



Qualys Indication of Compromise v2.x

Release Notes

Version 2.2

November 14, 2019

Here's what's new in Qualys IOC 2.2!

[New Filters Added to group Incidents and Events](#)

[Find More Information on Web for MD5 and SHA256 hash values](#)

[Added Details Column on the Events List Page to Show Malware Information](#)

[Links Shown in Columns on Incidents/Hunting/Assets pages to Open in a New Browser](#)

Qualys IOC 2.2 brings you many more improvements and updates! [Learn more](#)

Enhancements to IOC UI

New Filters Added to group Incidents and Events

We have added two new group by options: "Malware Category" and "Score". "Malware Category" option on the Incidents > Hosts tab groups hosts by the malware category and "Score" option groups events on the Hunting tab by a malware score. Operating System filter on the Hosts tab is removed.

The screenshot displays the Qualys IOC UI with two main sections: Incidents and Hunting. The Incidents section shows a filter for 'asset.malware.category:trojan' and a table of incidents. The Hunting section shows a table of events. Red circles highlight the 'INCIDENTS' and 'HUNTING' tabs, the 'MALWARE CATEGORY' filter, and the 'SCORE' filter.

Malware Family	Score	Age	Name
trojan	8	5 months ago	WIN10-98-57
trojan	8	4 months ago	W7-IOC-71-228
trojan	8	3 months ago	WIN-890BLRMESC6
trojan	8	5 months ago	WIN-890BLRMESC6

TYPE	SCORE
file	42.0K
mutex	1.04K
network	577
process	326
registry	64.0K

TIME	OBJECT
2 minutes ago	10.115.27.54 : 3128
12:41:47 PM	TCP CONNECTION - ESTABLISHED by QualysAgent.exe
2 minutes ago	\BaseNamedObjects\Spooler_Perf_Library_Lo...
12:41:47 PM	WmiPrivSE.exe
2 minutes ago	\BaseNamedObjects\Lsa_Perf_Library_Lock_P...
12:41:47 PM	WmiPrivSE.exe
2 minutes ago	\BaseNamedObjects\MSDTC Bridge 4.0.0.0_P...
12:41:47 PM	WmiPrivSE.exe
2 minutes ago	\BaseNamedObjects\PerfOS_Perf_Library_Loc...
12:41:47 PM	WmiPrivSE.exe
2 minutes ago	\BaseNamedObjects\Windows Workflow Foun...
12:41:47 PM	WmiPrivSE.exe
2 minutes ago	\BaseNamedObjects\TermService_Perf_Librar...
12:41:47 PM	WmiPrivSE.exe
2 minutes ago	\BaseNamedObjects\NET CLR Data_Perf_Libr...
12:41:47 PM	WmiPrivSE.exe

Find More Information on Web for MD5 and SHA256 hash values

On the Event Details page, we now show a Google icon next to MD5 and SHA256 hash values for all the 5 types of events, such as file, process and so on. When you click the Google icon, we find and show, on a browser window, links to the Web sites that provides more information on MD5 and SHA256 hash values detected for events.

The screenshot displays the Event Details page for a file named 'AM_2_KNOWN (4)11.exe'. It shows event details, file details, and file properties. A red circle highlights the Google icon next to the MD5 and SHA256 hash values.

FILE

File Name: AM_2_KNOWN (4)11.exe
Score: 8

EVENT DETAILS

ID: F_fe1378a2-631a-4981-aecb-28edac4ff332_7672350864194888312
Event Collected Date: Aug 4, 2019 07:28 PM
Object Type: FILE

FILE DETAILS

File Action: CREATED
File Name: AM_2_KNOWN (4)11.exe
Path: C:\\$Recycle.bin\S-1-5-21-371398205-1171949018-4186074538-500\SRM08D8T
Full Path: C:\\$Recycle.bin\S-1-5-21-371398205-1171949018-4186074538-500\SRM08D8T\AM_2_KNOWN (4)11.exe
MD5: ee59d48138ba340578c8ff8d1436d
SHA256: 2da488fcca1c206db6e54a844b1654e478e82308dab03c5ff0ebf605f9d22605

FILE PROPERTIES

File Size: 180736
File Created: Aug 4, 2019 02:03 PM
File Modified: Apr 24, 2019 04:16 AM
File Accessed: Aug 4, 2019 02:03 PM
Product: --
Company: --
Copyright: --
Description: --
Version: --

Added Details Column on the Hunting page to Show Malware Information

We have added a new column "Details" on the Hunting page to show malware family and category information for the events.

Indication of Compromise ▾ DASHBOARD INCIDENTS **HUNTING** ASSETS RULES

Hunting

108K Total Events

TYPE

- file 42.0K
- mutex 1.02K
- network 576
- process 325
- registry 64.0K

EVENT ACTION

- created 106K
- established 239
- listening 337
- running 1.34K

Search for events... Active View ▾

1 - 50 of 107888

TIME ▾	OBJECT	ASSET	SCORE	DETAILS
4 months ago 7:28:00 PM	AM_2_KNOWN (4)11.exe C:\\$Recycle.bin\S-1-5-21-371398205-1171949018-418...	WIN-890BLRMESC6 10.115.71.159	8	Generic Trojan
4 months ago 3:56:27 PM	AM_2_MALICIOUS - Copy1.exe C:\Users\Administrator\OD\Sanity	W7-IOC-71-228 10.115.71.228	8	Generic Trojan
4 months ago 3:54:49 PM	AT_KNOWN (2).exe C:\\$Recycle.bin\S-1-5-21-122566442-3410611961-122...	W7-IOC-71-228 10.115.71.228	8	Generic Trojan
4 months ago 3:54:50 PM	AM_2_MALICIOUS - Copy.exe C:\\$Recycle.bin\S-1-5-21-122566442-3410611961-122...	W7-IOC-71-228 10.115.71.228	8	Generic Trojan
4 months ago 12:22:44 PM	AM_MALICIOUS_123.exe C:\Users\Administrator\OD\10Aug	WIN-890BLRMESC6 10.115.71.159	8	Generic Trojan
4 months ago 12:22:44 PM	AM_2_KNOWN (2).exe C:\Users\Administrator\OD\10Aug	WIN-890BLRMESC6 10.115.71.159	8	Generic Trojan

Links Shown in Columns on Incidents/Hunting/Assets pages to Open in a New Browser

You can now open the links shown in columns on Incidents/Hunting/Assets pages in a new browser window. We support this action for these columns: 1) Name and Infections columns in the Incidents > Hosts tab, 2) Object and Score columns in the Hunting tab and Name column in the Assets tab can be opened in the new browser window. 3) Infected Assets columns in the Incidents > Malware tab.

Indication of Compromise ▾ DASHBOARD INCIDENTS **HUNTING** ASSETS RULES

Incidents

6 Total Incidents

MALWARE FAMILY

- generic 6
- psexec 2

MALWARE CATEGORY

- trojan 6
- pua 2

Search for incidents... Active View ▾

10 5 0

2 3 4 5 6 7 8 9 10

1 - 6 of 6

SCORE ▾	AGE	NAME	OPERATING SYSTEM	# INFECTIONS	MALWARE FAMILIES
8	5 months ago 10:00:20 PM	WIN10-98-57	Windows	6	Generic
8	4 months ago 3:58:33 PM	W7-IOC-71-228	Microsoft Windows 7 Professiona...	84	Psexec Generic
8	3 months ago 2:08:30 PM	WIN-890BLRMESC6	Windows	82	Generic
8	5 months ago 6:13:01 PM	WIN-890BLRMESC6	Windows Server 2012 R...	46	Generic
8	5 months ago 6:12:59 PM	W7-IOC-71-228	Microsoft Windows 7 Professiona...	17	Psexec Generic
8	3 months ago 5:58:53 PM	WIN10-98-91	Windows	41	Generic

Issues Addressed

- We fixed an issue where the user was not receiving email alerts for events even after configuring SMTP.
- In the Date time picker, we renamed the option "Current State" to "Active View" on Dashboard, Incidents and Hunting pages. You will see date time picker next to Search box at the top of the page.
- We fixed an issue where the data in the downloaded Malware report was showing incorrect data. Now the report data matches the Malware data shown on UI.
- We fixed an issue where on the Incident > Malware tab, the malware family name was not shown in the "Malware Family Name" column.
- We added a new token "process.fullPath" to search events by full path of the process on the Hunting page.
- The host/incidents listed in the Incidents > Hosts tab and events listed in the Hunting tab are now sorted by malware score in the descending order (high to low score).
- We made the #Infections column on the Incidents > Hosts page sortable.
- We fixed an issue where in the Incidents/Hunting/Assets page longer search queries in the search bar was getting overlapped with the text below the search bar. Now we have provided an opaque background when displaying longer queries in the search bar to fix this issue.
- We are showing more information for events in the CSV file downloaded using the Download option on the Hunting page. We have added the following columns: TIME , TYPE, ACTION, IMAGE_NAME, IMAGE_FULL_PATH, PROCESS_ARGS, PROCESS_ELEVATED, PROCESS_USERNAME, MD5, SHA256, PID, PARENT_PID, HANDLE_NAME, SRC_IP, SRC_PORT, DST_IP, DST_PORT, DST_FQDN, PROTO, REG_KEY, REG_VALUE, REG_DATA, ASSET_HOSTNAME, ASSET_IP4, INDICATOR_SCORE, EVENT_ID.