Duration: 2 Days

Security Incidents and Event Management with QRadar [Foundation]

Module 1 Introduction to IBM Security QRadar SIEM

- Purposes of QRadar SIEM
- QRadar SIEM and the IBM Security Framework
- Identifying suspected attacks and policy breaches
- Providing context
- Key QRadar SIEM capabilities
- QRadar SIEM Console

Module 2 How QRadar SIEM collects security data

- Normalizing log messages to events
- Event collection and processing
- Flow collection and processing
- Reporting
- Asset profiles
- Active scanners
- QRadar Vulnerability Manager scanner
- Gathering asset information

Module 3 Using the QRadar SIEM dashboard

- Navigating the Dashboard tab
- Dashboard overview
- Default dashboard
- QRadar SIEM tabs
- Other menu options
- Context-sensitive help
- Dashboard refresh
- Dashboard variety
- Creating a custom dashboard
- Managing dashboard items

Module 4 Investigating an offense that is triggered by events

- Introduction to offenses
- Creating and rating offenses
- Instructor demonstration of offense parameters
- Selecting an offense to investigate
- Offense Summary window
- Offense parameters
- Top 5 Source IPs
- Top 5 Destination IPs
- Top 5 Log Sources
- Top 5 Users
- Top 5 Categories
- Last 10 Events

- Last 10 Flows
- Annotations
- Offense Summary toolbar
- Lesson 4 Acting on an offense
- Offense actions
- Offense status and flags

Module 5 Investigating the events of an offense

- Navigating to the events
- List of events
- Event details: Base information
- Event details: Reviewing the raw event
- Event details: Additional details
- Returning to the list of events
- Filtering events
- Applying a Quick Filter to the payload
- Using another filter option
- Grouping events
- Grouping events by low-level category
- Removing grouping criteria
- Viewing a range of events
- Monitoring the scanning host
- Saving search criteria
- Event list using the saved search
- About Quick Searches
- Using alternative methods to create and edit searches
- Finding and loading a saved search
- Search actions
- Adding a saved search as a dashboard item
- Saving a search as a dashboard item
- Enabling time-series data
- Selecting the time range
- Displaying 24 hours in a dashboard item
- Modifying items in the chart type table

Module 6 Using asset profiles to investigate offenses

- About asset profiles
- Creating asset profiles
- Navigating from an offense to an asset
- Assets tab
- Asset summary
- Vulnerabilities

Module 7 Investigating an offense that is triggered by flows

- About flows
- Network Activity tab
- Grouping flows
- Finding an offense
- Offense parameters
- Top 5 Source and Destination IPs

- Top 5 Log Sources
- Top 5 Categories
- Last 10 Events
- Last 10 Flows
- Annotations
- Base information
- Source and destination information
- Layer 7 payload
- Additional information
- Creating a false positive flow or event
- Tuning a false positive flow or event

Module 8 Using rules and building blocks

- About rules and building blocks
- About rules
- About building blocks and functions
- Navigating to rules
- Finding the rules that fired for an event or flow
- Finding the rules that triggered an offense
- Rule Wizard demonstration
- Rule Wizard
- Rule actions
- Rule response

Module 9 Creating QRadar SIEM reports

- Reporting introduction
- Reporting demonstration
- Reports tab
- Finding a report
- Running a report
- Selecting the generated report
- Viewing a report
- Reporting demonstration
- Creating a new report template
- Choosing a schedule
- Choosing a layout
- Defining report contents
- Configuring the upper chart
- Configuring the lower chart
- Verifying the layout preview
- Choosing a format
- Distributing the report
- Adding a description and assigning the group
- Verifying the report summary
- Viewing the generated report
- Best practices when creating reports

Module 10 Performing advanced filtering

- Filtering demonstration
- Flows to external destinations
- Remote to Remote flows

- Scanning activity
- Applications not running on the correct port
- Data loss
- Flows to suspect Internet addresses
- Filtering on custom rules and building blocks
- Grouping by custom rules
- Charts on Log and Network Activity tabs: Grouping
- Charts on Log and Network Activity tabs: Time range
- Capturing time-series data
- Viewing time series charts: Zooming to focus