IBM QRadar SIEM Advanced Topics Training

Duration: **2 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Learn this 2-day course walks you through various advanced topics about QRadar such as custom log sources

QRadar SIEM provides deep visibility into network, 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.

This 2-day course walks you through various advanced topics about QRadar such as custom log sources, reference data collections and custom rules, X-Force data and the Threat Intelligence app, UBA and QRadar Advisor, tuning and custom action scripts. The course also discusses integration with IBM SOAR. Hands-on exercises reinforce the skills Learned.

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

Is This The Right Course?

Students should be knowledgeable about the following topics:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog
- Foundational skills for the IBM QRadar Security Intelligence Platform (at least the skills that are taught in the IBM QRadar SIEM Foundations - BQ104 course)

Who Should Attend?

This course is designed for security administrators and security analysts.

Prerequisites

Students should be knowledgeable about the following topics:

- IT infrastructure
- IT security fundamentals
- Linux
- Windows
- TCP/IP networking
- Syslog
- Foundational skills for the IBM QRadar Security Intelligence Platform (at least the skills that are taught in the IBM QRadar SIEM Foundations - BQ104 course)

IBM QRadar SIEM Advanced Topics Training

Duration: **2 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

- Learn how to create custom log sources
- Discover how to work with reference data collections and custom rules
- Use X-Force data and Threat Intelligence app
- Use the Use Case Manager app
- Learn how to use UBA and QRadar Advisor
- Discover Tuning
- Explore Custom action scripts
- Discuss Integration with IBM SOAR

Training Outline

- Module 1: Learn how to create custom log sources
- Module 2: Discover how to work with reference data collections and custom rules
- Module 3: Use X-Force data and Threat Intelligence app
- Module 3: Use the Use Case Manager app
- Module 4: Learn how to use UBA and QRadar Advisor
- Module 5: Discover Tuning
- Module 6: Explore Custom action scripts
- Module 7: Discuss Integration with IBM SOAR