IBM Security QRadar SIEM V7.4.3 Analysis

Test C1000-139

Certification overview, objectives, exam preparation and registration

IBM **Security**

IBM

Certification Overview

Prerequisite Knowledge:

Recommended Skills

- Knowledge of SIEM concepts
- Knowledge of TCP/IP Networking
- Knowledge of IT Security concepts
- Knowledge of MITRE ATT&CK Framework

Key Areas of Competency

- Offense and log analysis
- Understanding reference data
- Rule and building block understanding
- Searching and reporting, regular and adhoc reports
- Understanding basic QRadar tuning and network hierarchy

Key Areas of Competency

- This certification requires one exam.

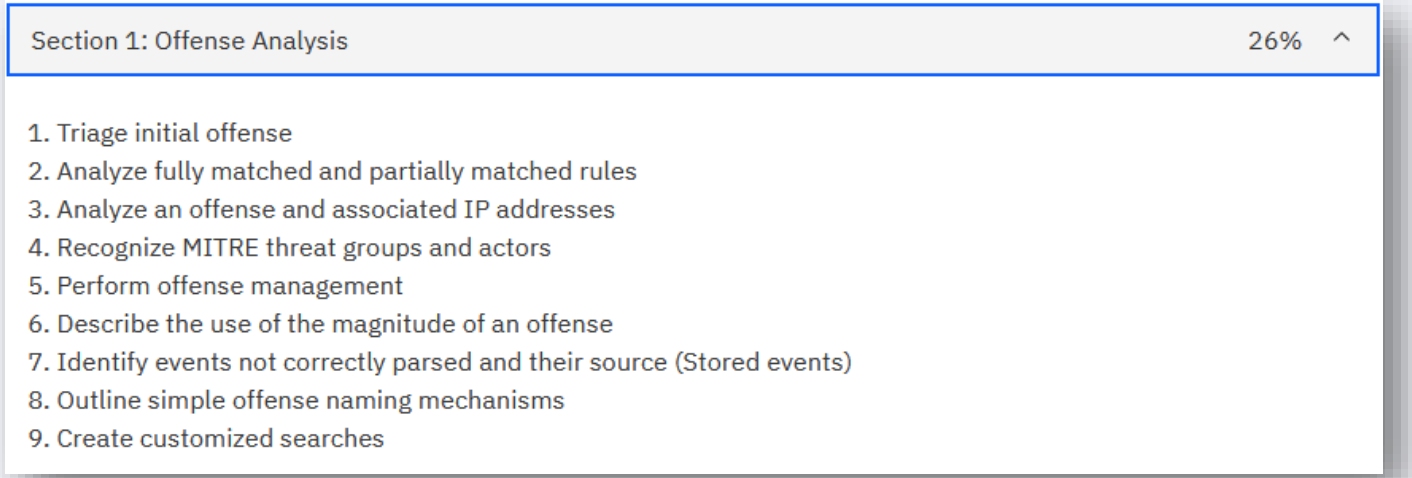
Exam C1000-139: IBM Security QRadar SIEM V7.4.3 Analysis

Exam Objectives

Test Details:

Number of Questions	Number of Questions to Pass	Time Allowed
62	38	90 Min

Section 1: Offense Analysis



Section 2: Rules & Building Black Design

Section 2: Rules and Building Block Design	26%

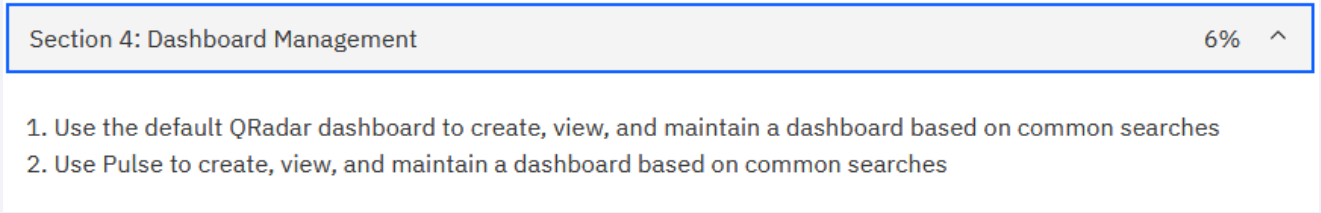
1. Interpret rules that test for regular expressions
2. Create and manage reference sets and populate them with data
3. Install QRadar Content Packs using the QRadar Assistant App
4. Analyze rules that use Event and Flow data
5. Analyze Building Blocks: Host definition, category definition, Port definition
6. Review and recommend updates to the network hierarchy
7. Review and recommend updates to building blocks and rules
8. Describe the different types of rules, including behavioral, anomaly and threshold rules

Section 3: Threat Hunting

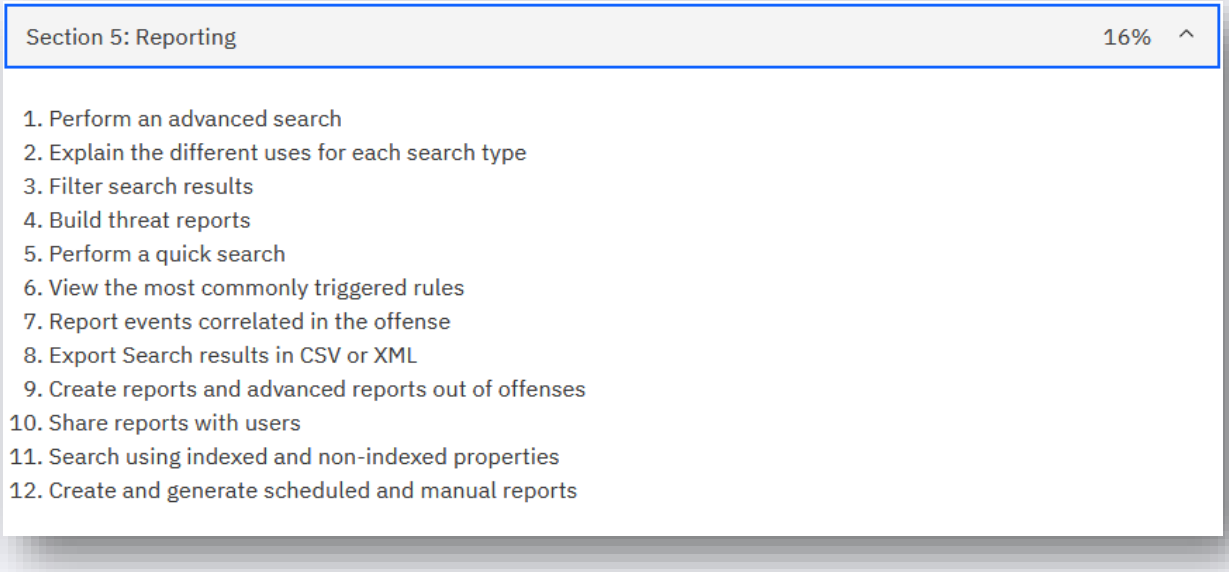
Section 3: Threat Hunting 26%

1. Investigate Event and Flow parameters
2. Perform AQL query
3. Search & filter logs by specific log source type
4. Configure a search to utilize time series
5. Analyze potential IoCs
6. Break down triggered rules to identify the reason for the offense
7. Recommend changes to tune QRadar SIEM after offense analysis identifies issues
8. Distinguish potential threats from probable false positives
9. Add a reference set based filter in log analysis
10. Investigate the payload for additional details on the offense
11. Recommend adding new custom properties based on payload data
12. Perform "right-click Investigations" on offense data

Section 4: Dashboard Management



Section 5: Reporting



Course Content

IBM Security QRadar SIEM V7.4.3 Analysis

Offense Management & 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 of an offense
- Identify events not correctly parsed and their source (Stored events)
- Outline simple offense naming mechanisms
- Create customized searches

Topic covers

26%

Of the Exam

Rules & Building Block Design

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

Topic covers

26%

Of the Exam

Threat Hunting

- Investigate Event and Flow parameters
- Search & filter logs by specific log source type
- Configure a search to utilize time series
- Analyze potential IoCs
- Break down triggered rules to identify the reason for the offense
- Recommend changes to tune QRadar SIEM after offense analysis identifies issues
- 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

Topic covers

26%

Of the Exam

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

Topic covers

06%

Of the Exam

Reporting

- Perform an advanced search
- Explain the different uses for each search type
- 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

Topic covers

16%

Of the Exam