COURSE TABLE OF CONTENTS

IBM Certified Analyst — Security QRadar SIEM V7.5

OEM: IBM • Duration: 3 Days (24 hrs) • Code: C1000-162

COURSE MODULES & TOPICS

Section 1: Offense Analysis (23%)

- 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 magnitude within an offense
- Identify Stored and Unknown events and their source
- Create customized searches

Section 2: Rules and Building Block Design (18%)

- Interpret rules that test for regular expressions
- Create and manage reference sets
- Identify the need for QRadar Content Packs
- Analyze rules that use Event and Flow data
- Analyze Building Blocks: Host, category, and Port definitions
- Review and understand the network hierarchy
- Describe different types of rules: behavioral, anomaly and threshold

Section 3: Threat Hunting (24%)

- Investigate Event and Flow parameters
- Perform AQL query
- Search and 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
- Investigate the payload for additional details on the offense

Section 4: Dashboard Management (14%)

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

Section 5: Searching and Reporting (21%)

- Explain the different uses and benefits for each Ariel search type
- Perform an advanced search
- Filter search results
- Build threat reports
- Export search results in CSV or XML
- Create and generate scheduled and manual reports
- Search using indexed and non-indexed properties