IBM Professional Certification Program

Study Guide Series

Exam C1000-139

IBM Security QRadar SIEM V7.4.3 Analysis

Purpose of Exam Objectives

When a certification exam is being developed, a team of Subject Matter Experts work together to define the job role the certified individual will fill. They define all the tasks and knowledge that an individual would need know to successfully perform that role. This creates the foundation for the objectives and measurement criteria, the foundation of the certification exam. The Certification item writers used these objectives write questions that appear on the exam.

It is recommended that you review these objectives carefully. Do you know how to complete the tasks in the objective? Do you know why that task needs to be done? Do you know what will happen if you do it incorrectly? If you are not familiar with a task, then work through the objective and perform that task in your own environment. Read more information about the task. If there is an objective on a task, it is almost certain that you WILL see questions about it on the actual exam.

After you have reviewed the objectives and completed your own research, don't forget to review the free sample questions for this exam on the IBM Certification website. These sample questions come complete with an answer key and will give you a feel for the type and style of question on the actual exam.

After that, take the assessment exam. The questions on the assessment exam were developed at the same time and by the same people who wrote the questions on the actual exam. The assessment exam is weighted to be equally difficult to the actual test so your results should be predictive of your expected results on the actual test. While the assessment exam will not tell which questions are answered incorrectly, it will tell you how you did on a section-by-section basis so you will know where to focus your further studies.

Contents

Role Definition

This intermediate level certification is intended for security analysts who wish to validate their comprehensive knowledge of IBM Security QRadar SIEM V7.4.3.

These security analysts will understand basic networking, basic IT security, SIEM and QRadar concepts. They will also understand how to log in to, navigate within, and explain capabilities of the product using the graphical user interface. Additionally, they will also be able to identify causes of offenses, and access, interpret, and report security information in a QRadar deployment.

Note: The function of specific apps, apart from those bundled with the product, is out of scope, but the concept of extending the capability of using apps is in scope.

Key Areas of Competency

- Offense and log analysis
- Understanding reference data
- Rule and building block understanding
- Searching and reporting, regular and adhoc reports
- Understanding basic QRadar tuning and network hierarchy
- Basic concepts of multi-domain QRadar instances

Prerequisite Knowledge

Knowledge and foundational skills one must possess before acquiring skills measured on the certification test. These foundational skills are NOT measured on the test.

- Knowledge of SIEM concepts
- Knowledge of TCP/IP Networking
- Knowledge of IT Security concepts
- General IT skills (browser navigation etc...)
- Knowledge of Internet security attack types, including but not limited to the MITRE ATT&CK Framework
- Additional features that need additional licenses including but not limited to QRadar Network Insights, QRadar Incident Forensics

Section 1: Offense Analysis

QRadar uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected. But knowing that an offense occurred is only the first step. Offense Analysis is all about initially identifying how it happened, where it happened, and who are the players involved in the offense.

This section accounts for approximately 26% of the exam.

TASK: 1.1 Triage initial offense

SUBTASKS:

1.1.1 Open an offense to view the details
-- Identify the status of the offense
-- Identify the last event/flow contributed to the offense

1.1.2 Review offense source and destination
-- Identify the attack based on description.
-- Using source IP and location, identify the source or origin of the attack
-- Identify the destination IPs or target system involved in the attack.

1.1.3 Review vulnerability and evidence
-- Check the vulnerability status of the targets
-- Identify the events associated or contributed to the offense
-- If the offense is validated as false positive, close the offense with the appropriate closing reason

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=management-offense-investigations
- https://www.ibm.com/docs/en/qsip/7.4?topic=retention-protecting-offenses
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-offense-chaining
- https://www.ibm.com/support/pages/qradar-information-about-offense-duration-retention-and-activity
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=indexing-example-detecting-malware-outbreaks-based-md5-signature

TASK: 1.2 Analyze fully matched and partially matched rules

SUBTASKS:

1.2.1 From the Offense Summary, In Event/Flow Count, click on the events/flows to view all the contributed logs.
-- Analyze the different types of events by event name, low level category, high level category

1.2.2 Select the event that can provide more evidence for the offense
-- In the Event details -> Additional Information -> look for custom rule and custom rules partially matched

1.2.3 Analyze the rules and building blocks contributed/triggered the offense

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=siem-rules
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-offense-chaining
- https://www.ibm.com/docs/en/qsip/7.4?topic=monitoring-viewing-event-details
- https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-flows
- https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-events
- https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-offense-by-using-summary-information

TASK: 1.3 Analyze an offense and associated IP addresses

SUBTASKS:

1.3.1 Analyze Associated IPs of an Offense
-- Go to Offenses tab- Read The offense information listed in the Table
-- Double click on the offense to open it
-- In the offense Read the information about the offense
-- In the Source IP(s)/Destination IP(s) fields investigate the IPs associated, use right click options to determine the following:
--- DNS Lookup
--- WHOIS Lookup
--- X-Force Exchange Lookup

REFERENCES:

- https://www.ibm.com/docs/en/qradar-on-cloud?topic=siem-offense-management
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=management-offense-investigations
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=procedures-investigating-ip-addresses
- https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-offense-by-using-summary-information

TASK: 1.4 Recognize MITRE threat groups and actors

SUBTASKS:

1.4.1 Open a Offense for investigation -- Select the rules contributing to offense by Clicking Display and Select Rules.
-- Open the rule and review the MITRE threat from the rule and rule notes

1.4.2 Open a Offense for investigation -- Select the rules contributing to offense by Clicking Display and Select Annotations.
-- Review the annotations to understand rule intent and MITRE threat

1.4.3 Use Case Manager to determine MITRE Threat group
-- Open Use Case Manager App
-- Select ATT&CK Actions -> Coverage Map and Report
-- Review the rules and the corresponding MITRE threat group

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=siem-rules
- https://www.securitylearningacademy.com/course/view.php?id=5143
- https://www.securitylearningacademy.com/course/view.php?id=5325
- https://www.ibm.com/docs/pl/qradar-common?topic=app-mitre-attck-mapping-visualization

TASK: 1.5 Perform offense management

SUBTASKS:

1.5.1 Prioritize the offenses
-- Click the offenses tab.
-- Double click on the magnitude field of the list to arrange the offenses by magnitude

1.5.2 Assign an offense.
-- Click the Offenses tab.
-- Select the offense that you want to assign.
-- To assign multiple offenses, hold the Control key while you select each offense.
-- From the Actions list, select Assign.
-- In the Assign To User list, select the user that you want to assign this offense to.
-- Click save.

1.5.3 Document an offense.
-- Click the Offenses tab. Select the offense to which you want to add the note.
-- To add the same note to multiple offenses, press the Ctrl key while you select each offense.
-- From the Actions list, select Add Note.
-- Type the note that you want to include for this offense.
-- Click Add Note.

1.5.4 Send Email notifications from an offense
-- Click the Offenses tab.
-- Select the offense for which you want to send an email notification.
-- From the Actions list box, select Email.
-- Configure the following parameters:
--- To:
--- From:
--- Email Subject:
--- Email Message:
-- Click Send.

1.5.5 Hide an offense
-- Click the Offenses tab.- Select the offense that you want to hide.
-- To hide multiple offenses, hold the Control key while you select each offense.
-- From the Actions list box, select Hide.
-- Click OK.

1.5.6 Show a hidden offense.
-- Click the Offenses tab
-- To clear the filter on the offense list, click Clear Filter next to the Exclude Hidden Offenses search parameter.
-- To create a new search that includes hidden offenses, follow these steps:
--- From the Search list box, select New Search.
--- In the Search Parameters window, clear the Hidden Offenses check box in the Exclude options list.
--- Click Search.
-- To remove the hidden flag from an offense:

--- Select the offense for which you want to remove the hidden flag. To select multiple offenses, hold the Control key while you click each offense.
--- From the Actions list box, select Show.

1.5.7 Close an offense.
-- Click the Offenses tab.
-- Select the offense that you want to close.
--- To close multiple offenses, hold the Control key while you select each offense.
-- From the Actions list, select Close.
-- In the Reason for Closing list, specify a closing reason.
--- To add a close reason, click the icon beside Reason for Closing to open the Custom Offense Close Reasons dialog box.
-- Optional: In the Notes field, type a note to provide more information.
--- The Notes field displays the note that was entered for the previous offense closing. Notes must not exceed 2,000 characters.

1.5.8 Mark up an offense for follow up.
-- Click the Offenses tab.
-- Find the offense that you want to mark for follow-up.
-- Double-click the offense.
-- From the Actions list, select Follow up.

1.5.9 Protect an offense for follow up.
-- Click the Offenses tab and click All Offenses.
-- Choose one of the following options:
---Select the offense that you want to protect, and then select Protect from the Actions list.
--- From the Actions list box, select Protect Listed.
-- Click OK.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=management-offense-prioritization
- https://www.ibm.com/docs/en/qsip/7.4?topic=actions-assigning-offenses-users
- https://www.ibm.com/docs/en/qsip/7.4?topic=actions-adding-notes
- https://www.ibm.com/docs/en/qsip/7.4?topic=actions-sending-email-notifications
- https://www.ibm.com/docs/en/qsip/7.4?topic=actions-hiding-offenses

- https://www.ibm.com/docs/en/qsip/7.4?topic=actions-closing-offenses
- https://www.ibm.com/docs/en/qsip/7.4?topic=actions-marking-offense-follow-up
- https://www.ibm.com/docs/en/qsip/7.4?topic=retention-protecting-offenses

TASK: 1.6 Describe the use of the magnitude of an offense

SUBTASKS:

1.6.1 Review offense by magnitude
-- Open the offense tab
-- Review the offense by magnitude by hovering on magnitude column
-- select an offense with highest magnitude or magnitude with high severity

1.6.2 Review offense with high magnitude
-- Review the severity, relevance and credibility contributing to the magnitude of the offense
-- Review other contributing factors for the offense magnitude rating
--- Number of events
--- Number of Log Sources
--- Age of the offense
--- Weight of the assets

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.3.3?topic=management-offense-prioritization

TASK: 1.7 Identify events not correctly parsed and their source (Stored events)

SUBTASKS:

1.7 1 Identify Unknown Events
-- Click Log Activity Tab
-- Add a filter for High Level Category - Unknown

1.7.2 Select a timeline for last 30 mins based on the load.

1.7.3 Review and recommend parsing and mapping of unknown and stored events

REFERENCES:

- https://www.youtube.com/watch?v=GgPW5OVwoMY
- https://www.ibm.com/docs/en/qsip/7.4?topic=data-routing-options-rules
- https://www.ibm.com/docs/en/dsm?topic=management-troubleshooting-dsms
- https://www.ibm.com/docs/en/qsip/7.4?topic=appliances-events-routed-directly-storage

- https://www.ibm.com/docs/en/qsip/7.4?topic=appliances-maximum-events-flows-reached
- https://www.reddit.com/r/QRadar/comments/fpwvv4/events_with_stored_category_even_being_parsed/

TASK: 1.8 Outline simple offense naming mechanisms

SUBTASKS:

1.8.1 Review offense names
-- Open offense tab
-- Review different Description column of offense and the rule associated with offense

1.8.2 Review rules to manage offense names
-- Select Display -> Rules from Offense summary
-- Review the rule name and Offense description
-- Click and open the rule and go to Rule Response and review offense naming

1.8.3 Change offense naming
-- If the offense description does not explain the attack properly, dispatch a new event with information
-- Use the event information to set or replace the name of the associated offense.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-creating-custom-rule
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-anomaly-detection

TASK: 1.9 Create customized searches

SUBTASKS:

1.9.1 Search offenses on my offenses / all offenses page
-- Click the Offenses tab.
-- From the Search list box, select New Search.
-- Choose one of the following options:
-- Select a previously saved search using one of the following options:
  --- From the Available Saved Searches list, select the saved search that you want to load.
  --- In the Type Saved Search or Select from List field, type the name of the search you want to load.
-- Click Load.
-- Click Search.

1.9.2 Search offenses on my offenses / all offenses page creating a new search
-- Click the Offenses tab.
-- From the Search list box, select New Search.
-- On the Time Range pane, select an option for the time range you want to capture for this search.
-- On the Search Parameters pane, define your specific search criteria.

-- On the Offense Source pane, specify the offense type and offense source you want to search:

--- From the list box, select the offense type that you want to search for.

--- Type your search parameters.

-- In the Column Definition pane, define the order in which you want to sort the results:

--- From the first list box, select the column by which you want to sort the search results.

--- From the second list box, select the order that you want to display for the search results. Options include Descending and Ascending.

-- Click Search.

1.9.3 Search offenses by source IP.

-- Click the Offenses tab.

-- Click by Source IP. - From the Search list box, select New Search.

-- On the Time Range pane, select an option for the time range you want to capture for this search.

-- On the Search Parameters pane, define your specific search criteria.

-- On the Column Definition pane, define the order in which you want to sort the results:

--- From the first list box, select the column by which you want to sort the search results.

--- From the second list box, select the order that you want to display for the search results. Options include Descending and Ascending.

-- Click Search.

1.9.4 Search offenses by destination IP

-- Click the Offenses tab.

-- On the navigation menu, click By Destination IP.

-- From the Search list box, select New Search.

-- On the Time Range pane, select an option for the time range you want to capture for this search.

-- On the Search Parameters pane, define your specific search criteria.

-- On the Column Definition pane, define the order in which you want to sort the results:

--- From the first list box, select the column by which you want to sort the search results.

--- From the second list box, select the order in which you want to display the search results. Options include Descending and Ascending.

-- Click Search.

1.9.5 Saving Search criteria on the offenses tab

-- Perform a search. See Offense searches.

-- Click Save Criteria.

-- Enter values for the following parameters

--- Search Name

--- Manage Groups

--- Time span options (all offenses, Recent, Specific Interval)

--- Set as Default (to make the search a default search)

-- Click OK

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.3.2?topic=searches-scheduled-search
- https://www.ibm.com/docs/en/qsip/7.4?topic=investigation-exporting-events
- https://www.ibm.com/docs/en/qsip/7.4?topic=searches-quick-filter-search-options
- https://www.ibm.com/docs/en/qsip/7.3.2?topic=searches-advanced-search-options
- https://www.ibm.com/docs/en/qsip/7.3.2?topic=searches-creating-customized-search
- https://www.ibm.com/docs/en/qsip/7.4?topic=os-searching-offenses-by-source-ip-page-offense-tab
- https://www.ibm.com/docs/en/qsip/7.4?topic=searches-searching-offenses-my-offenses-all-offenses-pages
- https://www.ibm.com/docs/en/qsip/7.4?topic=SS42VS_7.4/com.ibm.qradar.doc/t_qrm_ug_man_srch_rslts.html
- https://www.ibm.com/docs/en/qsip/7.4?topic=os-saving-search-criteria-offenses-tab-that-you-can-reuse-future-searches

Section 2: Rules and Building Block Design

QRadar rules are applied to all incoming events, flows, or offenses to search for or detect anomalies. If all the conditions of a test are met, the rule generates a response. A building block is a collection of tests that don't result in a response or an action. A building block groups commonly used tests to build complex logic so that it can be reused in rules. As an Analyst you need to fully understand how rules and building blocks are designed and used, and although you are not responsible for implementing new or tuning existing rules and building blocks, you can and should make recommendations on updating QRadar components that may improve rules and building block design based on your daily exposure to them.

This section accounts for approximately 26% of the exam.

TASK: 2.1 Interpret rules that test for regular expressions

SUBTASKS:

2.1.1 Open Rule Wizard for the rule to investigate

2.1.2 Identify regular expressions to match patterns of text in the log source file

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=siem-rules
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-rule-performance-visualization
- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-types-reference-data-collections

TASK: 2.2 Create and manage reference sets and populate them with data

SUBTASKS:

2.2.1 Review the types of Reference Data

2.2.2 Investigate reference sets via the GUI

2.2.3 Create, edit, and delete reference sets
-- GUI
-- API
-- Command Line

2.2.4 Understand Building Blocks and reference sets

REFERENCES:

- https://youtu.be/mNyd8FNns_4
- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-types-reference-data-collections
- https://www.ibm.com/docs/en/qsip/7.4?topic=overview-viewing-contents-reference-set
- https://www.ibm.com/docs/en/qsip/7.4?topic=overview-adding-editing-deleting-reference-sets
- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-creating-reference-data-collections-apis
- https://www.ibm.com/docs/en/qsip/7.4?topic=urdiq-creating-reference-data-collections-by-using-command-line
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-configuring-rule-response-add-data-reference-data-collection

TASK: 2.3 Install QRadar Content Packs using the QRadar Assistant App

SUBTASKS:

2.3.1 Navigating to the QRadar Assistant App

2.3.2 Search for Content Packs

2.3.3 Install Content Packs

REFERENCES:

- https://www.ibm.com/docs/en/qradar-common?topic=app-downloading-apps
- https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-assistant-app

TASK: 2.4 Analyze rules that use Event and Flow data

SUBTASKS:

2.4.1 Identify the types of rules
-- Event
-- Flow

-- Common

2.4.2 Understand Event Rule Parameters

2.4.3 Understand Flow Rule Parameters

2.4.4 Understand Common Rule Parameters

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=siem-rules
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-custom
- https://www.ibm.com/support/pages/qradar-support-geodata-faq
- https://www.ibm.com/docs/en/qsip/7.4?topic=overview-qradar-rules
- https://www.ibm.com/docs/en/qsip/7.4?topic=tasks-network-hierarchy
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-anomaly-detection
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-creating-custom-rule
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-offense-chaining
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-offense-prioritization
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-configuring-event-flow-as-false-positive
- https://www.ibm.com/docs/en/qsip/7.4?topic=content-installing-extensions-by-using-extensions-management

TASK: 2.5 Analyze Building Blocks: Host definition, category definition, Port definition

SUBTASKS:

2.5.1 Identify Host Definition
-- From Log Activity tab -> Rules
-- Select Building Blocks from Display
-- Search for HostDefinition and HostReference
-- Review the configuration of hosts

2.5.2 Identify Port Definition
-- From Log Activity tab -> Rules
-- Select Building Blocks from Display
-- Search for Port Definition
-- Review the configuration of hosts

2.5.3 Identify Building Block definitions and tuning opportunities
-- Host Definitions
-- Port Definitions
-- False Positive Definitions
-- Network Definitions
-- Compliance Definitions

2.5.4 View of Building Blocks and reference sets

REFERENCES:

- https://youtu.be/mNyd8FNns_4
- https://www.youtube.com/watch?v=xhrYeD3Pxiw
- https://www.youtube.com/watch?v=UmKMbfmjqKQ
- https://socprime.com/blog/creating-rules-in-ibm-qradar/
- https://www.securitylearningacademy.com/enrol/index.php?id=3384
- https://www.ibm.com/docs/en/qsip/7.4?topic=blocks-tuning-building
- https://www.ibm.com/support/pages/qradar-defining-qradar-flow-bias
- https://www.ibm.com/docs/en/qsip/7.4?topic=phase-qradar-building-blocks
- https://www.ibm.com/docs/en/qradar-common?topic=tuning-reviewing-building-blocks
- https://www.ibm.com/docs/en/SS42VS_7.4/com.ibm.qradar.doc/b_qradar_tuning_guide.pdf
- https://www.ibm.com/docs/en/qradar-common?topic=app-investigating-qradar-rules-building-blocks
- https://www.ibm.com/docs/en/qradar-common?topic=blocks-filtering-rules-building-by-their-properties
-

TASK: 2.6 Review and recommend updates to the network hierarchy

SUBTASKS:

2.6.1 Organize systems and networks by roles or similar traffic patterns in the network hierarchy

2.6.2 Combine multiple CIDRs or subnets into a single network group

2.6.3 Consider using the most effective method to viewing network activity.

-- Net Hierarchy does not need to resemble the physical deployment.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=hierarchy-acceptable-cidr-values
- https://www.ibm.com/docs/en/qsip/7.4?topic=configuration-network-hierarchy
- https://www.ibm.com/docs/en/qsip/7.4?topic=nh-defining-your-network-hierarchy
- https://www.ibm.com/docs/en/qsip/7.4?topic=hierarchy-guidelines-defining-your-network

TASK: 2.7 Review and recommend updates to building blocks and rules

SUBTASKS:

2.7.1 Review active rules that generates offenses

-- From QRadar, use Case Manager, Click Active Rules

-- Apply filters to active rules to fine-tune the investigation

--- Filter rules that contribute to offense by time frame

--- Select parameters to exclude offenses from results

--- Select the closure reason for an offense as filters

--- Review offense by rule

2.7.2 Apply Filters

-- Apply filters to active rules to fine-tune the investigation

--- Filter rules that contribute to offense by time frame

--- Select parameters to exclude offenses from results

--- Select the closure reason for an offense as filters

--- Click Apply Filters

2.7.3 Review by rule, by category and rule, and by closed reason

-- Hover over the chart segments to see more details about an offense,

--- Hide of show chart legends

--- Click legend keys to fine-tune chart display

--- Zoom in for further investigation

2.7.4 Tune the rules by choosing the following methods:

-- Toggle between the top noisy rules or all the rules from the list

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

REFERENCES:

- https://www.ibm.com/docs/en/qradar-common?topic=app-video-demonstrations
- https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-use-case-manager-app
- https://www.ibm.com/docs/en/qradar-common?topic=tuning-active-rules-that-generate-offenses
- https://www.ibm.com/docs/en/qradar-common?topic=tuning-active-rules-that-generate-cre-events

TASK: 2.8 Describe the different types of rules, including behavioral, anomaly and threshold rules

SUBTASKS:

2.8.1 Understand the types of rule behaviors
-- Anomaly
-- Behavior
-- Threshold

2.8.2 Understand how an Anomaly rule is created and how that is different than a Custom Rule

2.8.3 Create behavior, anomaly and threshold rules in QRadar

REFERENCES:

- https://www.youtube.com/watch?v=LgksZvchS38
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-custom
- https://www.ibm.com/docs/en/qsip/7.4?topic=overview-qradar-rules
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-anomaly-detection
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-creating-anomaly-detection-rule
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-configuring-event-flow-as-false-positive
- https://www.ibm.com/docs/en/qsip/7.4?topic=rules-configuring-rule-response-add-data-reference-data-collection

Section 3: Threat Hunting

After the initial Offense Analysis and based on technical skills in understanding QRadar rules and building block design, it is time to focus on the Analyst's main task of Threat Hunting. Starting with the results presented in an offense, the Analyst will investigate the evidence inside an offense, such as event and flow details, triggered rules, payloads, and more. Utilizing filters and advanced searches the Analyst will be able to distinguish real threats from false positives.

This section accounts for approximately 26% of the exam.

TASK: 3.1 Investigate Event and Flow parameters

SUBTASKS:

3.1.1 Investigate Event details
-- In the Offense Summary window, click Events. The List of Events window shows all events that are associated with the offense.
-- Specify the Start Time, End Time, and View options to view events that occurred within a specific time frame.

-- Click the event column header to sort the event list.
-- In the list of events, right-click the event name to apply quick filter options to reduce the number of events to review. You can apply quick filters to other columns in the event list as well.
-- Double-click an event to view the event details. The Event Information and the Source and Destination Information window show only the information that is known about the event. Depending on the type of event, some fields might be empty.
-- Learn more about the time fields on the Event Information:
--- Field
--- Description
--- Start Time
--- The time that QRadar received the raw event from the log source.
--- Storage Time
--- The time that QRadar stored the normalized event.
--- Log Source Time
--- The time that is recorded in the raw event from the log source.
-- In the Payload Information box, review the raw event for information that QRadar did not normalize. Information that is not normalized does not appear in the QRadar interface, but it may be valuable to your investigation.

3.1.2 Investigate Flow details
-- In the Offense Summary window, click Flows in the upper right menu. The Flow List window shows all flows that are associated with the offense.
-- Specify the Start Time, End Time, and View options to view flows that occurred within a specific time frame.
-- Click the flow column header to sort the flow list.
-- In the list of flows, right-click the flow name to apply quick filter options to reduce the number of flows to review. You can apply quick filters to other columns in the flow list as well.
-- Double-click a flow to review the flow details.
-- Learn more about the flow details:
--- Event Description
---- When the application is not identified in the payload, QRadar uses built-in decoding to determine the application, and shows Application detected with state-based decoding in Event Description.
--- Source Payload and Destination Payload
---- Shows the size of the payload.
---- When the size exceeds 64 bytes, the payload might contain additional information that is not shown in the QRadar interface.
--- Custom Rules Partially Matched
---- Shows rules for which the threshold value was not met, but otherwise the rule matched.
--- Flow Direction
----Specifies the flow direction, where L indicates local network, and R indicates remote network.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=events-investigating

- https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-flows

TASK: 3.2 Perform AQL query

SUBTASKS:

3.2.1 Perform detailed searches to find similar log and flow activity at any level of granularity:
-- On the QRadar Log and Network Activity tabs, select "Advanced" in the list beside the search field.
-- Enter an AQL query and click Search

3.2.2 Understand the AQL and QRadar interfaces

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=aql-query-structure
- https://www.ibm.com/docs/en/qsip/7.4?topic=language-time-criteria-in-aql-queries
- https://www.ibm.com/docs/en/qsip/7.4?topic=language-aql-logical-comparison-operators
- https://www.ibm.com/docs/en/qsip/7.4?topic=aql-ariel-query-language-in-qradar-interface

TASK: 3.3 Search & filter logs by specific log source type

SUBTASKS:

3.3.1 Searching events:
-- Click the Log Activity tab.
-- On the toolbar, select Search > New Search.
-- In the Time Range pane, define the time range for the event search:
--- Click Recent.
--- In the Recent list, select Last 6 Hours.
-- In the Search Parameters pane, define the search parameters:
--- In the first list, select Category [Indexed].
--- In the second list, select Equals to.
--- In the High-Level Category list, select Authentication.
--- In the Low-Level Category list, accept the default value of Any.
--- Click Add Filter.
-- In the Column Definition pane, select Event Name in the Display list and drag it to the Columns list.
-- Click Search.

3.3.2 Filtering Events:
-- To apply a filter, click any of the following categories to see filtering options for that category:
--- Event Time
--- Magnitude
--- Log Source Name
--- Category
--- Source IP

--- Source Port
--- Destination IP
--- Destination Port
--- Event Name
--- User
-- To include only events with specific attributes, select that attribute in the filters list. To exclude events with specific attributes, click the vertical ellipsis icon next to the attribute, and click Apply IS NOT Filter.
Tip: You can right-click on a Log Source, Source IP, Destination IP, Category, or Username in the events table and quickly apply an IS or IS NOT filter to the events.
-- To sort the events table in ascending or descending order by an attribute, click the appropriate table heading.
-- To clear individual filters, click the close icon [x] on the filter indicator. To clear all filters, click Clear filters.
-- Click Update events to refresh the events results.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-searching-events
- https://www.ibm.com/docs/en/qsip/7.4?topic=events-filtering

TASK: 3.4 Configure a search to utilize time series

SUBTASKS:

3.4.1 Create a time series graph:
-- Click the Log Activity or Network Activity tab.
-- To create a grouped search, follow these steps:
--- On the toolbar, click Search > New Search.
--- From the Available Saved Searches, select a search and click Load.
--- Go to the Column Definition pane and if the Group By list box is empty, from the Available Columns list, select a column.
--- Click Search.
--- To use a grouped search, on the toolbar, click Quick Searches and select a grouped search.
--- In the Charts pane, click the Configure icon ().
--- Configure the following parameters:
-- Value to Graph
--- The object type that you want to graph on the Y axis of the chart.
--- Options include all normalized and custom event or flow parameters that are included in your search parameters.
-- Display Top
--- The number of objects that you want to view in the chart. The default is 10. If you include more than 10 items in your chart, your data might be illegible.
-- Chart Type

--- If your bar, pie, or table chart is based on saved search criteria with a time range of more than 1 hour, you must click Update Details to update the chart and populate the event details.
-- Capture Time Series Data
--- Enables time series data capture. When you select this check box, the chart begins accumulating data

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-configuring-time-series-chart
- https://www.ibm.com/docs/en/qradar-common?topic=app-time-series-charts-in-qradar-pulse
- https://www.ibm.com/docs/en/qradar-common?topic=adctsc-part-1-creating-aggregated-data-view-in-log-activity-tab

TASK: 3.5 Analyze potential IoCs

SUBTASKS:

3.5.1 Repeat Event and Flow analysis.

3.5.2 Review IoC reference sets

REFERENCES:

- https://www.securitylearningacademy.com/course/view.php?id=4975
- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-reference-sets-overview
- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-types-reference-data-collections
- https://www.ibm.com/docs/en/qsip/7.4?topic=iauc-finding-ip-address-url-information-in-x-force-exchange

TASK: 3.6 Break down triggered rules to identify the reason for the offense

SUBTASKS:

3.6.1 Investigate Event details
-- In the Offense Summary window, click Events.
The List of Events window shows all events that are associated with the offense.
-- Specify the Start Time, End Time, and View options to view events that occurred within a specific time frame.
-- Click the event column header to sort the event list.
-- In the list of events, right-click the event name to apply quick filter options to reduce the number of events to review. You can apply quick filters to other columns in the event list as well.
-- Double-click an event to view the event details.
The Event Information and the Source and Destination Information window show only the information that is known about the event. Depending on the type of event, some fields might be empty.
-- Scroll down below the payload to view a list of rules that the event triggered.

-- Click on each rule to determine how the event triggered it.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=monitoring-viewing-event-details
- https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-events
- https://www.ibm.com/docs/en/qradar-common?topic=tuning-active-rules-that-generate-offenses
- https://www.ibm.com/support/pages/qradar-event-details-and-difference-between-start-time-storage-time-and-log-source-time

TASK: 3.7 Recommend changes to tune QRadar SIEM after offense analysis identifies issues

SUBTASKS:

3.7.1 Review Source and destination IP addresses

3.7.2 Look for remote to remote (R2R) events

3.7.3 Look for potential building block issues

3.7.4 **All covered in event investigation, above

REFERENCES:

- none

TASK: 3.8 Distinguish potential threats from probable false positives

SUBTASKS:

3.8.1 Distinguish potential threats from probable false positives

-- Click the Log Activity tab.

-- Optional. If you are viewing events in streaming mode, click the Pause icon to pause streaming.

-- Select the event that you want to tune.

-- Click False Positive.

-- In the Event/Flow Property pane on the False Positive window, select one of the following options:

--- Event/Flow(s) with a specific QID of <Event>

--- Any Event/Flow(s) with a low-level category of <Event>

--- Any Event/Flow(s) with a high-level category of <Event>

-- In the Traffic Direction pane, select one of the following options:

--- <Source IP Address> to <Destination IP Address>

--- <Source IP Address> to Any Destination

--- Any Source to <Destination IP Address>

--- Any Source to any Destination

--- Click Tune.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=tasks-network-hierarchy
- https://www.ibm.com/docs/en/qsip/7.4?topic=performance-tuning-false-positives
- https://www.ibm.com/docs/en/qsip/7.4?topic=phase-guidelines-tuning-system-performance#c_tuning_guide_tuning_tuning_methodology

TASK: 3.9 Add a reference set based filter in log analysis

SUBTASKS:

3.9.1 This task is covered under Search & filter logs task.

3.9.2 Add a reference set based filter in log analysis
-- On the navigation menu, click Admin.
-- In the System Configuration section, click Reference Set Management.
-- To add a reference set:
--- Click Add and configure the parameters.
--- Learn more about reference set parameters: The following table describes each of the parameters that are used to configure a reference set.
-- Name
--- The maximum length of the reference set name is 255 characters.
-- Type
--- Select the data types for the reference elements. You can't edit the Type parameter after you create a reference set. The IP type stores IPv4 addresses. The Alphanumeric (Ignore Case) type automatically changes any alphanumeric value to lowercase. To compare obfuscated event and flow properties to the reference data, you must use an alphanumeric reference
-- Time to Live of elements
---Specifies when reference elements expire. If you select the Lives Forever default setting, the reference elements don't expire. If you specify an amount of time, indicate whether the time-to-live

interval is based on when the data was first seen, or was last seen. QRadar removes expired elements from the reference set periodically (by default, every 5 minutes).
-- When elements expire
--- Specifies how expired reference elements are logged in the qradar.log file when they are removed from the reference set. The Log each element in a separate log entry option triggers an Expired ReferenceData element log event for each reference element that is removed. The event contains the reference set name and the element value. The Log elements in one log entry option triggers one Expired ReferenceData element log event for all reference elements that are removed at the same time. The event contains the reference set name and the element values. The Do not log elements option does not trigger a log event for removed reference elements.
--- Click Create.
--- Click Edit or Delete to work with existing reference sets.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-reference-sets-overview
- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-types-reference-data-collections
- https://www.ibm.com/docs/en/qsip/7.4?topic=overview-viewing-contents-reference-se

TASK: 3.10 Investigate the payload for additional details on the offense

SUBTASKS:

3.10.1 Investigate flows

3.10.2 Determine what sort of things to use from payload.

-- AQL searches for parameters that "do not match" to identify potential new custom entries.

REFERENCES:

- https://regex101.com/
- https://www.ibm.com/docs/en/qsip/7.4?topic=content-importing-yara-rules
- https://www.ibm.com/docs/en/qradar-common?topic=extensions-blue-coat
- https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-flows
- https://www.ibm.com/docs/en/qsip/7.4?topic=administration-managing-suspicious-content

TASK: 3.11 Recommend adding new custom properties based on payload data

SUBTASKS:

3.11.1 Review the payload.

-- See what's left after you exclude known entities from payload.

-- Do this with AQL?

3.11.2 Custom property management

-- Click the Log Activity tab or the Network Activity tab.

-- If you are viewing the events or flows in streaming mode, click the Pause icon to pause streaming.

-- Double-click the event or flow that contains the data that you want to extract, and then click Extract Property.

-- In the Property Type Selection pane, select the type of custom property that you want to create.

-- Configure the custom property parameters.

-- Click the help icon to see information about the custom property parameters.

-- If you are creating an extraction-based custom property that is to be used in rules, search indexes, or forwarding profiles, ensure that the Parse in advance for rules, reports, and searches check box is selected.

-- Optional: Click Test to test the expression against the payload.

-- Click Save.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=properties-creating-custom-property

TASK: 3.12 Perform "right-click Investigations" on offense data

SUBTASKS:

3.12.1 Perform "right-click Investigations" on offense data
-- Open the Log Activity tab.
-- In the Log Activity tab, right-click an event to view options for investigations:
--- Filter on
--- False positive - Select this option to open the False Positive window, which will allow you to tune out events that are known to be false positives from creating offenses. This option is disabled in streaming mode.
--- More options
---- Navigate: View by network, View source summary, View destination summary
---- Information: DNS Lookup, Whois Lookup, Port Scan, Asset profile, Search Events, Search Flows
---- Plugin options: X-Force Exchange Lookup
--- Quick filter - Match or do not match the selection

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=overview-right-click-menu-options
- https://www.ibm.com/docs/en/qsip/7.4?topic=investigation-tuning-false-positives

Section 4: Dashboard Management

Use the QRadar Dashboard tab to focus on specific areas of your network security. The workspace supports multiple dashboards on which you can display your views of network security, activity, or data that is collected. You can use the QRadar Pulse app for an enhanced dashboard experience.

This section accounts for approximately 6% of the exam.

TASK: 4.1 Use the default QRadar dashboard to create, view, and maintain a dashboard based on common searches

SUBTASKS:

4.1.1 Review QRadar Dashboard for Event Category Distribution
-- Open Dashboard Tab
-- Select Compliance Overview dashboard from Show Dashboard drop down.
-- Review the different event category and event count for each.

4.1.2 Add Most Severe Offenses in System Monitoring Dashboard
-- Open System Monitoring from show dashboard drop down
-- Click Add Item -> Offenses -> Offenses -> Most Server Offenses

4.1.3 Delete Dashboard
-- From the Dashboard tab, select the dashboard from Show Dashboard drop down that need to be deleted.
-- Click Delete Dashboard

4.1.4 Configure Time Series Chart
-- In chart title bar, click configure icon
In value to graph, select Destination IP(Unique Count)
In Chart Type, Select Time Series and Click Save and Click Update Details

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=siem-dashboard-management
- https://www.ibm.com/docs/en/qsip/7.3.3?topic=siem-dashboard-management
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-default-dashboards
- https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-configuring-time-series-chart
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-creating-custom-dashboard
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-managing-system-notifications
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-configuring-dashboard-chart-types

TASK: 4.2 Use Pulse to create, view, and maintain a dashboard based on common searches

SUBTASKS:

4.2.1 Create a New Dashboard and add widgets from searches for monitoring
-- From the Dashboard Tab, Click New Dashboard
-- Click Add Item -> Log Activity -> Top Log Sources
-- Click Add Item --> Log Activity --> Event Searches -> Top Rules

4.2.2 Review Pulse Offense Overview Dashboard
-- Open the pulse app and select Offense overview dashboard from the dashboard drop down.
-- Review Different widgets within the dashboard
--- My Offenses
--- Number of Offenses, Critical Offenses
--- Top Offense Categories
--- Most Server offense

4.2.3 Share Pulse Dashboards
-- Open the dashboard that you want to share and Click Share this dashboard icon
-- Set Has share link to Yes and copy the provided URL
-- Share the URL with other users

4.2.4 Share drill down target dashboards

-- If the shared dashboard drills down to other dashboards, the target dashboards are listed. Select the target dashboards to share.

REFERENCES:

- https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-pulse-app
- https://www.ibm.com/docs/en/qsip/7.3.3?topic=siem-dashboard-management
- https://www.ibm.com/docs/en/qradar-common?topic=app-qradar-pulse-dashboard-components-workspaces
- https://www.ibm.com/docs/en/qradar-common?topic=workspaces-sharing-dashboard-links-others

Section 5: Reporting

The Analyst can create, edit, distribute, and manage reports, including flexible options to satisfy your organization’s various regulatory standards, such as PCI compliance, and offense and threat related reports.

This section accounts for approximately 16% of the exam.

TASK: 5.1 Perform an advanced search

SUBTASKS:

5.1.1 Investigate advanced search options - Ariel Query Language (AQL)
-- Access the Advanced Search option from the Search toolbar that is on the Network Activity and Log Activity tabs to type an AQL query.
--- Select Advanced Search from the list box on the Search toolbar.
--- Expand the Advanced Search field by following these steps:
--- Drag the expand icon that is at the right of the field.
--- Press Shift + Enter to go to the next line.
--- Press Enter.
--- You can right-click any value in the search result and filter on that value.

5.1.2 Query with dynamic search
-- Use of functions like count, SUM, MAX, AVG
--- Click the Admin tab.
--- In the Dynamic Search section, click Dynamic Search.
--- Select a Data Source.
--- Complete the Available Columns and Available Filters sections.
--- To add a name, description, range of the search, retention period, or search type to your query, enable one or more Extra Search Properties.
--- To copy your JSON script, click Generate JSON.
--- Your results appear in the JSON generated by your query section. Click Copy to Clipboard to copy your JSON script.
--- To reset your selections, click Reset.
--- Click Run Query.

REFERENCES:

- https://www.ibm.com/docs/en/qradar-on-cloud?topic=searches-advanced-search-options
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=searches-querying-dynamic-search
- https://www.ibm.com/support/pages/searching-your-qradar-data-efficiently-part-1-quick-filters
- https://www.ibm.com/docs/en/qradar-common?topic=widgets-creating-from-dynamic-query-data-source
- https://info.techdata.com/rs/946-OMQ-360/images/Section 1 - Technical Sales Foundations for IBM QRadar for Cloud (QRoC)V1 P10000-017.pdf

TASK: 5.2 Explain the different uses for each search type

SUBTASKS:

5.2.1 Advance Search

5.2.2 Customized search
-- Search form data that match the criteria by using specific search options
--- Group:

--- Include quick searches
--- Include in dashboard
--- Share with everyone
--- Real time search
--- Specific interval search

5.2.3 Offense search
-- Search offenses by using specific criteria to display offenses that match the search criteria in a results list.
--- Search offenses by source IP
--- Search offenses by destination IP
--- Search offenses by network page
--- Save search criteria
--- Search offenses that are indexed on a custom property

REFERENCES:

- https://www.ibm.com/docs/en/qradar-on-cloud?topic=searches-offense
- https://www.ibm.com/docs/en/qsip/7.4?topic=searches-advanced-search-options
- https://www.ibm.com/docs/en/qsip/7.4?topic=searches-creating-customized-search
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=indexing-offense-considerations
- https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_qradar_sav_search_off_tab.html
- https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_qradar_search_off_by_dest_IP_page.html
- https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_qradar_search_off_by_network_page.html
- https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_qradar_search_off_by_source_IP_page.html
- https://www.ibm.com/docs/en/SSKMKU/com.ibm.qradar.doc/t_qradar_ug_search_by_custom_property.html
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=searches-searching-offenses-by-networks-page-offense-tab

TASK: 5.3 Filter search results

SUBTASKS:

5.3.1 Initiate a Search
-- From Log Activity Tab
--- Click Search -> New Search
--- Select properties to view in the search
--- In the time frame -> select recent -> last 1 hour

5.3.2 Group and Filter by Username
-- From the Search Results
--- Select Username from Display column (This will group results by username)
--- Add Filter for Username Is Not N/A
--- Double click on the top username. (This will filter the results for that username)

5.3.3 Filter by Log Source Type

-- From the search results
--- Click Add Filter
--- Select Log Source Type from the properties
--- Select Microsoft Windows Security Event Log

5.3.4 Filter using Reference Set
-- From the search results
--- Select Reference Set from the Parameter List
--- For Value ->Data Entry -> Select Source IP
--- Operator -> Exists in any of
--- Reference Set -> Malicious IPs

5.3.5 Filter using Regex Expression
-- From the search results
--- Select Username from Parameter
--- Select Matches Expression from Operator
--- Add ^adm* and Click + and Add Filter
--- (This will filter search results with usernames starting with adm)

REFERENCES:

- none

TASK: 5.4 Build threat reports

SUBTASKS:

5.4.1 Create custom reports
-- Report wizard: step-by-step guide on how to design, schedule and generate reports
--- Frequency
--- Configuration of the layout of the report
--- Container configuration (placeholder for the featured content)
--- Distribution channel (for auto reports)

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=management-creating-custom-reports

TASK: 5.5 Perform a quick search

SUBTASKS:

5.5.1 Do a Quick Search

-- Click Log Activity Tab
-- Click Quick Searches drop down
-- Select Event Rate (EPS) - Last 15 Minutes

REFERENCES:

- https://www.ibm.com/support/pages/searching-your-qradar-data-efficiently-part-1-quick-filters
- https://info.techdata.com/rs/946-OMQ-360/images/Section 1 - Technical Sales Foundations for IBM QRadar for Cloud (QRoC)V1 P10000-017.pdf

TASK: 5.6 View the most commonly triggered rules

SUBTASKS:

5.6.1 Use the IBM QRadar Use Case Manager to view and tune the most active rules that create offenses and to tune the rules that generate CRE events

5.6.2 Explore rules through visualization and generated reports

REFERENCES:

- https://www.ibm.com/docs/en/qradar-common?topic=app-video-demonstrations
- https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-use-case-manager-app
- https://www.ibm.com/docs/en/qradar-common?topic=tuning-active-rules-that-generate-offenses
- https://www.ibm.com/docs/en/qsip/7.4?topic=offenses-viewing-rules-that-are-deployed#t_tuning_guide_tuning_viewing_current_config

TASK: 5.7 Report events correlated in the offense

SUBTASKS:

5.7.1 Events that belongs to a specific events

REFERENCES:

- none

TASK: 5.8 Export Search results in CSV or XML

SUBTASKS:

5.8.1 Exporting offenses
-- Export offenses when you want to reuse the data or when you want to store the data externally.
--- Export offenses in Extensible Markup Language (XML)
--- Export Offenses in comma-separated values (CSV)

5.8.2 Exporting Events

-- Export events in Extensible Markup Language (XML) or Comma-Separated Values (CSV) format.
--- Export to XML > Visible Columns - Select this option to export only the columns that are visible on the Log Activity tab.
--- Export to XML > Full Export (All Columns) - Select this option to export all event parameters. A full export can take an extended period of time to complete.
--- Export to CSV > Visible Columns - Select this option to export only the columns that are visible on the Log Activity tab.
--- Export to CSV > Full Export (All Columns) - Select this option to export all event parameters. A full export can take an extended period of time to complete.

REFERENCES:

- https://www.ibm.com/docs/en/qradar-on-cloud?topic=actions-exporting-offenses
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=investigation-exporting-events
- https://www.ibm.com/support/pages/qradar-column-headers-are-not-present-export-csv-option

TASK: 5.9 Create reports and advanced reports out of offenses

SUBTASKS:

5.9.1 Create Search to Show Offense Data
-- From QRadar Web UI, Click Log Activity Tab* Click Search -> Edit Search
-- Under Search Parameters -> Select Associated With Offense Equal True, Select Log Source Type is Custom Rule Engine
-- Click Filter to do the
-- Click Search -> Save Search -> Offense Data

5.9.2 Create report from Saved Search Offense Data
-- Go to Reports and Click Actions -> Create
-- Create a new report using the saved search Offense Data

REFERENCES:

- https://www.ibm.com/support/pages/qradar-creating-search-report-show-offense-data

TASK: 5.10 Share reports with users

SUBTASKS:

5.10.1 Share a report.
-- Click the Reports tab.
-- Select the reports that you want to share.
-- From the Actions list box, click Share.
-- From the list of users, select the users with whom you want to share this report.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=management-sharing-report

TASK: 5.11 Search using indexed and non-indexed properties

SUBTASKS:

5.11.1 Search using indexed and non-indexed properties
-- Indexed Filters
--- Click Log Activity Tab
--- Click Add Filter
--- Review Indexed Properties (Properties with the tag (Indexed) in the end)
--- Add one of the indexed parameter
--- Click Add Filter

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=tasks-index-management
- https://www.ibm.com/docs/en/SS42VS_7.4/com.ibm.qradar.doc/b_qradar_users_guide.pdf

TASK: 5.12 Create and generate scheduled and manual reports

SUBTASKS:

5.12.1 Manually Generate a Report
-- Click the Reports tab.
-- Select the report that you want to generate.
-- Click Run Report

5.12.2 Create a Report.
-- Click the Reports tab.
-- From the Actions list box, select Create.
-- On the Welcome to the Report wizard! window, click Next.
- Select the option "Manually" or Schedule frequency of Hourly, Daily, Weekly or Monthly
-- In the Allow this report to generate manually pane, Select Yes.
-- Configure the layout of your report:
-- From the Orientation list box, select Portrait or Landscape for the page orientation.
-- Select one of the six layout options that are displayed on the Report wizard.
-- Click Next
-- Specify values for the following parameters (Report title, Logo, Pagination options, Report Classification)
-- Configure each container in the report:
--- From the Chart Type list box, select a chart type.
--- On the Container Details window, configure the chart parameter
--- Click Save Container Details.
-- Preview the Layout Preview page, and then click Next.

-- Select the check boxes for the report formats you want to generate, and then click Next.
-- Select the distribution channels for your report, and then click Next. Options include the following distribution channels:
--- Report console, select user, select all users, email, enter the distribution email address(es), include report as attachment, include link to report console
-- On the Finishing Up page, enter values for the following parameters: Report description,
-- Select group for the report to show for, Run the report now.
-- Click Next to view the report summary.
-- On the Report Summary page, select the tabs available on the summary report to preview your report configuration.

5.12.3 Brand a report
-- Click the Reports tab.
-- On the navigation menu, click Branding.
-- Click Browse to browse the files that are located on your system.
-- Select the file that contains the logo you want to upload. Click Open.
-- Click Upload Image.
-- Select the logo that you want to use as the default and click Set Default Image.

REFERENCES:

- https://www.ibm.com/docs/en/qsip/7.4?topic=management-branding-reports
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=management-chart-types
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=management-report-groups
- https://www.ibm.com/docs/en/qsip/7.4?topic=management-creating-custom-reports
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=management-viewing-generated-reports