KOENIG
step forward

KOENIG SOLUTIONS · COURSE OUTLINE

QRadar SIEM Admin: Log Sources, Rules & Tuning

Learn to configure QRadar SIEM administration, log sources and rules, and tune the system to reduce false positives.

2 Days	12	159
DURATION	MODULES	TOPICS

COURSE OVERVIEW

This course covers QRadar SIEM administration tools, including host context, licensing, system settings and authorized services, followed by building the network hierarchy and working with asset profiles, reference sets and index management. It addresses user account and security profile management, data backup and retention configuration, and the collection of log and flow records from standard, Windows and custom log sources. It then covers the use of Building Blocks and the custom rule engine to create and combine rules, manage false positives through tuning, and apply reference maps within rules.

WHO THIS COURSE IS FOR

- **SIEM Administrators**
- **Security Analysts**
- **Network Security Engineers**
- **IT Security Operations Staff**
- **System Administrators**

LEARNING OBJECTIVES

- Configure administration tools such as host context and licensing
- Build a network hierarchy using group and leaf nodes
- Manage asset profiles, reference sets and index settings
- Create user roles and security profiles with defined permissions
- Configure data backup schedules and event or flow retention buckets
- Add log sources and flow sources, including Windows log agents
- Create Building Blocks and rules using the custom rule engine
- Tune false positives using rule and Building Block adjustments

COURSE SYLLABUS

12 Modules, 159 Topics

01

Using Administration Tools

TOPICS

- 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

02

Creating the Network Hierarchy

TOPICS

- 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

03

Updated Administration Tools

TOPICS

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

04

Managing Users

TOPICS

- 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

05

Managing Data

TOPICS

- 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

06

Collecting Log and Flow Records

TOPICS

- **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

07

Collecting Windows Log Records

TOPICS

- 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

08

Managing Custom Log Sources

TOPICS

- 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

Managing Custom Log Sources (continued)

TOPICS (CONTINUED)

- Mapping Log Source Event IDs to existing QIDs
- Testing the mapping
- Points to remember about mapping

09

Using Rules

TOPICS

- 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

10

Creating Rules

TOPICS

- 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

11

Managing False Positives

TOPICS

- 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

12

Using Reference Maps in Rules

TOPICS

- 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

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com