Qualys Indication of Compromise v2.x

Release Notes

Version 2.2
November 14, 2019

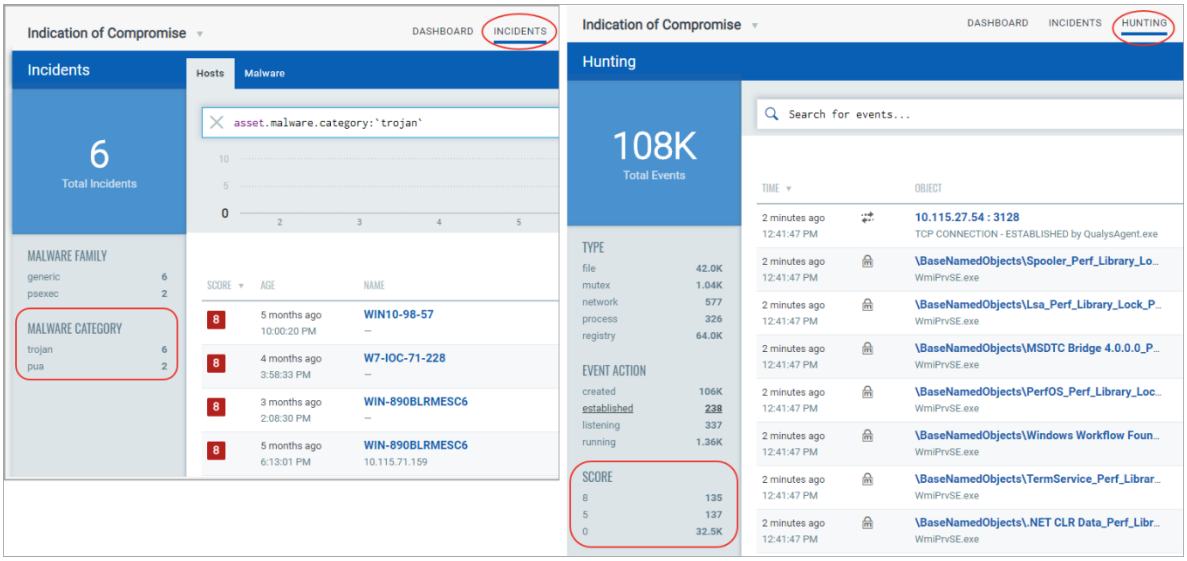
Here's what's new in Qualys IOC 2.2!

Qualys IOC 2.2 brings you many more improvements and updates! Learn more

Enhancements to IOC UI

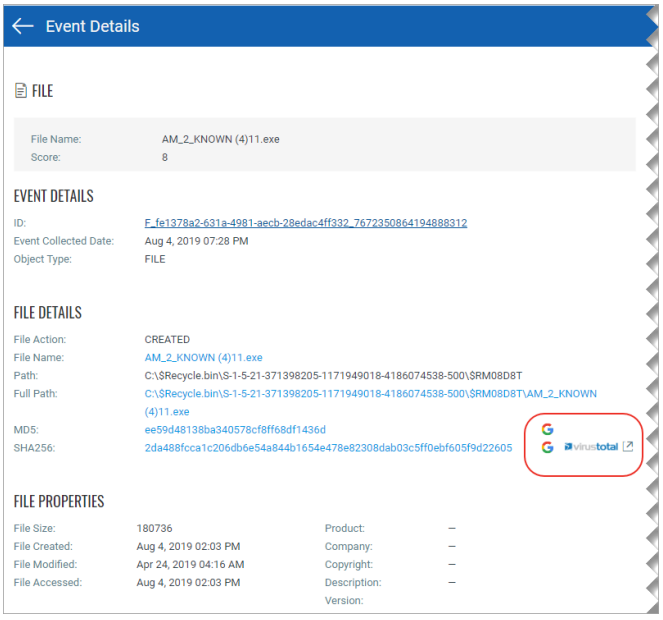
New Filters Added to group Incidents and Events

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.



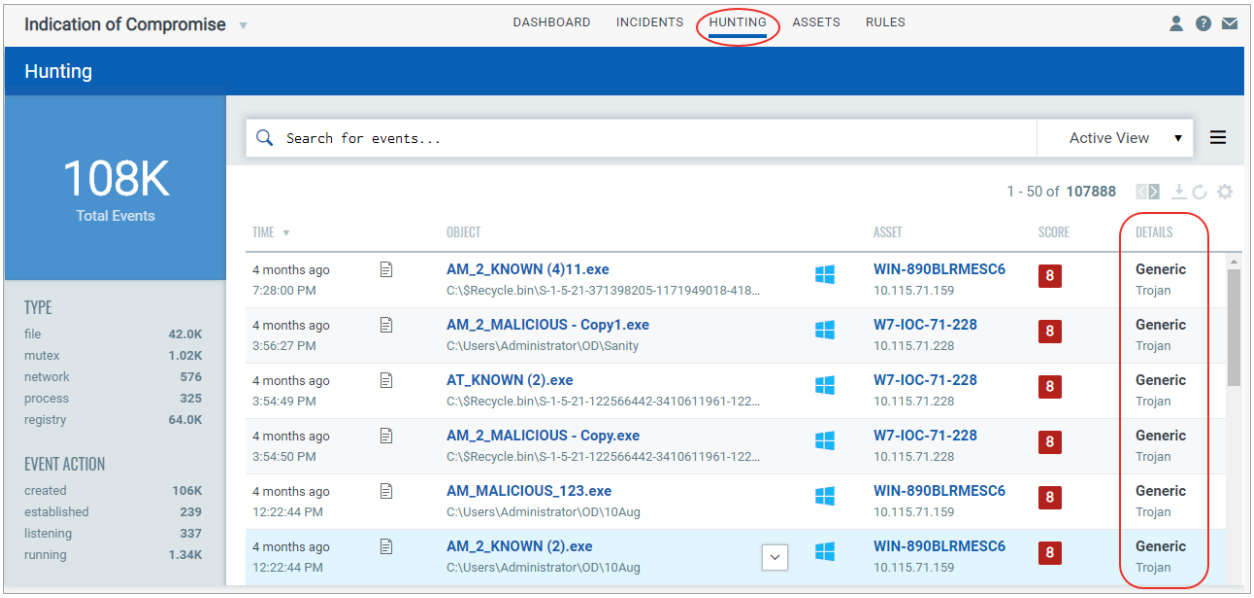
Find More Information on Web for MD5 and SHA256 hash values

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.



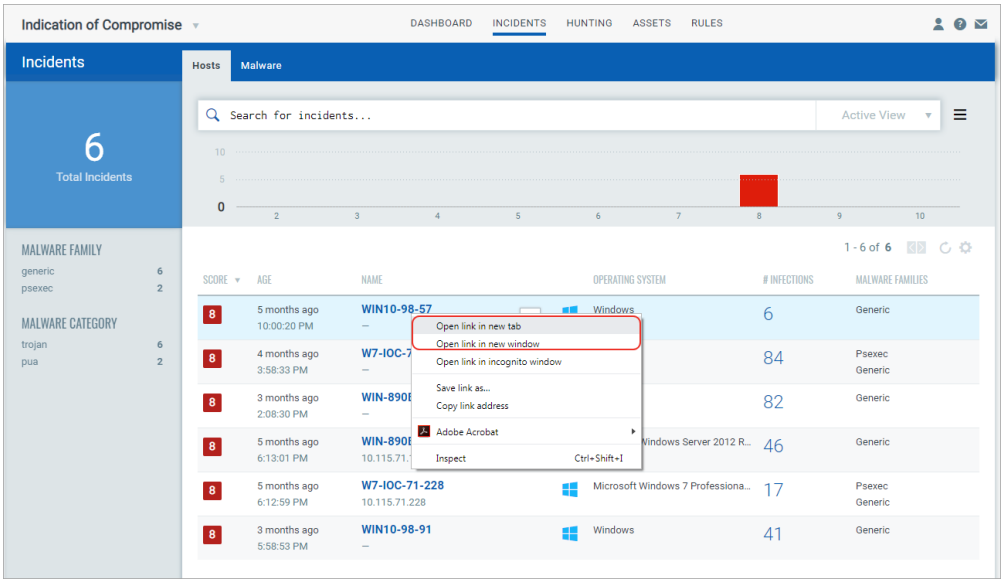
Added Details Column on the Hunting page to Show Malware Information

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



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.



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.