Qualys Endpoint Detection and Response v1.x

Release Notes

Version 1.6

July 7, 2021

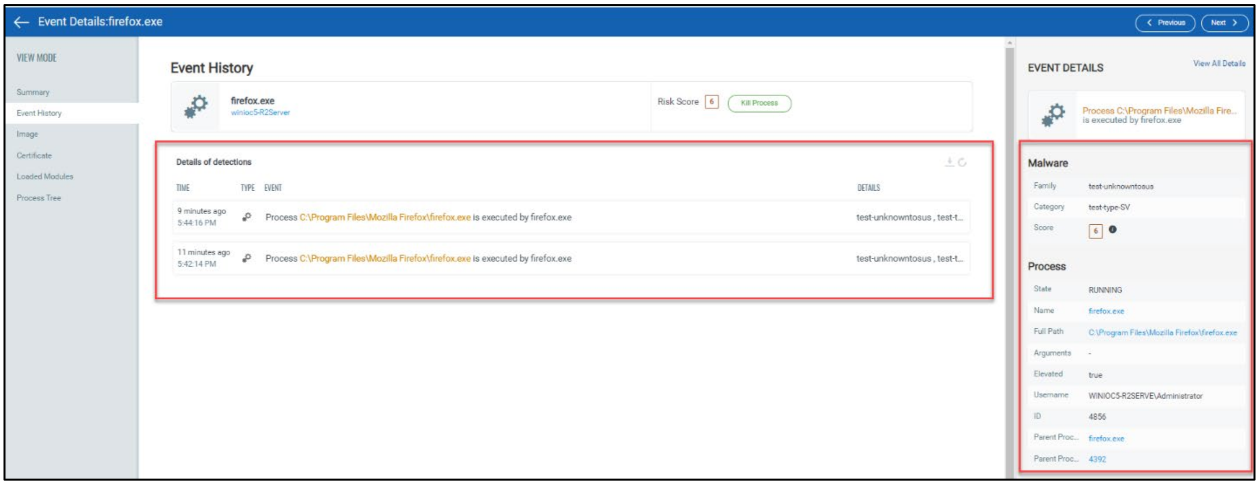
Here's what's new in Endpoint Detection and Response 1.6!

New Event History Tab

Endpoint Detection and Response 1.6 brings you more improvements and updates! Know more

New Event History Tab

You can now view the detailed history of an event. Simply click Event Details > Event History tab to view the detection history of the events. The list shows 50 most recent events for the File, Process, Mutex, Registry, and Network events.
You can refresh the list of events or download the event history in a CSV file. The Delete File, Quarantine File, and Kill Process options are shown only if the event is malicious type. To view details about each event, just click the individual event entry.



Event History

firefox.exe
winioc5-R2Server

Risk Score 6

Details of detections

TIME	TYPE	EVENT	DETAILS
9 minutes ago 5:44:16 PM		Process C:\Program Files\Mozilla Firefox\firefox.exe is executed by firefox.exe	test-unknowntosus , test-t...
11 minutes ago 5:42:14 PM		Process C:\Program Files\Mozilla Firefox\firefox.exe is executed by firefox.exe	test-unknowntosus , test-t...

EVENT DETAILS

Process C:\Program Files\Mozilla Fire...
is executed by firefox.exe

Malware

Family	test-unknowntosus
Category	test-type-SV
Score	6

Process

State	RUNNING
Name	firefox.exe
Full Path	C:\Program Files\Mozilla Firefox\firefox.exe
Arguments	-
Elevated	true
Username	WINIOC5-R2SERVE\Administrator
ID	4856
Parent Proc...	firefox.exe
Parent Proc...	4392

Issues Addressed

- We fixed an issue to monitor the following registry paths:
    - HKLM\SYSTEM\ControlSet001\Control\SecurityProviders*
    - HKLM\SYSTEM\ControlSet002\Control\SecurityProviders*
    - HKLM\SYSTEM\ControlSet001\Control\LSA\FIPSAlgorithmPolicy
    - HKLM\SYSTEM\ControlSet002\Control\LSA\FIPSAlgorithmPolicy
- We fixed an issue where a network connection was established with the Transmission Control Protocol (TCP) but closed with User Datagram Protocol (UDP).
- We fixed an issue where an incorrect asset count for Enabled with EDR, Not Enabled, and Host missing EDR was displayed on the EDR dashboard.
- We fixed an issue where the Process Parent PID: and Network Process PID: search tokens were not showing correct data.
- We fixed an inconsistency issue with the file.path: search token.