LevelBlue

Blueprint for the LevelBlue Security Engineer Exam

Contents

Exam Overview and Blueprint

The exam tests your knowledge and skills in the areas listed below. The percentages indicate the relative weight of each major category. Therefore, you are more likely to see questions from categories with a higher weight. The questions on the exam are not limited to the descriptions below within each category.

Preparation (9-11%)

- Demonstrate an understanding of the features of USM Anywhere™.
- Describe how to discover Assets in different environments.

Demonstrate how to use Filtering and Suppression rules. Tuning (6-8%)

- Explain how to use Suppression Rules.
- Demonstrate how and why to use Filter Rules.

Describe understanding of OTX Threat Intelligence (6-8%)

- Demonstrate an understanding of OTX Pulses and Indicators of Compromise
- Describe how OTX IOCs can create alarms in USM Anywhere™

Detection & Evaluation: (6-8%)

- Demonstrate an understanding of the Kill Chain concept.
- Explain **Alarm Intent** and how it is represented in USM Anywhere™.
- Explain what information is captured in Events and Alarms.
- Demonstrate an understanding of triage and prioritization of alarms.

Containment & Response (9-11%)

- Understand how Advanced BlueApps allow integration with third party systems.
- Describe how to use the Forensics & Response App.
- Describe how App Actions can be used to respond to alarms.

Root Cause Analysis: (9-11%)

- Demonstrate how to do a root cause analysis search of events
- Demonstrate the use of Investigations to track analysis of an incident.

Recovery (6-8%)

- Understand how to re-deploy a sensor

Reporting (6-8%)

- Identify compliance reports and how to generate them.
- Explain how reports can be scheduled.
- Identify the available report formats.

Deployment (3-5%)

- Demonstrate an understanding of the requirements for deployment.
- Understand sensor configuration.

Asset Management (11-13%)

- Explain how to create and assign credentials.
- Understand how to create and use Asset Groups
- Understand how scheduled tasks can keep the asset data up to date.

Log Collection (3-5%)

- Demonstrate how log data can be forwarded to the USM Anywhere™ sensor
- Explain how the USM Anywhere™ Agent can be used to collect logs
- Demonstrate how to export logs from cold storage

Authenticated scans and Vulnerabilities (1-3%)

- Demonstrate an understanding of authenticated scans.
- Describe how to view vulnerabilities and their histories.

Events, Alarms and Rules (9-11%)

- Demonstrate an understanding of how Correlation Rules create alarms from events.
- Demonstrate how to create alarms with Orchestration Rules.
- Understand best practices for Orchestration Rules

Administration (3-5%)

- Understand the different user roles.
- Understand the use of MFA when logging into USM Anywhere™
- Demonstrate how to check console and system events