KOENIG SOLUTIONS · COURSE OUTLINE

QRadar SIEM: Offense Investigation & Correlation Rules

Learn to investigate QRadar SIEM offenses, analyse events and flows, and build correlation rules and reports.

2 Days	10	135
DURATION	MODULES	TOPICS

COURSE OVERVIEW

This course covers the purpose and capabilities of IBM Security QRadar SIEM, how it collects and normalises security data through events and flows, and how to navigate the Dashboard tab to monitor activity. It then addresses investigating offenses triggered by events and by flows, using asset profiles to add context, and working with rules and building blocks that generate offenses. The course also covers creating QRadar SIEM reports and performing advanced filtering, including grouping, time-series data and identifying suspicious flow patterns.

WHO THIS COURSE IS FOR

- **SIEM Analysts**
- **Security Operations Analysts**
- **Incident Investigators**
- **Network Security Administrators**
- **Security Monitoring Staff**

LEARNING OBJECTIVES

- Explain the purposes and key capabilities of QRadar SIEM
- Describe how QRadar SIEM collects and normalises events and flows
- Navigate the Dashboard tab and create custom dashboard items
- Investigate offenses triggered by events using the Offense Summary window
- Investigate offenses triggered by flows and tune false positives
- Apply asset profiles to add context to an offense investigation
- Identify rules and building blocks that trigger an offense
- Create QRadar SIEM reports and apply advanced filtering techniques

COURSE SYLLABUS

10 Modules, 135 Topics

01

Introduction to IBM Security QRadar SIEM

TOPICS

- 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

02

How QRadar SIEM Collects Security Data

TOPICS

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

03

Using the QRadar SIEM Dashboard

TOPICS

- 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

04

Investigating an Offense That Is Triggered by Events

TOPICS

- 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

05

Investigating the Events of an Offense

TOPICS

- 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

Investigating the Events of an Offense (continued)

TOPICS (CONTINUED)

- Selecting the time range
- Displaying 24 hours in a dashboard item
- Modifying items in the chart type table

06

Using Asset Profiles to Investigate Offenses

TOPICS

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

07

Investigating an Offense That Is Triggered by Flows

TOPICS

- 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

08

Using Rules and Building Blocks

TOPICS

- 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

09

Creating QRadar SIEM Reports

TOPICS

- 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

10

Performing Advanced Filtering

TOPICS

- 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

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