Engineering
Simplicity

Use Case Manager

Published

2022-06-06

RELEASE
7.5.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Use Case Manager
7.5.0

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use QRadar Use Case Manager to ensure that QRadar is optimally configured to accurately detect threats throughout the attack chain.

1

CHAPTER

QRadar Use Case Manager

QRadar Use Case Manager

IN THIS SECTION

QRadar Use Case Manager includes a use case explorer that offers flexible reports that are related to your rules. QRadar Use Case Manager also exposes pre-defined mappings to system rules and helps you map your own custom rules to MITRE ATT&CK tactics and techniques.

Explore Rules Through Visualization and Generated Reports

- Explore the rules through different filters to ensure that they work as intended.
- Generate reports from predefined templates, such as searches based on rule response and actions, log source coverage, and many others.
- Customize reports to see only the information that is critical to your analysis.

Tune Your Environment Based on Built-in Analysis

- Gain tuning recommendations unique to your environment right within the app.
- Identify the topmost offense-generating or CRE-generating rules, and then follow the guide to tune them.
- Reduce the number of false positives by reviewing the most common configuration steps. Easily update network hierarchy, building blocks, and server discovery based on recommendations.

Visualize Threat Coverage Across the MITRE ATT&CK Framework

- Visually understand your ability to detect threats based on ATT&CK tactics and techniques.
- View predefined QRadar tactic and technique mappings and add your own custom mappings to help ensure complete coverage.
- Use new insights to prioritize the rollout of new use cases and apps to effectively strengthen your security posture.
- "What's new in QRadar Use Case Manager" on page 6

  Stay up to date with the new features that are available in the QRadar Use Case Manager app so that you get the most out of your use case management experience.
- "Known issues" on page 32

  The QRadar Use Case Manager app has required information for known issues.
- "Video demonstrations" on page 35

  Watch video tutorials to learn how to use the workflows and features in QRadar Use Case Manager.
- "Supported environments for QRadar Use Case Manager" on page 38

  For the features in QRadar products to work properly, you must use the supported environments.
- "Installation and configuration checklist" on page 41

  As you install the QRadar Use Case Manager app, review and complete all of the necessary tasks on the installation checklist.
- "MITRE ATT&CK mapping and visualization" on page 59

  The MITRE ATT&CK framework represents adversary tactics that are used in a security attack. It documents common tactics, techniques, and procedures that can be used in advanced persistent threats against enterprise networks.
- "Accessing report data by using QRadar Use Case Manager APIs" on page 105

  As an alternative to using the interface in QRadar Use Case Manager, you can use APIs to download report data to CSV or JSON files. Try using the interactive API documentation interface to test the APIs before you use them in your scripts.

RELATED DOCUMENTATION

What's New in QRadar Use Case Manager | 6

2

CHAPTER

What's New in QRadar Use Case Manager

What's New in QRadar Use Case Manager

IN THIS SECTION

Stay up to date with the new features that are available in the QRadar Use Case Manager app so that you get the most out of your use case management experience.

Version 3.4.1

This release includes the following changes:

- Added support for MITRE v10.1.
- Updated packages with known vulnerabilities.

"Earlier Versions" on page 7

In case you missed a release, review a list of features from previous versions of QRadar Use Case Manager.

RELATED DOCUMENTATION

Earlier Versions | 7

Known Issues | 32

Video Demonstrations | 35

Earlier Versions

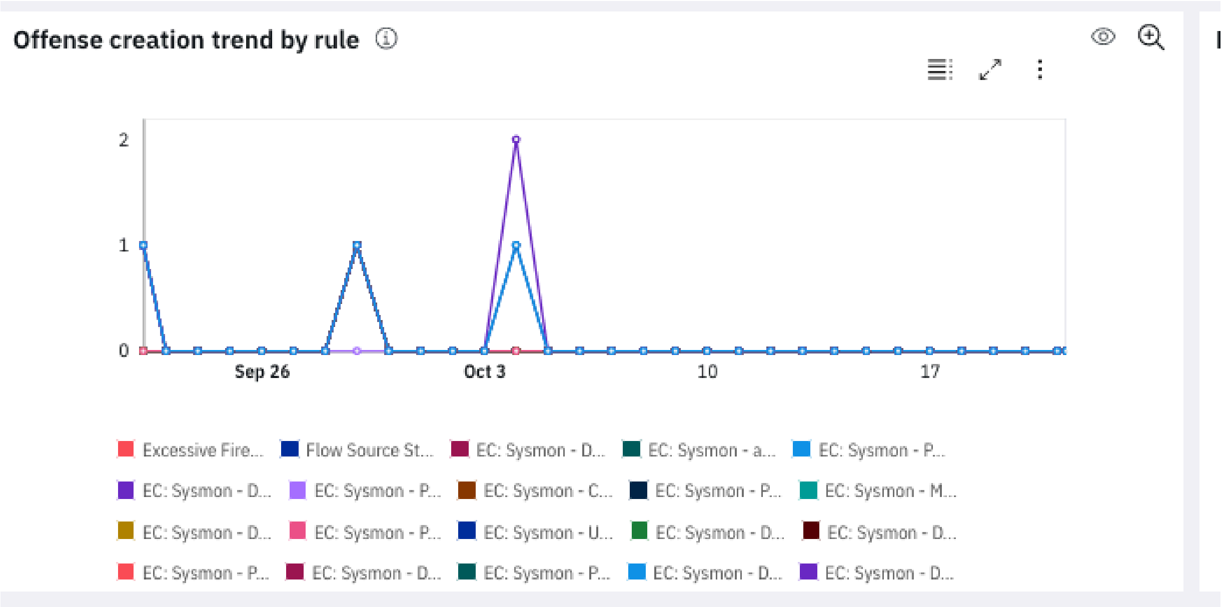
IN THIS SECTION

In case you missed a release, review a list of features from previous versions of QRadar Use Case Manager.

Version 3.4.0

Tuning active rules enhancements

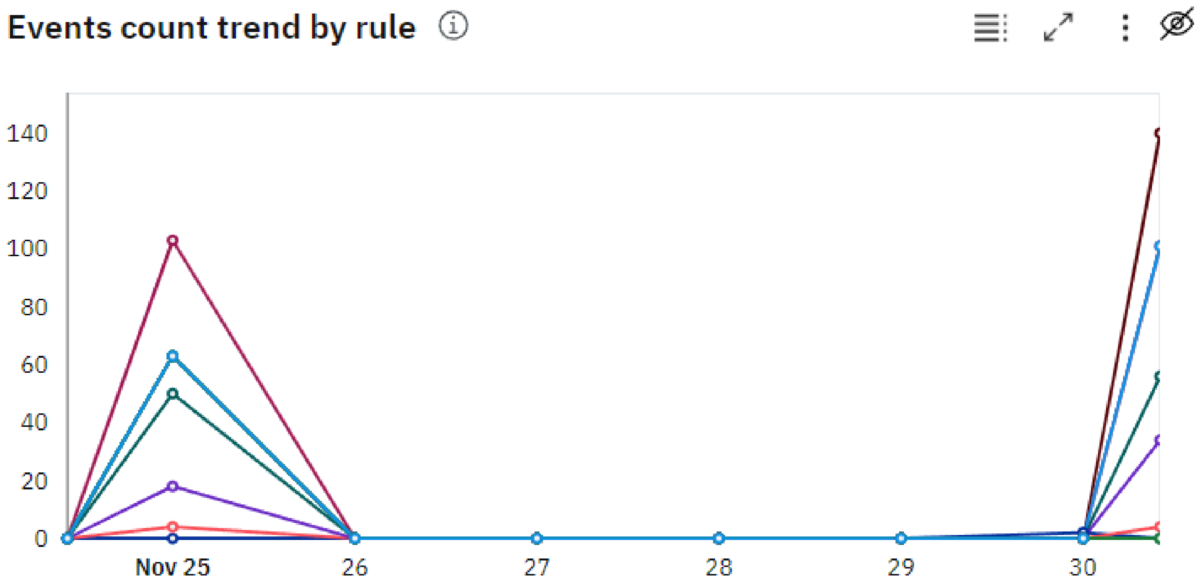
Added the **Offense creation trend by rule** chart to the Active rules page. For each rule that meets the conditions of the selected date filter, this trend chart shows the number of offenses that the rule started to contribute to on a specific day. For example, a rule started to contribute to three offenses yesterday, so the chart displays three offenses for that rule and yesterday's date. Today that same rule started to contribute to four new offenses and continued contributing to two offenses from yesterday. The chart displays four offenses for that rule and today's date. Because only four offenses are new for the rule, only four are shown on the chart instead of six.



NOTE: The chart is only supported on QRadar 7.4.1 Fix Pack 2 or later.

On the rule details page for a selected rule, you can change the date range for the trend of the selected rule in the **Offense creation by current rule in a certain time** chart. In previous versions, the time limit was the last three days only.

Added the **Events count trend by rule** chart to the Active rules page. For each rule that meets the conditions of the selected date filter, this trend chart shows the number of events per offense that the rule started to contribute to on a specific day. For example, a rule started to contribute to three offenses with 100 events yesterday, so the chart displays 100 events for that rule and yesterday's date. Today that same rule started to contribute to four new offenses with 200 events, and continued contributing to two offenses with 50 events from yesterday. The chart displays 200 events for that rule and today's date. Because only 200 events are new for the rule, only 200 are shown on the chart instead of 250.



Improved the display of bar charts on the Active rules page by sorting bars with the highest value in descending order. For better visual clarity, limitations were added to the number of bars that are displayed: a maximum of 15 bars on a small chart and a maximum of 30 bars when the chart is expanded to full screen.

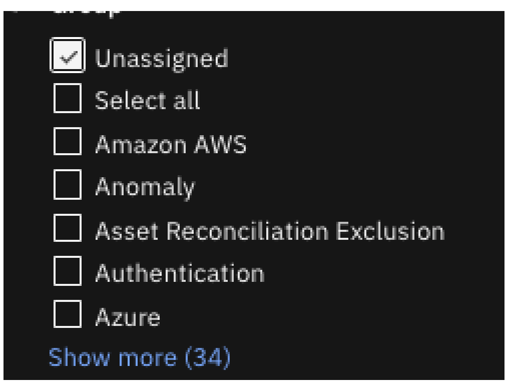
Enhanced the visualization capabilities on bar and timeline charts on the Active Rules, CRE Report, MITRE coverage summary and trend, and Rule-log source type coverage summary and trend pages. Now you can view the data in tabular format, expand the charts to full screen, and download the charts in PNG, JPB, or CSV formats.

Export rules as HTML documents to view offline.

Export selected rules to a formatted HTML report that you can view offline. By default, you can export the dependencies, dependents, and visualizations for the selected rules. Share the .zip file with colleagues or management who don't have access to QRadar or QRadar Use Case Manager. For more information, see "Exporting rules" on page 86.

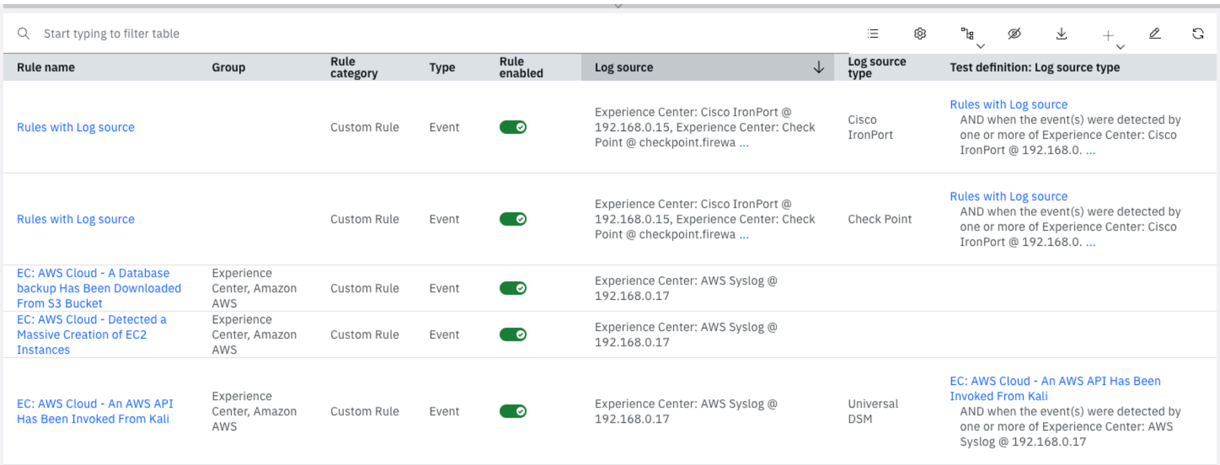
Rule table enhancements

Added an **Unassigned** filter option to the Group, Action, and Response filters. The **Unassigned** filter helps you see which rules don't belong to any group.



☑ Unassigned
□ Select all
□ Amazon AWS
□ Anomaly
□ Asset Reconciliation Exclusion
□ Authentication
□ Azure
Show more (34)

Added a **Test: Log source** column in the Use Case Explorer table report that returns specific references to log sources that are used in rule tests.



Start typing to filter table

Rule name	Group	Rule category	Type	Rule enabled	Log source	Log source type	Test definition: Log source type
Rules with Log source		Custom Rule	Event	✓	Experience Center: Cisco IronPort @ 192.168.0.15, Experience Center: Check Point @ checkpoint.firewa ...	Cisco IronPort	Rules with Log source AND when the event(s) were detected by one or more of Experience Center: Cisco IronPort @ 192.168.0. ...
Rules with Log source		Custom Rule	Event	✓	Experience Center: Cisco IronPort @ 192.168.0.15, Experience Center: Check Point @ checkpoint.firewa ...	Check Point	Rules with Log source AND when the event(s) were detected by one or more of Experience Center: Cisco IronPort @ 192.168.0. ...
EC: AWS Cloud - A Database backup Has Been Downloaded From S3 Bucket	Experience Center, Amazon AWS	Custom Rule	Event	✓	Experience Center: AWS Syslog @ 192.168.0.17		
EC: AWS Cloud - Detected a Massive Creation of EC2 Instances	Experience Center, Amazon AWS	Custom Rule	Event	✓	Experience Center: AWS Syslog @ 192.168.0.17		
EC: AWS Cloud - An AWS API Has Been Invoked From Kali	Experience Center, Amazon AWS	Custom Rule	Event	✓	Experience Center: AWS Syslog @ 192.168.0.17	Universal DSM	EC: AWS Cloud - An AWS API Has Been Invoked From Kali AND when the event(s) were detected by one or more of Experience Center: AWS Syslog @ 192.168.0.17

Create offense rules in rule wizard

Added the ability to create offense rules in the rule wizard. Click the plus sign icon in the report menu bar to access the rule wizard.

MITRE enhancements

Support was added for MITRE v10, which updates Techniques, Groups, and Software for Enterprise, Mobile, and ICS. Version 10 deprecates the **Scheduled Task/Job: Launchd** sub-technique. As a result, QRadar Use Case Manager redirects that mapping to the parent technique instead. For more information, see Updates - October 2021.

Custom rule attribute enhancements

Export or import custom rule attribute data, including rule mappings, in a JSON file. Sharing the data between colleagues or QRadar deployments helps to streamline your workflow by eliminating work effort. For more information, see "Exporting and Importing Custom Rule Attributes" on page 54 and "Exporting rules" on page 86.

Version 3.3.0

Custom rule attributes

A custom rule attribute represents a specific piece of information that you can attach to a rule that doesn't fit into existing rule attributes. For example, the use case the rule belongs to, the team who is responsible for creating or maintaining the rule, or who reviewed the rule. You can now define any custom rule attribute and its values, assign the custom attribute values to a rule, and add the custom attribute as a column in Use Case Explorer. For more information, see "Custom Rule Attributes" on page 52.

Rule management improvements

Added extra checks when rules are enabled or disabled, so that you cannot enable a rule that has disabled dependencies, or disable a rule that has enabled dependents.

You can now delete rules from QRadar by using QRadar Use Case Manager. The same restrictions apply as when you delete rules in QRadar. For more information, see "Deleting Rules" on page 87.

When you export rule data to a file to import into another QRadar deployment, you can now choose to enter details about the export, such as extension name and description. These details are included in the corresponding **manifest.txt** file, and displayed in the Extensions Management tool upon import. For more information, see "Exporting rules" on page 86.

MITRE improvements

Improved report filtering based on selected MITRE ATT&CK platforms so that no reports contain results that are related to non-selected platforms. To change the selected platforms, modify your user preferences. For more information, see "Customizing user preferences" on page 46.

Support was added for MITRE v9, which updates tactics, techniques, groups, software, and platforms.

Tuning active rules enhancements

A new **Event Count** column indicates how many events the rule associated to the number of offenses counted in the **Offense count** column.

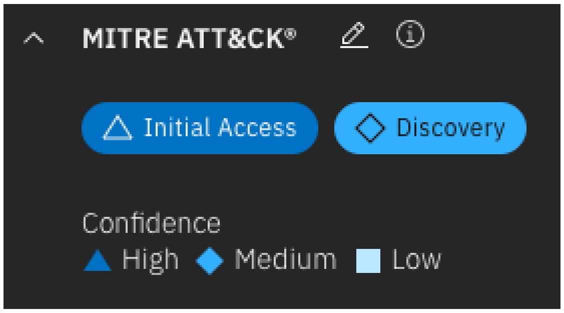
> **NOTE**: The column is supported on QRadar 7.4.1 Fix Pack 2 or later.

The **Total offenses by closure reason and rule** chart is renamed to **Closed offenses by reason and rule** to more accurately describe the contents.

Rule investigation details page enhancements

Added a Refresh icon to update edits to the page.

Enhanced the display of the MITRE tags in the **MITRE ATT&CK** section of the page. Previously, the confidence level was expressed only through the color shading, but a shape was added for accessibility reasons, and a legend was added for further explanation.



Content Extensions

After you install new content extensions, the Use Case Explorer page is refreshed with data within 15 minutes. In previous versions, the refresh only occurred overnight or by clearing the QRadar Use Case Manager cache on the Configuration page from the **Admin** tab.

Version 3.2.0

Rule enhancements

Now you can report on rules that assign events to offenses that are not active in a specific time period, or since installation. Rules that don't trigger in a certain timeframe might be misconfigured, and you might not be getting the most value out of your QRadar deployment. Review your inactive rules for possible tuning options. Filtering for inactive rules is supported on QRadar 7.4.1 Fix Pack 2 or later. For more information, see "Filtering rules and building blocks by their properties" on page 78.

APIs are available so that you can download rule report data to CSV or JSON formats in any configuration that is possible on the Use Case Explorer page. For more information, see "Accessing report data by using QRadar Use Case Manager APIs" on page 105.

Rule integration with IBM QRadar User Behavior Analytics 4.1.0

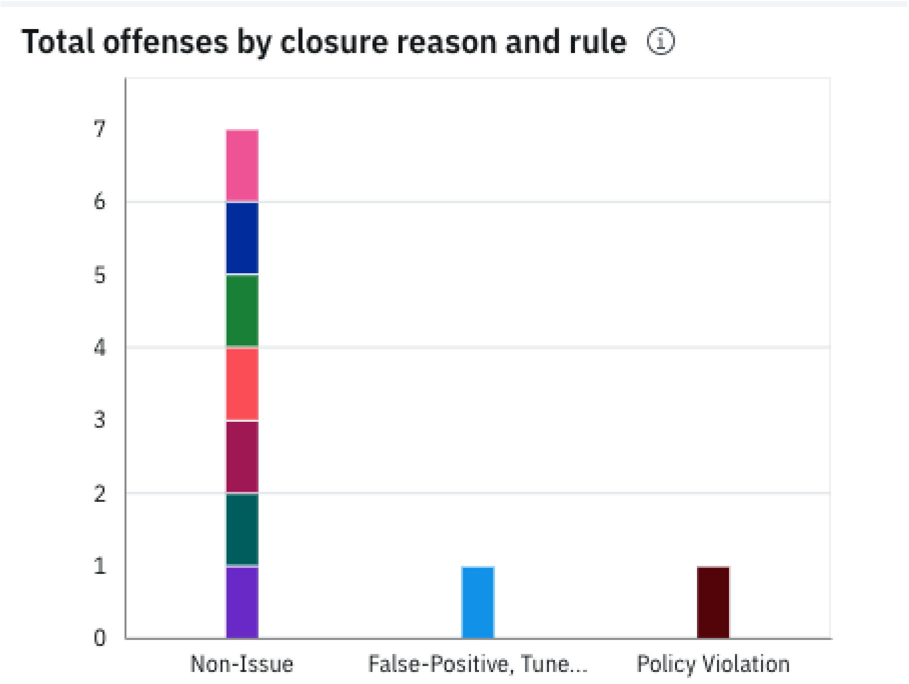
If you use QRadar User Behavior Analytics 4.1.0 in your environment, you now manage user analytics rules in QRadar Use Case Manager 3.2.0 instead of on the Rules and Tuning page in QRadar User Behavior Analytics.

During the upgrade for both apps, they communicate with each other and the rules are automatically integrated. After you tune the rules in the QRadar Use Case Manager app, the modifications are sent back to IBM QRadar User Behavior Analytics to use in the dashboards, which visualize user risks to your network.

For more information, see "Investigating user behavior analytics rules" on page 84.

Enhanced tuning active rules

A new chart was added to the Active Rules page to filter offenses by the closure reason and related rule. For example, you can filter to see which rules generated the offenses that were closed as false positives. For more information, see "Tuning the active rules that generate offenses" on page 98.



You can now export rule data from the Active rules that generate offenses page and the Active rules that generate CRE events page to CSV format.

MITRE enhancements

You can now exclude offenses from the **Detected in timeframe** chart based on their closure reasons. For example, you can exclude the rules that generated offenses that were closed as false positives. Rules with many false positives likely need tuning. Offenses that are closed as a non-issue are usually considered not critical to your organization. You might not want to include these offenses when you review the detected MITRE tactics and techniques.

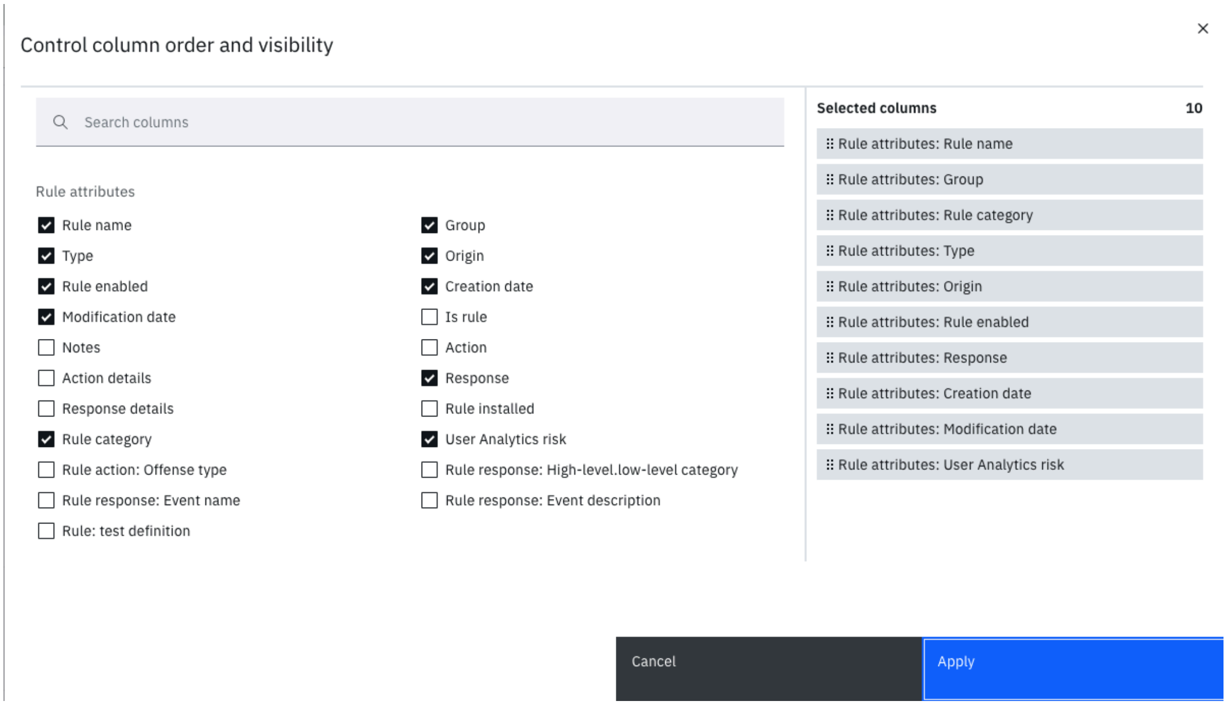
Support was added for MITRE v8.2, which updates Techniques, Groups, and Software for Enterprise.

Support was also added for all MITRE platforms to filter the **Detected in timeframe** and the **Coverage map** MITRE reports. By default, the Linux, macOS, and Windows platforms are supported. Changing the platform selection affects the heat maps, the tactic and technique selection in the filters, and the **MITRE ATT&CK Mappings** edit page. For more information, see "Customizing user preferences" on page 46.

Export MITRE coverage maps and MITRE coverage summary and trend charts as PNG images. Then, you can share the image with colleagues or executives who don't have access to the QRadar Use Case Manager app.

Workflow improvements

The window to add columns to the table reports was redesigned to make it easier to add columns and arrange the order that they are displayed in the report. Now you can search the columns or scroll through the window to find the column that you want to add.



Control column order and visibility

Search columns

Rule attributes

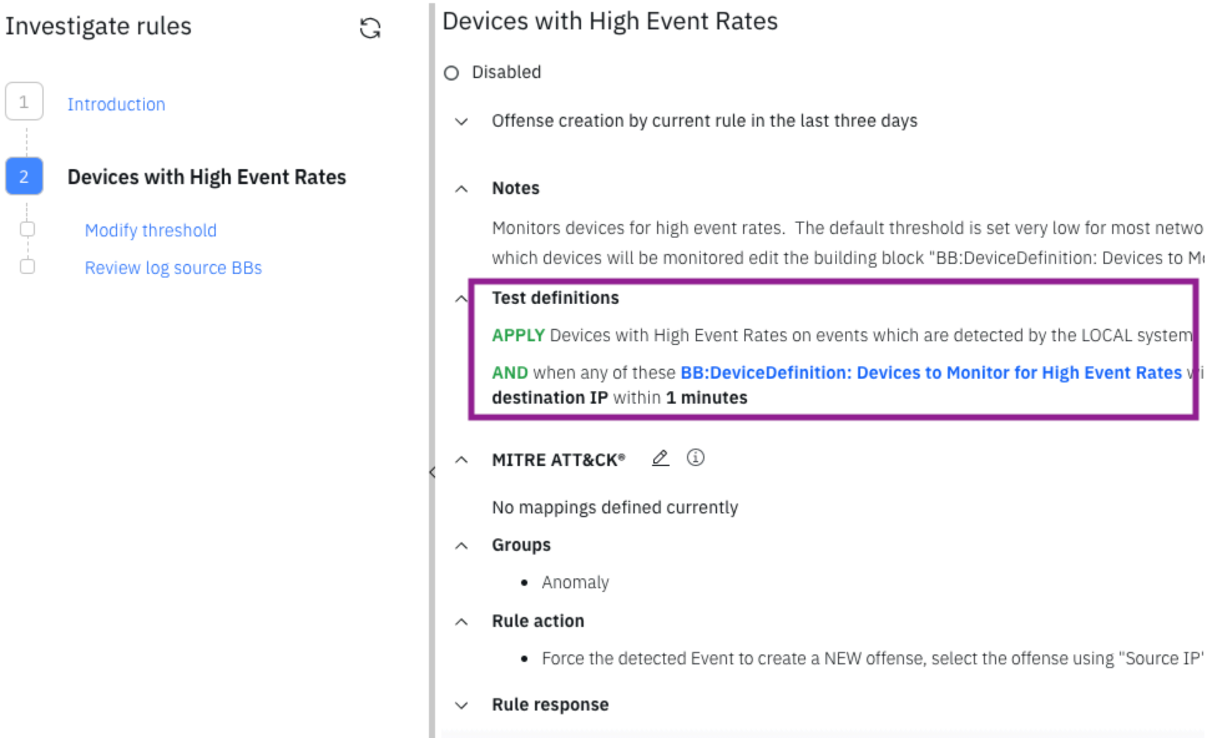
☑ Rule name
☑ Type
☑ Rule enabled
☑ Modification date
☐ Notes
☐ Action details
☐ Response details
☑ Rule category
☐ Rule action: Offense type
☐ Rule response: Event name
☐ Rule: test definition

☑ Group
☑ Origin
☑ Creation date
☐ Is rule
☐ Action
☑ Response
☐ Rule installed
☑ User Analytics risk
☐ Rule response: High-level.low-level category
☐ Rule response: Event description

Selected columns 10

- Rule attributes: Rule name
- Rule attributes: Group
- Rule attributes: Rule category
- Rule attributes: Type
- Rule attributes: Origin
- Rule attributes: Rule enabled
- Rule attributes: Response
- Rule attributes: Creation date
- Rule attributes: Modification date
- Rule attributes: User Analytics risk

On the rule details page, the name of the building block in the rule test now links and displays the test information for further investigation.



Devices with High Event Rates

○ Disabled

Offense creation by current rule in the last three days

Notes

Monitors devices for high event rates. The default threshold is set very low for most netwo which devices will be monitored edit the building block "BB:DeviceDefinition: Devices to M

Test definitions

APPLY Devices with High Event Rates on events which are detected by the LOCAL system

AND when any of these BB:DeviceDefinition: Devices to Monitor for High Event Rates wi destination IP within 1 minutes

MITRE ATT&CK®

No mappings defined currently

Groups

- Anomaly

Rule action

- Force the detected Event to create a NEW offense, select the offense using "Source IP'

Rule response

Version 3.1.0

Improved rule export capabilities

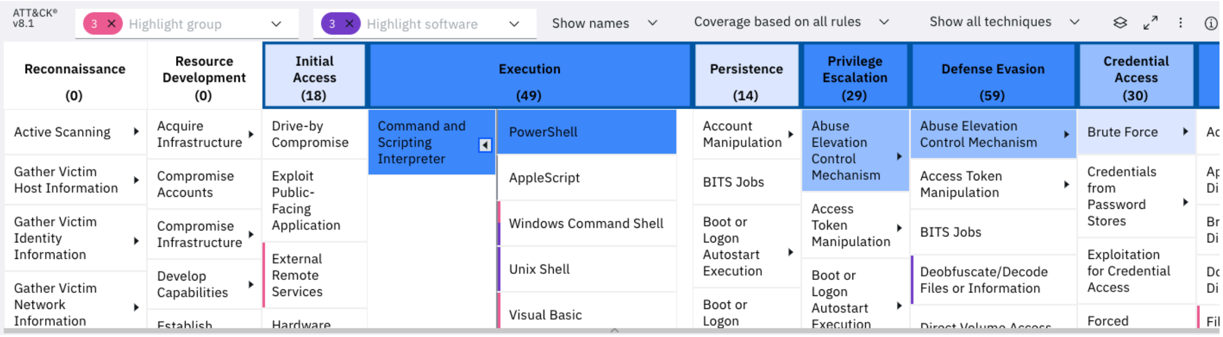
Added the ability to export rules and their dependencies as XML that can then be imported into another QRadar deployment using the Extension Management function on the Admin tab. This capability is supported on QRadar 7.4.0 or later. For more information, see "Exporting Rules" on page 86.

MITRE coverage enhancements

Support was added for MITRE v8.1. All custom mappings that were created in previous versions of the app are automatically migrated to the new version. Mappings to techniques that are now deprecated or don't exist under a given tactic will be deleted and included in the migration report. You can review a migration report to see the affected mappings so that you can consider creating new mappings to these rules. For more information about technique deprecation, see https://attack.mitre.org/resources/updates/.

Added support for MITRE sub-techniques in reports, filters, and templates. Sub-techniques provide a more specific description of the behavior an adversary uses to achieve their goal, such as dumping credentials by accessing the Local Security Authority (LSA) Secrets. Sub-techniques are added to the MITRE heat maps for the **Detected in timeframe** and **Coverage map and report** charts.

Figure 1: Heat Map that Shows MITRE Tactics and Techniques Coverage, Including Sub-techniques



ATT&CK® v8.1

3 × Highlight group

3 × Highlight software

Show names

Coverage based on all rules

Show all techniques

Reconnaissance (0)	Resource Development (0)	Initial Access (18)	Execution (49)		Persistence (14)	Privilege Escalation (29)	Defense Evasion (59)	Credential Access (30)	
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	PowerShell	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Ac
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application		AppleScript	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Ap Di
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services		Windows Command Shell	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Br Di
Gather Victim Network Information	Develop Capabilities	Hardware		Unix Shell	Boot or Logon		Deobfuscate/Decode Files or Information	Forced	Dc Di
	Establish			Visual Basic			Direct Volume Access		Fil

Enhanced the MITRE heat map chart displays by adding tooltips that list the software or group selections when you hover over vertical lines in the chart. The heat map calculations were adjusted for each technique; all mappings to its sub-techniques are counted as if they are mappings to that technique. Numbers in the chart header and cells indicate the number of enabled rules that are mapped to each tactic, technique, and sub-technique. Tooltips were added to explain how the color correlates with the heat map calculation. You can also choose how you see tactics and techniques that are displayed in the chart by showing their name, ID, or a combination of both. For more information, see Visualizing MITRE tactics and techniques that are detected in a specific timeframe and Visualizing MITRE tactic and technique coverage in your environment.

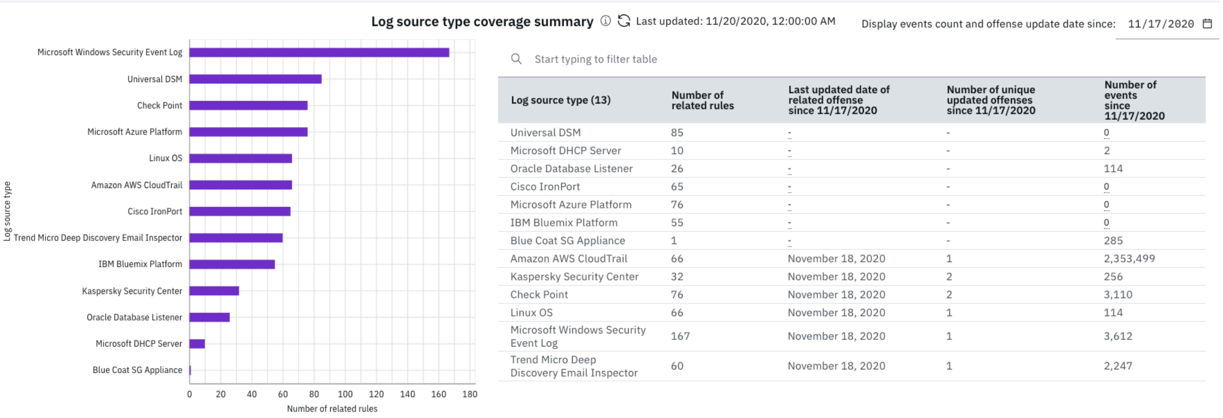
When you edit MITRE mappings in multiple rules or building blocks, you can now add or remove sub-techniques for each technique. For more information, see ."Editing MITRE Mappings in Multiple Rules or Building Blocks" on page 63

Now you can export MITRE mappings to a JSON file that can be imported as a layer into the MITRE ATT&CK Navigator. For more information, see "Sharing MITRE-mapping Files" on page 65.

Log source coverage enhancements

The **Log source type coverage summary** chart displays the number of rules that provide coverage for each log source type, and when the log source type last contributed to an offense, based on the last updated date. Use the table to review the number of events for log sources of that type. If the last updated date of an offense is old, try tuning some of the rules for the related log source type. For more information, see "Visualizing log source type coverage per rule" on page 91.

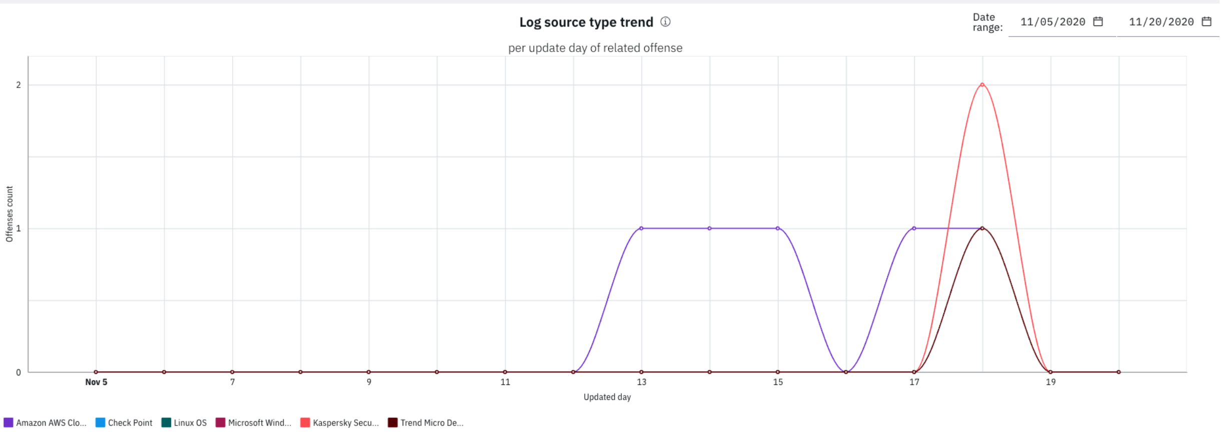
Figure 2: Log Source Type Coverage Summary Charts


Log source type coverage summary
Last updated: 11/20/2020, 12:00:00 AM
Display events count and offense update date since: 11/17/2020
Microsoft Windows Security Event Log
Universal DSM
Check Point
Microsoft Azure Platform
Linux OS
Amazon AWS CloudTrail
Cisco IronPort
Trend Micro Deep Discovery Email Inspector
IBM Bluemix Platform
Kaspersky Security Center
Oracle Database Listener
Microsoft DHCP Server
Blue Coat SG Appliance
Log source type
0
20
40
60
80
100
120
140
160
180
Number of related rules
Start typing to filter table

Log source type (13)	Number of related rules	Last updated date of related offense since 11/17/2020	Number of unique updated offenses since 11/17/2020	Number of events since 11/17/2020
Universal DSM	85	-	-	0
Microsoft DHCP Server	10	-	-	2
Oracle Database Listener	26	-	-	114
Cisco IronPort	65	-	-	0
Microsoft Azure Platform	76	-	-	0
IBM Bluemix Platform	55	-	-	0
Blue Coat SG Appliance	1	-	-	285
Amazon AWS CloudTrail	66	November 18, 2020	1	2,353,499
Kaspersky Security Center	32	November 18, 2020	2	256
Check Point	76	November 18, 2020	2	3,110
Linux OS	66	November 18, 2020	1	114
Microsoft Windows Security Event Log	167	November 18, 2020	1	3,612
Trend Micro Deep Discovery Email Inspector	60	November 18, 2020	1	2,247

The **Log source type trend** chart displays the number of offenses that log source types contributed to over time since the app was first installed. You can fine-tune the chart by specific log source type by clicking the checkboxes beneath the chart.

Figure 3: Log Source Type Trend Chart



Added the last updated date to the **Rules per used log source types** chart. The date can help you decide whether to refresh the rule data or wait for the automated refresh to occur.

For more information, see "Visualizing Log Source Type Coverage per Rule" on page 91.

Integrations

Packaged a QRadar Pulse dashboard template. QRadar Pulse users can import this template as a dashboard into their Pulse workspace to view the following charts:

- MITRE rule mappings per tactic
- MITRE rule mappings trend per tactic
- Current and potential rules per used log source type
- Log source type coverage and activity

For more information, see Synchronizing dashboard templates from content extensions.

Any links to offenses now link to the offenses page in the QRadar Analyst Workflow, if it is installed in your environment. When QRadar Use Case Manager opens from the QRadar Analyst Workflow, it appears in the theme that is selected in Analyst workflow.

Any links to reference sets now link to the reference sets in QRadar Reference Data Management app, if the app is installed in your environment.

Enhanced templates and report column data

You can edit the name and description of custom templates. For more information, see "Customizing Report Content Templates" on page 51.

Change the default template at any time. The default template now runs when the use case explorer page is first loaded.

Use the new column **Test: Reference set (number of elements)** for a quick reference to rules that depend on reference sets that are empty or have many elements. For example, select the **Rules per reference set** template, and then use the column customization option to replace the **Reference set** column with the **Reference set (number of elements)** column.

Version 3.0.0

Work more efficiently

Customizable user preferences include the option to use a light or dark theme and an option to reduce or increase table row height of the rule report. The default row height is now smaller than before to save space. For more information, see "Customizing User Preferences" on page 46.

Support for multiple languages was added based on QRadar user preferences. Supported languages include English, Simplified Chinese, Traditional Chinese, French, German, Korean, Portuguese, Russian, Spanish, Italian, and Japanese.

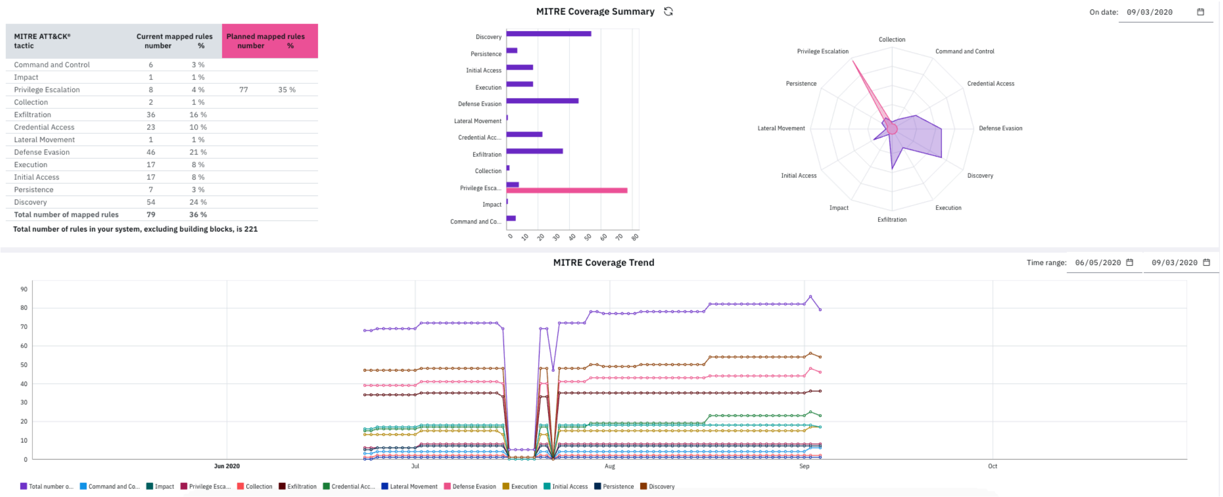
You can expand the relationship graph and MITRE coverage heat maps to fit the whole window, and zoom in or out to focus on details. Any filtering that you apply in the expanded pane is kept when you return to the Use Case Explorer page.

You can also further customize the table groupings in the rule report by choosing to show child rows or only the count of child rows in the grouped mode of the report. Click the arrow in the tree structure icon. Then, select from the groupable columns that are currently displayed or show only the number of child rows in the report instead of the actual rows. After you have the number of items in the report column, click the number to see the list of actual child items. For more information, see "Rule Report Presentation" on page 88.

Save time and effort from creating new rules by duplicating existing rules. Then, you can customize the duplicated rules to meet the needs of your environment. For more information, see "Duplicating Rules for Further Customization" on page 85.

Visualize MITRE coverage in new ways

The **MITRE Coverage Summary** and **MITRE Coverage Trend** reports provide new ways of visualizing MITRE ATT&CK coverage. In the coverage summary report, you can check the current number and percentage to see where you're lacking in rule coverage, and plan to increase coverage for some tactics. The trend report shows the total rule coverage trend over time. For more information, see "Visualizing MITRE Tactic and Technique Coverage in Your Environment" on page 66.



MITRE ATT&CK® tactic	Current mapped rules number	%	Planned mapped rules number	%
Command and Control	6	3 %		
Impact	1	1 %		
Privilege Escalation	8	4 %	77	35 %
Collection	2	1 %		
Exfiltration	36	16 %		
Credential Access	23	10 %		
Lateral Movement	1	1 %		
Defense Evasion	46	21 %		
Execution	17	8 %		
Initial Access	17	8 %		
Persistence	7	3 %		
Discovery	54	24 %		
Total number of mapped rules	**79**	**36 %**		

Total number of rules in your system, excluding building blocks, is 221

MITRE Coverage Summary

On date: 09/03/2020

MITRE Coverage Trend

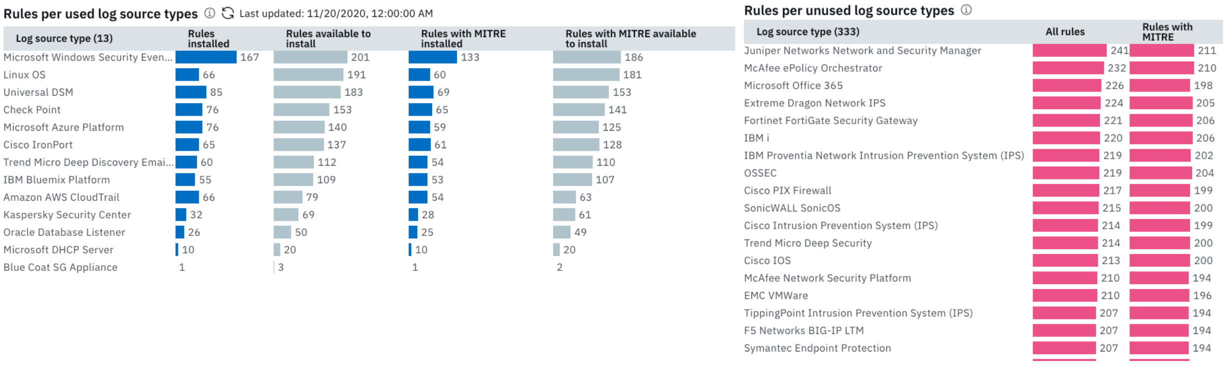
Time range: 06/05/2020 09/03/2020

On MITRE coverage heat maps, you can identify techniques that are used by groups or software that is identified by MITRE. You can also filter out (hide) techniques in the chart that are not related to the techniques currently selected in filter for report. For more information, see "Visualizing MITRE Tactic and Technique Coverage in Your Environment" on page 66.

Improve your rule coverage by adding content extensions from the IBM Security App Exchange

Content awareness capabilities help you see from which content extension the rules originate. Filter by content extensions for installed rules and uninstalled rules available in content extensions on IBM Security App Exchange. Link from content extension names in the report to the corresponding dialog in

QRadar Assistant app for easier installation or updating. New predefined templates recommend content extensions from IBM Security App Exchange based on increased log source and MITRE coverage.



Rules per used log source types Last updated: 11/20/2020, 12:00:00 AM

Log source type (13)	Rules installed	Rules available to install	Rules with MITRE installed	Rules with MITRE available to install
Microsoft Windows Security Even...	167	201	133	186
Linux OS	66	191	60	181
Universal DSM	85	183	69	153
Check Point	76	153	65	141
Microsoft Azure Platform	76	140	59	125
Cisco IronPort	65	137	61	128
Trend Micro Deep Discovery Emai...	60	112	54	110
IBM Bluemix Platform	55	109	53	107
Amazon AWS CloudTrail	66	79	54	63
Kaspersky Security Center	32	69	28	61
Oracle Database Listener	26	50	25	49
Microsoft DHCP Server	10	20	10	20
Blue Coat SG Appliance	1	3	1	2

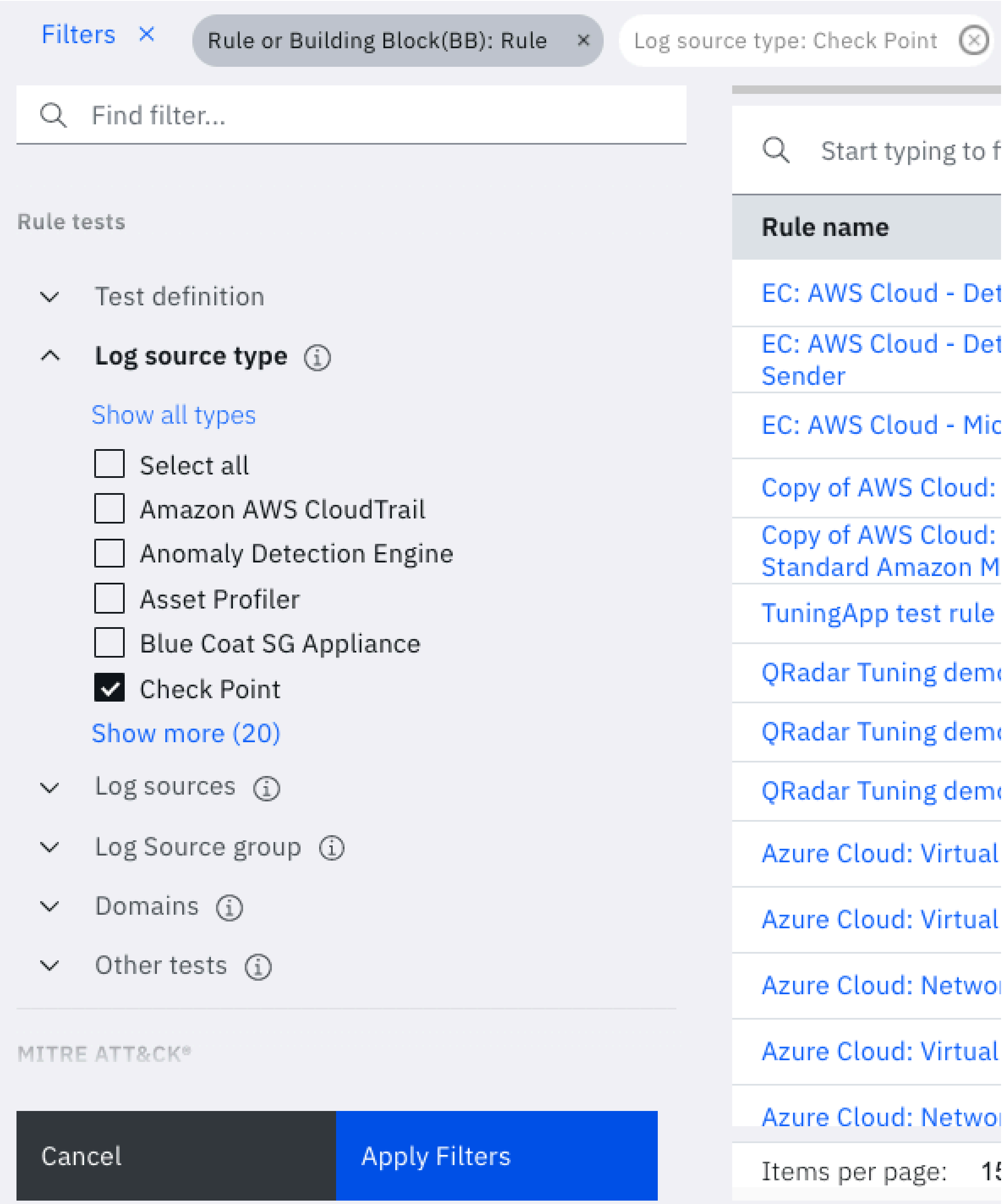
Rules per unused log source types

Log source type (333)	All rules	Rules with MITRE
Juniper Networks Network and Security Manager	241	211
McAfee ePolicy Orchestrator	232	210
Microsoft Office 365	226	198
Extreme Dragon Network IPS	224	205
Fortinet FortiGate Security Gateway	221	206
IBM i	220	206
IBM Proventia Network Intrusion Prevention System (IPS)	219	202
OSSEC	219	204
Cisco PIX Firewall	217	199
SonicWALL SonicOS	215	200
Cisco Intrusion Prevention System (IPS)	214	199
Trend Micro Deep Security	214	200
Cisco IOS	213	200
McAfee Network Security Platform	210	194
EMC VMWare	210	196
TippingPoint Intrusion Prevention System (IPS)	207	194
F5 Networks BIG-IP LTM	207	194
Symantec Endpoint Protection	207	194

New charts show an overview of log source coverage and MITRE coverage by currently installed rules and uninstalled rules that can be installed from IBM Security App Exchange. For more information, see "Identifying Gaps in QRadar Rule Coverage from Content Extensions" on page 82.

Apply rule and building block filters more easily

Previously, the **Apply** button was visible at the bottom of the pane, but it was often difficult to realize that you had to click it to apply the filters. Now, it appears only when you select at least one filter in the pane. As you select filters, they appear in a different color in the filter row, but they change color after you click **Apply Filters**.



Filters ✕ | Rule or Building Block(BB): Rule ✕ | Log source type: Check Point ⊗

Find filter...

Rule tests

- Test definition
- Log source type ⓘ
  - Show all types
  - □ Select all
  - □ Amazon AWS CloudTrail
  - □ Anomaly Detection Engine
  - □ Asset Profiler
  - □ Blue Coat SG Appliance
  - ☑ Check Point
  - Show more (20)
- Log sources ⓘ
- Log Source group ⓘ
- Domains ⓘ
- Other tests ⓘ

MITRE ATT&CK®

Start typing to f

Rule name
EC: AWS Cloud - Det
EC: AWS Cloud - Det Sender
EC: AWS Cloud - Mic
Copy of AWS Cloud:
Copy of AWS Cloud: Standard Amazon M
TuningApp test rule
QRadar Tuning dem
QRadar Tuning dem
QRadar Tuning dem
Azure Cloud: Virtual
Azure Cloud: Virtual
Azure Cloud: Netwo
Azure Cloud: Virtual
Azure Cloud: Netwo

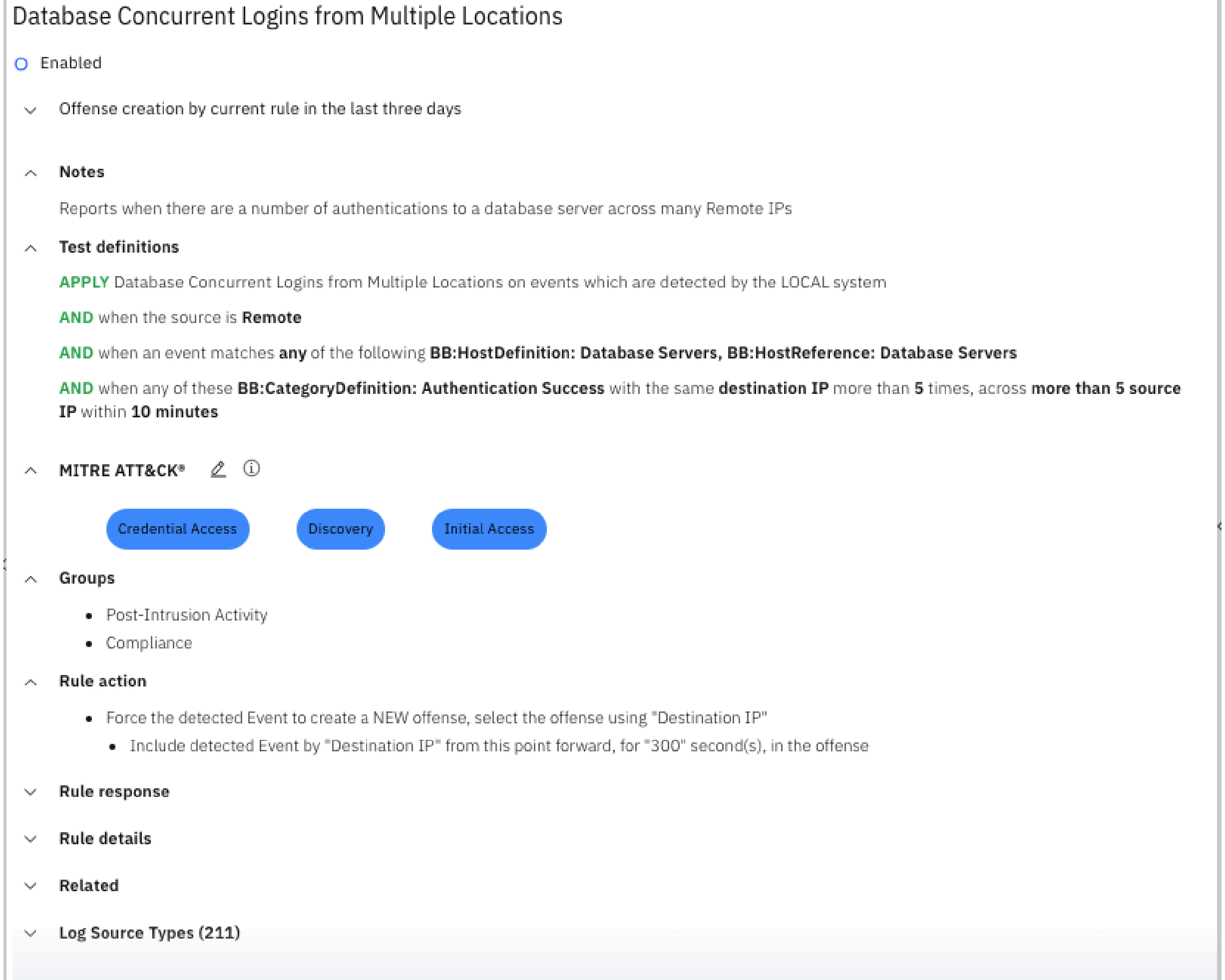
Items per page: 15

A new search filter in the log source rule test facilitates filtering when the list contains many log sources. You can also filter rules that are related to only used log sources types or unused log source types.

Rule wizard contains more data and is easier to read

The following enhancements were made to improve tuning in the rule wizard:

- Added all parts of rule action and rule response to rule details page. Also added two new columns: **Rule attribute: Rule action details** and **Rule attribute: Rule response details** that contain complete rule action and rule response information.
- Added the rule scope information before the test definition section to indicate whether the rule is global or local.
- The log source type section is now sorted and includes the number of log source types.
- Rule details are now refreshed automatically after you edit MITRE mappings for the rule.
- Improved layout of rule details page by rearranging sections and expanding some sections by default.



Database Concurrent Logins from Multiple Locations

○ Enabled

Offense creation by current rule in the last three days

Notes

Reports when there are a number of authentications to a database server across many Remote IPs

Test definitions

APPLY Database Concurrent Logins from Multiple Locations on events which are detected by the LOCAL system

AND when the source is **Remote**

AND when an event matches **any** of the following **BB:HostDefinition: Database Servers, BB:HostReference: Database Servers**

AND when any of these **BB:CategoryDefinition: Authentication Success** with the same **destination IP** more than **5** times, across **more than 5 source IP** within **10 minutes**

MITRE ATT&CK®

Groups

- Post-Intrusion Activity
- Compliance

Rule action

- Force the detected Event to create a NEW offense, select the offense using "Destination IP"
  - Include detected Event by "Destination IP" from this point forward, for "300" second(s), in the offense

Rule response

Rule details

Related

Log Source Types (211)

Configure a proxy

You can now configure a proxy so that QRadar Use Case Manager can access the IBM Security App Exchange to get up-to-date information about non-installed content extensions and MITRE mappings for all content extensions. If you don't configure the proxy, you can still see the information in the app, but be aware that it can become out of date.

Version 2.3.1

Performance improvements

Improved performance for generating MITRE-related reports and heat map coverage visualization, as well as overall report generation.

Version 2.3.0

Moved the MITRE-mapping capabilities into the app

The MITRE-mapping capabilities were moved to QRadar Use Case Manager. This streamlines the process of editing rule MITRE mappings. The Cyber Adversary Framework Mapping app is no longer included in the QRadar Use Case Manager installation package. If the Cyber Adversary Framework Mapping app is already installed, QRadar Use Case Manager gathers any existing mappings during installation. Afterward, you can delete the Cyber Adversary Framework Mapping app and use QRadar Use Case Manager instead to help ensure that all your rule mappings are up to date in the app.

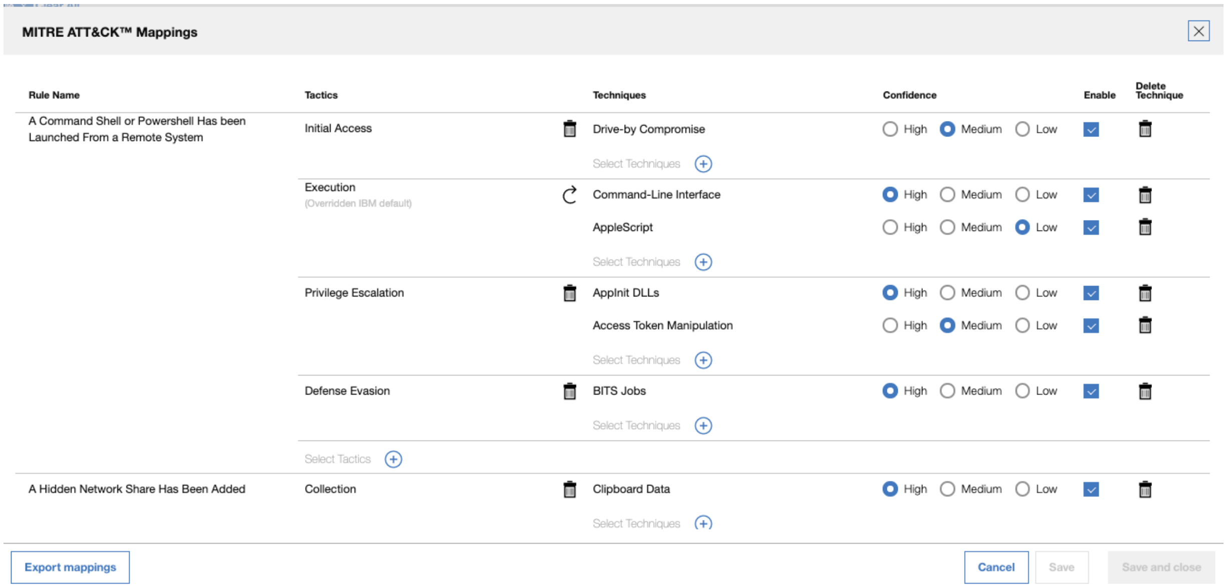
Reduced memory requirement

Reduced the memory requirement of the app to 500 MB.

Edit rule MITRE mappings

Save time and effort by selecting several rules and editing the MITRE mappings for all of them at once. If needed, you can also export the selected mappings that you edited.

Figure 4: Edit MITRE Mappings



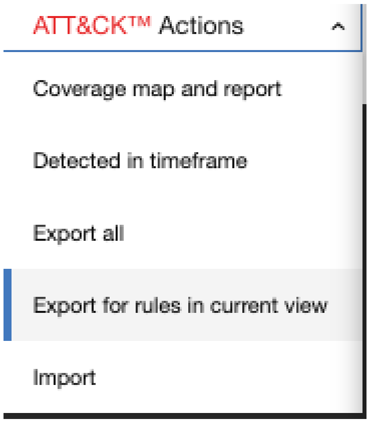
MITRE ATT&CK™ Mappings

Rule Name	Tactics		Techniques	Confidence	Enable	Delete Technique
A Command Shell or Powershell Has been Launched From a Remote System	Initial Access	🗑	Drive-by Compromise	○ High ● Medium ○ Low	☑	🗑
			Select Techniques ⊕			
	Execution (Overridden IBM default)	↻	Command-Line Interface	● High ○ Medium ○ Low	☑	🗑
			AppleScript	○ High ○ Medium ● Low	☑	🗑
			Select Techniques ⊕			
	Privilege Escalation	🗑	AppInit DLLs	● High ○ Medium ○ Low	☑	🗑
			Access Token Manipulation	○ High ● Medium ○ Low	☑	🗑
			Select Techniques ⊕			
	Defense Evasion	🗑	BITS Jobs	● High ○ Medium ○ Low	☑	🗑
			Select Techniques ⊕			
	Select Tactics ⊕					
A Hidden Network Share Has Been Added	Collection	🗑	Clipboard Data	● High ○ Medium ○ Low	☑	🗑
			Select Techniques ⊕			

Enhanced exporting capabilities

Added options to export only the MITRE mappings for the rules in the current report view or export all the rule mappings in the app. Share the JSON file with your other instances of QRadar Use Case Manager.

Figure 5: Export MITRE Mappings for All Rules or Just the Rules in the Current View

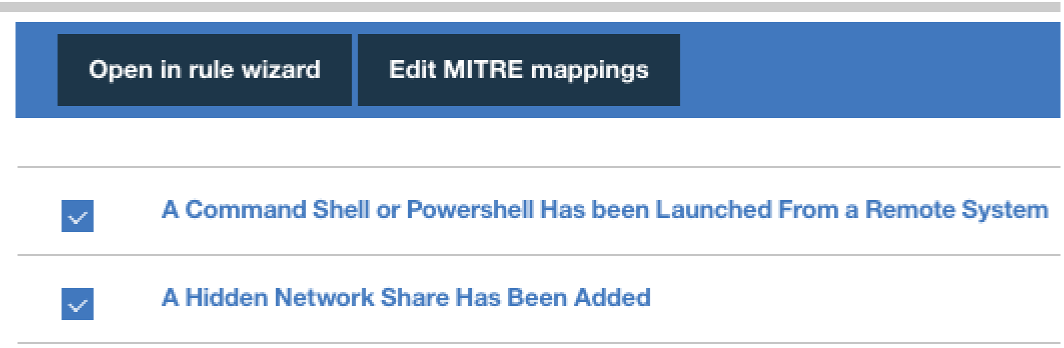


Rules Explorer enhancements

New **MITRE Tactic ID** and **MITRE Technique ID** columns are now available as options in the rule report to provide more context.

Select multiple rules and open them in the Rule Wizard for simultaneous investigation.

Figure 6: Select Multiple Rules to Edit or Investigate Simultaneously



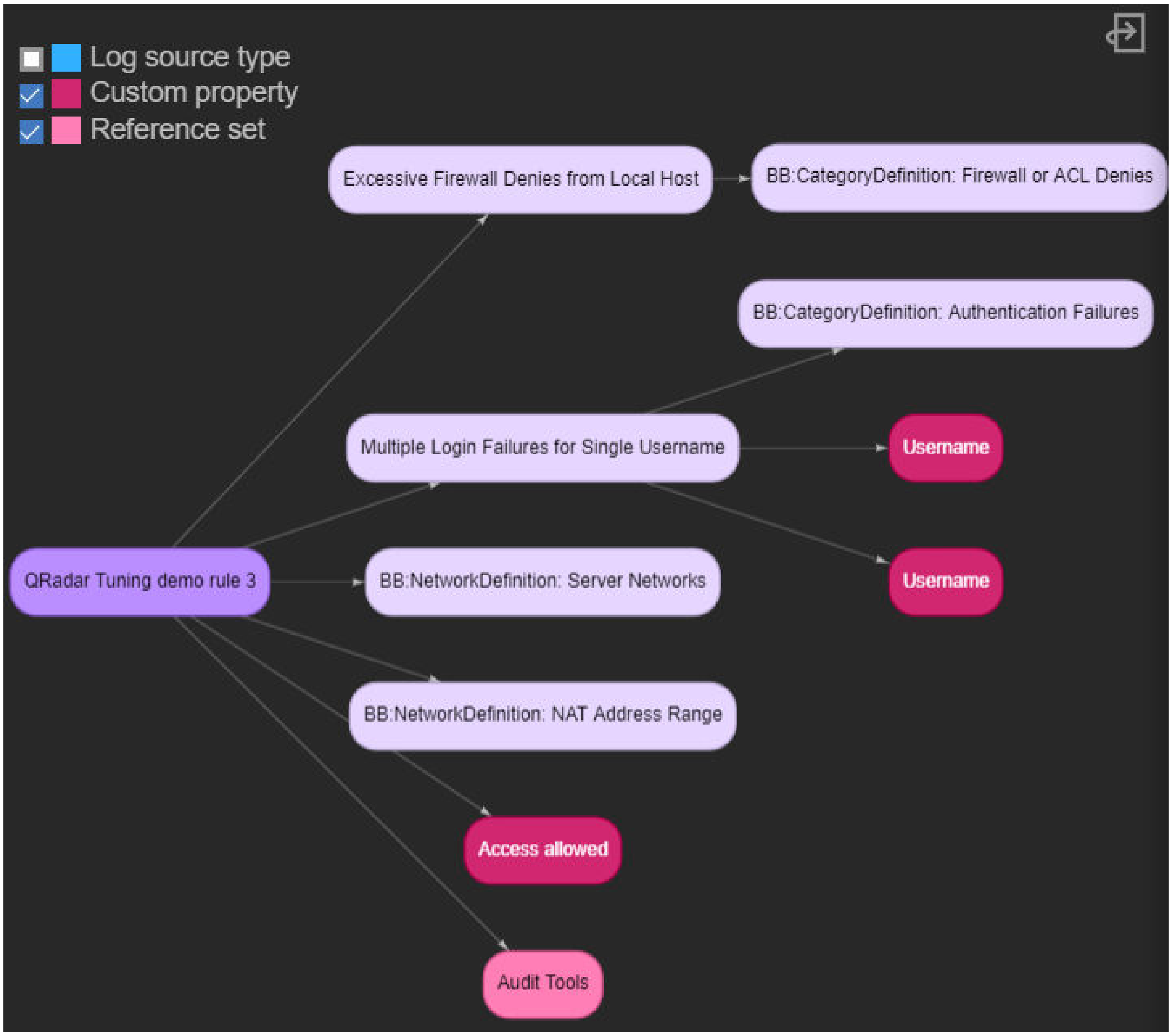
☑ A Command Shell or Powershell Has been Launched From a Remote System

☑ A Hidden Network Share Has Been Added

Rule visualization enhancement

Added options to show related reference sets, custom properties, and log source types.

Figure 7: Options to Show Related Reference Sets, Custom Properties, and Log Source Types for Rules


☐ Log source type
☑ Custom property
☑ Reference set
Excessive Firewall Denies from Local Host
BB:CategoryDefinition: Firewall or ACL Denies
BB:CategoryDefinition: Authentication Failures
Multiple Login Failures for Single Username
Username
QRadar Tuning demo rule 3
BB:NetworkDefinition: Server Networks
Username
BB:NetworkDefinition: NAT Address Range
Access allowed
Audit Tools

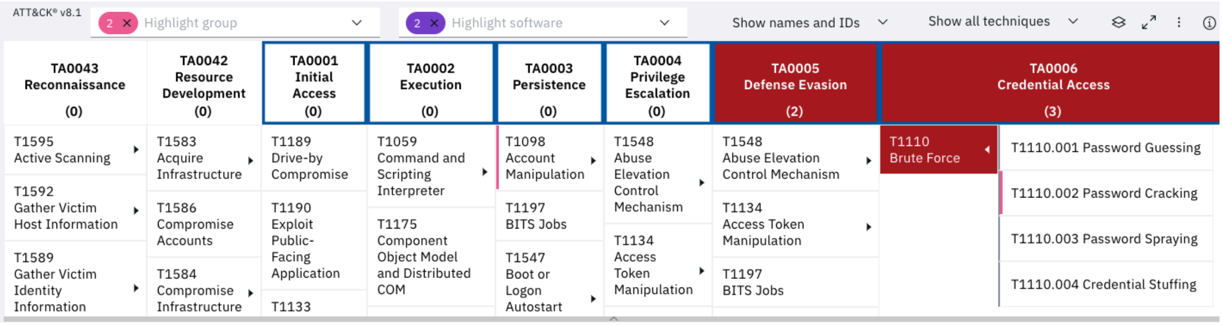
Fixed issue

Fixed an issue where the SNMP Trap was not visible in the rule details page when **SNMP Trap** was selected as a rule response attribute on the rule details page.

Version 2.2.0

MITRE improvements

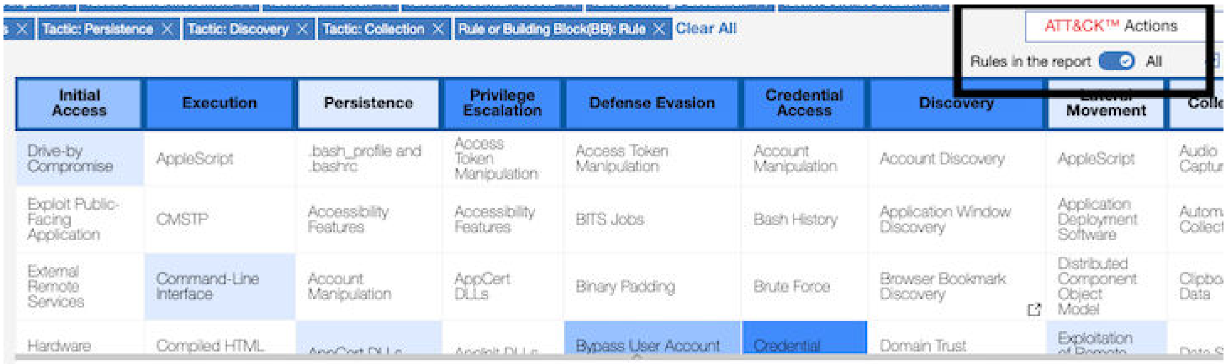
You can now see which MITRE ATT&CK tactics and techniques were detected in your environment in a specific time period. A heat map and flexible reports show the detected tactics and techniques and related rules and offenses. For more information, see "Visualizing MITRE Tactics and Techniques that are Detected in a Specific Timeframe" on page 70.



TA0043 Reconnaissance (0)	TA0042 Resource Development (0)	TA0001 Initial Access (0)	TA0002 Execution (0)	TA0003 Persistence (0)	TA0004 Privilege Escalation (0)	TA0005 Defense Evasion (2)	TA0006 Credential Access (3)	
T1595 Active Scanning	T1583 Acquire Infrastructure	T1189 Drive-by Compromise	T1059 Command and Scripting Interpreter	T1098 Account Manipulation	T1548 Abuse Elevation Control Mechanism	T1548 Abuse Elevation Control Mechanism	T1110 Brute Force	T1110.001 Password Guessing
T1592 Gather Victim Host Information	T1586 Compromise Accounts	T1190 Exploit Public-Facing Application	T1175 Component Object Model and Distributed COM	T1197 BITS Jobs	T1134 Access Token Manipulation	T1134 Access Token Manipulation		T1110.002 Password Cracking
T1589 Gather Victim Identity Information	T1584 Compromise Infrastructure	T1133		T1547 Boot or Logon Autostart		T1197 BITS Jobs		T1110.003 Password Spraying
								T1110.004 Credential Stuffing

ATT&CK options are now more visible in the Rule Explorer

An **ATT&CK Actions** menu makes it easier to access the heat maps to see rule coverage and detected tactics and techniques. A switch for the coverage heat map filters the table coloring based on only the rule mappings in the current report or by all the rules in your environment.



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Movement	Colle
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Captur
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Autom Collect
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipbo Data
Hardware	Compiled HTML	AppCert DLLs	AppInit DLLs	Bypass User Account	Credential	Domain Trust	Exploitation of Remote	Data S

MITRE tactics table header stays fixed for easier scrolling

The tactics header in the heat map is now in a fixed state while you scroll down the table, making it easier to track the tactics and techniques that you're reviewing.

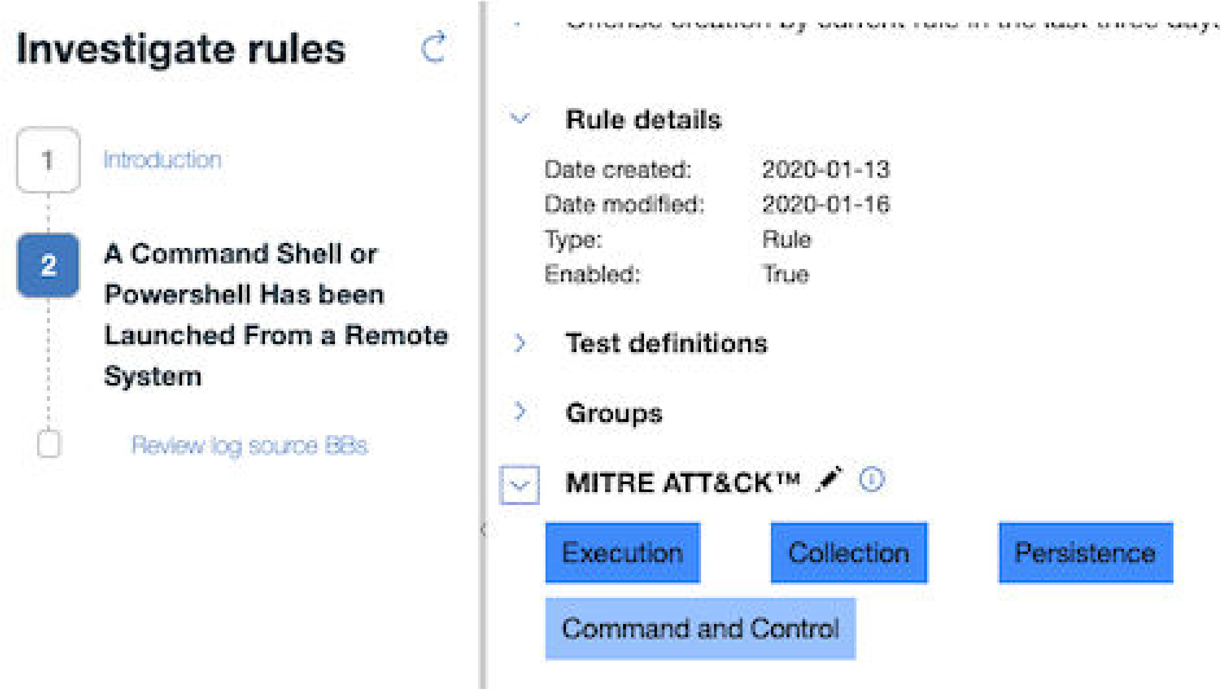
Rule Explorer enhancements

Domains are now represented by the rule test filters. The domain filter group lists all the domains in a multi-domain environment. For more information, see "Filtering Rules and Building Blocks by their Properties" on page 78.

A new **Rule Response: Event Description** column is available as an option in the rule report to provide more context.

Rule wizard enhancement

A MITRE tag in the rule details screen of the rule wizard now shows the source BB or rule from where the mapping originates. This information also displays as a column in the rule report.



Date created:	2020-01-13
Date modified:	2020-01-16
Type:	Rule
Enabled:	True

Fixed issues

- Problems related to renaming system rules when either old name or duplicate name shows up in Rule Explorer
- Problems in early patches of QRadar 7.3.1 where QRadar Use Case Manager 2.1.0 didn't work.

Version 2.1.0

- Added an option to group related data properties in the report table. For more information, see "Rule Report Presentation" on page 88.
- Create custom templates in the Rules Explorer from existing templates or create new ones. For more information, see "Customizing Report Content Templates" on page 51.
- Added a "Select all" option to the rules attribute filter to make it easier to select all the groups in the list.
- Added a **Notes** filter to the **Rule Attributes** page to search for specific rules with notes.
- The app now detects when newer versions are available to download on the IBM Security App Exchange.

- Implemented the following usability improvements that are related to MITRE ATT&CK:
  - Added an exploratory icon link to the MITRE documentation for each tactic and technique in the technique coverage heat map.
  - Added a **Mapping enabled** column to the filters and the report, which indicates that the mapping between Cyber Adversary Framework Mapping app and QRadar is turned on. Mappings that are disabled are not added to the technique coverage heat map.
  - Added capabilities to the rule wizard to open the rule directly in the Cyber Adversary Framework Mapping app for editing.
  - Re-calibrated the heat map formula to use only enabled rules to calculate the heat map colors.
  - Added a tooltip to the MITRE ATT&CK filter page to remind users to set an authentication token for the Cyber Adversary Framework Mapping app.
  - Added a column selection option for **Tactic (at rule level)** and **Technique (at rule level)** to show only values that are mapped directly to the rule.
- Fixed an issue where the way QRadar handles incomplete rules causes some APIs in some product versions to fail, and causes data inconsistencies in QRadar Use Case Manager.
- Fixed an issue where the log source type filter doesn't have any values in cases where there are more than 50,000 log sources.

Version 2.0.0

- Added a rule explorer to filter rules by different properties, such as attributes, rule tests, and MITRE ATT&CK tactics and techniques. Use filters to ensure that the rules are defined and working as intended, including log source coverage. Determine which rules you might need to edit in QRadar or investigate further in QRadar Use Case Manager.
- Added the Cyber Adversary Framework Mapping app. With the Cyber Adversary Framework Mapping app, you can map your custom rules and building blocks to MITRE ATT&CK tactics and techniques and override the QRadar default rule mappings.
- Added MITRE ATT&CK tactics visualization and the ability to customize your mappings with the Cyber Adversary Framework Mapping app.
- Made the following minor UI improvements:
  - Added a wrench icon to any links and buttons that lead to the investigation wizard.
  - Added links for reference sets to open in QRadar.

Version 1.1.0

- Automatically download rules in IBM QRadar 7.3.2 or later.
- Added the ability to edit IP addresses of reference sets in the **IPs & Ports** tab of the **Host definitions** page. Supported in IBM QRadar 7.3.1 or later.
- Added the ability to edit ports of building blocks and rules in the **IPs & Ports** tab of the **Host definitions** page. Supported in IBM QRadar 7.3.2 or later.

Version 1.0.1

Increased the **rules.xml** file upload limit to 50 MB.

Version 1.0.0

- Tune most active rules
- Tune most active rules based on the CRE event report
- Review network hierarchy
- Review building blocks

In this early access version, you need to run a script on the QRadar Console to generate a rules data file and then upload it to the app. This temporary step might not be required in later releases.

RELATED DOCUMENTATION

What's New in QRadar Use Case Manager | 6
Known Issues | 32
Video Demonstrations | 35

3

CHAPTER

Known Issues

Known Issues

IN THIS SECTION

The QRadar Use Case Manager has required information for known issues.

Unable to use APIs outside of QRadar in QRadar Use Case Manager 3.1.0

In version 3.1.0, custom integrations might stop working, resulting in the inability to connect to the QRadar Use Case Manager APIs from outside your QRadar environment. The workaround in QRadar Use Case Manager 3.1.0 or later is to authenticate the API calls by using the same token that is used on the Configuration page (add a SEC header in the API call). If you upgrade to version 3.2.0 or later and use the token that you used to configure QRadar Use Case Manager, the custom integrations work.

Commonly referenced elements appear with different names

Commonly referenced elements, such as log sources, custom properties, or reference sets, can appear with old names in QRadar Use Case Manager and the rule details section in QRadar. QRadar Use Case Manager retrieves the names of elements that are referenced by rule tests from the text in the rule XML. When a referenced element changes its name, the text in the rule XML is not updated. As a workaround, you can edit the rule in the rule wizard in QRadar Use Case Manager and save it (click **Finish** without changing anything) to resolve the text mismatch.

QRadar Use Case Manager updates log source type names in the rule within 15 minutes of the update, or when you explicitly refresh the rule.

TIP: Add this filter to all of your report templates so that you don't need to keep manually selecting the filters.

Unable to Search for the Forward Slash Character in Regex

The app cannot search for the forward slash character (/) in regular expressions. For example, on the **Use Case Explorer** page in the rule name or test definition in the filters, and rule name in the search bar of the table. As a work-around, use a question mark (?) as a wild character.

Corrupted Custom Rule Prevents Using Related Functions

A corrupted rule in QRadar prevents the QRadar API from returning required data. This prevents the QRadar Use Case Manager app from using rule-related functions.

NOTE: This issue was fixed in QRadar 7.3.3 Fix Pack 4 or later, 7.4.0 Fix Pack 2, and 7.4.1 or later.

RELATED DOCUMENTATION

What's New in QRadar Use Case Manager | 6

Earlier Versions | 7

Video Demonstrations | 35

4

CHAPTER

Video Demonstrations

Video Demonstrations

IN THIS SECTION

Watch video tutorials to learn how to use the workflows and features in QRadar Use Case Manager.

Video Demonstrations on YouTube

Tutorials and general overview of the QRadar Use Case Manager.

Version 3.0.0

- Version 3 Overview
- Tutorial: Intro and Navigation
- Tutorial: Recommended Apps and Log Sources
- Tutorial: Improving my QRadar without spending a penny
- Tutorial: Making the case for additional log sources
- Tutorial: Log sources per Rule
- Tutorial: Using filters
- Tutorial: MITRE Part One
- Tutorial: MITRE Part Two

Version 2.1 - 2.3

- QRadar Use Case Manager v2.2 + 2.3 updates
- MITRE ATT&CK Framework

Version 2.0.0

- QRadar Use Case Manager Overview
- 2.0 Overview

Version 1.0.0

- Part One: Tune the most active rules
- Part Two: Tune the active rules that generate CRE events
- Part Three: Review network hierarchy
- Part Four: Review building blocks
- Part Five: Installation script

Videos Within the App

Learn how to investigate rules and tune them to prevent false positive offenses. Watch a short video before you begin investigating rules in the rule wizard. For more information about accessing the video, see "Tuning the Active Rules That Generate Offenses" on page 98.

A well-defined and maintained network hierarchy can help prevent the generation of false positive offenses. Watch tuning videos to learn more about your network hierarchy and how to keep it up-to-date. For more information about accessing the video, see "Reviewing Your Network Hierarchy" on page 101.

RELATED DOCUMENTATION

What's New in QRadar Use Case Manager | 6

Earlier Versions | 7

Known Issues | 32

5

CHAPTER

Supported Environments for QRadar Use Case Manager

Supported Environments for QRadar Use Case Manager

IN THIS SECTION

For the features in QRadar products to work properly, you must use the supported environments.

Supported Versions of QRadar

QRadar Use Case Manager	QRadar
3.4.1	7.3.3 Fix Pack 6 or later 7.4.2 Fix Pack 3 or later
3.2.0 to 3.4.0	7.3.3 Fix Pack 6 or later 7.4.1 Fix Pack 2 or later 7.4.2 or later **NOTE**: QRadar Use Case Manager 3.2.0 or later is not supported on QRadar 7.4.0.
3.1.0 or earlier	7.3.2 or later

Supported Browsers

The QRadar Use Case Manager app is supported on Google Chrome and Mozilla Firefox.

Supported languages

The following languages are supported based on QRadar user preferences: English, Simplified Chinese, Traditional Chinese, French, German, Korean, Portuguese, Russian, Spanish, Italian, and Japanese.

RELATED DOCUMENTATION

Installing QRadar Use Case Manager | 41
Upgrading QRadar Use Case Manager | 55

6

CHAPTER

Installation and Configuration Checklist

Installation and Configuration Checklist

As you install QRadar Use Case Manager, review and complete all of the necessary tasks on the installation checklist.

- Review the supported environments. See "Supported Environments for QRadar Use Case Manager" on page 38.
- Ensure that you have an IBM ID. If you don't have one, you can sign up on the IBM Security App Exchange.
- Install QRadar Use Case Manager. See "Installing QRadar Use Case Manager" on page 41.
- Create an authorized service token. See "Creating an Authorized Service Token" on page 42.
- Configure the Use Case Explorer page. See "Configuring the Use Case Explorer in QRadar Use Case Manager" on page 43.
- Assign user permissions. See "Assigning User Permissions for QRadar Use Case Manager" on page 44.

Installing QRadar Use Case Manager

Before you install the QRadar Use Case Manager app, ensure that it meets the minimum memory (RAM) requirements. QRadar Use Case Manager requires 500 MB of free memory from the application pool of memory. If QRadar Use Case Manager fails to install, then your application pool does not have enough free memory to run the app. Consider adding an App Host to your QRadar deployment. For more information about calculating the required memory, see Apps and Resource Limitation.

QRadar 7.3.2 or later uses an App Host, which is a managed host, that is dedicated to running apps. App Hosts provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your QRadar Console. For more information, see https://www.juniper.net/documentation/en_US/jsa7.4.2/jsa-administration-guide/topics/concept/concept-jsa-admin-app-host.html.

Use the QRadar Extensions Management tool or the QRadar Assistant app to install the QRadar Use Case Manager app on your QRadar Console.

1. Choose one of the following methods to download your app:
   - If the IBM QRadar Assistant app is configured on QRadar, use the following instructions to install the QRadar Use Case Manager app: QRadar Assistant app.

- If the QRadar Assistant app is not configured, download the QRadar Use Case Manager app archive from the IBM Security App Exchange.

2. If you downloaded the app from the App Exchange, complete the following steps:

   a. On the QRadar Console, click **Admin >Extensions Management**.

   b. In the **Extension Management** window, click **Add** and select the app archive that you want to upload to the console.

   c. Select the **Install immediately** checkbox.

      NOTE: You might have to wait several minutes before your app becomes active.

   d. To preview the contents of an app after it is added and before it is installed, select it from the list of extensions, and click **More Details**. Expand the folders to view the individual content items in each group.

3. If IBM QRadar Advisor with Watson is installed in your environment, it includes the Cyber Adversary Framework Mapping app. This MITRE-mapping app is no longer needed when you install QRadar Use Case Manager 2.3.0 or later. To remove the Cyber Adversary Framework Mapping app, follow steps 5 and 6 in "Upgrading QRadar Use Case Manager" on page 55.

If the app installed successfully, you see it listed as 'Installed' on the **Extensions Management** page of the **Admin** tab. If the app didn't install correctly, see QRadar apps troubleshooting.

RELATED DOCUMENTATION

Creating an Authorized Service Token | 42

Creating an Authorized Service Token

Before you can configure QRadar Use Case Manager, you must create an authorized service token.

1. On the QRadar Console, click **Admin** > **Authorized Services**.
2. In the Manage Authorized Services page, click **Add Authorized Service**.
3. Add the relevant information in the following fields and click **Create Service**:

   a. In the **Service Name** field, type a name for this authorized service. The name can be up to 255 characters in length.

   b. From the **User Role** list, select the **Admin** user role.

   c. From the **Security Profile** list, select the security profile that you want to assign to this authorized service. The security profile determines the networks and log sources that this service can access on the QRadar Console.

   d. In the **Expiry Date** list, type or select a date that you want this service to expire. If an expiry date is not necessary, select **No Expiry**.

   e. Click **Create Service**.

4. Click the row that contains the service you created, select and copy the token string from the **Selected Token** field in the menu bar, and close the Manage Authorized Services page.
5. On the **Admin** page, click **Deploy Changes** so that the new token works with the app.
6. Click **Apps >QRadar Use Case Manager >Configuration**, paste the token string into the **Authorized service token** field, and click **Submit**.

RELATED DOCUMENTATION

Assigning User Permissions for QRadar Use Case Manager | 44

Configuring the Use Case Explorer in QRadar Use Case Manager

The Use Case Explorer uses QID records and DSM event-mapping information to help determine rule coverage by log source type. The Use Case Explorer loads automatically, but you can refresh the settings at any time.

1. On the **Admin** tab, click **QRadar Use Case Manager > Configuration**.
2. To sync with the data in QRadar, click **Sync QID Records**. This process might take approximately 30 minutes to complete. You can still use the app while the records are syncing, but the data you work with might not be accurate.
3. To manually refresh event mappings, click **Sync DSM event mappings**.

   When you install the app for the first time, it automatically syncs after installation. If you upgrade to QRadar Use Case Manager 2.0.0 or later, you don't need to sync.
4. To back up your MITRE mappings (custom and IBM default), click **Export MITRE mappings**. You can then import this backup file later on the Use Case Explorer page.

   Only the custom mappings are imported from the file.
5. If you're upgrading to QRadar Use Case Manager 3.1.0 or later, you might see a section that is called **Report on migration from MITRE v6.3 to v8.x**. This report appears if there were MITRE mappings in

the previous version of the app that are now deprecated with the support for MITRE v8.1. All custom mappings that were created in previous versions of the app are automatically migrated to the new version. Mappings to techniques that are now deprecated or don't exist under a particular tactic are deleted and included in the migration report. Consider creating new mappings to these rules.

When you've noted the mappings that are affected, you can click **Clear migration report** to permanently remove the report notification. Non-administrative users can see the report migration notification on the Use Case Explorer page.

6. To configure a proxy server, expand the **Proxy configuration** section and enter the following information for your proxy server:

   - Protocol
   - Address or hostname
   - Port
   - Username
   - Password

7. Click **Save** and then close the Settings page.

RELATED DOCUMENTATION

Assigning User Permissions for QRadar Use Case Manager | **44**

Assigning User Permissions for QRadar Use Case Manager

After you install the QRadar Use Case Manager, you can share the app with non-administrative users by adding it to a user role.

After you install QRadar Use Case Manager, it is displayed as a capability in the User Roles window on the **Admin** tab. *Capabilities* are sets of permissions that user roles have. To use the app, a QRadar administrator must assign the app, and any other capabilities that it requires, to a user role.

1. Click **User Roles** on the **Admin** tab.
2. On the User Roles window, select the user role that you want to assign the app permissions to.
3. Select the checkbox for QRadar Use Case Manager and the permissions in the following table.

User permission	Capabilities
Offenses	**View Custom Rules** Read-only access to offense rules **Maintain Custom Rules** Full access to offense rules, including ability to edit MITRE mappings.
Log Activity	**View Custom Rules** Read-only access to common, event, and anomaly rules **Maintain Custom Rules** Full access to common, event, and anomaly rules, including ability to edit MITRE mappings.
Network Activity	**View Custom Rules** Read-only access to common, flow, and anomaly rules **Maintain Custom Rules** Full access to common, flow, and anomaly rules, including ability to edit MITRE mappings.
Offenses	The trend charts on the home page and the tuning active rules feature.
Delegated Administration	**Define Network hierarchy** View and edit the **Check Network Hierarchy** page and any link that opens Network Hierarchy. **Manage Reference Data** Edit reference sets.

(Continued)

User permission	Capabilities
Log Activity	View and edit R2R (Remote to Remote) events and tuning based on CRE reports.

The level of rule permissions assigned to a user affects what they can do and see in the following pages:

- Use Case Explorer
- Active Rules
- Tuning home page
- CRE Event Report
- Network Hierarchy
- Host Definitions

4. Click **Save**, and then click **Deploy Changes** so that your user role updates take effect.

RELATED DOCUMENTATION

Customizing User Preferences | 46

Customizing User Preferences

Customizable user preferences include color themes, table row height options, and MITRE ATT&CK platform support. Themes control the background color display for QRadar Use Case Manager. Table row height options reduce empty white space to control the amount of data you can display in a table. Platform support affects MITRE ATT&CK visualizations, and the contents of related filter controls.

1. From the QRadar Use Case Manager menu, click **Settings** > **User Preferences**.
2. Select either a light or dark theme.
3. Select from the following height options for the table row: **Compact**, **Short**, **Tall**, or **None**. The default setting is **Short**.

TIP: To see as much data as possible on the screen, choose **Compact**.

4. Set the selected platforms and the contents of related filter controls to filter the Detected in timeframe and the Coverage map MITRE reports.

   By default, the Linux, macOS, and Windows platforms are supported. Changing the platform selection affects the tactic count in the heat maps, the tactic and technique selection in the filters, and the MITRE ATT&CK Mappings edit page. For more information, see https://attack.mitre.org/matrices/enterprise/.

QRadar saves your preferences so they remain in effect each time you log in.

RELATED DOCUMENTATION

Upgrading QRadar Use Case Manager | 55

Uninstalling QRadar Use Case Manager | 56

Predefined Report Content Templates

IN THIS SECTION

Predefined content templates define the filters and columns of the rule reports, including column order and sorting options.

Rule Dependencies

Rules perform tests on events, flows, or offenses, and if all the conditions of a test are met, the rule generates a response. The tests in each rule can also reference other building blocks and rules; these relationships are called dependencies.

Name	Description
Default template - All rules	See a default view of your rules in QRadar; building blocks are not included in this view.
Reference sets per rule	For each rule that uses reference sets in a rule test, show the reference sets.
Reference sets per rule including test definition	For each rule that uses reference sets in a rule test, show the reference sets and the rule tests.
Number of reference sets per rule	See how many reference sets are referenced by each rule.
Rules per reference set	For each reference set that is used by a rule, show the rules that use it and the rule tests.
Rules per custom property	For each custom property used by a rule, show the rules that use it and the rule tests. Use this report to identify custom properties that have the same purpose but a different name. Or see whether your new log source can be expanded by the rules that use a custom property that is applicable for the new log source.
Log source coverage by rules - my log sources only	For each log source type, show which rules are related to it. Use this report to help you determine which log sources need more coverage.
Log source coverage by rules	For each log source type, show which rules are related to it.

(Continued)

Name	Description
Log source coverage by rules including tests	For each log source type, show which rules are related to it and which tests tie the rule to the log source type. Use this report to help you determine which devices need more coverage. The test definition explains why the rule is related to the specific log source type.
Log source types per rule	For each rule, see which log source types each rule works for. Use this report to help you determine what log coverage you need for a specific rule or whether rules are covering less than intended. You can add the log source type test definition to this report to see how the rule is related to a specific log source.
Log source types per custom property	For each custom property referenced by a rule, show the log source types that are related to the rule. Use this report to identify the log source types that need a custom property defined.

MITRE ATT&CK Coverage

Tactics represent the goal of an ATT&CK technique or sub-technique. For example, an adversary might want to get credential access to your network. Techniques represent how an adversary achieves their goal. For example, an adversary might dump credentials to get credential access to your network. Use the predefined templates to create or modify rules and building block mappings.

Name	Description
MITRE ATT&CK tactics and techniques mapped to rules	Shows all tactics and their techniques that are mapped to rules.
Rules mapped to MITRE ATT&CK tactics and techniques	Shows all rules that are mapped to at least one tactic and view its techniques.

Installed Content Extensions

See the list of all content extensions that are installed from the IBM Security App Exchange, and the list of rules for each of them.

Name	Description
Content extensions installed from IBM Security App Exchange	See the list of all content extensions that are installed from IBM Security App Exchange and the list of rules for each of them.

Recommended Non-installed Content Extensions

Content extensions update QRadar security information or add new content, such as rules, reports, searches, reference sets, and custom properties. Use the predefined templates to see how you can increase rule coverage for log sources or MITRE tactics and techniques in your environment by installing content extensions from the IBM Security App Exchange.

Name	Description
Recommended non-installed content based on my log sources	Explore how adding new non-installed content from the IBM Security App Exchange can expand coverage based on the number of rules per log source type in each content extension.
Recommended non-installed content based on MITRE coverage	Explore how adding new non-installed content from the IBM Security App Exchange can expand coverage for MITRE tactics and techniques.
Recommended unused log sources	Explore how adding new log sources can expand coverage for use cases.
All non-installed content	See the list of all non-installed content extensions and their rules. The list is displayed in an ungrouped table format.

User Behavior Analytics

User Behavior Analytics rules can help you identify potential insider threats inside your network.

Name	Description
All User Behavior Analytics rules	For all the installed and non-installed User Behavior Analytics rules, show the risk score.
Installed User Behavior Analytics rules	For installed User Behavior Analytics rules, show the risk score.
Non-installed User Behavior Analytics rules	For non-installed content extensions, show the User Behavior Analytics rules that are available when the extensions are installed.

Inactive Rules

Rules that don't trigger in a certain time period might be misconfigured, and you might not be getting the most value out of your IBM QRadar deployment. Review your inactive rules for possible tuning options.

Name	Description
Rules not active in the past week	See the list of rules that did not assign an event to an offense in the past week.
Rules not active since installation	See the list of rules that never assigned an event to an offense since the date they were installed in QRadar.

Customizing Report Content Templates

QRadar Use Case Manager includes several predefined content templates that define the filters and columns of the rule reports, including column order and sorting options. You can also create custom templates by using an existing template and modify it as necessary, or create new ones.

1. From the report menu bar, click the list icon and "pick a template" on page 47.
2. Select the relevant filters in the **Filters** pane and click **Apply Filters**.
3. To modify the column settings, click the gear icon.
   a. Search or scroll down the window to find the column that you want to add to the report.
   b. In the **Selected columns** section of the window, drag the columns in the order that you want them displayed in the report.
   c. Click **Apply**.
4. Click **Select a template >Add custom template**.
5. Type a **Name** and **Description** for the template.
6. Choose whether to set the template as your default. The default template is applied when you open the app.

   You can change the default template at any time.
7. Click **OK**.
8. To edit the custom template name and description, hover over the template name, click the pencil icon, and make your changes. Then click **OK**.
9. To delete a custom template from the list, hover over the template name and click the delete icon.

Custom report templates include the number of items per page in the rule report.

RELATED DOCUMENTATION

Rule Report Presentation | 88

Custom Rule Attributes

IN THIS SECTION

A custom rule attribute represents a specific piece of information that you can attach to a rule that doesn't fit into existing rule attributes. For example, the use case the rule belongs to, the team who is responsible for creating or maintaining the rule, or who reviewed the rule.

You can define any custom rule attribute and its values, assign the custom attribute values to a rule, and add the custom attribute as a report column on the Use Case Explorer page. Custom rule data appears only for installed rules. Then, you can search for the attribute to fine-tune the report, which is useful when the rule list is long.

Attribute Examples

Define another cyber adversary framework that is not supported by default by QRadar Use Case Manager, such as the Cyber Kill Chain. Then create attribute values for each of the seven steps in the Cyber Kill Chain. For more information, see https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks.

Create tags with arbitrary values, such as a year or status of the rule. For example, "2021", "In review", "Out-of-date", or "Deprecated".

Define security use cases, such as threat detection, cloud services, user behavior analysis, or network traffic analysis.

RELATED DOCUMENTATION

Investigating QRadar Rules and Building Blocks | 76

Creating Custom Rule Attributes | 53

Creating Custom Rule Attributes

Create, edit, or delete custom rule attributes and their values. Then, you can assign the custom attribute values to a rule and add the custom attribute as a report column on the Use Case Explorer page. An attribute can be any string, and can have one or more values on the rule.

1. From the QRadar Use Case Manager menu, click **Settings** > **Custom Rule Attributes**.
2. Click the plus sign icon in the **Custom rule attribute** section of the window, add a unique name for attribute, and click the checkmark icon to add it to the list.

   The name is used as a column header in the reports. Custom attribute data appears only for installed rules.
3. Click the plus sign icon in the **Custom rule attribute value** section of the window and enter a value for the attribute. Each custom attribute must include at least one value.

> **NOTE**: A value can be numerical, text, or special characters.

4. Click **Save and close** when you are finished.
5. To add custom rule attributes to the table report, modify the column settings by clicking the gear icon in the report menu bar.
   a. Search or scroll down the window to find the column that you want to add to the report.
   b. In the **Selected columns** section of the window, drag the columns in the order that you want them displayed in the report.
   c. Click **Apply**.

You can export rules with their custom attribute mappings from the report menu bar. For more information, see "Exporting rules" on page 86.

RELATED DOCUMENTATION

Custom Rule Attributes | 52

Exporting and Importing Custom Rule Attributes | 54

Investigating QRadar Rules and Building Blocks | 76

Exporting and Importing Custom Rule Attributes

Export or import custom rule attribute data, including rule mappings, in a JSON file. Sharing the data between colleagues or QRadar deployments helps to streamline your workflow by eliminating work effort.

1. To export custom rule attributes, follow these steps:
   a. Go to **Settings** > **Custom Rule Attributes**.
   b. To export the rule mappings for the custom rule attributes, select the checkbox. Otherwise, only the custom rule attributes are exported.
   c. Click **Export**.
   d. Save the file and then close the Custom rule attribute management window.
2. To import custom rule attributes, following these steps:
   a. Go to **Settings** > **Custom Rule Attributes**.
   b. Click **Import**.

c. In the Import custom rule attributes page, click **Select JSON file to import** and browse to where the exported JSON file is located.

d. Select the JSON file and click **Open** > **Import** > **Close**.

e. Close the Custom rule attribute management window.

You can export rules with their custom attribute mappings from the report menu bar. For more information, see "Exporting rules" on page 86.

RELATED DOCUMENTATION

Custom Rule Attributes | 52

Creating Custom Rule Attributes | 53

Investigating QRadar Rules and Building Blocks | 76

Upgrading QRadar Use Case Manager

You must have an IBM ID to access the IBM Security App Exchange. If you don't have an ID, you can create one by clicking **Create IBM ID** on the upper right of the IBM Security App Exchange login page.

To take advantage of new capabilities, defect fixes, and updated workflows, upgrade to new versions of the QRadar Use Case Manager app. Use either the Extensions Management tool in QRadar or the QRadar Assistant app to upgrade the app.

In QRadar Use Case Manager 2.3.0 or later, the Cyber Adversary Framework Mapping app is no longer required. QRadar Use Case Manager detects the presence of the Cyber Adversary Framework Mapping app and prompts you to uninstall the app on the configuration page. QRadar Use Case Manager gathers any existing mappings from the Cyber Adversary Framework Mapping app during installation. If you continue to use the Cyber Adversary Framework Mapping app to edit MITRE mappings, any new or updated mappings are not added to QRadar Use Case Manager and the data becomes out of sync. In that case, you must manually export and import the mappings into QRadar Use Case Manager.

1. If the QRadar Assistant app is configured on QRadar, use the following instructions to install the QRadar Use Case Manager app: QRadar Assistant app.
2. If the QRadar Assistant app is not configured, download the QRadar Use Case Manager app archive from the IBM Security App Exchange.

   a. On the **Admin** tab, click **Extension Management**.

   b. In the Extension Management page, click **Add** and select the app archive that you want to upload to the console.

c. Select the **Install immediately** checkbox.

> **NOTE**: You might have to wait several minutes before your app becomes active. When the installation is complete, clear your browser cache and refresh the browser window before you use the app.

3. On the page that prompts you to update the current app version, leave the **Replace existing items** option selected, and click **Install**.
4. After the installation is complete, go to **Admin** >**Apps** >**QRadar Use Case Manager** >**Configuration**.
5. On the **Configuration** page, click **Uninstall** to remove the Cyber Adversary Framework Mapping app from your environment.

   All of your previous MITRE-mappings are preserved.
6. After the Cyber Adversary Framework Mapping app is removed, export your MITRE mappings as a backup copy, in case you delete the QRadar Use Case Manager app later. If you uninstall QRadar Use Case Manager later, all of the mappings are deleted from your environment.

In deployments where QRadar User Behavior Analytics 4.1.0 or later and QRadar Use Case Manager 3.2.0 or later are both installed, the two apps automatically communicate with each other. The rules from QRadar User Behavior Analytics are integrated into the QRadar Use Case Manager app for further investigation and tuning.

RELATED DOCUMENTATION

Uninstalling QRadar Use Case Manager | 56

Uninstalling QRadar Use Case Manager

> **WARNING**: If you reinstall the QRadar Use Case Manager app later, old data is not retained. Export the MITRE mappings file in case you need to reinstall the app later.

Use the QRadar Extensions Management tool to uninstall the QRadar Use Case Manager app from your QRadar Console.

1. To export MITRE mappings before you uninstall the app, follow these steps:

   a. On the Apps page of the **Admin** tab, click **QRadar Use Case Manager** > **Configuration**.

   b. Click **Export MITRE mappings**. If you decide later to reinstall the app, you can then import this backup file later on the Use Case Explorer page. Only the custom mappings are imported from the file.

2. To uninstall the app, follow these steps:

   a. On the **Admin** tab, go to the System Configuration section and click **Extensions Management**.

   b. On the **INSTALLED** tab of the Extension Management page, select the QRadar Use Case Manager app and then click **Uninstall**.

RELATED DOCUMENTATION

Customizing User Preferences | **46**

Upgrading QRadar Use Case Manager | **55**

7

CHAPTER

MITRE ATT&CK Mapping and Visualization

MITRE ATT&CK Mapping and Visualization

The MITRE ATT&CK framework represents adversary tactics that are used in a security attack. It documents common tactics, techniques, and procedures that can be used in advanced persistent threats against enterprise networks.

The following phases of an attack are represented in the MITRE ATT&CK framework:

MITRE ATT&CK Tactic	Description
Reconnaissance	Gather information to use in future malicious operations. This tactic displays in the MITRE reports only when the PRE platform is selected in your user preferences.
Resource Development	Establish resources to support malicious operations. This tactic displays in the MITRE reports only when the PRE platform is selected in your user preferences.
Impact	Tries to manipulate, interrupt, or destroy systems and data.
Initial Access	Gain entry to your environment.
Execution	Run malicious code.
Persistence	Maintain foothold.
Privilege Escalation	Gain higher-level permissions.
Defense Evasion	Avoid detection.
Credential Access	Steal login and password information.
Discovery	Figure out your environment.

(Continued)

MITRE ATT&CK Tactic	Description
Lateral Movement	Move through your environment.
Collection	Gather data.
Exfiltration	Steal data.
Command and Control	Contact controlled systems.

Tactics, techniques, and sub-techniques

Tactics represent the goal of an ATT&CK technique or sub-technique. For example, an adversary might want to get credential access to your network.

Techniques represent how an adversary achieves their goal. For example, an adversary might dump credentials to get credential access to your network.

Sub-techniques provide a more specific description of the behavior an adversary uses to achieve their goal. For example, an adversary might dump credentials by accessing the Local Security Authority (LSA) Secrets.

Workflow for MITRE ATT&CK mapping and visualization

Create your own rule and building block mappings in QRadar Use Case Manager, or modify QRadar default mappings to map your custom rules and building blocks to specific tactics and techniques.

Save time and effort by editing multiple rules or building blocks at the same time, and by sharing rule-mapping files between QRadar instances. Export your MITRE mappings (custom and IBM default) as a backup of custom MITRE mappings in case you uninstall the app and then decide later to reinstall it. For more information, see "Uninstalling QRadar Use Case Manager" on page 56.

After you finish mapping your rules and building blocks, organize the rule report and then visualize the data through diagrams and heat maps. Current and potential MITRE coverage data is available in the following reports: **Detected in timeframe** report, **Coverage map and report**, and **Coverage summary and trend.**

- "Editing MITRE Mappings in a Rule or Building Block" on page 61

  Create your own rule and building block mappings or modify QRadar default mappings to map your custom rules and building blocks to specific tactics and techniques.

- "Editing MITRE Mappings in Multiple Rules or Building Blocks" on page 63

  Save time and effort by editing multiple rules or building blocks at the same time.

- "Sharing MITRE-mapping Files" on page 65

  Save time and effort when mapping rules and building blocks to tactics and techniques by sharing rule-mapping files between QRadar instances.

- "Visualizing MITRE Tactic and Technique Coverage in Your Environment" on page 66

  Visualize the coverage of MITRE ATT&CK tactics and techniques that the rules provide in QRadar. After you organize the rule report, you can visualize the data through diagrams and heat maps and export the data to share with others.

- "Visualizing MITRE Coverage Summary and Trends" on page 69

  The MITRE summary and trend reports provide an overview of the different tactics that are covered by QRadar Use Case Manager. You can analyze the summary data in table, bar, and radar charts. Only the number of enabled mappings to enabled rules are counted in the charts because disabled mappings don't contribute to your security posture.

- "Visualizing MITRE Tactics and Techniques that are Detected in a Specific Timeframe" on page 70

  Tune your rules by the MITRE ATT&CK tactics and techniques that are detected in your environment within a specific timeframe. QRadar Use Case Manager displays a list of the offenses and their related rules that were found within that timeframe.

- "MITRE Heat Map Calculations" on page 73

  The colors in the MITRE heat maps are calculated based on the number of rule mappings to a tactic or technique plus the level of mapping confidence (low, medium, or high).

RELATED DOCUMENTATION

Editing MITRE Mappings in a Rule or Building Block | 61

Editing MITRE Mappings in Multiple Rules or Building Blocks | 63

Editing MITRE Mappings in a Rule or Building Block

Create your own rule and building block mappings or modify IBM QRadar default mappings to map your custom rules and building blocks to specific tactics and techniques.

1. In the report section of the Use Case Explorer page, select the relevant rule.

   > **TIP**: Filter on the rule name, tactic, or technique to find the rule you want to edit or search by using a regular expression. You can also use the **Group** filter to select the group you want to search, such as authentication or compliance.

2. On the Investigate rules page, click the pencil icon in the **MITRE ATT&CK** section.
3. On the MITRE ATT&CK Mapping page, customize rule-mapping options by either adding new tactics or editing existing ones.

   > **TIP**: The MITRE ATT&CK Mapping page shows only the mappings that are directly related to a rule. You can see mappings that the rule inherited from its dependencies in the rule details section of the Investigate rules page or in the report on the Use Case Explorer page.

   a. To add or remove tactics with the rule or building block, click the plus sign icon, select the relevant tactics, and then click **Apply**.

   b. To add or remove techniques for a tactic, click the plus sign icon for the tactic, select the relevant techniques, and then click **Apply**.

   c. To add or remove sub-techniques for a technique, click the plus sign icon for the technique, select the relevant sub-techniques, and then click **Apply**.

   Sub-techniques are identified by a dot in the ID, such as "T1003.002 Security Account Manager".

   d. To include the tactic and technique in the heat map calculation, keep the **Enable** checkbox selected.

   e. Select the confidence level for each tactic and click **Save**. You must set a confidence level; otherwise, you can't save the mapping.

   f. To reset to the IBM default mappings, click the **Reset** icon in the **Tactics** or **Techniques** columns.
4. After you finish customizing your mappings, click **Save** or **Save and close** to return to the Use Case Explorer page.
5. To see the relationships between the rules and their mappings in the rule report, complete the following steps:

   a. Click the gear icon in the rule report menu bar and add the **Mapping source** column to the report.

   > **TIP**: Either search or scroll down the window to find the column.

b. Add the **Tactic** or the **Tactic (at rule level only)** column.

   The **Tactic** column shows all the tactics that are directly mapped to the rule, including the mappings to BBs and rules in the rule's dependencies list.

   The **Tactic (at rule level only)** column shows only the tactics that are mapped directly to the rule, excluding the mappings to BBs and rules in the rule's dependencies list.

c. Add the **Technique** or the **Technique (at rule level only)** column.

   The **Technique** column shows all the techniques that are directly mapped to the rule, including the mappings to BBs and rules in the rule's dependencies list.

   The **Technique (at rule level only)** column shows only the techniques that are mapped directly to the rule, excluding the mappings to BBs and rules in the rule's dependencies list.

d. Add the **Sub-Technique** or the **Sub-technique (at rule level only)** column.

   The **Sub-Technique** column shows all the sub-techniques that are directly mapped to the rule, including the mappings to BBs and rules in the rule's dependencies list.

   The **Sub-technique (at rule level only)** column shows all the sub-techniques that are mapped directly to the rule, excluding the mappings to BBs and rules in the rule's dependencies list.

e. In the **Selected columns** section of the window, drag the columns in the order that you want them displayed in the report and click **Apply**.

If you create content extensions for the IBM Security App Exchange, and you want to map rules in them, export the mappings and upload them when you submit your content.

To edit multiple rules or building blocks at one time, see "Editing MITRE Mappings in Multiple Rules or Building Blocks" on page 63.

RELATED DOCUMENTATION

Editing MITRE Mappings in Multiple Rules or Building Blocks | 63

Editing MITRE Mappings in Multiple Rules or Building Blocks

Save time and effort by editing multiple rules or building blocks at the same time. Export your mappings to a JSON file to share with other colleagues.

1. On the Use Case Explorer page, click the **Toggle table view** icon to ungroup the report's table columns.

   > **TIP**: Filter on the rule name, tactic, or technique to find the rule you want to edit or search by using a regular expression. You can also use the **Group** filter to select the group you want to search, such as authentication or compliance.

2. Click the pencil icon in the report table to display checkboxes for each table row.
3. Select the relevant rules or building blocks that you want to edit, and then click **Edit MITRE mappings**.
4. On the MITRE ATT&CK Mapping page, customize rule-mapping options by either adding new tactics or editing existing ones.

   > **TIP**: The MITRE ATT&CK Mapping page shows only the mappings that are directly related to a rule. You can see mappings that the rule inherited from its dependencies in the rule details section of the Investigate rules page or in the Use Case Explorer report. Use the **Mapping source** column in the report, or in the MITRE ATT&CK section of the rule details page, to see the relationships between the rules and their mappings. Or, if you create content extensions for the IBM Security App Exchange, and you want to map rules in them, export the mappings and upload them when you submit your content.

   a. To add or remove tactics with the rule or building block, click the plus sign icon, select the relevant tactics, and then click **Apply**.

   b. To add or remove techniques for a tactic, click the plus sign icon for the tactic, select the relevant techniques, and then click **Apply**.

   c. To add or remove sub-techniques for a technique, click the plus sign icon for the technique, select the relevant sub-techniques, and then click **Apply**.

      Sub-techniques are identified by a dot in the ID, such as "T1003.002 Security Account Manager".

   d. Select the confidence level for each tactic and click **Save**. You must set a confidence level; otherwise, you can't save the mapping.

   e. To include the rule in the heat map calculation, keep the **Enable** checkboxes selected for the tactic and technique.

   f. To reset tactics or techniques that were customized in IBM default mappings, click the **Reset** in the **Tactics** column.

5. To export a JSON file of the mappings in the MITRE ATT&CK Mapping page to share with others, click **Save** >**Export mappings**.

6. After you finish your mappings, click **Save and close**.
7. To refresh the report to see updated content, click **Apply** in the **Filters** pane.

RELATED DOCUMENTATION

Editing MITRE Mappings in a Rule or Building Block | **61**

Sharing MITRE-mapping Files | **65**

Sharing MITRE-mapping Files

Save time and effort when mapping rules and building blocks to tactics and techniques by sharing rule-mapping files between QRadar instances.

The export capability provides MITRE mappings directly to rules only, not their dependencies. If you use the default MITRE-related templates on the Use Case Explorer page, you can see the direct mappings to the rules and their dependencies. You can also customize the template to see only the direct mappings if necessary. For more information, see "Customizing Report Content Templates" on page 51.

Use the **Export** option to create backups of the mappings in your environment. You can also use the **Export** and the **Import** options to move rules from one deployment to another, rather than manually copying the rules.

1. To export MITRE mappings use the following steps:
   a. On the Use Case Explorer page, click **ATT&CK Actions >Export**.
   b. Select which MITRE mappings you want to export: **All** or **Export mappings to rules or building blocks in current view**.
   c. Select one of the following export formats:
      - Export to a JSON file that can be imported in QRadar Use Case Manager. Use this option to create a backup of your mappings, or to move the mappings and their corresponding rules to another QRadar deployment.
      - Export information about MITRE coverage to a JSON file that can be imported as a layer into the MITRE ATT&CK Navigator.
   d. Click **Export**.
2. To exportmappings from the MITRE ATT&CK Mapping page, see step 5 in "Editing MITRE Mappings in Multiple Rules or Building Blocks" on page 63.

3. To import a rule mappings file, use the following steps:
    a. On the Use Case Explorer page, click **ATT&CK Actions** >**Import**.
    b. Click the import icon, browse to the file location on your system and select the file, and then click **Import**.

RELATED DOCUMENTATION

Editing MITRE Mappings in a Rule or Building Block | 61

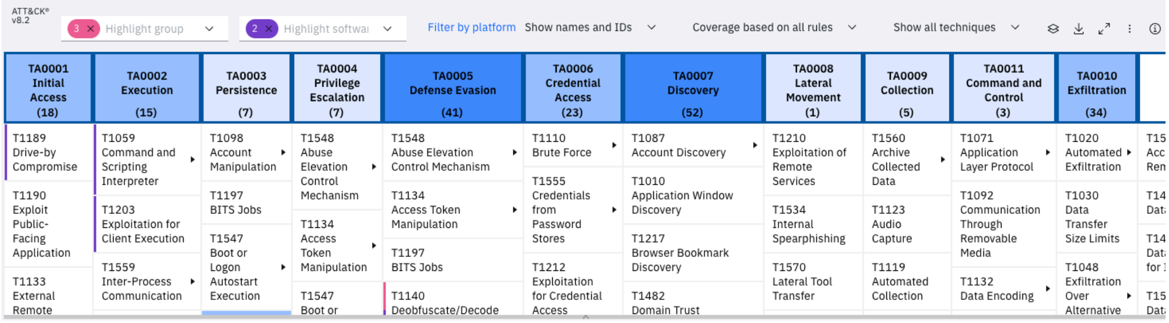
Editing MITRE Mappings in Multiple Rules or Building Blocks | 63

Visualizing MITRE Tactic and Technique Coverage in Your Environment

If you want to filter by MITRE ATT&CK tactics, you must first map your rules to MITRE tactics and techniques. For more information, see "Editing MITRE Mappings in a Rule or Building Block" on page 61.

Visualize the coverage of MITRE ATT&CK tactics and techniques that the rules provide in IBM QRadar. After you organize the rule report, you can visualize the data through diagrams and heat maps and export the data to share with others.

1. Click **ATT&CK Actions** > **Coverage map and report** in the upper right of the visualization pane.



TA0001 Initial Access (18)	TA0002 Execution (15)	TA0003 Persistence (7)	TA0004 Privilege Escalation (7)	TA0005 Defense Evasion (41)	TA0006 Credential Access (23)	TA0007 Discovery (52)	TA0008 Lateral Movement (1)	TA0009 Collection (5)	TA0011 Command and Control (3)	TA0010 Exfiltration (34)	
T1189 Drive-by Compromise	T1059 Command and Scripting Interpreter	T1098 Account Manipulation	T1548 Abuse Elevation Control Mechanism	T1548 Abuse Elevation Control Mechanism	T1110 Brute Force	T1087 Account Discovery	T1210 Exploitation of Remote Services	T1560 Archive Collected Data	T1071 Application Layer Protocol	T1020 Automated Exfiltration	T15 Acc Ren
T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1197 BITS Jobs	T1134 Access Token Manipulation	T1134 Access Token Manipulation	T1555 Credentials from Password Stores	T1010 Application Window Discovery	T1534 Internal Spearphishing	T1123 Audio Capture	T1092 Communication Through Removable Media	T1030 Data Transfer Size Limits	T14 Dat
T1133 External Remote	T1559 Inter-Process Communication	T1547 Boot or Logon Autostart Execution	T1547 Boot or	T1197 BITS Jobs	T1212 Exploitation for Credential Access	T1217 Browser Bookmark Discovery	T1570 Lateral Tool Transfer	T1119 Automated Collection	T1132 Data Encoding	T1048 Exfiltration Over Alternative	T14 Dat for I
				T1140 Deobfuscate/Decode		T1482 Domain Trust					T15 Dat

2. Select from the filters in the **MITRE ATT&CK** section. The following options are available to filter:

    Tactics

    Select tactics from the list. For example, an Initial Access tactic is used by adversaries who are trying to get into your network.

    Technique

Search for techniques and their sub-techniques or select them from the list. The techniques are pre-filtered to match the selected tactic. For example, an Account Discovery technique occurs when adversaries attempt to get a list of your local system or domain accounts.

Sub-techniques are identified by a dot in the ID, such as "T1003.002 Security Account Manager". Sub-techniques provide a more specific description of the behavior an adversary uses to achieve their goal. For example, an adversary might dump credentials by accessing the Local Security Authority (LSA) Secrets.

Mapping confidence

Indicates mappings that are assigned a specific level of confidence for rule coverage.

Mapping enabled

Indicates for each rule whether the mapping between the tactic or technique and rules is turned on. Mappings that are not enabled are not added to the technique coverage heat map.

3. To update the rule report with your filters, click **Apply Filters**.
4. Scroll through the heat map visualization to see the different techniques that are covered by QRadar Use Case Manager. The number in the chart header indicates the number of rules that are mapped per tactic. (This number might be larger than the sum of the number of mappings of its techniques because the mappings are done directly to the tactic, not to the technique.)

   Hover over the number in each technique cell to see the number of rules that are mapped to the technique, and then click the number in the cell to see the heat map calculation for the technique. For more information, see "MITRE Heat Map Calculations" on page 73.
5. Click the arrow in the cell to expand the columns to display the sub-techniques for the technique. Hover over the sub-technique cell to see the number of rules that are mapped to the sub-technique, and then click the number to see the heat map calculation for that sub-technique. For more information, see "MITRE Heat Map Calculations" on page 73.
6. To change the labeling in the chart, click the **Show** option in the report menu bar and select from names, technique IDs, or technique names and IDs. By default, the technique names are displayed.
7. To see only the mappings for rules that are currently in the coverage map and report, select the **Coverage based on rules in report** option in the report menu bar. Click any section in the heat map and then click **Apply Filters** to update the filtered list in the table report.
8. To see which MITRE techniques are being used by adversary groups and software, select the appropriate filters from the **Highlight groups** and **Highlight software** lists. Relevant groups are highlighted in the heat map by pink sidebars, and relevant software are highlighted by purple sidebars.
9. To see only the techniques that are selected in the filter, hold the control key (on Windows) or the command key (on Mac) of your keyboard and select the relevant techniques on the heat map. Then select the **Show techniques in filter** option in the report menu bar. All other filters are hidden in the heat map.

> **TIP**: If you don't see any technique filters in the heat map, add techniques in the **MITRE ATT&CK** section of the filter pane or select techniques in the map.

10. To see only the sub-techniques for each tactic and technique, click the stack icon in the report menu bar.
11. To change the platforms that are filtered in the heat map, click **Filter by platform** and change the selection in your user preferences.

    By default, the heat map shows tactics, techniques, and sub-techniques from three platforms: Linux, macOS, and Windows.

    The **Selected platforms** filter tag in the filter bar is not selectable, but represents the selected MITRE ATT&CK platforms, and is added whenever the report includes ATT&CK-related filters or columns. To change the selected platforms, modify your user preferences. For more information, see "Customizing user preferences" on page 46.
12. To work with tactics, techniques and sub-techniques from other platforms, click **Filter by platform** and change the selection in your user preferences. Changing the platform also affects the contents of MITRE filters on the Use Case Explorer page and **MITRE ATT&CK Mappings** edit page.
13. To export the current display of the chart as a PNG image, click the export icon. Then, you can share the image with colleagues or executives who don't have access to QRadar Use Case Manager.
14. To expand the visualization pane to the width of your screen, click the maximize icon on the menu bar of the pane. Zoom in or out to see the visualization at the size you want. Any filtering that you apply in the expanded pane is kept when you return to the Use Case Explorer.

    > **NOTE**: The zoom capability is not supported on Mozilla Firefox. Use the browser control to zoom in and out.
15. Close the report visualization to return to the dashboard.

RELATED DOCUMENTATION

Visualizing Log Source Type Coverage per Rule | 91

Visualizing Rules and Building Blocks | 91

Visualizing MITRE Tactics and Techniques that are Detected in a Specific Timeframe | 70

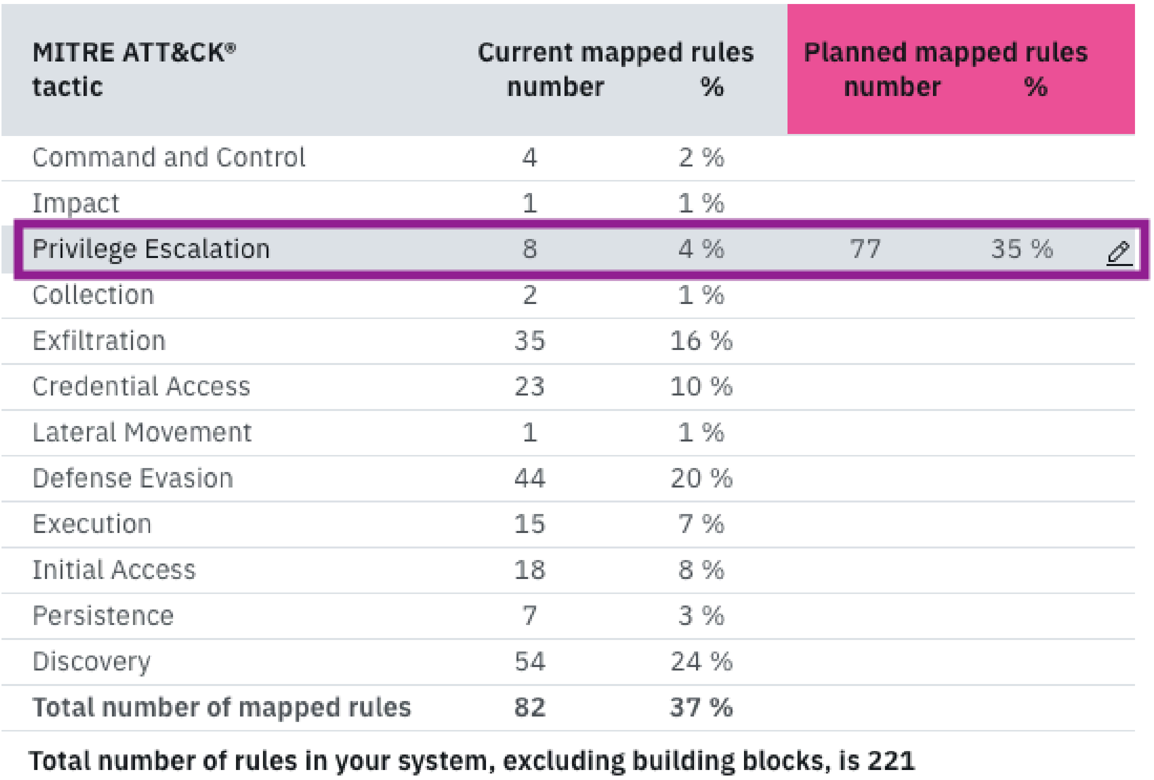
Visualizing MITRE Coverage Summary and Trends

The MITRE summary and trend reports provide an overview of the different tactics that are covered by QRadar Use Case Manager. You can analyze the summary data in table, bar, and radar charts. Only the number of enabled mappings to enabled rules are counted in the charts because disabled mappings don't contribute to your security posture.

If you want to filter by MITRE ATT&CK tactics, you must first map your rules to MITRE tactics and techniques. For more information, see "Editing MITRE Mappings in a Rule or Building Block" on page 61.

1. Click **ATT&CK Actions** > **Coverage summary and trend** in the upper right of the visualization pane.
2. Edit the **MITRE Coverage Summary** table chart to change the planned number and percentage to see where you're lacking in coverage.

   For example, the current number of rules for the Privilege Escalation tactic is 8 and represents 4% coverage, but you want 35% coverage. When you edit the planned percentage, you see that you need 77 rules to provide the level of coverage you want.



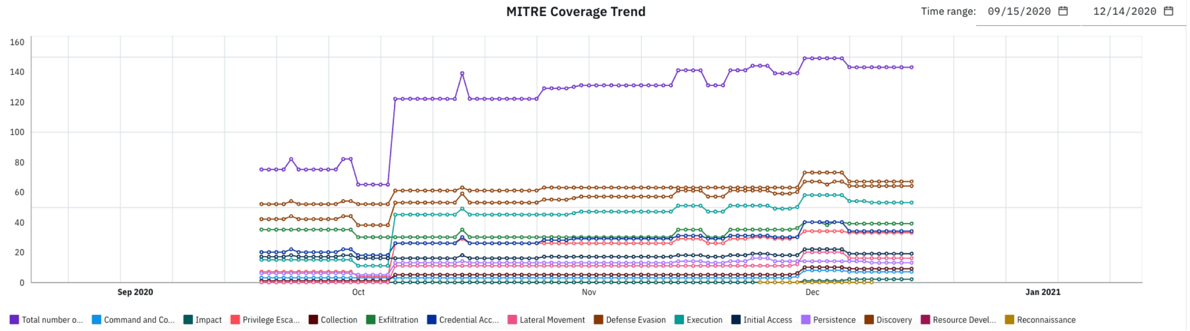
MITRE ATT&CK® tactic	Current mapped rules		Planned mapped rules	
	number	%	number	%
Command and Control	4	2 %		
Impact	1	1 %		
Privilege Escalation	8	4 %	77	35 % ✎
Collection	2	1 %		
Exfiltration	35	16 %		
Credential Access	23	10 %		
Lateral Movement	1	1 %		
Defense Evasion	44	20 %		
Execution	15	7 %		
Initial Access	18	8 %		
Persistence	7	3 %		
Discovery	54	24 %		
Total number of mapped rules	**82**	**37 %**		

Total number of rules in your system, excluding building blocks, is 221

   a. After you add the rule mappings you need to improve your coverage, check the coverage report again to see whether your coverage improved.

   b. Change the date for the chart coverage by clicking the calendar icon for **On date**. You can change the date as far back as three months before the current date, which is the default.

3. In the **MITRE Coverage Trend** chart, click a tactic in the legend to fine-tune the view or view the total coverage trend over time. The default time range is three months. Hover over the vertical line of each day to see the total coverage for each tactic.



4. To update the charts with live data from QRadar, click the refresh icon. Data is automatically refreshed every 24 hours at night.
5. To export the summary or trend report, or the entire page, as a PNG image, click the export icon in each relevant section of the page. Then, you can share the images with colleagues or executives who don't have access to QRadar Use Case Manager.
6. Close the report visualization to return to the dashboard.

Visualizing MITRE Tactics and Techniques that are Detected in a Specific Timeframe

If you want to filter by MITRE ATT&CK tactics, you must first map your rules to MITRE tactics and techniques. For more information, see "Editing MITRE Mappings in a Rule or Building Block" on page 61.

See which MITRE ATT&CK tactics and techniques were detected in your environment based on the offenses that were updated within a specific timeframe. QRadar Use Case Manager displays a list of the offenses and their related rules that were found within that timeframe, along with the tactics and techniques that are mapped to those rules.

The more filters that you apply to the rules, the more fine-tuned the list of results you get. QRadar Use Case Manager uses the OR condition within the options of one filter group, and uses the AND condition across multiple groups of filters. Any column that you can filter on can also be added to the rule report through the column selection feature (gear icon).

1. On the Use Case Explorer page, click **ATT&CK Actions >Detected in timeframe**.
2. Select a content template.

   If you don't select a template, the default template (**ATT&CK tactics and techniques detected in offenses in the last 24 hours**) is used.

3. If you want to change the timeframe, in the **Offenses** filter, select a timeframe or a specific interval to filter the offenses.
4. Select parameters to exclude offenses from the results, such as hidden or closed offenses. Offenses that are marked for follow-up are flagged for further investigation. You might have offenses that you want to retain regardless of the retention period; those offenses are protected to prevent them from being removed from QRadar after the retention period elapses. Inactive offenses are removed from visualization so that reports aren't cluttered.

   Filter out the offenses that are closed. For example, you can exclude the rules that generated offenses that were closed as false positives. Rules with many false positives likely need tuning. Offenses that are closed as a non-issue are usually considered not critical to your organization. You might not want to include these offenses when you review the detected MITRE tactics and techniques.
5. Select from the filters in the **MITRE ATT&CK** section. The following options are available to filter:

   Tactics - Select tactics from the list. For example, an Initial Access tactic is used by adversaries who are trying to get into your network.

   Technique - Search for techniques and their sub-techniques or select them from the list. The techniques are pre-filtered to match the selected tactic. For example, an Account Discovery technique occurs when adversaries attempt to get a list of your local system or domain accounts.

   Sub-techniques are identified by a dot in the ID, such as "T1003.002 Security Account Manager". Sub-techniques provide a more specific description of the behavior an adversary uses to achieve their goal. For example, an adversary might dump credentials by accessing the Local Security Authority (LSA) Secrets.

   Mapping confidence - Indicates mappings that are assigned a specific level of confidence for rule coverage.

   Mapping enabled - Indicates for each rule whether the mapping between the tactic or technique and rules is turned on. Mappings that are not enabled are not added to the technique coverage heat map.
6. To update the rule report with your filters, click **Apply Filters**.

   QRadar Use Case Manager displays a list of the offenses and their related rules that were found within that timeframe. If you click an offense to further investigate it, and the QRadar Analyst Workflow is installed on the QRadar Console, the offense opens in the workflow view. For more information, see QRadar Analyst Workflow.
7. To change the labeling in the chart, click the **Show** option in the report menu bar and select from names, technique IDs, or technique names and IDs. By default, the technique names are displayed.
8. Scroll through the heat map visualization to see the different techniques that are affected by those rules. The number in the chart header indicates the number of rules that are mapped per tactic. (This number might be larger than the sum of the number of mappings of its techniques because the mappings are done directly to the tactic, not to the technique.)

9. To see the sub-techniques for a MITRE technique, click the expand icon to extend the column. Sub-techniques provide a more specific description of the behavior an adversary uses to achieve their goal. For example, an adversary might dump credentials by accessing the Local Security Authority (LSA) Secrets.
10. To see only the sub-techniques for each tactic and technique, click the stack icon in the report menu bar.
11. To see which MITRE techniques are being used by adversary groups and software, select the appropriate filters from the **Highlight groups** and **Highlight software** lists. Relevant groups are highlighted in the heat map by pink sidebars, and relevant software are highlighted by purple sidebars.
12. To see only the techniques that are selected in the filter, hold the control key (on Windows) or the command key (on Mac) of your keyboard and select the relevant techniques on the heat map. Then select the **Show techniques in filter** option in the report menu bar. All other filters are hidden in the heat map.

   TIP: If you don't see any technique filters in the heat map, add techniques in the **MITRE ATT&CK** section of the filter pane or select techniques in the map.

13. To change the platforms that are filtered in the heat map, click **Filter by platform** and change the selection in your user preferences.

    By default, the heat map shows tactics, techniques, and sub-techniques from three platforms: Linux, macOS, and Windows.
14. To work with tactics, techniques and sub-techniques from other platforms, click **Filter by platform** and change the selection in your user preferences. Changing the platform also affects the contents of MITRE filters on the Use Case Explorer page and **MITRE ATT&CK Mappings** edit page.
15. To export the current display of the chart as a PNG image, click the export icon. Then, you can share the image with colleagues or executives who don't have access to QRadar Use Case Manager.
16. To expand the visualization pane to the width of your screen, click the maximize icon on the menu bar of the pane. Zoom in or out to see the visualization at the size you want. Any filtering that you apply in the expanded pane is kept when you return to the Use Case Explorer page.

    NOTE: The zoom capability is not supported on Mozilla Firefox. Use the browser control to zoom in and out.

RELATED DOCUMENTATION

Visualizing Log Source Type Coverage per Rule | **91**

Visualizing Rules and Building Blocks | 91
Visualizing MITRE Tactic and Technique Coverage in Your Environment | 66

MITRE Heat Map Calculations

The colors in the MITRE heat maps are calculated based on the number of rule mappings to a tactic or technique plus the level of mapping confidence (low, medium, or high).

The more rules that map to the technique, the darker the hue of color. Only enabled rules are included in the calculation; disabled rules do not contribute to the colors in the heat map. For each technique, all mappings to its sub-techniques are counted as if they are mappings to that technique.

After QRadar Use Case Manager calculates the numbers for all the techniques and tactics, the maximum number that is associated with a technique and the maximum number that is associated with a tactic are determined:

- All techniques or tactics whose number is ≥ 66% of the maximum technique number are mapped to the darkest color.
- All techniques or tactics whose number is ≥ 33% and < 66% of the maximum technique number are mapped to the mid-range color.
- All techniques or tactics whose number is > 0 and < 33% of the maximum technique number are mapped to the lightest color.

Each cell in the heat map has a number that indicates the number of rules that are mapped to the technique or the sub-technique. Each number has a tooltip that explains how the calculation was determined. For example, four enabled rules are mapped to the selected technique. Based on the number of mappings and the confidence level, the technique score is 16, and it is assigned a medium color hue. The biggest technique score in the environment is 40.

In the red heat map (**Detected in timeframe** report), the mappings that are counted in the calculation are enabled mappings to enabled rules that are related to offenses in the report.

Building blocks do not directly contribute to the colors either; they contribute to the coloring only through the rules that reference them. For example, if the report lists building blocks only and the **Coverage based on rules in report** option is selected in the coverage heat map, the map doesn't show any coloring because there are no rules in the report.

RELATED DOCUMENTATION

Visualizing Rules and Building Blocks | **91**

Visualizing Log Source Type Coverage per Rule | **91**

Visualizing MITRE Tactic and Technique Coverage in Your Environment | **66**

Visualizing MITRE Tactics and Techniques that are Detected in a Specific Timeframe | **70**

8

CHAPTER

Investigating QRadar Rules and Building Blocks

Investigating QRadar Rules and Building Blocks

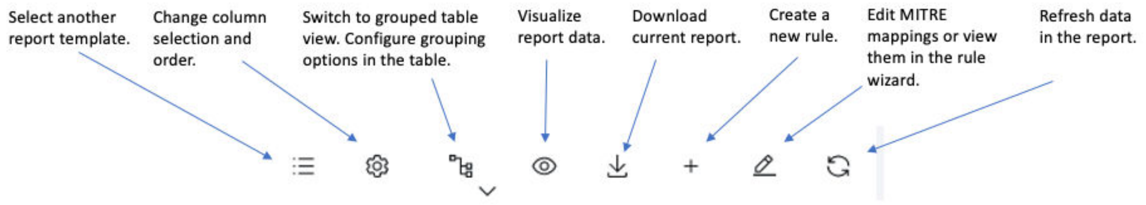
Ensure you have the proper user permissions to view and maintain QRadar rules. For more information, see "Assigning User Permissions for QRadar Use Case Manager" on page 44.

Investigate your rules by filtering different properties to ensure that the rules are defined and working as intended, including log source coverage. Determine which rules you might need to edit in QRadar or investigate further in QRadar Use Case Manager.

Follow the suggested workflow for investigating your rules.

1. Go to the Use Case Explorer page, click the list icon, and "pick a template to use" on page 47.
2. Filter rules and building blocks by attributes, tests, content extension attributes, activity, tests, and MITRE ATT&CK tactics and techniques.
3. To find the rule you want to edit or search, filter on the rule name, tactic, or technique by using a regular expression. You can also use the **Group** filter to select the group you want to search, such as authentication or compliance.
4. To create new rules, click the plus sign icon and complete the rule wizard.

   It might take several minutes for the new rule to appear in the report. To see the new rule immediately, click the **Refresh** icon in the report menu bar.
5. Customize the report presentation to make it easier to investigate the rules and building blocks.


Select another report template.
Change column selection and order.
Switch to grouped table view. Configure grouping options in the table.
Visualize report data.
Download current report.
Create a new rule.
Edit MITRE mappings or view them in the rule wizard.
Refresh data in the report.

6. To investigate an individual rule or building block, make sure that the report table is ungrouped, and then select the rule name to open the rule wizard.
7. To investigate multiple rules or building blocks simultaneously, click the pencil icon in the report table to display checkboxes for each table row. Select the relevant rules or building blocks that you want to edit, and then click **Open in rule wizard**.

   > **NOTE**: On QRadar 7.4.1 Fix Pack 2 or later, you can change the date range for the trend of the selected rule in the **Offense creation by current rule in a certain time** chart. The date range defaults back to the filtered date range (1 month) when you close and reopen the rule. On QRadar 7.3.3, the default date range is 3 days and cannot be edited.

8. To enable or disable rules, make sure that the **Rule enabled** column is visible in the report, and then switch the toggle to **On** or **Off**.

NOTE: You cannot disable an enabled rule if it has dependents. You cannot enable a rule if it has any disabled or noninstalled dependencies. A list of dependents or dependencies is available for review in the warning messages.

9. Edit MITRE mappings for rules or building blocks. For more information, see "Editing MITRE Mappings in a Rule or Building Block" on page 61.
10. To add custom rule attributes to the selected rule or building block, follow these steps:

    a. Click **Open in rule wizard** on the report menu bar.

    b. In the center pane of the screen, expand the **Custom attributes** section.

    c. If no custom attributes are currently added to the rule, click the plus sign icon and select the checkbox for each relevant attribute and value. Then, click **Save and apply**.

    TIP: You can also define new custom attributes in this window.

    d. If you want to add more values to the custom attributes already added to the rule, click the plus sign icon for the attribute and select values from the list.

    TIP: You can also define new custom attribute values in this window.

    e. Close the wizard.

    TIP: To fully manage custom rule attributes and their values, such as editing or deleting, go to **Settings** > **Custom Rule Attributes**.

11. To investigate QRadar User Behavior Analytics rules, see "Investigating user behavior analytics rules" on page 84.
12. Visualize your rules and building blocks after you organize the report data.
13. Export the report as a CSV or XML file to share with others.
14. Export the MITRE mappings as a JSON file to share with others.

RELATED DOCUMENTATION

Filtering Rules and Building Blocks by their Properties | **78**

Filtering Rules and Building Blocks by their Properties

If you want to filter by MITRE ATT&CK tactics, you must first map your rules to MITRE tactics and techniques. For more information, see "Editing MITRE Mappings in a Rule or Building Block" on page 61.

Tune your rules or building blocks by filtering their attributes, such as type, origin, group, and many more. You can also tune rules or building blocks by filtering them based on their test definitions. For example, you can add a test that matches only events from a specific log source. Examine and improve your MITRE ATT&CK coverage by filtering your rules based on their mappings to tactics and techniques.

The more filters that you apply to the rules, the more fine-tuned the list of results you get. QRadar Use Case Manager uses the OR condition within the options of one filter group, and uses the AND condition across multiple groups of filters. The only exception to the rule is in the **Other tests** filter group, where the AND condition is used for multiple options of that filter group. Any column that you can filter on can also be added to the rule report through the column selection feature (gear icon).

As you select filters, the unapplied filter tags appear in the filters row with a lighter colored background. After you apply the filters, the tags change to a darker color background.

1. On the Use Case Explorer page, select from the filters in the **Rule attributes** section. The following list describes some of the rule attributes you can filter and how to use them:

   Rule name

   Enter a specific rule name or search for it by using regular expressions.

   Rule enabled

   Enable or disable the appropriate rules to ensure that your system generates meaningful offenses for your environment.

   Rule category

   Filter by custom or anomaly detection rules in the report. Custom rules perform tests on events, flows, and offenses to detect unusual activity in your network. Anomaly detection rules perform tests on the results of saved flow or event searches as a means to detect when unusual traffic patterns occur in your network.

   Group

   Categorize the rules or building blocks into groups to help you efficiently view and track your rules. For example, you can view all rules that are related to compliance. Select specific groups or click **Select all**.

   Action

Select the action that you want the rule to take when an event occurs.

Response

Select the response that you want QRadar to take when a rule is triggered.

Creation and modification dates

Use the date filters to see what changed during the last week, or to see rules that were modified. The modification date shows the rules that were modified but not the modified content of the rules.

> **NOTE**: Enter a specific note or search for it by using regular expressions. For example, you can enter ^$ to find rules with empty notes and then add information to the note.

User Behavior Analytics rules

Filter rules on whether they are related to QRadar User Behavior Analytics. This filter displays only when the QRadar User Behavior Analytics app is installed in your QRadar deployment.

> **TIP**: For a rule to be considered related to QRadar User Behavior Analytics, the following conditions must be met:
>
> - The **Dispatch New Event** option must be selected in the **Rule Response**.
> - The **User Behavior Analytics risk score** must be set on the Rule Details page in QRadar Use Case Manager.

For more information, see Integrating new or existing QRadar content.

2. Select from the filters in the **Rule activity** section. Filtering for inactive rules is supported on QRadar 7.4.1 or later.

   Rule active

   Select **Never** to see which rules have never assigned an event to an offense since they were installed in QRadar.

   Rule not active (timeframe)

   The default date is in the past week. Change the time period, or choose to filter rules that aren't active since a specific date.

3. Select from the filters in the **Rule tests** section. The following list describes some of the rule tests you can filter:

   Test definition

   Enter a specific test definition or search for it by using regular expressions.

Log source type

A rule relates to log source types if it directly references the log source type, or if it references a log source, QID, or event category that maps to the log source type. By default, you see only the log source types that are used by log sources in your QRadar environment. Click **Show all types** to see the log source types that you can use directly in a test or by the QID or event categories.

Log Sources

A rule relates to log sources when the log source that is referenced by a test is used in the rule. Use the search filter to find specific log sources to filter or click **Select all** to filter all of the log sources in the list. You can filter on the log source name or by using a regular expression. This type of search is useful when you have hundreds of thousands of log sources in your environment.

Log Source Group

A rule relates to log source groups when a log source in the log source group that is referenced by a test is used in the rule. For example, you can select sensor device as the log source group and see only rules that run tests on log sources that are part of the sensor device log source group.

Domains

A rule can work in the context of a single domain or in the context of all domains. If there is more than one domain in your environment, they are added to the filter list. Use this option to filter the domains in a multi-domain environment by each individual domain.

To add a domain column to the rule report, click the gear icon. Scroll down to the **Rule tests** section of the window, select **Domain** in the **Test** option list, and then click **Apply**.

Other tests

Hover over each checkbox label to see the specific rule tests. For example, search for a rule that references a specific value of a test, such as an IP like "Identity IP is not 0."

TIP:

- To identify source IP addresses only, add a column for Test: IP, and then a **source** filter in the **Test definition** field.
- If you have multi-tenancy, use the Domain test to distinguish rules from one tenant to another. Select the Domain filter, and then add the Domain column.
- If you're looking for custom properties or reference sets, use the predefined templates.

- If you want to see the log source types that are used or unused, select the appropriate filter. For example, the **Log source coverage by rule** template shows the rules that are related to log source types based on tests. Assume that 342 log source types are available in your environment. To see only the rules for log source types that are currently used (log source types that have at least one log source), select the **Log source type - used** filter.

4. Select from the filters in the **MITRE ATT&CK** section. The following options are available to filter:

   Tactics

   Select tactics from the list. For example, an Initial Access tactic is used by adversaries who are trying to get into your network.

   Technique

   Search for techniques and their sub-techniques or select them from the list. The techniques are pre-filtered to match the selected tactic. For example, an Account Discovery technique occurs when adversaries attempt to get a list of your local system or domain accounts.

   Sub-techniques are identified by a dot in the ID, such as "T1003.002 Security Account Manager". Sub-techniques provide a more specific description of the behavior an adversary uses to achieve their goal. For example, an adversary might dump credentials by accessing the Local Security Authority (LSA) Secrets.

   Mapping confidence

   Indicates mappings that are assigned a specific level of confidence for rule coverage.

   Mapping enabled

   Indicates for each rule whether the mapping between the tactic or technique and rules is turned on. Mappings that are not enabled are not added to the technique coverage heat map.
5. If you have many log sources in your environment, you can search for specific ones by using the **Search** field in the **Filters** pane and then select them to fine-tune the report. This search can make it easier to find a specific filter in the large list of filters and log sources.
6. To filter content extension attributes, follow the steps in "Identifying Gaps in QRadar Rule Coverage from Content Extensions" on page 82.
7. To clear the report results, click **Clear filters**, choose new filters in the left pane, and then click **Apply filters** to display new results.

RELATED DOCUMENTATION

Identifying Gaps in QRadar Rule Coverage from Content Extensions | **82**

Identifying Gaps in QRadar Rule Coverage from Content Extensions

Content extensions update IBM QRadar security information or add new content such as rules, reports, searches, reference sets, and custom properties. Filter the rule report by content extensions to see how you can increase rule coverage for log sources or MITRE tactics and techniques in your environment by installing content extensions from the IBM Security App Exchange.

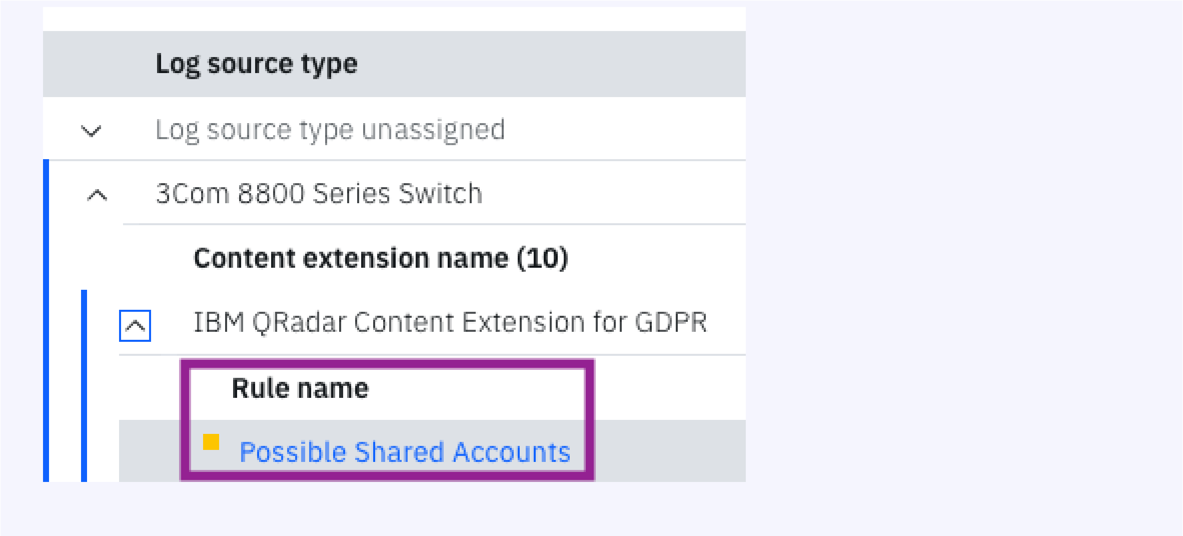
QRadar Use Case Manager automatically syncs with QRadar each day at midnight. If you install a content extension from the IBM Security App Exchange, you might not see updated rule coverage for up to 24 hours later. To immediately sync the rule coverage with QRadar, go to the configuration page and clear the cache for the app.

TIP: You can use predefined templates to see recommended content extensions to install or currently installed extensions, or manually filter your report results by content extension attributes. Predefined templates are available through the template icon on the menu bar of the rule report. Select the template you'd like to use from the categories in the template filter list.

1. On the Use Case Explorer page, go to the filters in the **Content extension attributes** section. By default, QRadar Use Case Manager filters on the installed content extensions in your environment.
   a. To include any IBM-created content extensions that are not installed in your environment in your search, select the **Include non-installed content extensions** checkbox.

   b. To filter only the content extensions that are not installed in your environment, select **Include non-installed content extensions** and then select **Include only non-installed content extensions**.
2. Filter by specific content extension name from a list of currently installed extensions or the ones that aren't yet installed in your environment.
3. Filter by specific content extension categories from the IBM Security App Exchange.
4. Add the following columns to the rule report as needed: **Content extension: Content extension name, Content extension: Content category**, and **Rule attributes: Rule installed**. If you don't immediately see the columns in the report, ungroup the table rows.

   TIP: Any content extensions in the report that aren't installed in your environment are indicated in the **Rule name** column by a **Missing content** icon. Hover over each icon to see which content extension can provide the missing rules.



Log source type

Log source type unassigned

3Com 8800 Series Switch

Content extension name (10)

IBM QRadar Content Extension for GDPR

Rule name

🟨 Possible Shared Accounts

5. To see details about a rule that is not currently installed, click the rule name. Exploring the rule details helps you determine whether the rule can add important coverage in your environment, and then you can download the content extension that contains the rule.
6. To customize how the table rows are grouped, click the **Configure grouping** arrow icon on the tree structure icon.
   a. Select the columns that you want to group by selecting the corresponding checkbox. Only groupable columns that are currently listed in the report are shown, in the order in which they appear in the report.

      As you make your selections, a sample of what the report looks like displays in the **Configure options for grouping rows** window.

   b. To show only the number of child rows in the report, select the corresponding checkbox.

   c. Make your selections and then click **Apply**.
7. To download the content extension, click the link in the **Content extension name** column to go to the extension's page in the IBM Security App Exchange. If QRadar Assistant 2.0.0 app is installed in your QRadar deployment, you can download the content extension from there.
8. To clear the report results, click **Clear filters**, choose new filters in the left pane, and then click **Apply filters** to display new results.

RELATED DOCUMENTATION

Filtering Rules and Building Blocks by their Properties | 78

Investigating User Behavior Analytics Rules

User Behavior Analytics rules can help you identify potential insider threats inside your network. After the user analytics rules from QRadar User Behavior Analytics 4.1.0 or later are integrated in QRadar Use Case Manager 3.2.0 or later, you can manage and tune them to best suit your organization's needs. Then, the data automatically displays in the QRadar User Behavior Analytics dashboards so that you can visualize the risks to your network.

For a rule to be considered relevant to QRadar User Behavior Analytics, the **Dispatch new event** option must be selected in the **Rule Response**. You can also associate any other rules to work with QRadar User Behavior Analytics by editing them in the rule wizard in QRadar Use Case Manager.

NOTE: In QRadar User Behavior Analytics, the dashboard rule count is based on the total number of rules that QRadar User Behavior Analytics detects, regardless of whether the rules are installed or not. In QRadar Use Case Manager, filtering is based on what rules are installed.

1. On the Use Case Explorer page, click the list icon, and pick one of the following templates to use:

   All User Behavior Analytics rules

   Shows the risk score for all the installed and non-installed User Behavior Analytics rules.

   Installed User Behavior Analytics rules

   Shows the risk score for installed User Behavior Analytics rules.

   TIP: To use filters that are similar to the Rules and Tuning page in QRadar User Behavior Analytics, select this template. To view category information, add the **Content category** column. QRadar Use Case Manager does not contain kill chain information.

   Non-installed User Behavior Analytics rules

   For non-installed content extensions, this template shows the User Behavior Analytics rules that are available when the extensions are installed.

2. To modify the risk score for a predefined QRadar User Behavior Analytics rule, click the name of the rule, expand the **User Behavior Analytics risk score** section, and adjust the number. The user risk score in QRadar User Behavior Analytics automatically updates.

   A risk score is the summation of all risk events that are detected by QRadar User Behavior Analytics rules. The higher the risk score, the more likely an internal user is to be a security risk and warrants further review of your user's network activity. The risk score reduces over time if no new events occur. Rules that are integrated from the QRadar User Behavior Analytics app typically have a risk score in the range of 5 - 25. You can display the risk score in any report by adding the **Rule attributes: User Behavior Analytics risk** column to your current template. For more information, see Configuring application settings.

3. To add a risk score to a rule and associate it with QRadar User Behavior Analytics, follow these steps:

   a. Open the selected rule in the rule wizard and expand the **User Behavior Analytics risk score** section.

   b. If the **Dispatch New Event** option isn't selected in the **Rule response** section, click **Edit in rule wizard** and complete that step now.

   c. Assign a risk score to the rule.

   The QRadar User Behavior Analytics app tracks any events that the rule generates, and considers the risk score in its analysis.

4. If you no longer want a rule to be associated with QRadar User Behavior Analytics, follow these steps:

   a. Open the selected rule in the rule wizard and expand the **User Behavior Analytics risk score** section.

   b. Follow the instructions in the tooltip to disconnect the rule from QRadar User Behavior Analytics.

   When you remove the references to the rule from the reference table in QRadar User Behavior Analytics, any events that are triggered by the rule stop contributing to the user's risk score.

Review the relevant reports that include the User Behavior Analytics rules. The rules also contribute to the tactic counts in the MITRE ATT&CK reports. You can also visualize rules on the dashboards in the QRadar User Behavior Analytics app.

Duplicating Rules for Further Customization

Save time from creating new rules by duplicating existing rules. Then, you can customize the duplicated rules to meet the needs of your environment. For example, you might have several rules that are associated with a domain through their tests, but now you want to associate the rules with another domain. You can duplicate the rules in batch mode rather than copying each rule individually for the second domain.

1. On the Use Case Explorer page, click the **Toggle table view** icon to ungroup the report's table columns when the report is in the grouped mode.

TIP: Use any of the filters, such as the rule name, tactic, or technique to find the rule you want to copy, or search by using a regular expression. You can also use the **Group** filter to select the group you want to search, such as authentication or compliance.

2. Click the pencil icon in the report table to display checkboxes for each table row.
3. Select the checkbox for each rule that you want to copy, and click **Duplicate**.

NOTE: Rule grouping information is not duplicated in new rules.

4. Change the new rule name to something meaningful to your organization.
5. Click **Save** to see the status of the duplication before closing the window, or click **Save and close**.

RELATED DOCUMENTATION

Customizing Report Content Templates | 51

Exporting Rules

Export rule data in CSV or XML formats. Use CSV format to further process rule data or view it in Excel. Export rules in HTML format to view offline. Use XML format so that you can import the rule data into another QRadar deployment. Export rules with MITRE and custom rule attribute mappings. You can also create a **manifest.txt** file that is added to the **exported .zip** file.

You must be an administrator to export rule data to XML format.

1. On the Use Case Explorer page, pick one of the following methods.
   a. To export all the rules in the table report, click the **Download** icon in the menu bar.
   b. To export selected rules in the table report, click the pencil icon in the report table to display checkboxes for each table row. Then, select the relevant rules or building blocks that you want to export, and click **Export selected rules**.
2. To export rule data in the report to CSV format that you can further process or view in Excel, select the first option in the Export window, and enter a name for the CSV file.

   If you want to adjust the content to export, use the option to control column visibility and order (gear icon) on the report view.

3. To export rules and their dependencies, such as custom properties and reference sets, to an XML file for importing into another QRadar deployment, select the second option in the Export window. By default, the checkboxes for exporting MITRE mappings and for custom rule attribute mappings are enabled if the rules contain the mappings. The exported files are generated concurrently.

   > **TIP**: Exporting to XML is supported on QRadar 7.4.0 or later.

   a. Click **Next**.

   b. To create a **manifest.txt** file that is added to the **exported .zip** file, select the **Include manifest.txt** checkbox. The manifest file contains the extension name (mandatory), author (mandatory), description, unique ID, version, and support email information. These fields appear in the Extensions Management page when you import the file in another QRadar deployment.

      If you export more rules and use the same extension name and unique ID in the **manifest.txt** file, there is one entry in the Extensions Management window upon import.

4. To export rules to a formatted HTML report that you can view offline, select the third option in the Export window. By default, the dependencies, dependents, and visualizations for the selected rules are included in the exported .zip file. Share the .zip file with colleagues or management who don't have access to QRadar or QRadar Use Case Manager.

   The exported HTML file includes instructions on how to use the exported report.

5. Click **Export**.

Use the CSV file to further investigate your rules. Share or import the XML file into another QRadar deployment.

Deleting Rules

Delete user-created rules from QRadar that you no longer need. You can't delete system or override rules, or rules that have dependencies.

1. On the Use Case Explorer page, expand the **Origin** rule attribute in the **Rule attributes** filter, select the **User** checkbox, and click **Apply Filters**.

   You cannot delete rules with a system or override origin, so filtering the list fine-tunes the results for you to work with. System rules are default rules. Override rules are customized default rules.

2. Click the pencil icon in the report table to display checkboxes for each table row.
3. Select the checkbox for each rule that you want to delete and click **Delete**.
4. In the Delete rules window, review the status of each rule that you want to delete.

   Rules that have dependent rules are not deleted.

5. Click **Delete** to see the status of the delete process, or **Delete and close**.

   If you click **Delete and close**, and a rule cannot be deleted because it has dependencies, the window remains open to display the rules that aren't deleted.

The rules are permanently deleted from QRadar. If you want to add them back in, you must re-create them.

Rule Report Presentation

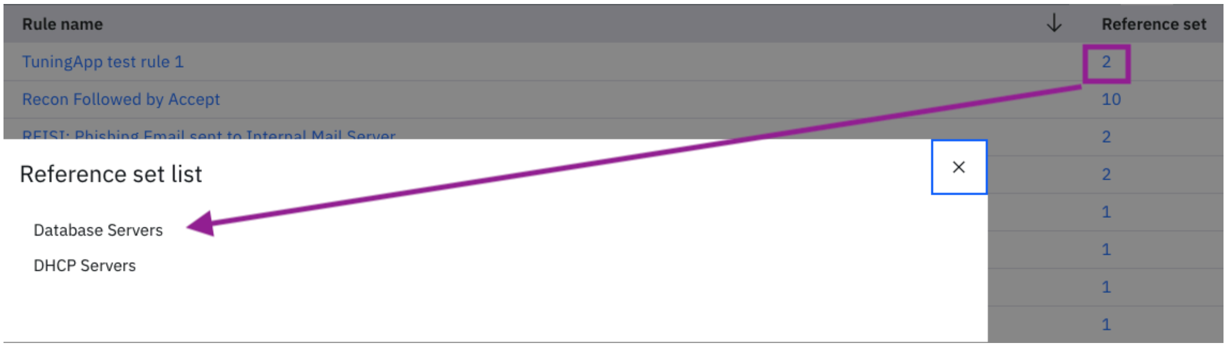
IN THIS SECTION

Fine-tune the report presentation so that it's easier to investigate and visualize the rules and building blocks. After you customize the report presentation, share the data results with others by creating CSV or XML reports.

To make it easier to see related data properties, click the tree structure icon to display the table view with groupable columns. The table must contain at least two of the following groupable columns: log source type, rule name, test, tactic, and technique. For example, you can group the table by the rules that are associated per log source type, or by the related rule names per reference set. The following rule tests are also groupable:

- Reference set
- Reference set (number of elements)
- Network hierarchy
- X-Force
- Custom property
- Domain
- Reference data
- MITRE
- Content extension

When you're investigating rules, grouping rule tables makes it easier to see related data properties. To switch to the grouped table mode, click the tree structure icon. In the grouped table mode, the table must contain at least two of the following groupable columns: log source type, rule name, test, tactic, and technique. Columns are grouped in the order that they are defined in the column list, which is available from the gear icon. You can also further customize the table groupings by clicking the arrow in the tree structure icon. Then, select from the groupable columns that are currently displayed or show only the number of child rows in the report instead of the actual rows. After you have the number of items in the report column, click the number to see the list of actual child items. For example, you have rule name and reference set columns in your report. You can see the number of reference sets per rule by clicking the number in the report to get the list of related references sets.



Rule name	Reference set
TuningApp test rule 1	2
Recon Followed by Accept	10
REISI: Phishing Email sent to Internal Mail Server	2
	2
	1
	1
	1
	1

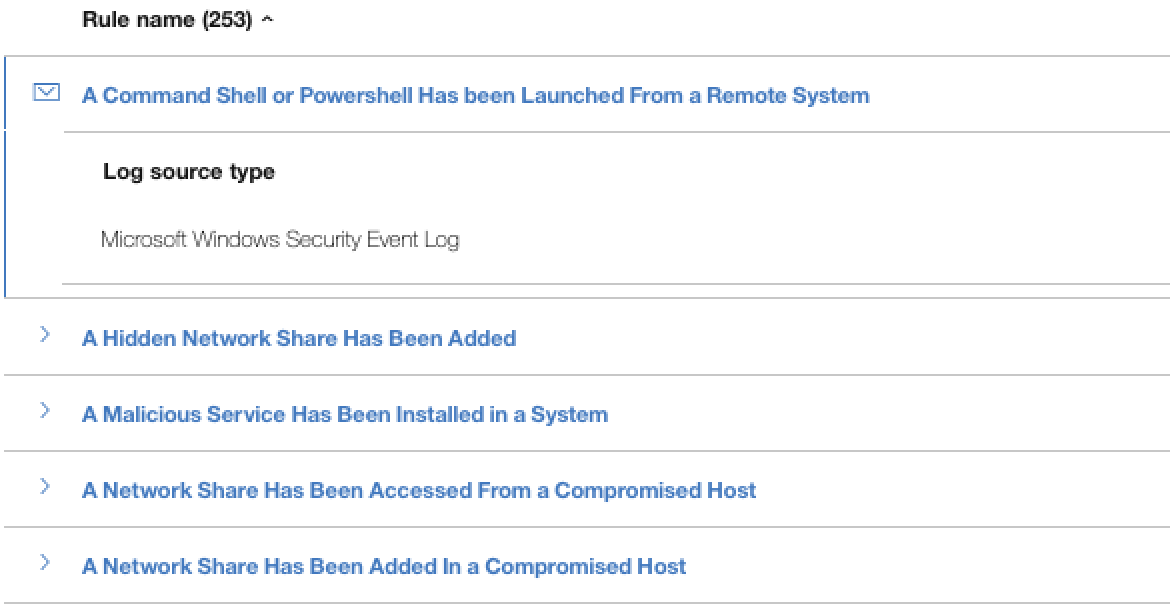
Reference set list

Database Servers

DHCP Servers

Change the column order in the list to change the grouped table display. All other non-groupable data properties that are in the table appear at the same level as the groupable columns. For example, rule creation date displays as a column in the same table as the rule name. At any time you can switch between the grouped and flat viewing modes, without losing your current results.

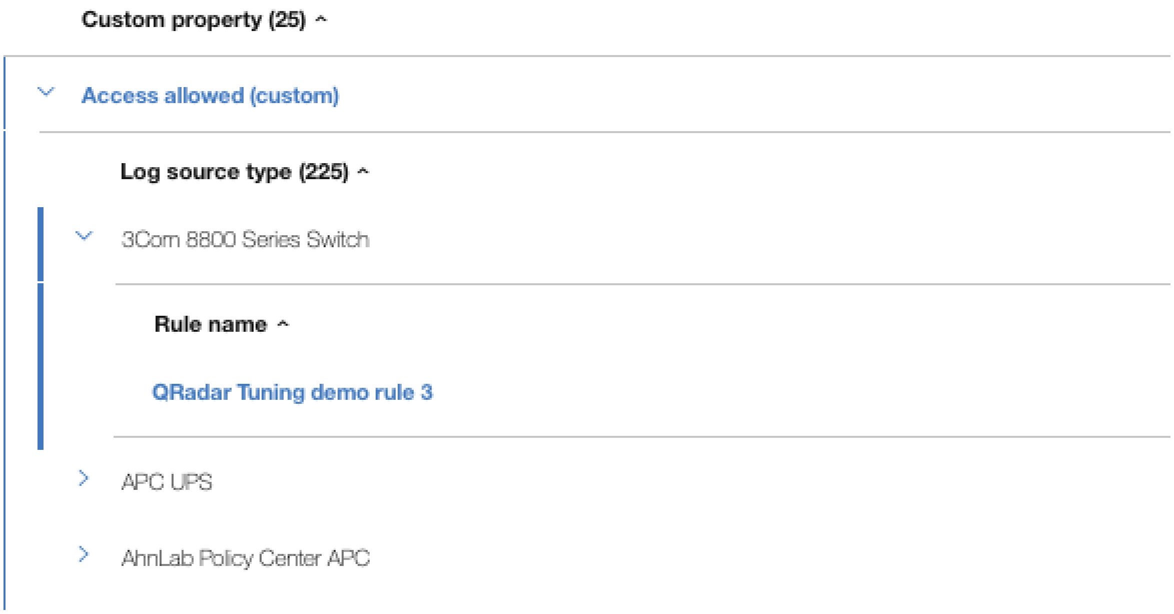
If the table contains two groupable columns, one nested level shows in the table. In the following image, the two groupable columns are rule name and log source type.



Rule name (253) ^

- A Command Shell or Powershell Has been Launched From a Remote System
  - Log source type
  - Microsoft Windows Security Event Log
- A Hidden Network Share Has Been Added
- A Malicious Service Has Been Installed in a System
- A Network Share Has Been Accessed From a Compromised Host
- A Network Share Has Been Added In a Compromised Host

If the report contains three groupable columns, two nested levels show in the table. In the following image, the three groupable columns are custom property, log source type, and rule name.



Custom property (25) ^

Access allowed (custom)

Log source type (225) ^

3Com 8800 Series Switch

Rule name ^

QRadar Tuning demo rule 3

APC UPS

AhnLab Policy Center APC

If there are more than three groupable columns, beginning with the third column, all of them display in a flat table on a second nested level. There can be no more than two nested levels.

Downloading the Report

When you finish fine-tuning the report data, you can download the rule report as a CSV or XML file to share with colleagues and managers. You can also visualize the grouped content by clicking the eye icon.

To export or import the rule mappings or to export only the rules that display in the current view of the report, use the options in the **ATT&CK Actions** menu. The mappings are exported in JSON format.

RELATED DOCUMENTATION

Visualizing Rules and Building Blocks | 91

Visualizing Rules and Building Blocks

Visualize the rules and building blocks that are used in IBM QRadar. After you organize the rule report, you can visualize the data through relationship graphs and coverage maps, and export the data to share with others.

1. To show or hide the visualization pane, click the eye icon. Zoom in or out to see the relationships of rules or building blocks and their dependencies. Depending on the number of items, the graph visualizes a portion of the results.
2. To get better results, refine the search by using the filters.
3. To ensure that you're visualizing up-to-date content, refresh the rules with content from QRadar. The default refresh interval is every 15 minutes.

   For example, you install a new content extension and want to see the data right away, rather than wait for the next refresh interval.
4. To expand the visualization pane to the width of your screen, click the maximize icon on the menu bar of the pane. Zoom in or out to focus on details.

   > **NOTE**: The zoom capability is not supported on Mozilla Firefox. Use the browser control to zoom in and out.
5. To switch between visualization charts, click **View visualization charts** and select from **Relationship graph, MITRE ATT&CK**, or **Current and potential log source type coverage**. For more information about log source type coverage, see "Visualizing Log Source Type Coverage per Rule" on page 91.

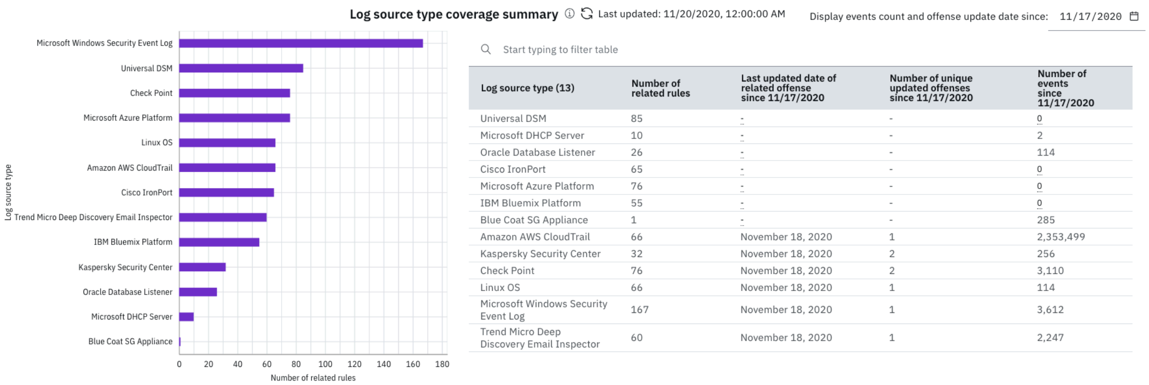
Visualizing Log Source Type Coverage per Rule

IN THIS SECTION

Explore current and potential log source type coverage per rule, and see how your rule coverage can expand if new log source types are added to your environment. See the number of rules that provide current coverage for each log source type, based on the rule test definitions.

1. To see the number of rules that provide current coverage for each log source type based on the rule test definitions, click **Rule-log source type coverage** > **Summary and offense update trends**.

   a. In the **Log source type coverage summary** table, check when the log source type last contributed to an offense based on the last updated date. Then, review the number of events for log sources of that type. If the last updated date of an offense is old, try tuning some of the rules for the related log source type. For example, you have 81 rules for a log source type that stopped contributing to an offense for three weeks and has no events that are associated with it. The 81 rules require investigation to see whether there's something wrong with them. You can also filter the list in the table chart to fine-tune the log source types you want to investigate.



Log source type coverage summary Last updated: 11/20/2020, 12:00:00 AM

Display events count and offense update date since: 11/17/2020

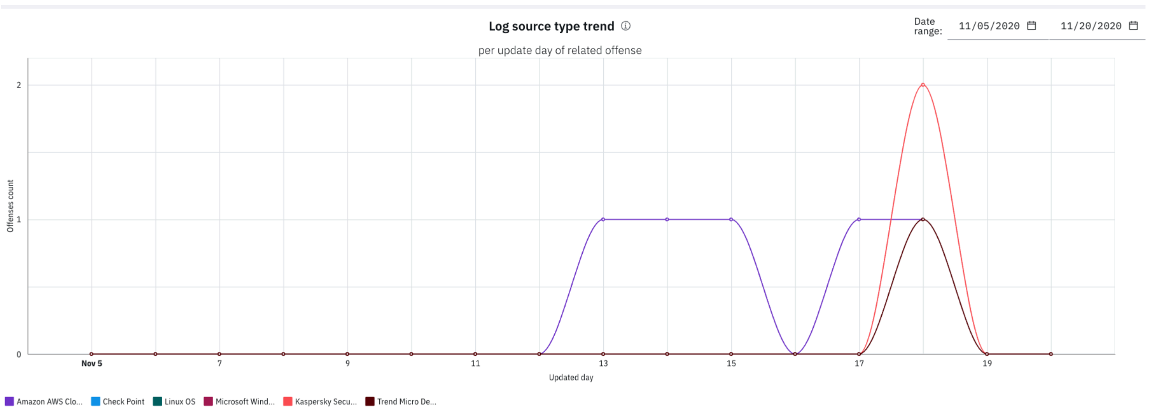
Log source type (13)	Number of related rules	Last updated date of related offense since 11/17/2020	Number of unique updated offenses since 11/17/2020	Number of events since 11/17/2020
Universal DSM	85	-	-	0
Microsoft DHCP Server	10	-	-	2
Oracle Database Listener	26	-	-	114
Cisco IronPort	65	-	-	0
Microsoft Azure Platform	76	-	-	0
IBM Bluemix Platform	55	-	-	0
Blue Coat SG Appliance	1	-	-	285
Amazon AWS CloudTrail	66	November 18, 2020	1	2,353,499
Kaspersky Security Center	32	November 18, 2020	2	256
Check Point	76	November 18, 2020	2	3,110
Linux OS	66	November 18, 2020	1	114
Microsoft Windows Security Event Log	167	November 18, 2020	1	3,612
Trend Micro Deep Discovery Email Inspector	60	November 18, 2020	1	2,247

   The bar chart is a visualization of the table chart.

   b. Change the date for the **Log source type coverage summary** chart coverage by clicking the calendar icon for **Display events and offense updated date since: <date>**. QRadar Use Case Manager initially fetches 90 days of data from QRadar, and keeps collecting data daily for 1 year. Data older than 1 year is then deleted from the database. The default date is one day before the current day's date.

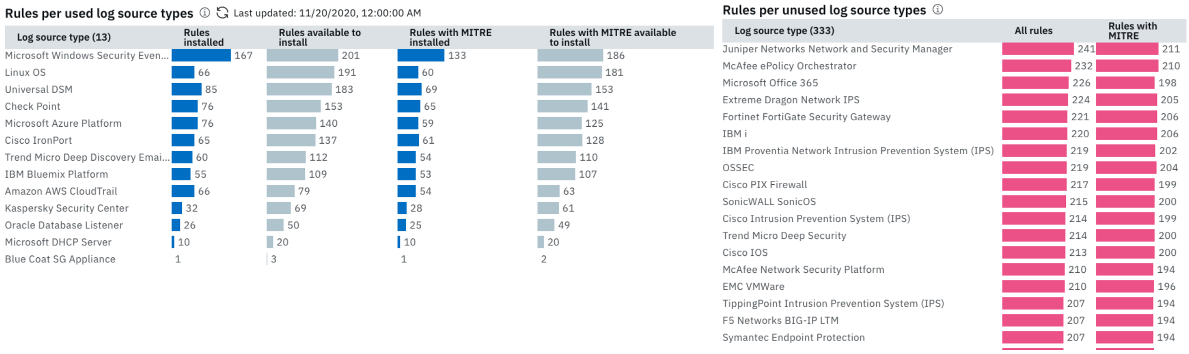
   For more information, see Example log source type coverage summary table.

   c. In the **Log source type trend** chart, review the number of offenses that are updated on a specific day and related to a specific log source type. Updated offenses are counted against each related log source type, regardless of the log source type that caused the update. Fine-tune the chart by specific log source type by clicking the checkboxes beneath the chart.



d. Change the date for the **Log source type trend** chart coverage by clicking the calendar icons for Date range. Trend data is only available from the date of app installation.

2. To see current and potential log source type coverage, click **Rule-log source type coverage > Current and potential**.



Rules per used log source types ⓘ Last updated: 11/20/2020, 12:00:00 AM

Log source type (13)	Rules installed	Rules available to install	Rules with MITRE installed	Rules with MITRE available to install
Microsoft Windows Security Even...	167	201	133	186
Linux OS	66	191	60	181
Universal DSM	85	183	69	153
Check Point	76	153	65	141
Microsoft Azure Platform	76	140	59	125
Cisco IronPort	65	137	61	128
Trend Micro Deep Discovery Emai...	60	112	54	110
IBM Bluemix Platform	55	109	53	107
Amazon AWS CloudTrail	66	79	54	63
Kaspersky Security Center	32	69	28	61
Oracle Database Listener	26	50	25	49
Microsoft DHCP Server	10	20	10	20
Blue Coat SG Appliance	1	3	1	2

Rules per unused log source types ⓘ

Log source type (333)	All rules	Rules with MITRE
Juniper Networks Network and Security Manager	241	211
McAfee ePolicy Orchestrator	232	210
Microsoft Office 365	226	198
Extreme Dragon Network IPS	224	205
Fortinet FortiGate Security Gateway	221	206
IBM i	220	206
IBM Proventia Network Intrusion Prevention System (IPS)	219	202
OSSEC	219	204
Cisco PIX Firewall	217	199
SonicWALL SonicOS	215	200
Cisco Intrusion Prevention System (IPS)	214	199
Trend Micro Deep Security	214	200
Cisco IOS	213	200
McAfee Network Security Platform	210	194
EMC VMWare	210	196
TippingPoint Intrusion Prevention System (IPS)	207	194
F5 Networks BIG-IP LTM	207	194
Symantec Endpoint Protection	207	194

NOTE: QRadar Use Case Manager excludes log source types that QRadar considers 'internal' from these charts; for example, Health Metrics, SIM Audits, Custom Rule Engine, System Notifications, and Asset Profiler.

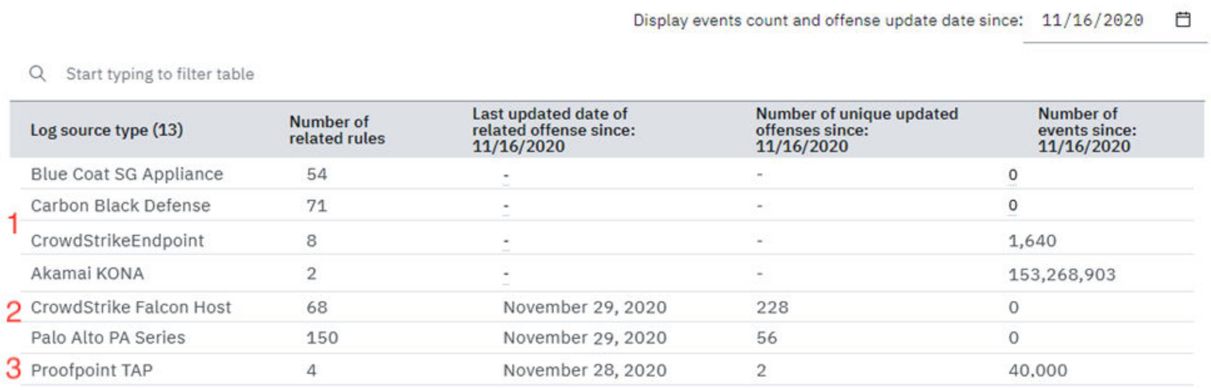
3. Explore current and potential coverage in the **Rules per used log source types** chart. The **Rules available to install** and the **Rules with MITRE available to install** columns indicate the number of rules from content extensions that are available on the IBM Security App Exchange. To generate a report of content extensions for a selected log source type, select the corresponding bar and click **Apply Filters** in the filter pane. Then, click the content extension name link in the table report to view or install the content extension.

4. Explore how coverage can expand if new log source types are added in the **Rules per unused log source types** chart. Rules that are represented in the bars are either already installed or available to install from content extensions on the IBM Security App Exchange. To generate a report of the rules and their origin for a selected log source type, select the corresponding bar and then click **Apply Filters** in the filter pane. Then, click the content extension name link in the table report to view or install the content extension.

Example Log Source Type Coverage Summary Table

The **Log source type coverage summary** table shows some coverage results since November 16, 2020. Learn how to use these examples to interpret your own results.

Figure 8: Sample Log Source Type Coverage Table



Display events count and offense update date since: 11/16/2020

Start typing to filter table

Log source type (13)	Number of related rules	Last updated date of related offense since: 11/16/2020	Number of unique updated offenses since: 11/16/2020	Number of events since: 11/16/2020
Blue Coat SG Appliance	54	-	-	0
Carbon Black Defense	71	-	-	0
CrowdStrikeEndpoint	8	-	-	1,640
Akamai KONA	2	-	-	153,268,903
CrowdStrike Falcon Host	68	November 29, 2020	228	0
Palo Alto PA Series	150	November 29, 2020	56	0
Proofpoint TAP	4	November 28, 2020	2	40,000

The report was run on 30 November 2020 to track coverage that began on 16 November 2020.

1. The first 4 log source types did not contribute events to any offense since 16 November 2020. Events coming from these log source types didn't affect any offense in two weeks. The CrowdStrikeEndpoint and Akamai KONA log source types received events, and although Akamai KONA had almost 154,000,000 events, none of them contributed to any offense. Follow these steps to resolve these types of cases:

   - Investigate the rules that are related to these log source types for any tuning actions. Run one of the log source coverage templates and add the filter for any needed log source types.

   - Check whether more rules are available to install from the IBM Security App Exchange that can provide better coverage for these log source types. Select **Rule-log source type coverage** > **Current and potential coverage**, find the log source type in the chart, and click the bar next to it in the **Rules available to install** column. Then, apply the filters and check the resulting report.

2. The CrowdStrike Falcon Host and Palo Alto PA Series log source types show that several offenses were updated, but neither received any events. Because these log source types don't have any events, this means that these log source types are related to some offenses that were updated by events from other log source types.

3. The Proofpoint TAP log source type had many events that contributed to two offenses. This is a common example.

RELATED DOCUMENTATION

Visualizing Rules and Building Blocks | 91

9

CHAPTER

QRadar Tuning

QRadar Tuning

IN THIS SECTION

QRadar Use Case Manager provides several ways to tune your QRadar environment.

Tune Your QRadar Offenses by Analyzing Rules That Cause the Biggest Number Of Offenses

Tune most active rules

QRadar Use Case Manager can help you determine which rules generate the most offenses, and then guide you through the steps to tune them.

Tune based on the CRE event report

The Custom Rules Engine (CRE) event report shows which CRE events were generated most often. It also provides information about the rule activity. You can tune these rules or use the event information from the report to update your QRadar environment.

Tune Your QRadar Offenses by Going Through the Most Common Configuration Steps

Review network hierarchy

Network Hierarchy is used to define which IP addresses and subnet are part of your network. Defining your network hierarchy and keeping it up to date is an important step in helping prevent false offenses.

Review building blocks

Rules use information about your servers to determine whether to generate the rule responses. Review and update common rule building blocks to enable QRadar to discover and classify more servers on your network, and prevent false positives.

Tuning the Active Rules That Generate Offenses

Tuning the top most noisy rules can have a significant impact on reducing false positives.

1. From the QRadar Use Case Manager main menu, click **Active Rules**.
2. Apply filters to the active rules to fine-tune your investigation.
   a. Filter the rules that started to contribute to offenses according to the calendar or by timeframe. The default date is in the last three days. Change the timeframe, or choose to filter the rules that began to contribute to offenses between specific dates and times.

   b. Select parameters to exclude offenses from the results, such as hidden or closed offenses. Offenses that are marked for follow-up are flagged for further investigation. You might have offenses that you want to retain regardless of the retention period; those offenses are protected to prevent them from being removed from QRadar after the retention period elapses. Inactive offenses can be removed from visualization so that reports aren't cluttered.

   c. Select the closure reason for an offense. For example, you can filter to see which rules generated the offenses that were closed as false positives. Rules with many false positives likely need tuning. Offenses that are closed as a non-issue are usually considered not critical to your organization.

   d. Click **Apply Filters**.
3. Review the **Offenses by rule, Offenses by category and rule, Closed offenses by reason and rule, Events count trend by rule,** and **Offense creation trend by rule** charts.

   > **TIP**: The **Offense creation trend by rule** chart is supported on QRadar 7.4.1 Fix Pack 2 or later.

   a. Hover over the chart segments to see more details about an offense.

   b. Hide or show chart legends.

   c. Click legend keys to fine-tune the chart display.

   d. Zoom in for further investigation.

   e. Expand bar and timeline charts to full screen.

   f. Export bar and timeline charts to CSV, PNG, or JPG formats.

   g. View bar and timeline chart data in tabular format. Then, export the data in CSV format to view offline or share with colleagues.

4. In the table, tune the rules by choosing from the following methods:

   a. Toggle between the top noisy rules or all the rules from the list.

   b. Add more rules to investigate by selecting a group of rule or an individual rule from the list.

   > **TIP**: The **Event count** column in the report indicates how many events the rule associated to the offenses counted in the **Offense count** column. The **Event count** column is supported on QRadar 7.4.1 Fix Pack 2 or later.

5. Click **Investigate**.

   a. Watch a short video to learn how to use the rule wizard.

   b. Review each individual rule and the BBs that contribute to the active rule. For each rule, you can further investigate it by clicking **Show dependency tree** or **Edit in rule wizard**.

   c. Use the visualization diagram to further fine-tune any related options for the rule or building block, such as log source types, custom properties, or reference sets.

   d. Review the offenses that are generated by each active rule.

   e. Review the values in the various groups of tests, and tune if necessary.

   f. Review the MITRE ATT&CK mappings for the rule, and edit if necessary.

   g. To add custom rule attributes to the selected rule or building block, see Step 10 in "Investigating QRadar rules and building blocks" on page 76.

   h. To investigate QRadar User Behavior Analytics rules, see "Investigating user behavior analytics rules" on page 84.

   i. To return to the **Active Rules** page, click **Active Rules** in the breadcrumbs.

6. To export selected rule data in the report to CSV format that you can further process or view in Excel, select the relevant checkboxes and then click **Export**.

RELATED DOCUMENTATION

Tuning the Active Rules That Generate CRE Events | **100**

Tuning the Active Rules That Generate CRE Events

The Custom Rules Engine (CRE) event report shows which active rules generate CRE events. In many cases, a rule response is configured to generate CRE events, along with the offense or without it. The report shows which CRE events were generated most by which rule. In general, if the event is generated many times per day, the rule is firing too often. Consider tuning the rule. For example, 1 or 2 Source IPs in the report are related to all the CRE events generated by the rule. The Source IP might need to be added to one of Host Definition BBs that are referenced by the rule. Select the rule and click **Investigate** to see which Host Definition to update.

You can also use this report to test the rules. In this case, the rule response does not include the offense creation, only the CRE event dispatch. If the report shows that the rule is firing too often, consider tuning it. If you're using CRE events to test the rule, and the number of generated CRE events is only a few per week, change the rule response to generate an offense.

Unapplied filter tags appear in the filters row with a lighter colored background. After you apply the filters, the tags change to a darker colored background.

1. From the main menu, click **CRE Report**.
2. Filter the rules according to the calendar, or by time period.
3. Select the number of results to return, and click **Apply Filters**.
4. Review the **CRE events by rule** and the **CRE events by category and rule** reports.
   a. Hover over the chart segments to see more details about an offense.
   b. Hide or show chart legends.
   c. Click the legend keys in the **CRE events by rule** report to fine-tune the chart display.
   d. Zoom in for further investigation.
   e. Expand the **CRE events by category and rule** chart to full screen.
   f. Export the **CRE events by category and rule** chart to CSV, PNG, or JPG formats.
   g. View the **CRE events by category and rule** chart data in tabular format. Then, export the data in CSV format to view offline or share with colleagues.
5. Tune the rules by choosing from the following methods:
   a. Toggle between the topmost noisy rules or all the rules from the list.
   b. Add another rule to investigate by selecting a group of rule or an individual rule from the list.
6. Click **Investigate**.
   a. Review each individual rule and the BBs that contribute to the CRE event. For each rule, you can further investigate it by clicking **Show dependency tree** or **Edit in rule wizard**.

b. Use the visualization diagram to further fine-tune any related options for the rule or building block, such as log source types, custom properties, or reference sets.

c. Review the events that are generated by the current rule you selected.

d. To instantly refresh the rules from QRadar, click the **Refresh** icon. Otherwise, the app automatically updates data from the Console every 15 minutes.

e. Review the threshold values in the tests, and tune if necessary.

f. Review the values in the various groups of tests, and tune if necessary.

g. Review the MITRE ATT&CK mappings for the rule, and edit if necessary.

h. To add custom rule attributes to the selected rule or building block, see step 9 in "Investigating QRadar rules and building blocks" on page 76.

i. To investigate QRadar User Behavior Analytics rules, see "Investigating user behavior analytics rules" on page 84.

j. To return to the CRE events page, click **CRE Report** in the breadcrumbs.

7. To export selected rule data in the report to CSV format to process or view in Excel, select the relevant checkboxes and then click **Export**.

RELATED DOCUMENTATION

Reviewing Your Network Hierarchy | 101

Reviewing Your Network Hierarchy

A well-defined and maintained network hierarchy can help prevent the generation of false positive offenses. The network hierarchy is used to define which IP addresses and subnets are part of your network. Ensure that all internal address spaces, both routable and non-routable, are defined within your QRadar network hierarchy. QRadar can then distinguish your local network from the remote network. Event and flow context is based on whether the source and destination IPs are local or remote. Event and flow context, and data from your network hierarchy are used in rule tests.

1. From the navigation menu, click **Network Hierarchy**.
2. Optional: Watch tuning videos to learn more about your network hierarchy and how to keep it up to date.
3. Check the network hierarchy list to see which parts of your network hierarchy are not yet updated.

4. Check for R2R (Remote to Remote) events. The report identifies events with R2R direction or context. When an event has R2R direction, both its source and destination IPs are remote and aren't part of your local network. It means that there's external traffic from a remote network to another remote network, and indicates a possible network hierarchy misconfiguration.

   a. Consider whether either one or both of the event IPs are local and add them to the network hierarchy.

   b. Use the **Source IP**, **Source Company**, **Destination IP**, and **Destination Company** columns in the report to identify IPs that are local to your network.

   c. After you identify the local IP addresses, either add them from the **Network Hierarchy** page from the **Admin** tab or select them in the report to add them in the app.

   d. On the **Admin** tab, click **Deploy changes**.

5. Explore the rules that use your network hierarchy either directly or indirectly. Review and update any rules or building blocks that are out of date.

   a. To review rules in detail, select one from the list and then zoom in on the diagram. Drag the rule and BB icons on the pane.

   b. In the right pane of the window, click **List view** and then toggle between filtered BBs and non-filtered BBs to fine-tune the list. "Filtered BBs" displays the dependencies for the selected rule that have network tests. "All BBs" displays all the BBs that are used by the selected rule.

   c. Click **Show dependency tree** to see the dependencies and the dependents of the selected BB.

      Dependencies are referenced by the selected building block either directly or indirectly. If you update any of the dependencies, the building block is affected. Dependents reference the selected BB either directly or indirectly. If you update the building block, its dependents are affected.

RELATED DOCUMENTATION

Reviewing Building Blocks | 102

Reviewing Building Blocks

Building blocks are a reusable set of rule tests that can be used within rules when needed. Host definition building blocks (BB:HostDefinition) categorize assets and server types into CIDR/IP ranges. By populating host definition building blocks, QRadar can identify the type of appliance that belongs to an address or address range. These building blocks can then be used in rules to exclude or include entire asset categories in rule tests.

Use server discovery to populate host definition building blocks (BB:HostDefinition). Server discovery uses existing asset profile data so that administrators can define unknown server types and then assign them to a server definition and the network hierarchy.

1. From the main navigation menu in the app, click **Host Definitions**.
2. Optional: Watch tuning videos to learn more about the importance of defining host definitions, and to get tips on how to automatically populate them.
3. Click **Host definitions** and review and update IPs and ports in BBs from the Host Definition group or check when BBs were last updated.
4. Optional: To instantly refresh the rules from QRadar, click the **Refresh** icon. Otherwise, the app automatically updates data from the Console every 15 minutes.
5. To edit IPs in reference sets in building blocks, complete the following steps:
    a. Click **Host definitions >IPs & Ports**.

    b. Click a link or the pencil icon (Edit).

    c. On the Edit reference set page, add an IP or select an existing IP and delete it from the reference set.

       The reference set opens in the QRadar Reference Data Management app, if the app is installed on the QRadar Console.
6. To edit ports in building blocks or rules sets, complete the following steps:
    a. Click **Host definitions >IPs & Ports**.

    b. Click a link or the pencil icon (Edit).

    c. In the Edit ports window, edit the list of ports as needed, and click **OK**. A list accumulates the ports as you edit, displaying a star next to each update.

    d. Click **Save** when you're done.

RELATED DOCUMENTATION

Reviewing Your Network Hierarchy | 101

10

CHAPTER

Accessing Report Data by using QRadar Use Case Manager APIs

Accessing Report Data by using QRadar Use Case Manager APIs

As an alternative to using the interface in QRadar Use Case Manager, you can use APIs to download report data to CSV or JSON files. Try using the interactive API documentation interface to test the APIs before you use them in your scripts.

1. From the **Admin** tab, click **Apps** > **QRadar Use Case Manager** > **API Docs**.
2. Select a workflow to use. For more information, see "Public Use Case Manager API Workflows" on page 106.
3. Click **Try it** out and then complete the request parameters for the selected workflow. For more information, see "Use Case Explorer Filters" on page 110 and "Report Column Codes for Report APIs" on page 114.
4. Click **Execute** to send the API request to your console and receive a properly formatted HTTPS response.
5. Review and gather the information that you need to integrate with QRadar.

Review the endpoint workflows and try the example script or use the script as a base for your own scripts. Use the filters and report columns that make sense for your environment and needs.

- "Public Use Case Manager API Workflows" on page 106

  Use these workflows to download report data to CSV or JSON files.

- "Example API Workflow Script" on page 109

  Use the script in this example to download a Use Case Explorer report in CSV format.

- "Use Case Explorer Filters" on page 110

  Use these filters in the example script to download a Use Case Explorer report in CSV format.

- "Report Column Codes for Report APIs" on page 114

  Use the report column codes in the tables in the following APIs: POST

  /api/rules_explorer/{reportId}/download_csv, POST

  /api/rules_explorer/{reportId}/download_json, or GET /api/rules_explorer/{reportId}/result.

Public Use Case Manager API Workflows

IN THIS SECTION

Use these workflows to download report data to CSV or JSON files.

Workflow to generate a paginated result in JSON

Use this workflow to generate the Use Case Explorer report as a JSON array in a page by page format. The workflow uses the API endpoints in the order that is described in the following table:

Endpoint	Description
`POST /api/use_case_explorer`	Generates a Use Case Explorer report and returns a **reportId**. You must use this endpoint first when you start report generation. Fill the body of the request with the report columns and any filters or table groupings you want in the generated report. Use the returned **reportId** value in other API calls in the workflow.
`GET /api/use_case_explorer/{reportId}/status`	Returns the status of `/api/use_case_explorer`. Use the endpoint to see whether your report generation succeeded or failed.
`GET /api/use_case_explorer/{reportId}/result`	Returns the result of `/api/use_case_explorer` in a paginated JSON array. Include the **reportId** value that is returned from the `/api/use_case_explorer` endpoint in the path to get your result.

Workflow to generate and download reports in CSV

This workflow uses the API endpoints in the order that is described in the following table:

Endpoint	Description
`POST /api/use_case_explorer`	Generates a Use Case Explorer report and returns a **reportId**. You must use this endpoint first when you start report generation. Fill the body of the request with the report columns and any filters or table groupings you want in the generated report. Use the returned **reportId** value in other API calls in the workflow.
`GET /api/use_case_explorer/{reportId}/status`	Returns the status of `/api/use_case_explorer`. Use the endpoint to see whether your report generation completed or failed.
`POST /api/use_case_explorer/{reportId}/download_csv`	Starts the download of a Use Case Explorer report CSV file. Include the **reportId** value of the `/api/use_case_explorer result` in the path and fill the body of the request with your selected column codes, sort parameters, rule IDs, or search parameters to get a **jobId**.
`GET /api/use_case_explorer/download_csv/{jobId}/status`	Checks the status of a Use Case Explorer report CSV file download job. Include the **jobId** value returned from the `/api/use_case_explorer/{reportId}/download_csv` endpoint in the path to get a status on whether your job completed or failed.
`GET /api/use_case_explorer/download_csv/{jobId}/result`	Returns the Use Case Explorer report in a CSV file if the `/api/use_case_explorer/download_csv/{jobId}/status` endpoint returns a 'Completed' status. Include the **jobId** value that is returned by the `/api/use_case_explorer/{reportId}/download_csv` endpoint and the name you want for your CSV file in the query to get a download link for your CSV file.

Workflow to generate and download reports in JSON

This workflow uses the API endpoints in the order that is described in the following table:

Endpoint	Description
`POST /api/use_case_explorer`	Generates a Use Case Explorer report and returns a **reportId**. You must use this endpoint first when you start report generation. Fill the body of the request with the report columns and any filters or table groupings you want in the generated report. Use the returned **reportId** value in other API endpoints in the workflow.
`GET /api/use_case_explorer/{reportId}/status`	Returns the status of `/api/use_case_explorer`. Use the endpoint to see whether your report generation succeeded or failed.
`POST /api/use_case_explorer/{reportId}/download_json`	Downloads the Use Case Explorer report as a JSON file. Include the **reportId** value of the `/api/use_case_explorer` endpoint in the path and fill the body with your selected column codes, sort parameters, rule IDs, or search parameters to get a **jobId**.
`GET /api/use_case_explorer/download_json/{jobId}/status`	Checks the status of a Use Case Explorer report JSON file download job. Include the **jobId** value returned from the `/api/use_case_explorer/{reportId}/download_json` endpoint in the path to get a status on whether your job completed or failed.
GET /api/use_case_explorer/download_json/{jobId}/result	Returns the final result of the Use Case Explorer JSON file after the `/api/use_case_explorer/download_json/{jobId}/status` endpoint returns a 'Completed' status. Include the **jobId** value that is returned by the `/api/use_case_explorer/{reportId}/download_json` endpoint and the name you want for your JSON file in the query to get a download link for your JSON file.

Example API Workflow Script

Use the script in this example to download a Use Case Explorer report in CSV format.

NOTE: Due to formatting issues, paste the script into a text editor and then remove any carriage return or line feed characters.

You can replace the filters code with other filter details. In the following line, replace the bolded content with other filter content that is described in "Use Case Explorer Filters" on page 110.

```
--data-raw '{"filters":
[{"name":"rule","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
[true],"attributeName":"",valueType":"EXCLUSIVE_COMMON"}],"columns":
["N","GR","RC","T","RO","EN","RE","CD","MD"]}'
```

```
/* Begin by initiating the report generation with POST/api/use_case_explorer. */
curl --user admin --location --request POST 'https://{qradar ip}/console/plugins/{UCM App ID}/
app_proxy/api/use_case_explorer' \
--header 'Content-Type: application/json' \
--data-raw '{"filters":
[{"name":"rule","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
[true],"attributeName":"",valueType":"EXCLUSIVE_COMMON"}],"columns":
["N","GR","RC","T","RO","EN","RE","CD","MD"]}'

/* Return the current status of report generation from POST/api/use_case_explorer by calling
GET /api/use_case_explorer/{reportId}/status. */
curl --user admin --location --request GET 'https://{qradar ip}/console/plugins/{UCM App ID}/
app_proxy/api/use_case_explorer/{report id}/status' \
--header 'Cookie: csrfToken=DG0pShPY-Ks59qGwW_nraLhvdl1zzyQua9Tg;

/* To download the report in CSV format, once GET /api/use_case_explorer/{reportId}/status
 returns a status of COMPLETED, use POST /api/use_case_explorer/{reportId}/download_csv
 to initiate the job to generate a CSV report */
curl --user admin --location --request POST 'https://{qradar ip}/console/plugins/{UCM App ID}/
app_proxy/api/use_case_explorer/{report id}/download_csv' \
--header 'Content-Type: application/json' \
--data-raw '{"columns":"N,GR,RC,T,RO,EN,RE,CD,MD"}'
```

```
/* Return the current status of CSV report generation from POST /api/use_case_explorer/
{reportId}/download_csv by calling GET /api/use_case_explorer/download_csv/{jobId}/status */
curl --user admin --location --request GET 'https://{qradar ip}/console/plugins/{UCM App ID}/
app_proxy/api/use_case_explorer/download_csv/{download csv job id}/status' \
--header 'Content-Type: application/json' \
--data-raw '{"columns":"N,GR,RC,T,RO,EN,RE,CD,MD"}'

/* Finally, when GET /api/use_case_explorer/download_csv/{jobId}/status
 returns a status of COMPLETED, call GET /api/use_case_explorer/download_csv/{jobId}/result
 to download your generated report in CSV file format */
curl --user admin --location --request GET 'https://{qradar ip}/console/plugins/{UCM App ID}/
app_proxy/api/use_case_explorer/download_csv/{download csv job id}/result?csvName=test.csv' \
--header 'Content-Type: application/json' \
--data-raw '{"columns":"N,GR,RC,T,RO,EN,RE,CD,MD"}'
```

Use Case Explorer Filters

IN THIS SECTION

Use these filters in the example script to download a Use Case Explorer report in CSV format.

Rule Tests

Log source

```
{"name":"DeviceID_Test","type":"TEST","recursive":true,"matchCriteria":"PARTIAL","values":
["1","2"],"attributeName":"","valueType":"COMMON"}]
```

Log source type

```
{"name":"DeviceTypeID_Test","type":"TEST","recursive":true,"matchCriteria":"PARTIAL","values":
["1","2"],"attributeName":"","valueType":"COMMON"}]
```

Log source group

```
{"name":"DeviceGroupID_Test","type":"TEST","recursive":true,"matchCriteria":"PARTIAL","values":
["1","2"],"attributeName":"","valueType":"COMMON"}]
```

Other tests: Ariel search

```
{"name":"LST_ALL","type":"TEST","recursive":true,"matchCriteria":"IGNORE","values":
[],"attributeName":"LST_ALL","valueType":"TEST"}
```

Other tests: Domain

```
{"name":"DOMAIN_ALL","type":"TEST","recursive":true,"matchCriteria":"IGNORE","values":
[],"attributeName":"DOMAIN_ALL","valueType":"TEST"}
```

Rule Attributes

Rule name

```
{"name":"name","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
["Test"],"attributeName":"","valueType":"UNIQUE"}
```

Rule enabled: True

```
Rule Enabled: True
{"name":"enabled","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
[true],"attributeName":"","valueType":"EXCLUSIVE_COMMON"}
```

Rule

```
{"name":"rule","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
[true],"attributeName":"","valueType":"EXCLUSIVE_COMMON"}
```

Type: Events

```
{"name":"type","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
["EVENT"],"attributeName":"","valueType":"COMMON"}
```

Origin: System

```
{"name":"rule_orig","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
["SYSTEM"],"attributeName":"","valueType":"COMMON"}
```

Rule category: Custom rule

```
{"name":"rule_cat","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
["Custom Rule"],"attributeName":"","valueType":"COMMON"}
```

Group: Amazon AWS

```
{"name":"group","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":["Amazon
AWS"],"attributeName":"","valueType":"COMMON"}
```

Group: Botnet, Category Definitions (Multiple filter selection)

```
{"name":"group","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
["Botnet","Category Definitions"],"attributeName":"","valueType":"COMMON"}
```

Action: Event is part of an offense

```
{"name":"action","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
["offense"],"attributeName":"","valueType":"COMMON"}
```

Response: Email

```
{"name":"response","type":"ATTRIBUTE","recursive":true,"matchCriteria":"PARTIAL","values":
["email"],"attributeName":"","valueType":"COMMON"}
```

MITRE ATT&CK

Tactic: Collection

```
{"name":"tactic","type":"ATTCK","recursive":true,"matchCriteria":"PARTIAL","values":
["TA0009"],"attributeName":"","valueType":"EXCLUSIVE_COMMON"}
```

Technique: Data Obfuscation

```
{"name":"technique","type":"ATTCK","recursive":true,"matchCriteria":"PARTIAL","values":
["T1001"],"attributeName":"","valueType":"EXCLUSIVE_COMMON"}
```

Mapping confidence: High

```
{"name":"mapping_confidence","type":"ATTCK","recursive":true,"matchCriteria":"PARTIAL","values":
["high"],"attributeName":"","valueType":"COMMON"}
```

Mapping enabled: True

```
{"name":"mapping_enabled","type":"ATTCK","recursive":true,"matchCriteria":"PARTIAL","values":
[true],"attributeName":"","valueType":"EXCLUSIVE_COMMON"}
```

Tactic: Initial Access, Impact (Multiple filter selection)

```
{"name":"tactic","type":"ATTCK","recursive":true,"matchCriteria":"PARTIAL","values":
["TA0001","TA0040"],"attributeName":"","valueType":"EXCLUSIVE_COMMON"}
```

Report Column Codes for Report APIs

IN THIS SECTION

Use the report column codes in the tables in the following APIs: `POST /api/rules_explorer/{reportId}/download_csv`, `POST /api/rules_explorer/{reportId}/download_json`, or `GET /api/rules_explorer/{reportId}/result`.

Rule Attribute Columns

The following table describes the codes to use in the API for each report column.

Report column name	Code
Rule_ID	ID
Rule_UUID	UUID
Attribute_Name	N
Attribute_Rule	R

(Continued)

Report column name	Code
Attribute_Enabled	EN
Attribute_Action	A
Attribute_Response	RE
Attribute_Creation_Date	CD
Attribute_Modification_Date	MD
Attribute_Group	GR
Attribute_Type	T
Attribute_Notes	NO
Attribute_Offense_Type	OT
Attribute_Triggered	TG
Attribute_First_Triggered	FTG
Attribute_Last_Triggered	LTG
Test_Definition	TD
Event_Name	E
Event_Description	ED

(Continued)

Report column name	Code
Low_Level_Category	LLC
Rule_Category	RC
Rule_Origin	RO
Response_Details	RED
Action_Details	AD
UBA_Risk	URSK

Content Extension Columns

The following table describes the codes to use in the API for each report column.

Report column name	Code
Not_Installed_CE	NI
Content_Extension_name	CEN
Content_Extension_Category	CEG

Test Columns

The following table describes the codes to use in the API for each report column.

Report column name	Code
Log_Source_Type	LST
IP	IPC
Port	PR
Reference_Set	RS
Reference_Set_With_Number_Of_Elements	RSS
Xforce	XF
Network_Hierarchy	NH
Network_Hierarchy_And_Context	NHC
Network	NT
End_Point	EP
Custom_Property	CP
Domain	DOM
Reference_Data	RD
Log_Source	LS
QID_IDs	QID
Category_IDs	CAT

(Continued)

Report column name	Code
Errors	ER
GEO	GEO
Ariel_Search	ARL
Threshold	THR
Log_Source_Group	LSG
Log_Source_Type_ID	LST_ID
Log_Source_Type_RO	LST_RO

MITRE Columns

The following table describes the codes to use in the API for each report column.

Report column name	Code
Tactic	TAC
Technique	TEC
Sub_Technique	STEC
Tactic_RO	TAC_RO

(Continued)

Report column name	Code
Sub_Technique_RO	STEC_RO
Mapping_Enabled	MAP_EN
Mapping_Confidence	MAP_C
Tactic_ID	TAC_ID
Technique_ID	TEC_ID
Sub_Technique_ID	STEC_ID
Mapping_Source	MAP${SOURCE_COLUMN_SUFFIX}

Offense Columns

The following table describes the codes to use in the API for each report column.

Report column name	Code
Description	OD
Type	TP
Type_Value	TV
Status	ST

(Continued)

Report column name	Code
Event_Count	EC
Offense_ID	OID

Rule Activity Columns

The following table describes the codes to use in the API for each report column.

Report column name	Code
First_Triggered	FTG
Last_Triggered	LTG