



Qualys Indication of Compromise v2.x

Release Notes

Version 2.0

June 4, 2019

Here's what's new in Qualys IOC 2.0!

Qualys Cloud Platform

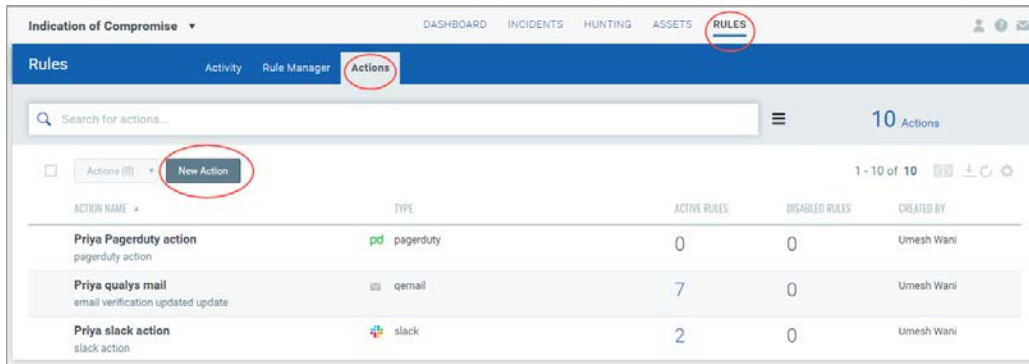
[Configure Rule Based Alerts for Events](#)
[New Default Date Filter "Current State" Added](#)
[Event Details to Show Hierarchy for Events](#)

Configure Rule Based Alerts for Events

You can now configure IOC to monitor events for conditions specified in a rule and send you alerts if events matching the condition is detected. For IOC to send alerts, you need to first configure a rule action to specify what action to be taken when events matching a condition is detected. IOC will use the rule action settings to send you the alerts. Finally, create a rule to specify the conditions for triggering the rule and select rule actions for sending the alert when a rule is triggered.

Create a New Action

To create an action, go to Rules > Actions > New Action.



Basic Information

Action Name Required

Description Required
Add a brief description for this action

Select Action Required
Send Email(Via Qualys)

Default Message Settings
You can add default recipients or edit the default message to be sent

Recipients Required
Separate emails using commas (,) between addresses

Subject Line Required

Message Required
7/5000

In the Basic Information section, provide name and description of the action in the Action name and Description fields respectively.

Select an action from the Select Action drop-down and provide the settings for configuring the messaging system that IOC will use to send alerts.

We support these three actions: Send Email (Via Qualys), Post to Stack and Send to Pager Duty for alerts.

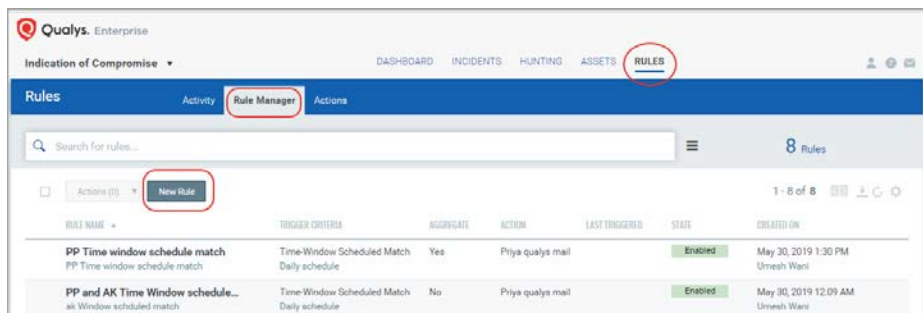
Select Send Email (Via Qualys) to receive email alerts and specify the recipients' email ID who will receive the alerts, subject of the alert message and the customized alert message.

Select "Send to PagerDuty" to send alerts to your PagerDuty account. Provide the service key that IOC will require to connect to your PagerDuty account. In Default Message Settings, specify the subject and the customized alert message.

Select “Post to Stack” to post alert messages to your Slack account. Provide the Webhook URI that IOC will use to connect to your slack account to post alert messages. In Default Message Settings, specify the subject of the alert message and the customized alert message.

Create a New Rule

To create a rule, go to Rules > Rule Manager > New Rule. You can also create rules from the customized queries that are used for widgets on your dashboard. Select the Widget menu and choose “Create Rule from this Widget”. This option is also available on the Hunting page. Go to the Hunting tab and select “Create Rule from Search Query” from the Actions menu on the top right.



In the Rule Information section, provide a name and description of the new rule in the Rule Name and Description.

In the Rule Query section, specify a query for the rule. The system uses this query to search for events. Use the Test Query button to test your query. Click Sample Queries link to select from predefined queries.

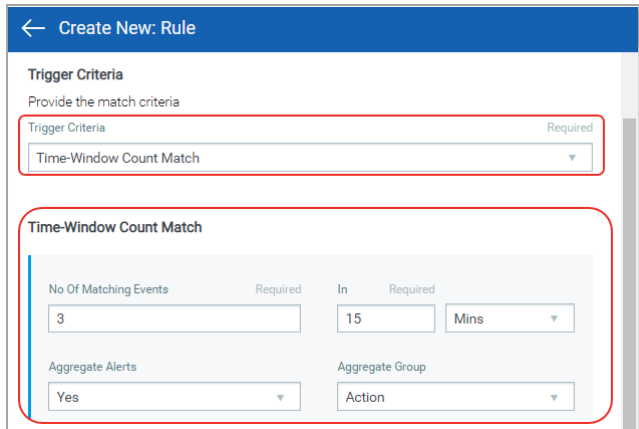
You can choose from three trigger criteria that work in conjunction with the rule query. The trigger criteria are: Single Match, Time-Window Count Match and Time-Window Scheduled Match.

In the Action Settings section choose the actions that you want the system to perform when an alert is triggered.

Trigger Criteria

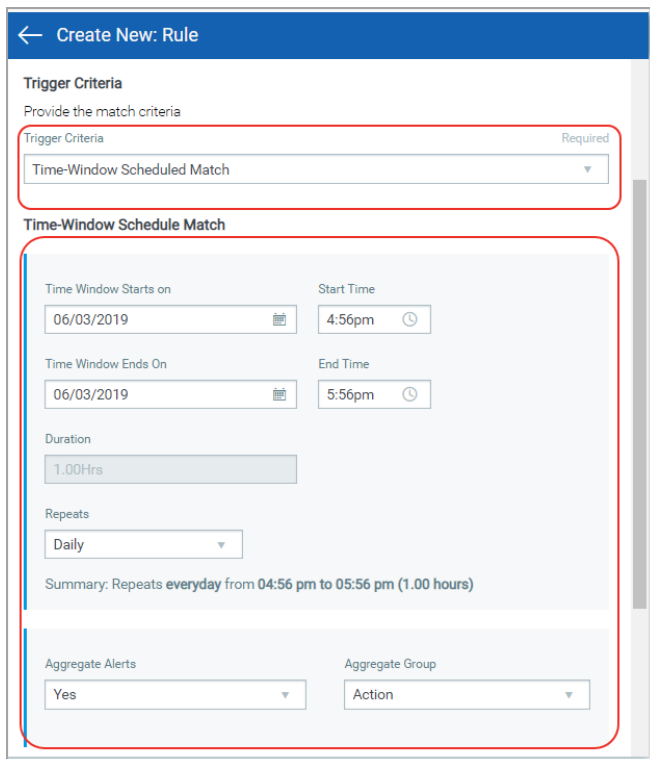
Select Single Match if you want the system to generate an alert each time the system detects an event matching your search query.

Select Time-Window Count Match when you want to generate alerts based on the number of events returned by the search query in a fixed time interval. For example, an alert will be sent when three matching events are found within 15 mins window.



The screenshot shows the 'Create New: Rule' interface. Under the 'Trigger Criteria' section, 'Time-Window Count Match' is selected. The configuration for this match type includes: 'No Of Matching Events' set to 3, 'In' set to 15 Mins, 'Aggregate Alerts' set to Yes, and 'Aggregate Group' set to Action.

Select Time-Window Scheduled Match when you want to generate alerts for matching events that occurred during a scheduled time. The rule will be triggered only when an event matching your search criteria is found during the time specified in the schedule. Choose a date and time range for creating a schedule and specify how often you want to run the schedule for example, daily, weekly and monthly. For example, send daily alerts with all matches in a scheduled window between 4 pm and 5 pm.



The screenshot shows the 'Create New: Rule' interface. Under the 'Trigger Criteria' section, 'Time-Window Scheduled Match' is selected. The configuration for this match type includes: 'Time Window Starts on' 06/03/2019, 'Start Time' 4:56pm, 'Time Window Ends On' 06/03/2019, 'End Time' 5:56pm, 'Duration' 1.00Hrs, and 'Repeats' set to Daily. A summary line reads: 'Summary: Repeats everyday from 04:56 pm to 05:56 pm (1.00 hours)'. 'Aggregate Alerts' is set to Yes and 'Aggregate Group' is set to Action.

For the Weekly option, select the days of the week on which schedule will run. For example, send weekly alerts with all matches generated between 4.56 pm and 5.56 pm on every Monday and Wednesday.

The screenshot shows the 'Create New: Rule' interface with the following configuration:

- Repeats:** Weekly
- On Day Of The Week:** S M T W T F S
- Summary:** Repeats **monday** from **04:56 pm** to **05:56 pm** (1.00 hours)

For the Monthly option, specify the day of the month on which the schedule will run. For example, send monthly alerts on the first day of every month.

The screenshot shows the 'Create New: Rule' interface with the following configuration:

- Repeats:** Monthly
- Recurring Day:** 1 day of the month
- Summary:** Repeats every 1st day of the month from **04:56 pm** to **05:56 pm** (1.00 hours)
- Aggregate Alerts:** Yes
- Aggregate Group:** Action

For “Select Time-Window Count Match” and “Select Time-Window Scheduled Match”, you have the option to aggregate the alerts by aggregate groups such as based on action, asset hostname and so on.

Manage Actions

View the newly created actions in the Actions tab with the details such as name of the action, type of the action, the number of rules for which this action is chosen are active or inactive and the user who created the rule. You can use the Actions menu or Quick Actions menu to edit, delete and rename an action. Use the search bar to search for actions using the search tokens.

The screenshot shows the 'Manage Actions' interface. The 'RULES' section is active, and the 'Actions' tab is selected. A search bar is present at the top. Below it, there's a table of actions. The first row is highlighted, and a 'Quick Actions' menu is open over it, showing options for 'Edit', 'Save As', and 'Delete'.

ACTION NAME	TYPE	ACTIVE RULES	DISABLED RULES	CREATED BY
<input checked="" type="checkbox"/> Priya Pagerduty action pagerduty action	pd pagerduty	0	0	Umesh Wani
<input type="checkbox"/> Priya qualys mail email verification updated update	qemail	7	0	Umesh Wani
<input type="checkbox"/> Priya slack action slack action	slack	2	0	Umesh Wani
<input type="checkbox"/> Qualys mail action test Qualys mail action test	qemail	0	0	Umesh Wani
<input type="checkbox"/> Test Action test	qemail	0	0	Umesh Wani

Manage Rules

Rule Manager tab lists all the rules that you have created with rule name, trigger criteria selected for the rule, alert message aggregating enabled or disabled for the rule, action chosen for the rule, date and time when the rule is last triggered and state of the rule, whether the rule is enabled or disabled and created date and time of the rule. You can use the Actions menu or Quick Actions menu to edit, enable, disable, delete and rename a rule. Use the search bar to search for rules using the search tokens.

The screenshot shows the 'Manage Rules' interface. The 'RULES' section is active, and the 'Rule Manager' tab is selected. A search bar is present at the top. Below it, there's a table of rules. The first row is highlighted, and a 'Quick Actions' menu is open over it, showing options for 'Edit', 'Enable', 'Disable', 'Save As', and 'Delete'.

RULE NAME	TRIGGER CRITERIA	AGGREGATE	ACTION	LAST TRIGGERED	STATE	CREATED ON
<input checked="" type="checkbox"/> PP Time window schedu PP Time window schedule	Time-Window Scheduled Match Daily schedule	Yes	Priya qualys mail		Enabled	May 30, 2019 1:30 PM Umesh Wani
<input type="checkbox"/> PP and AK Time Window ak Window scheduled match	Time-Window Scheduled Match Daily schedule	No	Priya qualys mail		Enabled	May 30, 2019 12:09 AM Umesh Wani
<input type="checkbox"/> PP windows count match PP windows count match	Time-Window Count Match Runs after every 5 matches in 1...	Yes	Priya qualys mail		Enabled	May 30, 2019 1:25 PM Umesh Wani
<input type="checkbox"/> Test rule by Priya_updat Test rule by Priya	Single Match	-	Priya qualys mail		Enabled	June 3, 2019 4:03 PM Umesh Wani
<input type="checkbox"/> Test_Amita Test_Amita	Time-Window Scheduled Match Daily schedule	No	Test Action Amita	June 1, 2019 5:28 PM	Enabled	May 23, 2019 2:56 PM Umesh Wani

Manage Alerts

Activity tab lists all the alerts. Here you will see for each alert, rule name, success or failure in sending the alert message, aggregate enabled (Yes) or disabled (No) for the rule, action chosen for the rule, matches found for the rule and the user who created the rule.

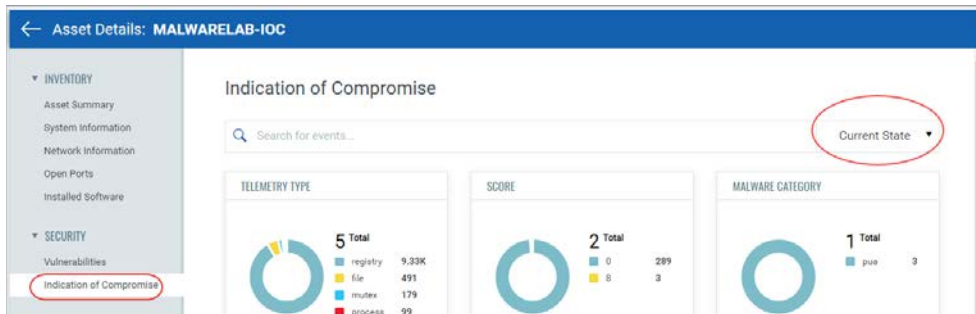
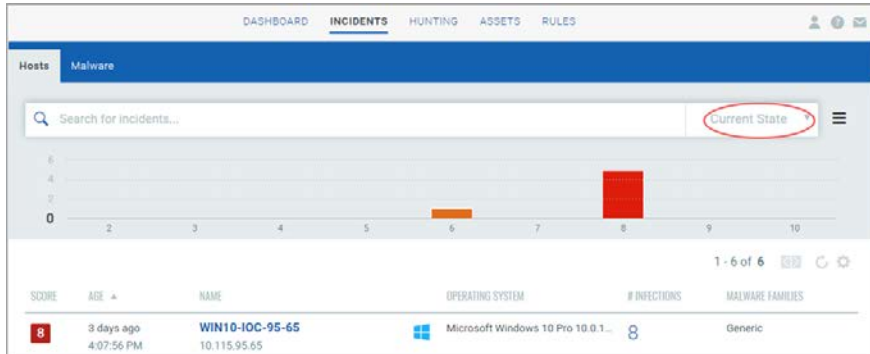
Search for alerts using our search tokens (1), select a period to view the rules triggered during that time frame (2), click any bar to jump to the alerts triggered in a certain timeframe (3), use these filters to group the alerts by rule name, action name, email recipients and status (4).

The screenshot displays the 'Rules' section in the 'Activity' tab. The interface includes a search bar (1) with the text 'Search for alerts...', a time filter set to 'Last 30 Days' (2), and a bar chart (3) showing activity levels from May 4th to June 3rd. On the left, there are filters for 'RULE NAME', 'ACTION NAME', 'EMAIL RECIPIENTS', and 'STATUS' (4). The main table lists alerts with columns for Rule Name, Status, Aggregate, Action, Matches, and Created By.

RULE NAME	STATUS	AGGREGATE	ACTION	MATCHES	CREATED BY
ak window count aggregate match	Success	Yes	slack action ak	5	Umesh Wani
ak window count aggregate match	Success	Yes	Priya qualys mail	5	Umesh Wani
ak window count aggregate match	Success	Yes	Priya qualys mail	5	Umesh Wani
asset.agentId single match	Success	Yes	Priya qualys mail	1	Umesh Wani
asset.agentId single match	Success	Yes	Priya qualys mail	1	Umesh Wani
ak window count aggregate match	Success	Yes	slack action ak	5	Umesh Wani
ak window count aggregate match	Success	Yes	Priya qualys mail	5	Umesh Wani
ak window count aggregate match	Success	Yes	slack action ak	5	Umesh Wani
ak window count aggregate match	Success	Yes	slack action ak	5	Umesh Wani

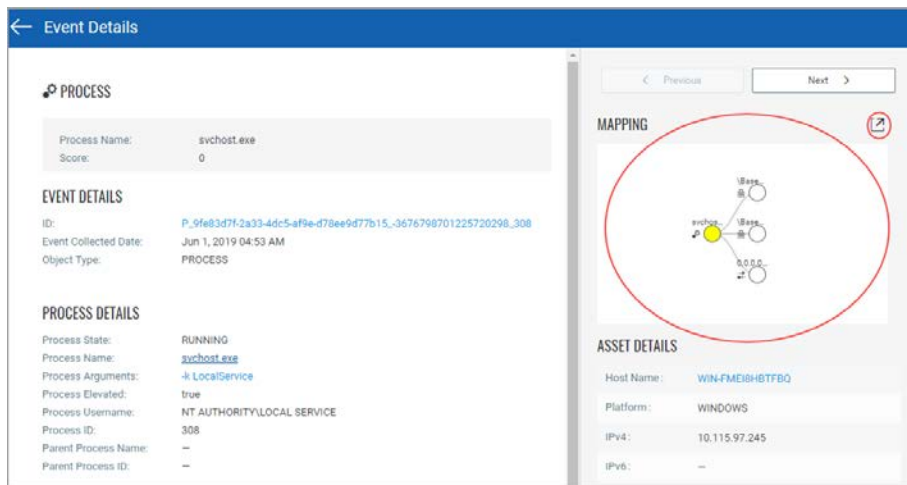
New Default Date Filter “Current State” Added

Now all the tabs that has date filter will show “Current State” as the new default date filter. In the Dashboards, Incidents and Hunting tabs, you will see Current State is selected as the default value for displaying incidents and events. Current state shows only those processes that are currently running on the assets and for which events or incidents are getting generated. IOC shows you the data that is made available during the last sync. This means that there might be some lag between the data shown in IOC and the actual data for the events and incidents. Note that IOC shows only current state data for incidents.



Event Details to Show Hierarchy for Events

Now we will show you a hierarchical view of events for Process, Mutex and Network event types on the Events Detail page. Hierarchical view will contain maximum 3 levels of hierarchies for an event.

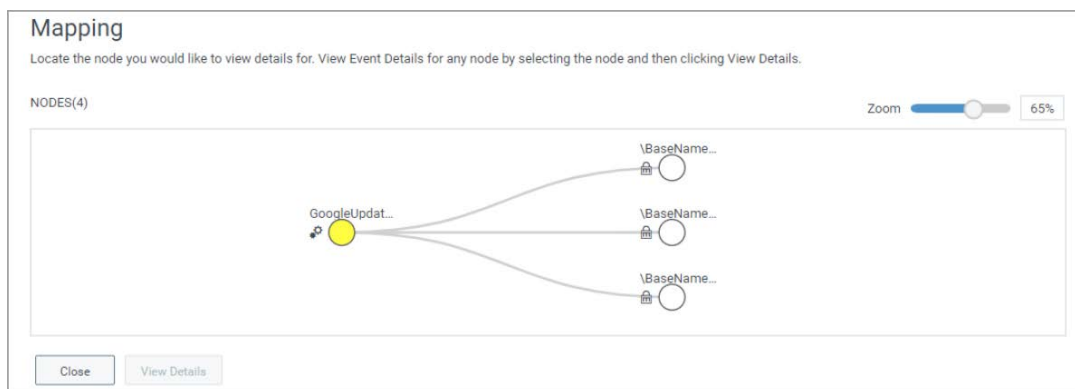


The screenshot shows the 'Event Details' interface. On the left, under 'PROCESS', the process name is 'svchost.exe' with a score of 0. Below this, 'EVENT DETAILS' shows an ID, collection date (Jun 1, 2019 04:53 AM), and object type (PROCESS). 'PROCESS DETAILS' lists the state as 'RUNNING', process name as 'svchost.exe', arguments as '-k LocalService', and other attributes like 'Process Elevated: true' and 'Process Username: NT AUTHORITY\LOCAL SERVICE'. On the right, a 'MAPPING' diagram shows a central node 'svchost.exe' connected to three parent nodes '\BaseName...' and three child nodes '\BaseName...'. A red circle highlights the 'svchost.exe' node. Below the mapping is an 'ASSET DETAILS' section with host name 'WIN-FMEI8HBTFBQ', platform 'WINDOWS', and IP addresses.

An event of process type will show its parent and child processes along with the mutex and network connection of the process. For Network and Mutex event types, we will show you network connection and mutex of a process respectively in the hierarchy.

In the hierarchical view, the node for which parent and child relationship is shown will be highlighted to help you identify the selected node. You can traverse between the nodes by clicking a node in the hierarchy. Selecting another node will highlight that node and show the details of that node on the Event Details Page. To help you identify event types of nodes in a hierarchy view, all the nodes will display the respective icons associated with that event type.

Click  to zoom out the hierarchy tree.



The 'Mapping' dialog box contains instructions: 'Locate the node you would like to view details for. View Event Details for any node by selecting the node and then clicking View Details.' It shows a hierarchy of nodes with a zoom slider set to 65%. The root node is 'GoogleUpdat...' with a yellow circle icon. It branches into three child nodes, each labeled '\BaseName...' with a folder icon. At the bottom are 'Close' and 'View Details' buttons.

To view hierarchy of a child node, select a child node and click View Details. The Event Details page will now show details of this node.