IBM QRadar SIEM Foundations Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Learn about the solution architecture, how to navigate the user interface, and how to investigate offenses.

IBM Security QRadar enables deep visibility into network, endpoint, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, assets, and vulnerabilities. Suspected attacks and policy breaches are highlighted as offenses. In this course, you learn about the solution architecture, how to navigate the user interface, and how to investigate offenses. You search and analyze the information from which QRadar concluded a suspicious activity. Hands-on exercises reinforce the skills learned.

In this 3-day instructor-led course, you learn how to perform the following tasks:

- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine
- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

Extensive lab exercises are provided to allow learners an insight into the routine work of an IT Security Analyst operating the QRadar SIEM platform. The exercises cover the following topics:

- Architecture exercises
- UI Overview exercises
- Log Sources exercises
- Flows and QRadar Network Insights exercises
- Custom Rule Engine (CRE) exercises
- Use Case Manager app exercises
- Assets exercises
- App Framework exercises
- Working with Offenses exercises.
- Search, filtering, and AQL exercises
- Reporting and Dashboards exercises
- QRadar Admin tasks exercises

The lab environment for this course uses the IBM QRadar SIEM 7.5 platform.

IBM QRadar SIEM Foundations Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend?

This course is designed for security analysts, security technical architects, offense managers, network administrators, and system administrators using QRadar SIEM.

Prerequisites

Before taking this course, make sure that you have the following skills:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog

What You Will Learn

- Describe how QRadar collects data to detect suspicious activities
- Describe the QRadar architecture and data flows
- Navigate the user interface
- Define log sources, protocols, and event details
- Discover how QRadar collects and analyzes network flow information
- Describe the QRadar Custom Rule Engine
- Utilize the Use Case Manager app
- Discover and manage asset information
- Learn about a variety of QRadar apps, content extensions, and the App Framework
- Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Search, filter, group, and analyze security data
- Use AQL for advanced searches
- Use QRadar to create customized reports
- Explore aggregated data management
- Define sophisticated reporting using Pulse Dashboards
- Discover QRadar administrative tasks

IBM QRadar SIEM Foundations Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

- Module 1: Describe how QRadar collects data to detect suspicious activities
- Module 2: Describe the QRadar architecture and data flows
- Module 3: Navigate the user interface
- Module 4: Define log sources, protocols, and event details
- Module 5: Discover how QRadar collects and analyzes network flow information
- Module 6: Describe the QRadar Custom Rule Engine
- Module 7: Utilize the Use Case Manager app
- Module 8: Discover and manage asset information
- Module 9: Learn about a variety of QRadar apps, content extensions, and the App Framework
- Module 10: Analyze offenses by using the QRadar UI and the Analyst Workflow app
- Module 11: Search, filter, group, and analyze security data
- Module 12: Use AQL for advanced searches
- Module 13: Use QRadar to create customized reports
- Module 14: Explore aggregated data management
- Module 15: Define sophisticated reporting using Pulse Dashboards
- Module 16: Discover QRadar administrative tasks