

Qualys Cloud Suite 2.31

Here's what's new in Qualys Cloud Suite 2.31!

AV AssetView

TP ThreatPROTECT

Terminated instances no longer added to assets list

CA Cloud Agent

New search tokens for Cloud Agent

SAQ Security Assessment Questionnaire

New and Enhanced Template Editor

WAS Web Application Scanning

New Quick Action for Web Applications

Error Indicator on UI for Multi-Scan

Smart Scan Indicator in Reports

Updated QID Mappings

WAF Web Application Firewall

Add timeout for a Web Server

Qualys Cloud Platform

EC2 Scanning Support for China Region

Qualys Cloud Suite 2.31 brings you many more
Improvements and updates! [Learn more](#)



AssetView



ThreatPROTECT

Terminated instances no longer added to assets list

EC2 connectors will no longer import and sync EC2 assets with a Terminated state. In other words, we will not add a new asset to your asset inventory for an EC2 instance that is Terminated.

Please note:

- Assets added prior to this release for Terminated instances will remain in your list until you purge them.
- If the status of an existing asset changes to Terminated then this will be updated in the asset details.

Use this query to easily find EC2 assets with a Terminated instance state:

`aws.ec2.instanceState:"TERMINATED"`

The screenshot shows the AssetView interface with the search bar containing the query `aws.ec2.instanceState:"TERMINATED"`. A red circle highlights the search bar, and a red arrow points to it with the text "query to find Terminated instances". Below the search bar, a table lists assets. The first asset, **ani-lxag**, is highlighted in yellow. A red circle highlights the "View Asset Details" link in the "Quick Actions" menu for this asset, with a red arrow pointing to it and the text "View EC2 information for the asset".

Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
ani-lxag 10.97.9.155	Linux		—	New November 27, 2017		AssetSear... us-east-1 3 more tags
PreAuth aka 54.164.55.64, 10.90.2.252 ec2-	ec2-		—	New May 18, 2017		us-east-1 AssetSear... 3 more tags
ws2016	windows	VM SCA	—	New 5 days ago		terminated2 AssetSear... 3 more tags
win2k8_target 10.90.0.188 ec2-	windows	VM	—	Scanned September 19, 2017		AssetSear... terminate...

Choose View Asset Details for any asset in your search results to see EC2 information, including state.

The screenshot shows the "View Asset Details" modal for the asset **ani-lxag**. The "EC2 Information" tab is selected. The "General" section shows the following details:

- Instance ID: i-091fa0b749a339cd2
- Instance Type: t2.micro
- Created Date: 2017-11-28 07:58:51.0
- State: **TERMINATED** (highlighted with a red circle)
- Spot Instance: Yes
- Image (AMI) ID: ami-aa2ea6d0
- Account ID: 205767712438

The "Location" section shows:

- Region: US East (N. Virginia)
- Availability Zone: us-east-1e

Use custom severities in AV searches and widgets

You can now use modified QID severities as set in the Knowledge Base for AssetView searches and widgets by using the `vulnerabilities.customSeverity` search token. Default severities are also auto-populated into this field if the severity has not been changed.

Please note that if you are using nested queries, you may have to modify the level of nesting.

Example:

`vulnerabilities.vulnerability:(severity:5 and title:"Microsoft")`

would become:

`vulnerabilities:(customSeverity:5 and vulnerability.title:"Microsoft")`

New search tokens for Cloud Agent

- “connectedFrom” search token for Cloud Agent IP address
Use the “connectedFrom” search token in AssetView and Cloud Agent modules to find agents connecting from a specific IP address last used by an agent connecting to the platform (if the agent is behind a NAT device or proxy, that device’s IP address will be used). The “Connected From” IP address has been displayed in the Agent Summary tab, this new search token lets you search by the IP address.

Example

Show findings for an external IP address that an agent connected from

connectedFrom: 10.0.100.11

- “errorStatus” search token for Cloud Agent errors
Use the “errorStatus” search token in AssetView and Cloud Agent modules to find agents with errors (**“errorStatus:true”**) or no errors (**“errorStatus:false”**)

Example

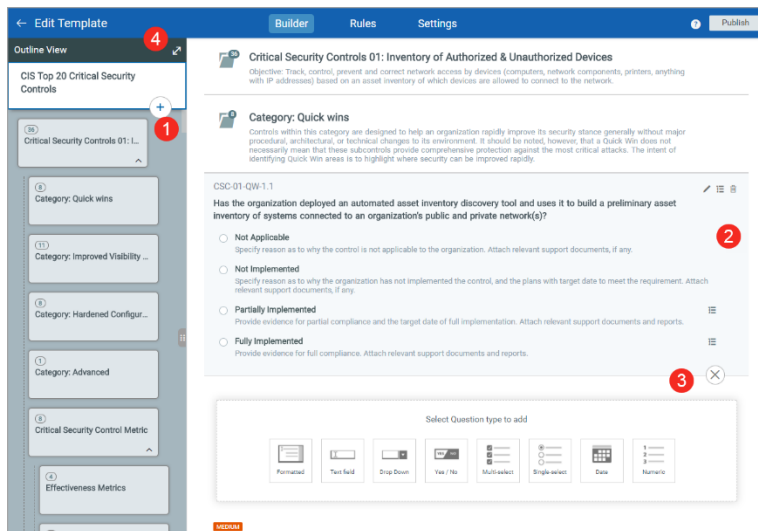
Show agents with error status True

errorStatus: "true"

New and Enhanced Template Editor

We now have a new template editor which makes it easier to create and edit templates. Just click New Template Editor on top right corner and get started.

You can create, edit, export, import, publish, and delete templates using the new editor.



With the new editor you can:

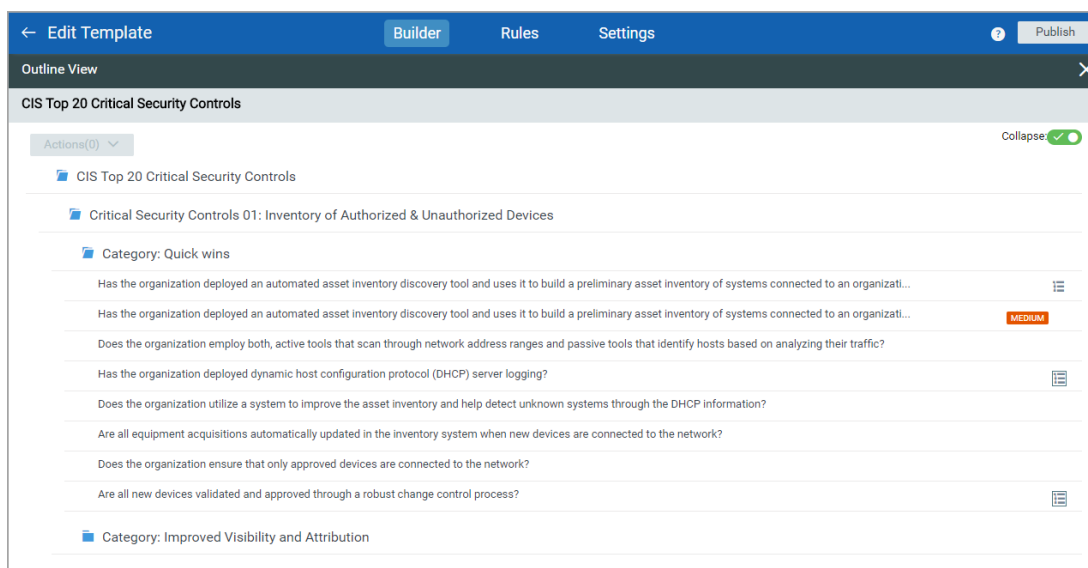
1 - Add new sections and subsections

2 – Edit questions and answers to manage rules, criticality, scores and settings

3 - Add new questions at the desired location in the template

4 - View the final layout in the outline view

Simply, drag and drop the sections and questions to reorganize your template to your liking, in the Outline View and Publish the template!



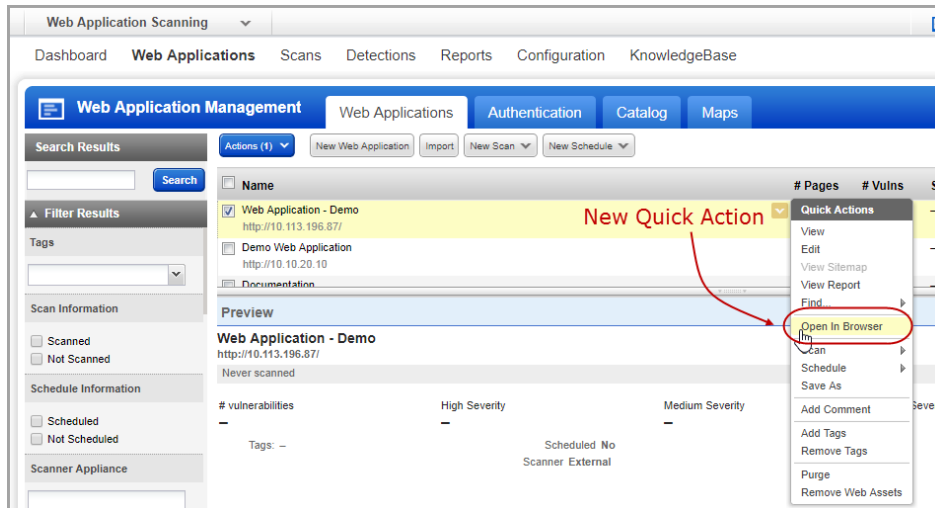


Web Application Scanning


New Quick Action for Web Applications

We have now introduced a new quick action menu for web applications – Open in Browser – that allows you to directly open the web application from the quick action menu.

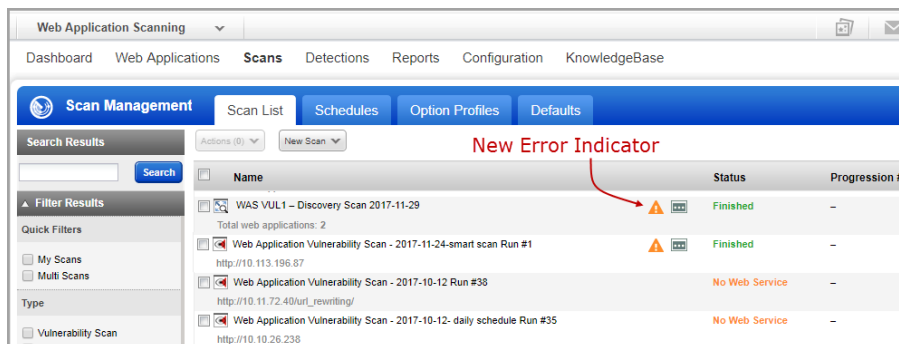
Go to Web Applications > Web Applications and select the required the web application. From, the quick action menu, select Open in Browser and your web application now directly opens a new tab of the same browser window.




Error Indicator on UI for Multi-Scan

We have now introduced a new icon  to indicate error in child scan and easily identify child scan failure in case of a multi-scan.

Let us consider an example of a multi scan that includes 50 child scans.



Once the scan is launched and completed, the Status column indicates the status of the multi-scan.

Now, if any of the child scan has failed, the  icon is displayed to indicate that although the multi-scan is complete, one or more child scan has failed. You can then drill down to know further details.

Smart Scan Indicator in Reports

We have now improved our WAS reports to tell you if the Smart Scan was enabled or disabled during the scan. All the download report formats (PDF, HTML, ZIP, XML, PPT, CSV) also display if Smart scan was enabled or disabled during the scan.

WAS Scan Report

Go to Scans > Scan List, select the scan and select View Report from the Quick Actions menu.

Web Application Scanning

Dashboard Web Applications Scans Detections **Reports** Configuration KnowledgeBase

Report Management Reports Schedules Templates Scan report Defaults

Scan Report

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Scans (1) Relaunch WAS VUL1 - Vulnerability Scan 2017-11-24-smart scan

Web Application (1) pune webapp url

Remediation Include ignored findings, Include patched findings

Summary

Appendix

▼ Scan Details

▼ Relaunch WAS VUL1 - Vulnerability Scan 2017-11-24-smart scan

Reference	was/1511523207980.4263103
Date	24 Nov 2017 5:03PM GMT+0530
Mode	On-demand
Type	Vulnerability
Progressive Scanning	Disabled
Authentication	None
Scanner Appliance	External (IP: 10.113.244.56, Scanner: 9.7.20-1, WAS: 4.4.102-1, Signatures: 2.4.183-2)
Profile	smart scan enabled
DNS Override	-
Duration	00:04:12
Status	Finished
Authentication Status	None
SmartScan Enabled	Yes

► Web Application Details: pune webapp url

► Severity Levels

The Smart Scan information is included in the Scan Details section of the Appendix in the Scan Report.

WAS Scan Report

Appendix

Scan Details

WAS VUL1 - Vulnerability Scan 2017-11-24-smart scan

Reference	was/1511506846813.4262975
Date	24 Nov 2017 12:30 null
Mode	On-Demand
Progressive Scanning	Disabled
Type	Vulnerability
Authentication	None
Scanner Appliance	External (IP: 10.113.244.56, Scanner: 9.7.20-1, WAS: 4.4.102-1, Signatures: 2.4.183-2)
Profile	smart scan enabled
DNS Override	-
Duration	00:04:11
Status	Finished
Authentication Status	None
SmartScan Enabled	Yes

Web Application Details: pune webapp url

Name	pune webapp url
URL	https://10.113.196.87/boq/acct/personal/creditcard.html

Let us see sample PDF report format. The Scan Details section displays the Smart Scan information.

Updated QID Mappings

We have now updated the mappings for WAS QIDs to various web application vulnerability classification lists. For each WAS vulnerability, you will now see accurate mappings to Common Weakness Enumeration (CWE), OWASP Top 10 (2013 edition), and WASC Threat Classification.

For example, let us consider QID 150046 and view its CWE, OWASP and WASC mappings.

Vulnerability Details

150046 Reflected Cross-Site Scripting (XSS) in HTTP Header [Install Patch](#) [Ignore](#) [Retest](#) [Active](#)

URL: <https://10.113.196.87/boq/aboutus.php>

Finding #	542196	Web Application	Pune-webapp-1
Patch #	—	Authentication	Not Used
Group	Cross-Site Scripting	First Time Detected	10 Jan 2018 11:55PM GMT+1400
CWE	CWE-79	Last Time Detected	13 Jan 2018 11:55PM GMT+1400
OWASP	A3 Cross-Site Scripting (XSS)	Last Time Tested	13 Jan 2018 11:55PM GMT+1400
WASC	WASC-8 Cross-Site Scripting	Times Detected	3 View History...
CVSS Base	4.3	CVSS Temporal	3.9

Updated QID mappings

Details [Show](#)

Detection Information

Parameter: It has been detected by exploiting the parameter **cookie3**

Access Path: The payloads section will display a list of tests that show how the param could have been exploited to collect the information

Here is the path followed by the scanner to reach the exploitable URL:

```
https://10.113.196.87/boq/acct/personal/creditcard.html
https://10.113.196.87/boq/acct/
```

An upcoming release of WAS will use the 2017 edition of the OWASP Top 10 instead of the 2013 edition.



Web Application Firewall

Add timeout for a Web Server

The Web Application wizard now includes an option to specify the server timeout. This is a mandatory field.

Server Timeout is the maximum time to wait for an HTTP connection attempt to a server to succeed. If the HTTP request does not respond before the duration set, it will timeout and return an HTTP 503 error code.

Specify a timeout period between 1 second to 3600 seconds. Default value is 60 seconds.

The screenshot shows the 'Web Application Creation' wizard, Step 2 of 6: Application. The left sidebar shows the progress: 1 Asset Details (checked), 2 Application (active), 3 Security, 4 WAF Clusters, 5 Comments, and 6 Review And Confirm. The main content area is titled 'Configure application and network settings'. It includes a 'Secondary URLs' section with a text input field containing 'http:// Type URL + Enter' and a message 'No secondary URLs entered.' Below this is the 'Web Servers' section, which contains a description: 'Select a pool of servers. You can also set the server(s) inactivity timeout (in seconds). If the pool holds several servers and the application is persistent, then enable persistency and specify a cookie name. Also pick a healthcheck for backend monitoring purpose and define a suitable client-side HTTP response code in case of unavailability.' The 'Server Pool*' dropdown is set to 'Please select a server pool' with 'Edit' and 'Create' links. The 'Server Timeout*' field is a text input containing '60', highlighted with a red circle. Below it is the 'Enable persistency' toggle, which is currently 'OFF'. The 'Healthcheck' dropdown is also set to 'Please select a healthcheck' with 'Edit' and 'Create' links. At the bottom, there are 'Cancel', 'Previous', and 'Continue' buttons.

Qualys Cloud Platform

EC2 Scanning Support for China Region

Now you can easily scan EC2 instances included in the AWS China region for vulnerabilities and policy compliance using the Qualys Cloud Platform. You can create/update EC2 connectors to pull instance info from the China region, activate discovered instances for the VM, PC or SCA module, and scan them using our EC2 scan workflow.

What are the steps?

Navigate to the AssetView (AV) module > Connectors section. Click the “Create EC2 Connector” button. Using the wizard, give the connector a name, select an authentication record and choose “Set EC2 connector only for AWS China”.

The screenshot shows the 'Create EC2 Connector' wizard at Step 2 of 5, titled 'EC2 Authentication Information'. The left sidebar shows the progress: 1. Connector Details (checked), 2. EC2 Authentication (active), 3. EC2 Regions, 4. Tags and Activation, and 5. Review. The main content area is titled 'EC2 Authentication Information' and includes a section 'Select one AWS Authentication Record' with a red asterisk indicating required fields. Below this is a table with columns 'ID', 'Title', and 'Comments'. The table lists three records: '265801 China-Region' (selected with a dropdown showing 'china region'), '236801 sada-auth-updated' (Record-updated), and '236802 sada-auth-updated1' (Record-updated). Below the table, there is a note: 'Create and select an authentication record then click the Test Connector button to validate the authorization and count its asset inventory.' At the bottom, there are two checkboxes: 'Set the connector only for AWS GovCloud (US) region' (unchecked) and 'Set the connector only for AWS China' (checked and circled in red). Navigation buttons at the bottom include 'Cancel', 'Previous', and 'Continue'.

ID	Title	Comments
265801	China-Region	china region
236801	sada-auth-updated	Record-updated
236802	sada-auth-updated1	Record-updated

Under EC2 Regions you’ll see AWS China regions only. Select this region and complete the steps for tags and activation as you like.

The screenshot shows the 'Create EC2 Connector' wizard at Step 3 of 5, titled 'EC2 Regions Information'. The left sidebar shows the progress: 1. Connector Details (checked), 2. EC2 Authentication (checked), 3. EC2 Regions (active), 4. Tags and Activation, and 5. Review. The main content area is titled 'EC2 Regions Information' and includes a section 'Select Regions' with a red asterisk indicating required fields. Below this is a text field 'Discovered asset count for selected regions : --' and a 'Sync. Assets' button. A table with columns 'Region Name' and 'Discovered' is shown. The table lists one record: 'AWS China (Beijing)' (checked and circled in red) with a value of '--'. Navigation buttons at the bottom include 'Cancel', 'Previous', and 'Continue'.

Region Name	Discovered
AWS China (Beijing)	--

Issues addressed in this release

Qualys Cloud Suite 2.31 brings you many more improvements and updates.

AV

AssetView

TP

ThreatPROTECT

- The new search token `vulnerabilities.customSeverity` lets user easily find vulnerabilities defined with a custom severity. For example `vulnerabilities.customSeverity: "4"`
- Fixed an issue with query generation when a user clicks on a dashboard widget having a group by query.
- We have fixed the issue and user can now create a Group By severity widget only if the query has valid severity parameters.
- Updated an issue with query generation when a user clicks on a dashboard widget having a query that includes vulnerability title.
- Now an asset tag search that returns no results displays "Asset Search Tags".
- Now widgets show correct data when using certain filters.
- Fixed an issue to allow users to export and then import the widget `WEBDAV NOT DISABLED [EXPLODINGCAN]`.
- Fixed an issue with query generation and now appropriate results are displayed when you click on a widget.
- Fixed an issue where the user could not configure an existing widget having certain query.
- Fixed an issue where the user could create a widget using an invalid asset search query.
- Now the Compliance tab in Asset Details displays correctly when Japanese is enabled.
- We have fixed an issue and the `agentId` search is now not case-sensitive.

CA

Cloud Agent

- The new toggle buttons for IOC configuration settings allow you to enable or disable a configuration setting in a profile. You must set at least one configuration setting to ON if you have enabled IOC for a CA configuration profile.
- The user will now see the correct Volume Size in Asset Details for a MAC agent.
- Fixed an issue where an empty warning message appeared in the CA UI.
- Now the user can successfully activate the FIM module for agents when Japanese is enabled.
- Fixed an issue where the `activatedForModules:"FIM"` query did not return the list of agents activated for FIM that had no FIM profile.

- Cloud Agent AIX is now GA. The “beta” label has been removed from the Cloud Agent UI and documentation.
- Fixed an issue where config profiles for a new subscription were not displayed in the correct order.
- Updated the help to point to the correct location of the Agent log files.
- Azure toggle button is now displayed on the install instructions for FIM / IOC enabled users.
- For the Suspend data collection option in the configuration profile, we've added SCA along with VM, PC and inventory to indicate this option applies to SCA data collection as well.

SAQ

Security Assessment Questionnaire

- We have fixed the issues and now the activity stream and campaign completion status show accurate information.
- The template is now loaded correctly in the Document View while editing a template.

WAS

Web Application Scanning

- When you schedule a single occurrence scan, the preview and edit mode now correctly display the correct occurrence for the scan.
- We have now fixed the PDF format of the WAS reports to include link to the CWE page on <http://cwe.mitre.org>.
- We have now fixed the mapping to CWE, OWASP, or WASC for various QIDs.
- We have now fixed the issue so that the scheduled reports are generated and are not deactivated due to server unavailability.
- We now correctly assign the UUID for Open in Browser.
- We now display correct count of HIGH severity vulnerabilities on the dashboard and is in sync with the Detections tab.
- The Web Application filter now functions correctly for Burp and Bugcrowd.
- The scan summary email now displays correct scan status if the scan fails due to unavailability of scanner.
- Fixed an issue with importing a certain Burp XML file using the Detections > Burp > Import workflow.
- Web page will show child scans as expected.
- We have now removed the additional Open in Browser button from the preview pane when a web application is selected.
- Fixed an issue where an error was thrown while re-testing finding ID '480896'.
- Fixed an issue where a scan report was showing errors related to data set column "DURATION".
- Filters applied in the Filter result section are now retained accurately if customer chooses to use the Search Result section.

WAF

Web Application Firewall

- Fixed an issue where the text in the Detections column in Event Details got spilled over to the adjacent columns. Now, width of the column has been increased.

- The Archive option under Actions in Events Details was click-able even though the Event was already archived. This is now fixed, and the Archive option is grayed out if the event is already archived.
- WAF Events List now shows a message when the event list fails to load due to huge quantity of logs, and suggests the user to refine the search.
- Event description in Event List and Event Details now display a '-' instead of null.
- Fixed an issue where a part of Event Details - Request / Response body got truncated on the UI. You can now view the complete Request / Response body using the horizontal scroll bar.
- Fixed an issue where using a delimiter other than a comma for IN-RANGE and NOT.IN-RANGE operators caused a WAF restart error. You are allowed to use only a comma as a delimiter. For example, request.header.cookie.count IN-RANGE "2,5"
- WAF now displays a message asking the user to contact Qualys Support if geographic statistics take a long time to load on the WAF dashboard.
- Fixed an issue where long parameter values in custom rules got truncated on the UI. You can now view the long parameter values using the horizontal scroll bar.
- Event Details now display XML or JSON content in Request / Response body, in an indented style.
- Labels for Status filters in Event List are modified to make them simple and intuitive.
- Active web applications help tip now displays correct description of each healthcheck status for a Web application.
- WAF now displays a proper error message when the primary/secondary URL is part of the Web server URL.

FIM

File Integrity Monitoring

- Now the Quick Actions menu for a selected event disappears when the user scrolls up or down on the Events tab.
- The quick filters on the Assets page will now behave like the other tabs. If the asset list only contains one filter (and therefore applies to all of the assets in the list) it will not be shown once applied.
- We've added our Getting Started video to the FIM welcome page.
- Fixed some data alignment issues in widgets and filters.
- Now users can create dashboard widgets with group by option set to Profile Category.

IOC

Indication of Compromise

- Now users can download the Malware data lists.
- Several new Group by fields are available for defining a dashboard widget including: Asset NetBIOS Name, Asset Platform, File Full Path, Hash MD5, Hash SHA256, Image Path, Network Remote DNS, Network Remote IP, Network Remote Port, Process Parent ID, Process Parent Name, Registry Data, Registry Key, Registry Value
- We added an IP geo location map in event details to show remote location for network type events.
- We added File Action field to event details whose search token value match either created or deleted.

- We added the Handle Action field to event details whose search token values match either running or terminated.
- We added the Registry Action field to event details whose search token values match either created or deleted.
- Now the user can successfully save their query on the Hunting tab using the Save this search query option.
- On the KnowledgeBase tab we changed the column name from AUTHOR to SOURCE.
- On the Asset Details > Vulnerabilities page we fixed some issues. Now when the user clicks "View (Total of all Sev)" the correct count is shown and the user can click the X icon to go back to asset details.
- Now when the user downloads the data list in any format from the Hunting tab, the correct timezone is shown in the "Created" field.
- Added malware category column in Asset Details > Indication of Compromise tab.

Qualys Cloud Platform

- User can now create a widget using the token activatedForModules in AssetView.
- The name of xsd which comes in the response of assetdataconnector API is changed from assetdataconnector to asset_data_connector.
- Now the system created asset tags Web Application Assets and Malware Domain cannot be deleted by the user.
- Now this API call evaluates a single tag as per the Qualys API documentation <https://qualysapi.qg2.apps.qualys.com/qps/rest/2.0/evaluate/am/tag/<ID>>
- We have fixed the issue of inconsistent search result and now support prefix matching for partial search.
- The SCA activation option is now available in the create connector workflow when SCA is enabled in the user's account.
- We have fixed the issue and now the user can only create a connector with both, SCA and VM selected. User can no more create a connector with SCA only.
- Fixed an issue where asset group tags were not deleted automatically. Now when a user deletes asset groups the corresponding asset group tags are deleted as well.
- We have fixed the issue and now tags created for EC2 instances are correctly applied for assets in AssetView and Vulnerability Management.