Qualys Endpoint Detection and Response v1.x

Release Notes

Version 1.3

February 2, 2021

Here's what's new in Endpoint Detection and Response 1.3!

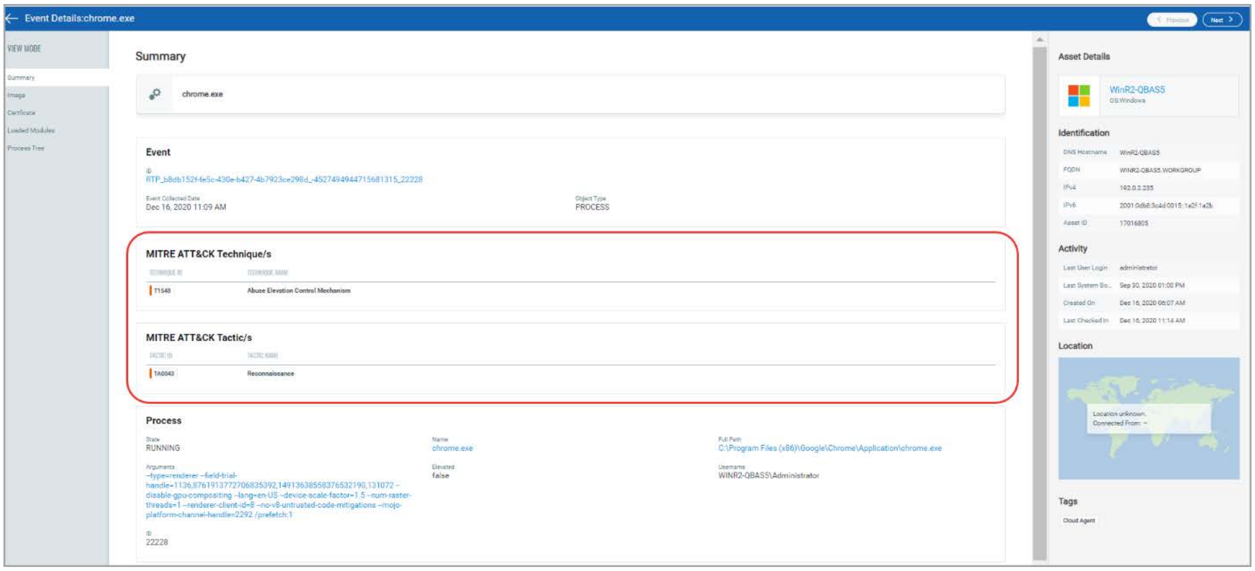
New Classification Rules per MITRE ATT&CK Framework

Endpoint Detection and Response 1.3 brings you more improvements and updates! Learn more

New Classification Rules per MITRE ATT&CK Framework

With this release, we have now added the listed rules as per the MITRE ATT&CK framework to help analyze the events registered on the agents. With each release, we will continue to add more rules to help classify the events appropriately.

The applied ATT&CK tactics and techniques are displayed for applicable events on the Event Details page.



Summary

chrome.exe

Event

ID
RTP_b8db152f-fe5c-430e-b427-4b7923ce298d_-4527494944715681315_22228

Event Collected Date
Dec 16, 2020 11:09 AM

Object Type
PROCESS

MITRE ATT&CK Technique/s

TECHNIQUE ID	TECHNIQUE NAME
T1548	Abuse Elevation Control Mechanism

MITRE ATT&CK Tactic/s

TACTIC ID	TACTIC NAME
TA0043	Reconnaissance

Process

State
RUNNING

Name
chrome.exe

Full Path
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Arguments
--type=renderer --field-trial-handle=1136,8761913772706835392,14913638558376532190,131072 --disable-gpu-compositing --lang=en-US --device-scale-factor=1.5 --num-raster-threads=1 --renderer-client-id=8 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=2292 /prefetch:1

Elevated
false

Username
WINR2-QBAS5\Administrator

ID
22228

Asset Details

WinR2-QBAS5
OS:Windows

Identification

DNS Hostname	WinR2-QBAS5
FQDN	WINR2-QBAS5.WORKGROUP
IPv4	192.0.2.235
IPv6	2001:0db8:3c4d:0015::1a2f:1a2b
Asset ID	17016805

Activity

Last User Login	administrator
Last System Bo...	Sep 30, 2020 01:00 PM
Created On	Dec 16, 2020 06:07 AM
Last Checked In	Dec 16, 2020 11:14 AM

Location

Location unknown.
Connected From: --

Tags

Cloud Agent

Classification Rules added in this release:

1 - T1053.005
Rule to detect the creation of scheduled task using different binaries listed

2 - T1090.003
Rule to detect establishment of multi-hop proxy using TOR

3 - T1098.002
Rule to detect PowerShell process running with argument Add-MailboxPermission

4 - T1115
Rule to detect PowerShell process running with argument Get-Clipboard

5 - T1127.001
Rule to detect events where msbuild.exe is running as a child process under given parent process list

6 - T1201
Rule to detect discovery of password policy using net1.exe binary

7 - T1218.001
Rule to detect execution of hh.exe binary

8 - T1218.005
Rule to detect execution of mshta.exe binary

9 - T1218.009
Rule to detect execution of Regasm/Regsvcs binary

10 - T1218.011
Rule to detect execution of Rundll32 binary

11 - T1220
Rule to detect execution of MSXSL binary

12 - T1569.002
Rule to detect execution of system services using processes listed

Issues Addressed

- We have fixed an issue where the incident data was not updating correctly. The threat information is now displayed accurately in the Incidents tab.