IBM Certified Analyst - Security QRadar SIEM V7.5

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

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

2.Rules and Building Block Design

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

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 triggerd 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
- Recommnd adding new custom proprts based on payload data
- Perform "right-click Investigations" on offense data

4.Dashboard Management

- Deflt QRadar dashboard to create, view, & maintn a dashboard
- Pulse to create, view, & maintain a dashboard based on common searches

5.Searching and Reporting

- Explain the different uses & 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

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474