multisoft
Systems

IBM Certified Analyst - Security QRadar SIEM V7.5 Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The IBM Certified Analyst - Security QRadar SIEM V7.5 training offered by Multisoft Systems is designed to equip participants with the skills needed to excel in the rapidly evolving field of cybersecurity analytics. This comprehensive course covers all aspects of IBM's Security QRadar SIEM V7.5, a powerful tool that helps organizations detect, prioritize, and respond to security threats.

Module 1: Offense Analysis

- ✓ Triage initial offense
- ✓ Analyze fully matched and partially matched rules
- ✓ Analyze an offense and associated IP addresses
- ✓ Recognize MITRE threat groups and actors
- ✓ Perform offense management
- ✓ Describe the use of the magnitude within an offense
- ✓ Identify Stored and Unknown events and their source
- ✓ Outline simple offense naming mechanisms
- ✓ Create customized searches

Module 2: Rules and Building Block Design

- ✓ Interpret rules that test for regular expressions
- ✓ Create and manage reference sets and populate them with data
- ✓ Identify the need for QRadar Content Packs
- ✓ Analyze rules that use Event and Flow data
- ✓ Analyze Building Blocks Host definition, category definition, Port definition
- ✓ Review and understand the network hierarchy
- ✓ Review and recommend updates to building blocks and rules
- ✓ Describe the different types of rules, including behavioral, anomaly and threshold rules

Module 3: Threat Hunting

- ✓ Investigate Event and Flow parameters
- ✓ Perform AQL query
- ✓ Search & filter logs
- ✓ Configure a search to utilize time series
- ✓ Analyze potential IoCs
- ✓ Break down triggered rules to identify the reason for the offense

- ✓ Distinguish potential threats from probable false positives
- ✓ Add a reference set based filter in log analysis
- ✓ Investigate the payload for additional details on the offense
- ✓ Recommend adding new custom properties based on payload data
- ✓ Perform "right-click Investigations" on offense data

Module 4: Dashboard Management

- ✓ Use the default QRadar dashboard to create, view, and maintain a dashboard based on common searches
- ✓ Use Pulse to create, view, and maintain a dashboard based on common searches

Module 5: Searching and Reporting

- ✓ Explain the different uses and benefits for each Ariel search type
- ✓ Explain the different uses of each search type
- ✓ Perform an advanced search
- ✓ Filter search results
- ✓ Build threat reports
- ✓ Perform a quick search
- ✓ View the most commonly triggered rules
- ✓ Report events correlated in the offense
- ✓ Export Search results in CSV or XML
- ✓ Create reports and advanced reports out of offenses
- ✓ Share reports with users
- ✓ Search using indexed and non-indexed properties
- ✓ Create and generate scheduled and manual reports