causing 8183 Events
edrqa1

Risk Score 10

Vulnerabilities

CVE ID	QUALYS VULNERABILITY SCORE
CVE-2014-0569	96
CVE-2009-1185	94
CVE-2013-1493	96
CVE-2007-1765	97
CVE-2013-0640	97
CVE-2011-1982	94

Asset Details

edrqa1
OS: windows
2

Identification

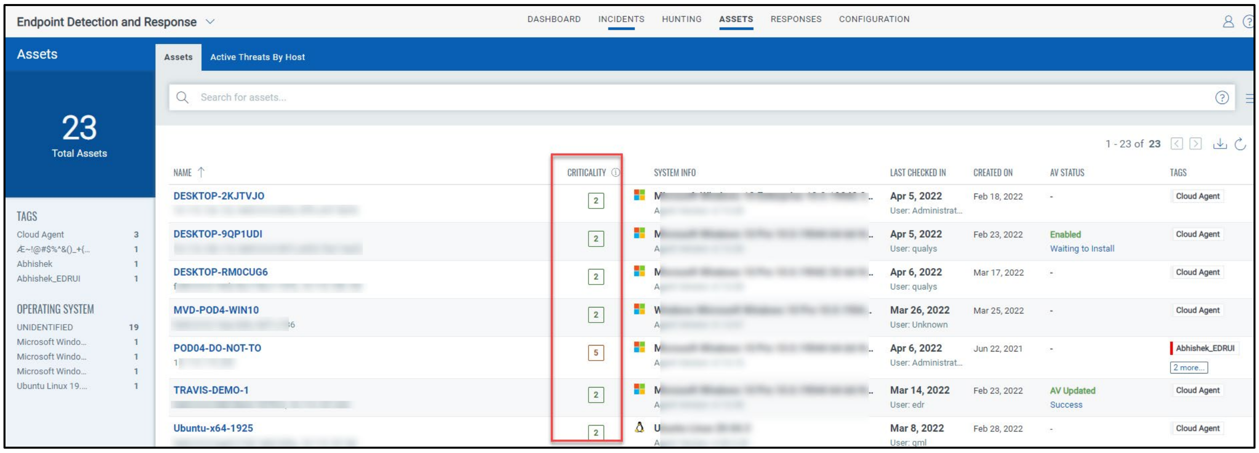
DNS Hostname	edrqa1
FQDN	EDRQA1.WORKGROUP
IPv4	10.115.127.155
IPv6	–
Asset ID	24164562

Activity

Last User Login	Administrator
Last System Bo...	Mar 25, 2022 10:37:50 AM
Created On	Mar 22, 2022 05:21:10 AM
Last Checked In	Apr 6, 2022 06:30:25 AM

New Criticality Score for Assets

The Asset Criticality Score (ACS) represents the criticality of the asset to your business infrastructure. You can view ACS on the **Assets** tab and the **Summary** tab of an Incident.



23
Total Assets

TAGS

Cloud Agent	3
Æ~!@#$%^&()_+{...	1
Abhishek	1
Abhishek_EDRUI	1

OPERATING SYSTEM

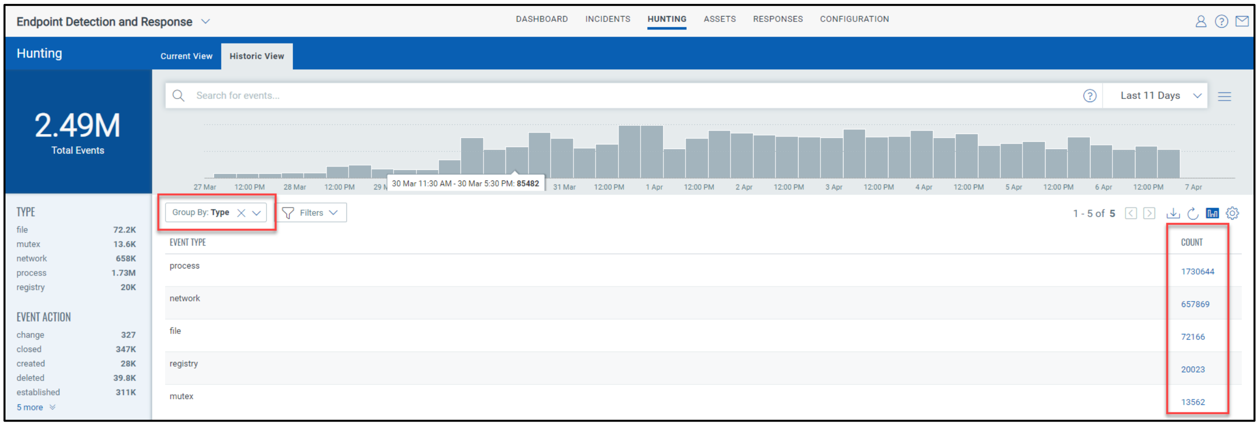
UNIDENTIFIED	19
Microsoft Windo...	1
Microsoft Windo...	1
Microsoft Windo...	1
Ubuntu Linux 19....	1

1 - 23 of 23

NAME	CRITICALITY	SYSTEM INFO	LAST CHECKED IN	CREATED ON	AV STATUS	TAGS
DESKTOP-2KJTVJO [redacted]	2	[redacted]	Apr 5, 2022 User: Administrat...	Feb 18, 2022	-	Cloud Agent
DESKTOP-9QP1UDI [redacted]	2	[redacted]	Apr 5, 2022 User: qualys	Feb 23, 2022	Enabled Waiting to Install	Cloud Agent
DESKTOP-RM0CUG6 [redacted]	2	[redacted]	Apr 6, 2022 User: qualys	Mar 17, 2022	-	Cloud Agent
MVD-POD4-WIN10 [redacted]	2	[redacted]	Mar 26, 2022 User: Unknown	Mar 25, 2022	-	Cloud Agent
POD04-DO-NOT-TO [redacted]	5	[redacted]	Apr 6, 2022 User: Administrat...	Jun 22, 2021	-	Abhishek_EDRUI 2 more...
TRAVIS-DEMO-1 [redacted]	2	[redacted]	Mar 14, 2022 User: edr	Feb 23, 2022	AV Updated Success	Cloud Agent
Ubuntu-x64-1925 [redacted]	2	[redacted]	Mar 8, 2022 User: qml	Feb 28, 2022	-	Cloud Agent

Group Events on the Hunting Tab

You can now group by events on the Hunting tab based on Assets, Type, Event Action, or Score.



2.49M Total Events

TYPE	
file	72.2K
mutex	13.6K
network	658K
process	1.73M
registry	20K

EVENT ACTION	
change	327
closed	347K
created	28K
deleted	39.8K
established	311K

EVENT TYPE	COUNT
process	1730644
network	657869
file	72166
registry	20023
mutex	13562

New Tokens Support

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

- **mitre.attack.tactic.id**: This token helps search for events with the tactic ID from the MITRE ATT&CK framework.
- **mitre.attack.tactic.name**: This token helps search for events with the tactic name from the MITRE ATT&CK framework.
- **mitre.attack.technique.id**: This token helps search for events with the technique ID from the MITRE ATT&CK framework.
- **mitre.attack.technique.name**: This token helps search for events with the technique name from the MITRE ATT&CK framework.
- **mitre.attack.software.id**: This token helps search for events with the software ID from the MITRE ATT&CK framework.
- **mitre.attack.software.name**: This token helps search for events with the software name from the MITRE ATT&CK framework.
- **mitre.attack.group.id**: This token helps search for events with the group ID from the MITRE ATT&CK framework.
- **mitre.attack.group.name**: This token helps search for events with the group name from the MITRE ATT&CK framework.
- **mitre.attack.rule.name**: This token helps search for events with the rule name from the MITRE ATT&CK framework.

Issues Addressed

- We fixed an issue on the **Assets** tab if you tried to display more than 150 rows; an error message about exceeding the permissible limit of 1469 was shown.
- We fixed an issue where the partial argument was visible on the event detail page of the process event. The search query for long argument length that exceeded 255 characters on the **Hunting** tab showed a value length exceeds error message incorrectly.