IBM QRADAR SIEM ADVANCED TOPICS

Course Code: 100034

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.

What You'll 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

Who Needs to 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

Course Code: 100034

CLASSROOM LIVE	$1,900 USD	2 Day

Classroom Live 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

IBM QRADAR SIEM ADVANCED TOPICS

Course Code: 100034

VIRTUAL CLASSROOM LIVE	$1,900 USD	2 Day

Virtual Classroom Live 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

Sep 18 - 19, 2025 | 9:30 AM - 5:30 PM EST

Oct 28 - 29, 2025 | 9:30 AM - 5:30 PM EST

Dec 18 - 19, 2025 | 9:30 AM - 5:30 PM EST

IBM QRADAR SIEM ADVANCED TOPICS

Course Code: 100034

ON-DEMAND	$1,070 USD

On-Demand 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

IBM QRADAR SIEM ADVANCED TOPICS

Course Code: 100034

PRIVATE GROUP TRAINING	2 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.