Qualys Endpoint Detection and Response (Beta)

Release Notes

Version Beta
August 11, 2020

Here is what you get with Qualys EDR Beta!

Introducing Qualys EDR (Beta)

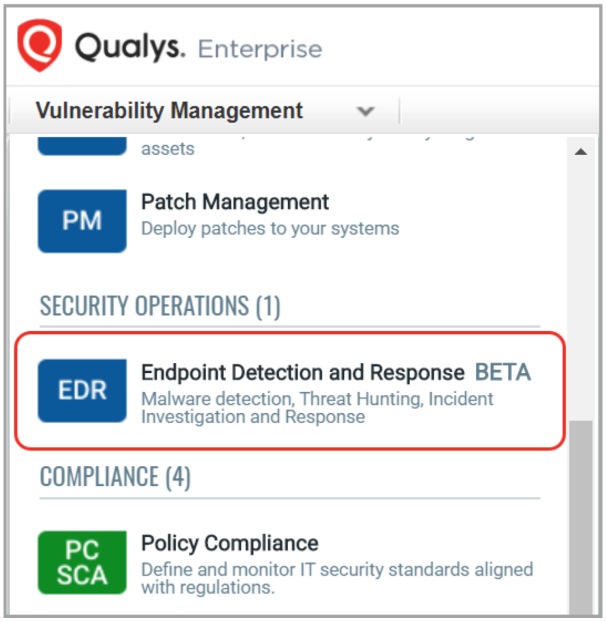
We are excited to introduce a new app, Endpoint Detection and Response (EDR).

EDR is an evolved superset of the IOC app. EDR expands the capabilities of the Qualys Cloud Platform to deliver threat hunting and Remediation response. EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation response for your assets.

EDR unifies different context vectors like asset discovery, rich normalized software inventory, end-of-life visibility, vulnerabilities and exploits, misconfigurations, in-depth endpoint telemetry, and network reachability with a powerful backend to correlate it all for accurate assessment, detection and response all, in a single, cloud-based app.

Once you are upgraded to EDR, the Indication of Compromise module will be renamed to Endpoint Detection and Response.

You will notice this change in the module picker.

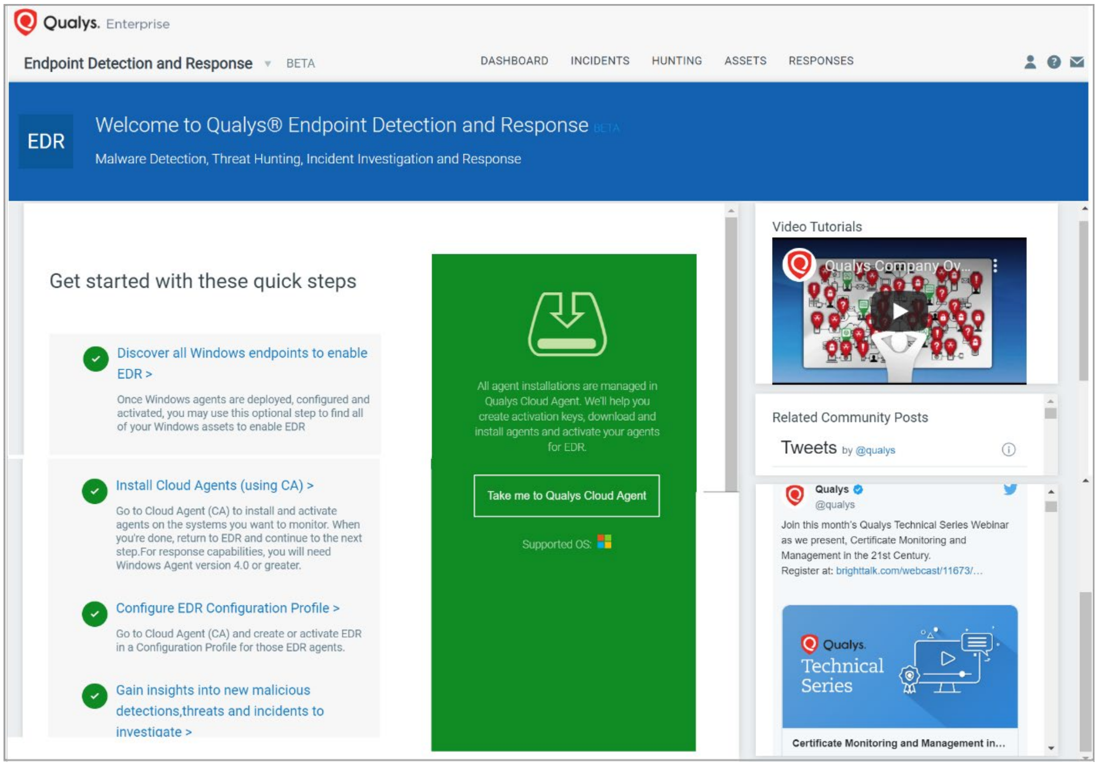

Qualys. Enterprise
Vulnerability Management
assets
PM
Patch Management
Deploy patches to your systems
SECURITY OPERATIONS (1)
EDR
Endpoint Detection and Response BETA
Malware detection, Threat Hunting, Incident Investigation and Response
COMPLIANCE (4)
PC SCA
Policy Compliance
Define and monitor IT security standards aligned with regulations.

For more information on the EDR app, contact your Technical Account Manager (TAM) or Qualys Support.

EDR Welcome Page

Once EDR is enabled in your subscription, you will see the Welcome page after you log in for the first time. The Welcome page helps you to get started in a few quick steps.

This page gives you a quick overview of what you'll get with EDR plus a high-level workflow of EDR.



Welcome to Qualys® Endpoint Detection and Response BETA

Malware Detection, Threat Hunting, Incident Investigation and Response

Get started with these quick steps

Discover all Windows endpoints to enable EDR >

Once Windows agents are deployed, configured and activated, you may use this optional step to find all of your Windows assets to enable EDR

Install Cloud Agents (using CA) >

Go to Cloud Agent (CA) to install and activate agents on the systems you want to monitor. When you're done, return to EDR and continue to the next step.For response capabilities, you will need Windows Agent version 4.0 or greater.

Configure EDR Configuration Profile >

Go to Cloud Agent (CA) and create or activate EDR in a Configuration Profile for those EDR agents.

Gain insights into new malicious detections,threats and incidents to investigate >

All agent installations are managed in Qualys Cloud Agent. We'll help you create activation keys, download and install agents and activate your agents for EDR.

Take me to Qualys Cloud Agent

Supported OS:

Video Tutorials

Related Community Posts

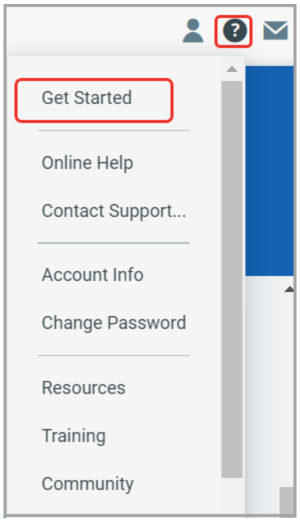
Tweets by @qualys

Qualys @qualys

Join this month's Qualys Technical Series Webinar as we present, Certificate Monitoring and Management in the 21st Century.
Register at: brighttalk.com/webcast/11673/...

Certificate Monitoring and Management in...

To revisit this page anytime just navigate to the Get Started in the Help menu.



New Remediation Response

The Remediation feature allows you to remediate the malicious events detected on the assets. You can perform the remediation action on file, process, mutex, and network events from the Hunting tab and Event Details page.

For malicious file events, you can perform the following remediation actions:

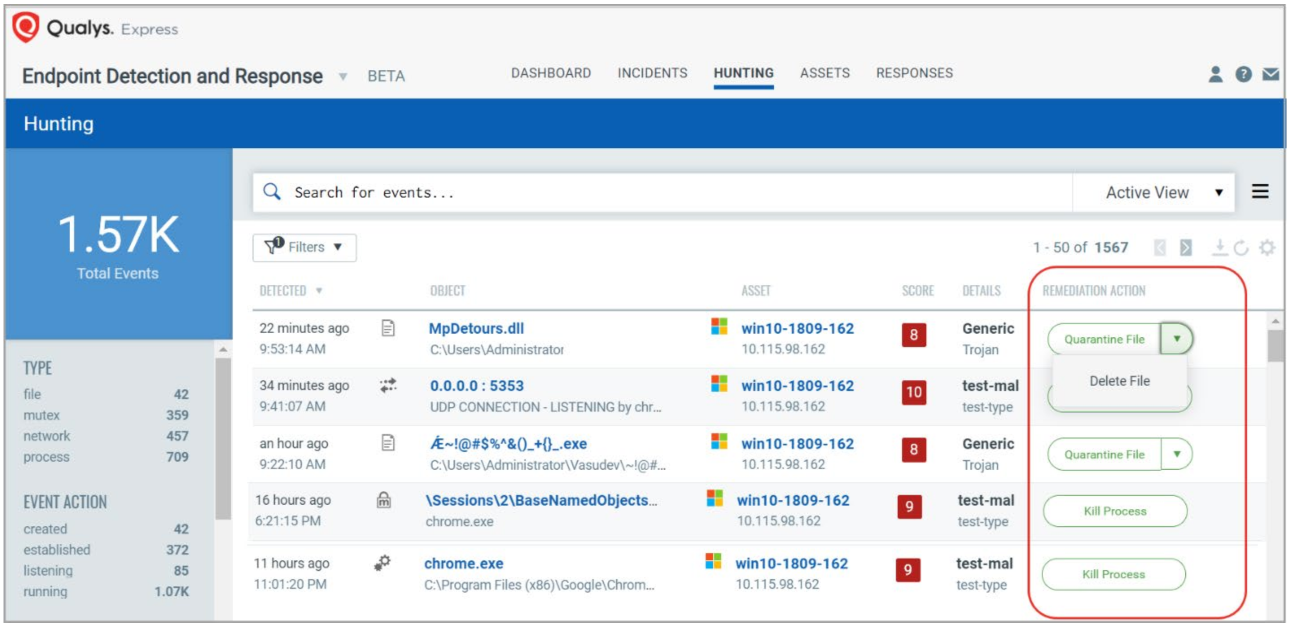
- **Quarantine File**: Using this option, the file is encrypted and moved to a Quarantine folder (C:\ProgramData\Qualys\QualysAgent\Quarantine\) on your asset. This Quarantine folder is automatically created once you upgrade to agent 4.0 and above. You can undo this action and restore the file to its original position using the Release option from the User Activity tab under Responses.
- **Delete File**: Using this option, the file is permanently deleted from your asset. You cannot undo this action.

For process, mutex, and network malicious events, you can perform the remediation action **Kill Process**.

All the remediation actions performed on events can be viewed from the User Activity tab.

The remediation actions under the Remediation Action column and Events Detail page are displayed only for:

- Events in Active View
- Events that score between 2 to 10
- Assets that have Cloud Agent version 4.0 and above installed.



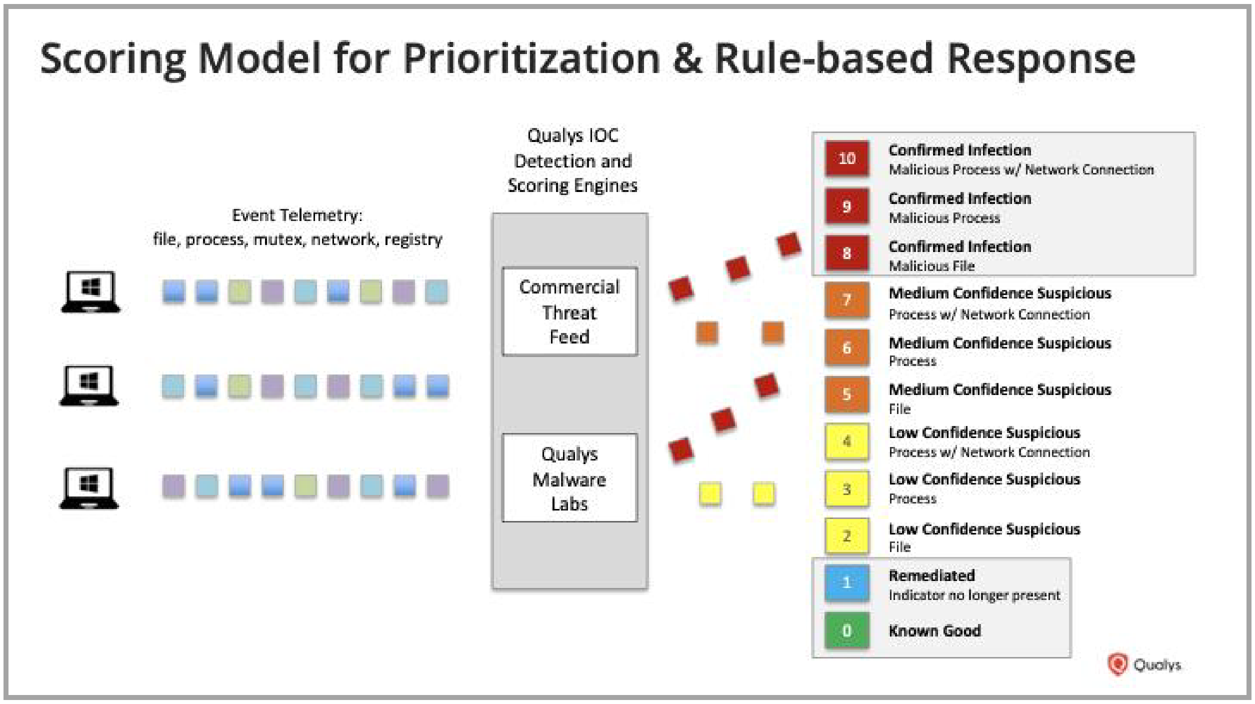
1.57K
Total Events

TYPE	
file	42
mutex	359
network	457
process	709

EVENT ACTION	
created	42
established	372
listening	85
running	1.07K

DETECTED	OBJECT	ASSET	SCORE	DETAILS	REMEDIATION ACTION
22 minutes ago 9:53:14 AM	MpDetours.dll C:\Users\Administrator	win10-1809-162 10.115.98.162	8	Generic Trojan	Quarantine File ▾ Delete File
34 minutes ago 9:41:07 AM	0.0.0.0 : 5353 UDP CONNECTION - LISTENING by chr...	win10-1809-162 10.115.98.162	10	test-mal test-type	
an hour ago 9:22:10 AM	Æ~!@#$%^&()_+{}_.exe C:\Users\Administrator\Vasudev\~!@#...	win10-1809-162 10.115.98.162	8	Generic Trojan	Quarantine File ▾
16 hours ago 6:21:15 PM	\Sessions\2\BaseNamedObjects... chrome.exe	win10-1809-162 10.115.98.162	9	test-mal test-type	Kill Process
11 hours ago 11:01:20 PM	chrome.exe C:\Program Files (x86)\Google\Chrom...	win10-1809-162 10.115.98.162	9	test-mal test-type	Kill Process

Score is automatically assigned to malicious events based on the severity, where 2 is lowest and 10 is the highest. Once the remediation action is executed on a malicious event, its score is reset to 1.



Scoring Model for Prioritization & Rule-based Response

Event Telemetry:
file, process, mutex, network, registry

Qualys IOC
Detection and
Scoring Engines

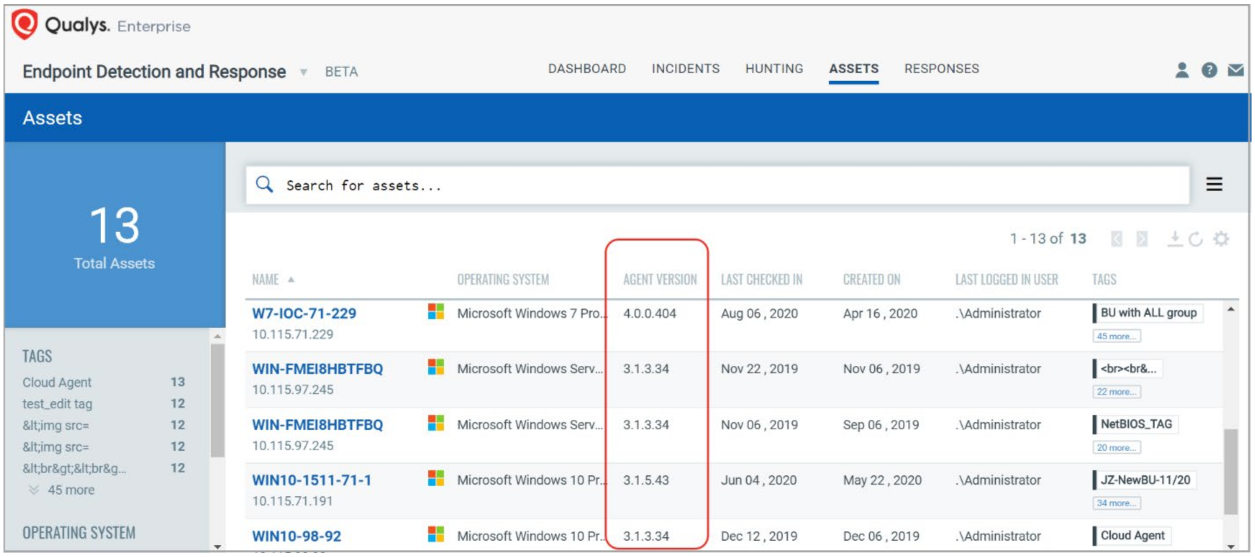
Commercial
Threat
Feed

Qualys
Malware
Labs

10	**Confirmed Infection** Malicious Process w/ Network Connection
9	**Confirmed Infection** Malicious Process
8	**Confirmed Infection** Malicious File
7	**Medium Confidence Suspicious** Process w/ Network Connection
6	**Medium Confidence Suspicious** Process
5	**Medium Confidence Suspicious** File
4	**Low Confidence Suspicious** Process w/ Network Connection
3	**Low Confidence Suspicious** Process
2	**Low Confidence Suspicious** File
1	**Remediated** Indicator no longer present
0	**Known Good**

View Cloud Agent Version for Asset

The Remediation response under the Hunting tab and Event Details page is displayed only if the Cloud Agent version is 4.0 and above. So, we have now added a new Agents Version column under the Assets tab to view the agent version installed on the asset.



TAGS	
Cloud Agent	13
test_edit tag	12
<img src=	12
<img src=	12

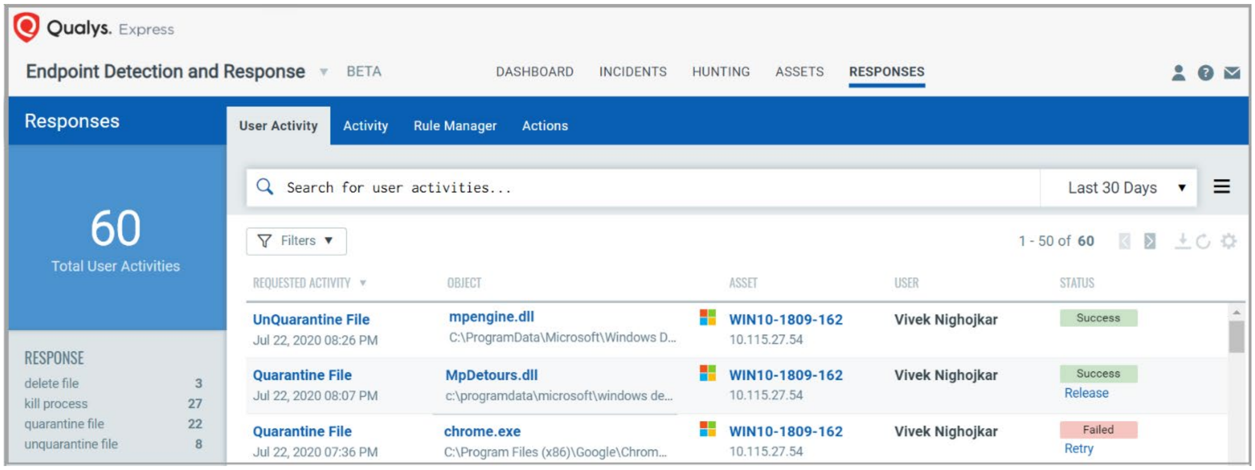
<br&g...	12
45 more	

NAME	OPERATING SYSTEM	AGENT VERSION	LAST CHECKED IN	CREATED ON	LAST LOGGED IN USER	TAGS
W7-IOC-71-229 10.115.71.229	Microsoft Windows 7 Pro...	4.0.0.404	Aug 06 , 2020	Apr 16 , 2020	.\Administrator	BU with ALL group 45 more...
WIN-FMEI8HBTFBQ 10.115.97.245	Microsoft Windows Serv...	3.1.3.34	Nov 22 , 2019	Nov 06 , 2019	.\Administrator	 <br&... 22 more...
WIN-FMEI8HBTFBQ 10.115.97.245	Microsoft Windows Serv...	3.1.3.34	Nov 06 , 2019	Sep 06 , 2019	.\Administrator	NetBIOS_TAG 20 more...
WIN10-1511-71-1 10.115.71.191	Microsoft Windows 10 Pr...	3.1.5.43	Jun 04 , 2020	May 22 , 2020	.\Administrator	JZ-NewBU-11/20 34 more...
WIN10-98-92	Microsoft Windows 10 Pr...	3.1.3.34	Dec 12 , 2019	Dec 06 , 2019	.\Administrator	Cloud Agent

New User Activity Page

The User Activity tab lists all the remediation actions performed on malicious events along with the following details:

- The requested remediation action along with the date and time.
- The object (file/process) and the asset on which the remediation action is performed.
- The user who performed the remediation action.
- The current status of the remediation action.

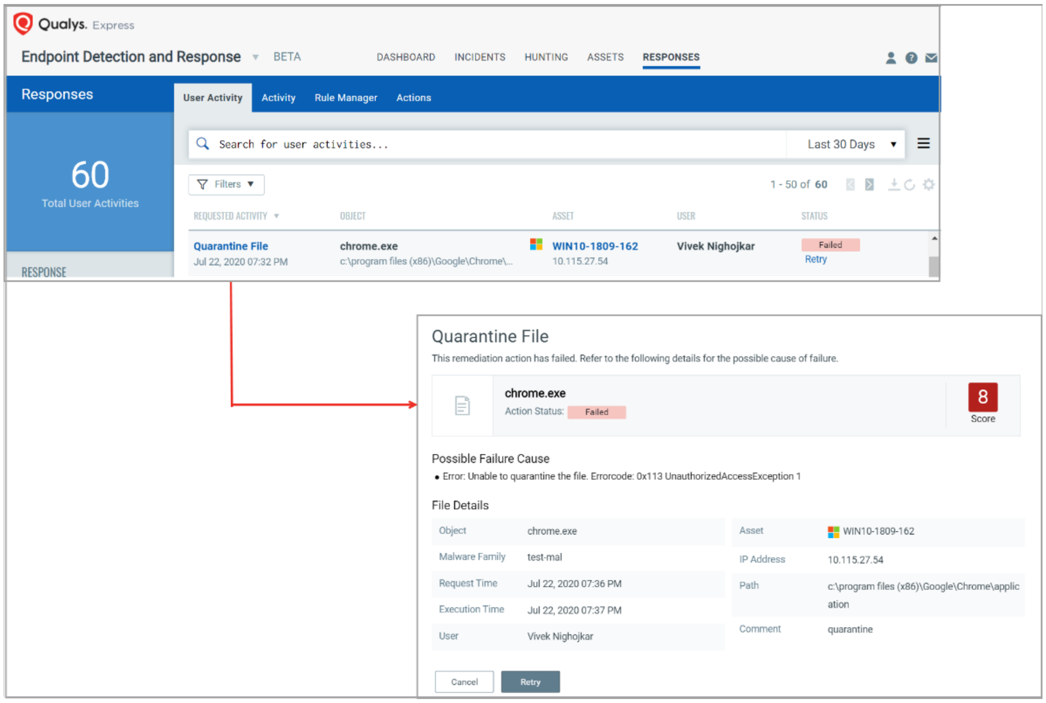


REQUESTED ACTIVITY	OBJECT	ASSET	USER	STATUS
UnQuarantine File Jul 22, 2020 08:26 PM	mpengine.dll C:\ProgramData\Microsoft\Windows D...	WIN10-1809-162 10.115.27.54	Vivek Nighojkar	Success
Quarantine File Jul 22, 2020 08:07 PM	MpDetours.dll c:\programdata\microsoft\windows de...	WIN10-1809-162 10.115.27.54	Vivek Nighojkar	Success Release
Quarantine File Jul 22, 2020 07:36 PM	chrome.exe C:\Program Files (x86)\Google\Chrom...	WIN10-1809-162 10.115.27.54	Vivek Nighojkar	Failed Retry

RESPONSE

delete file	3
kill process	27
quarantine file	22
unquarantine file	8

If you would like to know additional information about the remediation action, click on the remediation action from the Requested Activity column.



REQUESTED ACTIVITY	OBJECT	ASSET	USER	STATUS
Quarantine File Jul 22, 2020 07:32 PM	chrome.exe c:\program files (x86)\Google\Chrome\...	WIN10-1809-162 10.115.27.54	Vivek Nighojkar	Failed Retry

Quarantine File

This remediation action has failed. Refer to the following details for the possible cause of failure.

chrome.exe
Action Status: Failed
8 Score

Possible Failure Cause

- Error: Unable to quarantine the file. Errorcode: 0x113 UnauthorizedAccessException 1

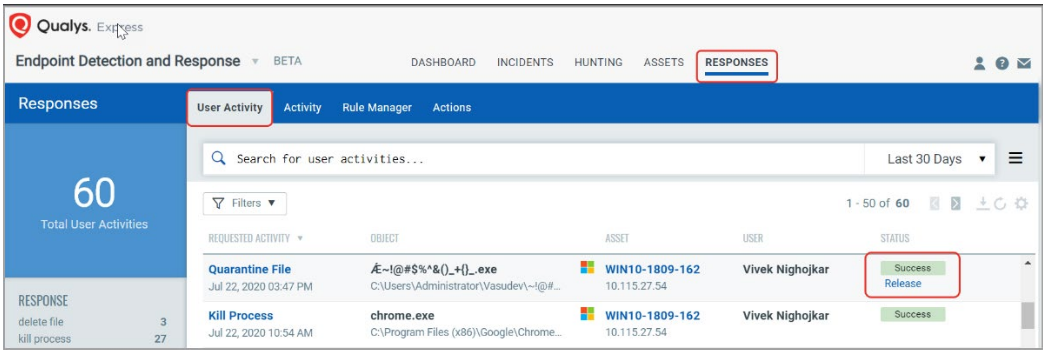
File Details

Object	chrome.exe	Asset	WIN10-1809-162
Malware Family	test-mal	IP Address	10.115.27.54
Request Time	Jul 22, 2020 07:36 PM	Path	c:\program files (x86)\Google\Chrome\application
Execution Time	Jul 22, 2020 07:37 PM	Comment	quarantine
User	Vivek Nighojkar		

Note: You can download the User Activity report in CSV format from the Responses tab.

You can also perform the following two actions from the User Activity tab:

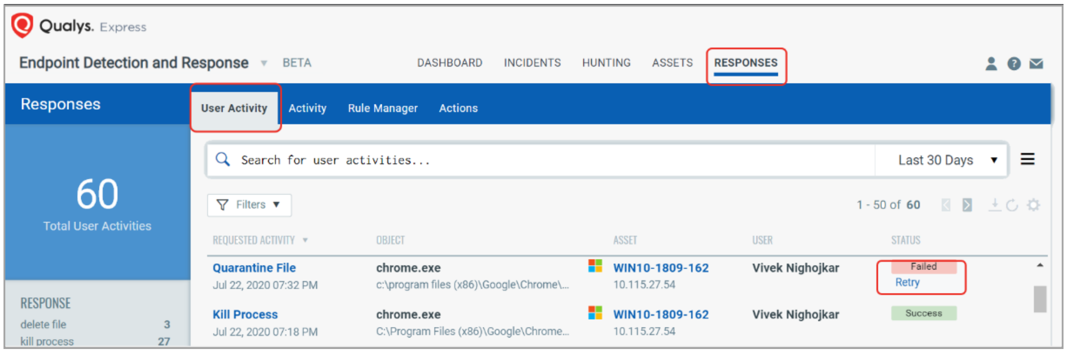
- **Release**: Using this option, you can restore the Quarantine file back to its original position.



RESPONSE	
delete file	3
kill process	27

REQUESTED ACTIVITY	OBJECT	ASSET	USER	STATUS
Quarantine File Jul 22, 2020 03:47 PM	Æ~!@#$%^&()_+{}_.exe C:\Users\Administrator\Vasudev\~!@#...	WIN10-1809-162 10.115.27.54	Vivek Nighojkar	Success Release
Kill Process Jul 22, 2020 10:54 AM	chrome.exe C:\Program Files (x86)\Google\Chrome...	WIN10-1809-162 10.115.27.54	Vivek Nighojkar	Success

- **Retry**: Using this option, you can retry the remediation action on failed events.



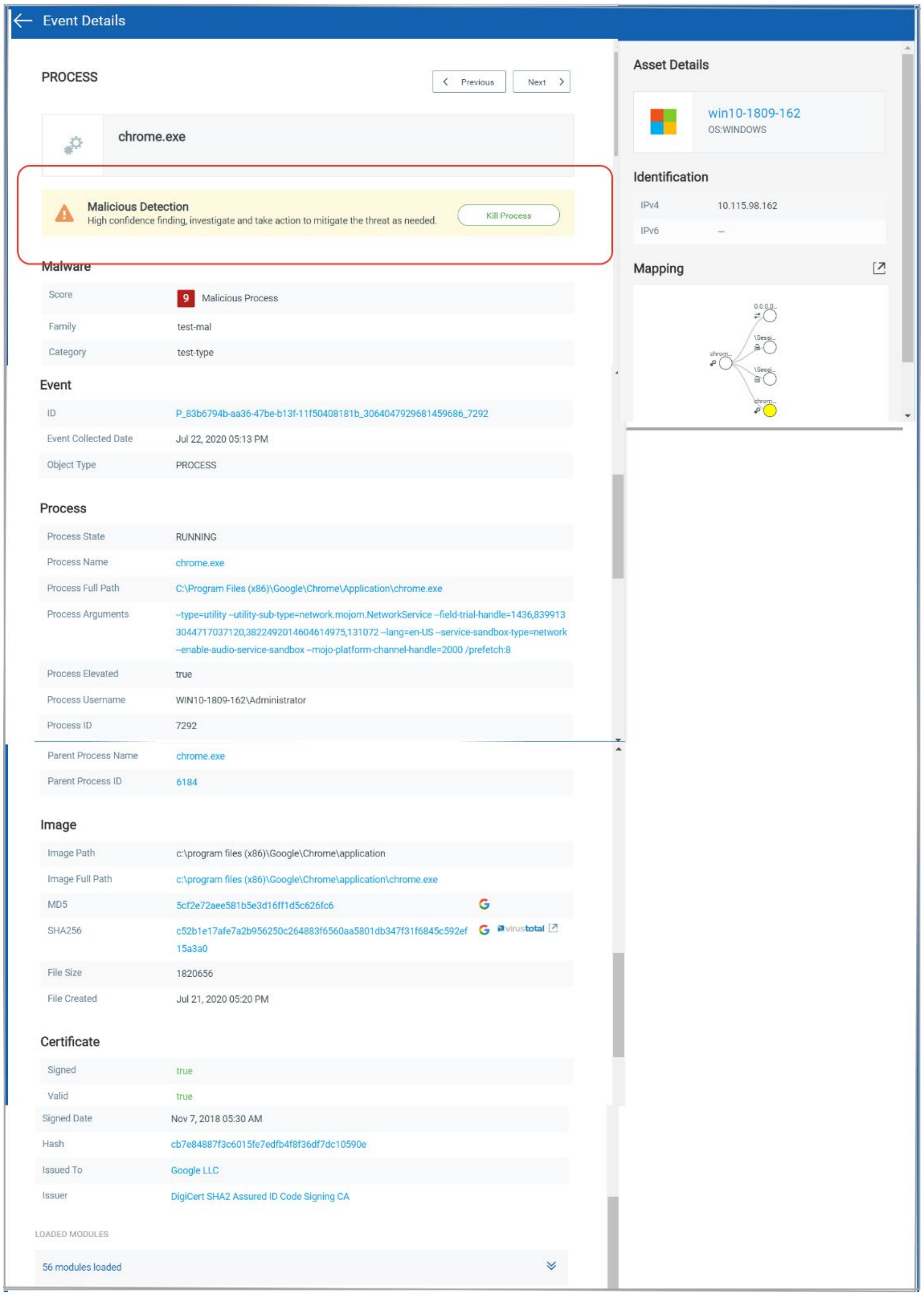
RESPONSE	
delete file	3
kill process	27

REQUESTED ACTIVITY	OBJECT	ASSET	USER	STATUS
Quarantine File Jul 22, 2020 07:32 PM	chrome.exe c:\program files (x86)\Google\Chrome\...	WIN10-1809-162 10.115.27.54	Vivek Nighojkar	Failed Retry
Kill Process Jul 22, 2020 07:18 PM	chrome.exe C:\Program Files (x86)\Google\Chrome...	WIN10-1809-162 10.115.27.54	Vivek Nighojkar	Success

View Events Details Page

We have made the following changes to Event Details tab:

- For enhanced customer experience and better usability, we have changed the layout of the Event Details page.
- You can also perform Remediation actions for File, Process, Network, and Mutex events from the Event Details page.



PROCESS

chrome.exe

Malicious Detection
High confidence finding, investigate and take action to mitigate the threat as needed.

Malware

Score	9 Malicious Process
Family	test-mal
Category	test-type

Event

ID	P_83b6794b-aa36-47be-b13f-11f50408181b_3064047929681459686_7292
Event Collected Date	Jul 22, 2020 05:13 PM
Object Type	PROCESS

Process

Process State	RUNNING
Process Name	chrome.exe
Process Full Path	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Process Arguments	--type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1436,8399133044717037120,3822492014604614975,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=2000 /prefetch:8
Process Elevated	true
Process Username	WIN10-1809-162\Administrator
Process ID	7292
Parent Process Name	chrome.exe
Parent Process ID	6184

Image

Image Path	c:\program files (x86)\Google\Chrome\application
Image Full Path	c:\program files (x86)\Google\Chrome\application\chrome.exe
MD5	5cf2e72aee581b5e3d16ff1d5c626fc6
SHA256	c52b1e17afe7a2b956250c264883f6560aa5801db347f31f6845c592ef15a3a0 virustotal
File Size	1820656
File Created	Jul 21, 2020 05:20 PM

Certificate

Signed	true
Valid	true
Signed Date	Nov 7, 2018 05:30 AM
Hash	cb7e84887f3c6015fe7edfb4f8f36df7dc10590e
Issued To	Google LLC
Issuer	DigiCert SHA2 Assured ID Code Signing CA

LOADED MODULES

56 modules loaded

Asset Details

win10-1809-162
OS:WINDOWS

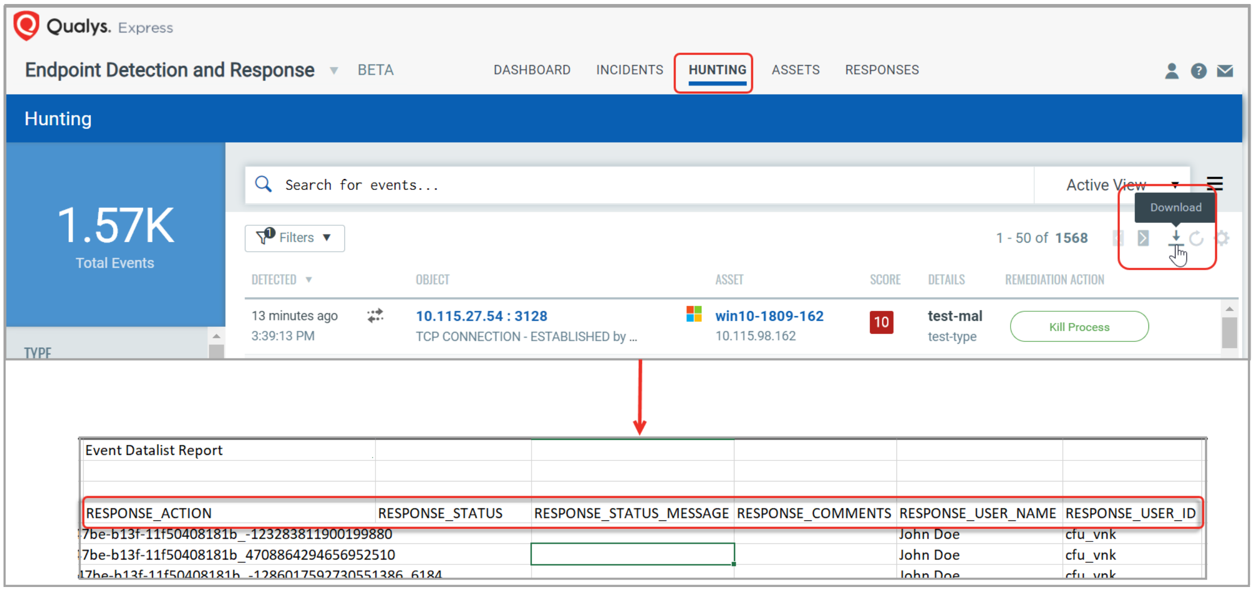
Identification

IPv4	10.115.98.162
IPv6	–

View Event Datalist Report

For better clarity and understanding of the remediation action performed, we have added the following new columns to the Event Datalist report:

- RESPONSE_ACTION
- RESPONSE_STATUS
- RESPONSE_STATUS_MESSAGE
- RESPONSE_COMMENTS
- RESPONSE_USER_NAME
- RESPONSE_USER_ID



Event Datalist Report

RESPONSE_ACTION	RESPONSE_STATUS	RESPONSE_STATUS_MESSAGE	RESPONSE_COMMENTS	RESPONSE_USER_NAME	RESPONSE_USER_ID
7be-b13f-11f50408181b_-123283811900199880				John Doe	cfu_vnk
7be-b13f-11f50408181b_4708864294656952510				John Doe	cfu_vnk
17be-b13f-11f50408181b_-1286017592730551386_6184				John Doe	cfu_vnk

New Remediation Tokens

We have added the following new tokens on the Hunting tab and User Activity tab to support the Remediation feature.

- **response.action:** This token allows you to find events based on the remediation action. Possible values: Delete File, Kill Process, Quarantine File, and Unquarantine File.
- **response.status:** This token allows you find events based on the remediation status Possible values: failed, in_progress, success.
- **response.user:** This token allows you to list remediation actions executed by a certain user.
- **response.userId:** This token allows you to list remediation actions executed by a certain username.
- **response.timestamp:** This token allows you to list all the remediation action executed on a specific date or in a time-frame.
- **response.comments:** This token allows you to list events by the comments added while initiating the remediation action**.**
- **response.priorScore:** This token allows you to list events by the score before executing the remediation action.
- **response.statusMessage:** This token allows you to list events by status message displayed after the remediation action is completed.

For more information on the token usage, refer to the Online Help.