Security Information and Event Management with QRadar (Administration)

Duration – 2 Days

Module 1 Using administration tools

- QRadar SIEM reminder
- Admin tab
- Advanced list options
- About the deployment editor
- Host Context overview
- Configuring Host Context
- Adding a managed host
- Deployment Editor: Configuring collectors
- Auto update overview
- Configuration auto updates: Basic tab
- Configuring auto updates: Advanced tab
- System and license management
- Uploading and allocating a license
- Reverting an allocation unlocks a license
- Replacing a license by allocating a new one
- Activating a license
- Exporting license key information
- Web-based System Administration Interface
- QRadar Console Settings
- QRadar System Settings
- Global System Notifications
- Managing custom offense close reasons
- Authorized services.
- Using authorized services
- Authorized services URLs

Module 2 Creating the network hierarchy

- Network hierarchy overview
- QRadar SIEM network hierarchy
- Network hierarchy recommendations
- Adding a network hierarchy

- Building a group node versus leaf node
- Remote networks and services overview
- Adding a remote networks object
- Managing remote services
- Adding remote services

Module 3 Updated administration tools

- Asset profiles overview
- Server discovery overview
- Importing and exporting assets
- Viewing scanners
- Reference Set overview
- Reference Set elements
- Index management overview
- Enabling indexes

Module 4 Managing users

- User account overview
- Creating user roles
- Security profile overview
- Security profile: Permission Precedence tab
- Security profile: Networks and Log Sources tab
- Editing a security profile
- Configuring authentication

Module 5 Managing data

- Introduction to data backups
- Creating an on-demand configuration backup
- Creating a backup schedule
- Restoring backup archives
- Using event and flow retention buckets
- Configure an event retention bucket
- Configuring flow retention buckets

Module 6 Collecting log and flow records

- Collecting data: Data sources
- Log sources through traffic analysis
- Adding log sources
- Adding log source extensions
- Log source parsing order
- Flow data overview
- Adding a flow source
- Adding a flow source with asymmetric routing
- Flow source aliases

- Adding a flow source alias

Module 7 Collecting Windows log records

- About Windows log collection agents
- WinCollect
- Adaptive Log Exporter (ALE)
- Snare agent
- WMI protocol
- Installing WinCollect
- Creating an authorized service for the WinCollect agent
- Installing the WinCollect agent software
- Applying the machine name, Service Token, and console IP
- Adding a log source to the WinCollect agent
- Installing an Adaptive Log Exporter (ALE) agent
- Configuring the ALE agent
- Configuring the destination

Module 8 Managing custom log sources

- Custom log sources
- Required tools
- Integrating unsupported Log Sources
- Obtaining a sample log
- Obtaining a log sample from a remote location
- Uploading the LSX_Template.xml file
- Creating a universal DSM log source
- Testing the universal DSM log source
- Mapping the unknown log records
- Example of a LEEF log record event category
- Creating a regular expression to extract the log source EventID from a LEEF event
- Creating an appropriate regular expression
- Common regular expressions
- Regular expression recommendations
- Using capture groups
- Inserting regular expression patterns in the LSX
- Cleaning the LSX template
- Testing modifications to the LSX document
- About QRadar Identifiers (QIDS)
- Creating a new QID entry with qidmap_cli.sh
- Mapping the Log Source ID to custom QIDs
- Mapping Log Source Event IDs to existing QIDs
- Testing the mapping
- Points to remember about mapping

Module 9 Using rules

- About QRadar SIEM rules
- About QRadar SIEM Building Blocks
- Using Building Blocks
- Combining Building Blocks to capture specific events or flows
- Linking tests
- Linking tests in the correct order
- The custom rule engine (CRE)
- Attack scenario example
- Detecting the attack with a rule

Module 10 Creating rules

- Creating rules overview
- Rule that captures account creation
- Rule that captures access to sensitive data
- Rule that captures account deletion
- Combining rules to capture a sequence of events
- Using time-series and anomaly rules
- Conficker example
- Creating a search to accumulate data
- Creating a time series for the search
- Creating an anomaly rule
- A CRE event is the default response
- Creating a custom rule to catch the pattern
- Custom rule response and action

Module 11 Managing false positives

- False positive overview
- Example 1: Suspicious access to sensitive data
- Example 2a: Botnet access: Determining the rule
- Example 2b: Searching for contributing events
- Example 2c: False positive wizard.
- Example 3a: Capturing events first, deciding later
- Example 3b: Finding rules with high offense counts
- Example 3c: Using the rule to capture events in a report
- Example 3d: Analyzing the report
- Example 4a: Analyzing offenses by category
- Example 4b: Listing the offenses by category
- Example 4c: Finding the first rule that triggered
- Example 4d: Determining a strategy to eliminate the false positive
- Example 4e: Modifying the appropriate Building Blocks
- Example 4f: Fine tune the rule that triggered the offense
- Tuning guidelines
- Commonly edited Building Blocks
- Tuning by changing rules

- Adjusting and enabling additional rules

Module 12 Using Reference Maps in rules

- Reference Maps overview
- Reference Maps use cases
- Using Reference Maps on the command line
- Using ReferenceDataUtil.sh
- Using Reference Maps in the user interface
- Using Reference Maps in searches
- Sample use case of Reference Map of Sets
- Creating a Reference Map of Sets
- Creating a CRE rule
- Creating a group by search
- Alternative to a CRE rule
- Creating an ADE rule
- Managing the Reference Map of Sets
- Using the CRE response
- Deleting records from the command line