Blueprint for the LevelBlue Security Engineer Exam

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 your understanding of the threat detection tools provided by AlienVault® USM Anywhere™.
- Describe how to discover Assets in different environments.
  Explain how to organize Assets using the different Asset Groups.

Demonstrate when and how to use Asset Scans. Tuning (6-8%)

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

Describe how to use Orchestration Rules Threat Intelligence (6-8%)

- Demonstrate an understanding of how HIDS and NIDS data is turned into Events using Data Source Plugins.
- Explain the benefits of Open Threat Exchange.

Detection & Evaluation: (6-8%)

- Demonstrate an understanding of the Kill Chain process including the attacks and stages.
- Explain Incident Types and how they're represented in AlienVault® USM Anywhere™.
- Explain the information captured in Events and Alarms.
- Demonstrate an understanding of triage and prioritization of alarms.

Containment & Response (9-11%)

- Discuss Sensor Apps and their capabilities.
- Identify and understand AlienApps and their capabilities.
- Describe how App Actions can be used to respond to attacks.

Root Cause Analysis: (9-11%)

- Demonstrate how to leverage tools to aid in investigation.
- Demonstrate an understanding of the investigation process.
- Identify data relevant to an incident.

Recovery (6-8%)

- Demonstrate an understanding of how to restore your environment to full health.
- Explain how to research and find information about vulnerabilities.

Reporting (6-8%)

- Identify compliance reports and how to generate them.
- Explain how reports can be customized.
- Identify reporting options available for AlienVault® USM Anywhere™ data.

Deployment (3-5%)

- Demonstrate an understanding of the basics of deployment.
- Explain the initial stages of configuration.

Asset Management (11-13%)

- Demonstrate an understanding of the relationship between Assets and Sensors.
- Explain how to assign credentials.
- Define Asset Groups and understand how Asset Groups can be used.
- Demonstrate an understanding of how to find information about Assets in your environment.

Log Collection (3-5%)

- Demonstrate how log information is sent.
- Explain how logs are collected and/or forwarded.
- Demonstrate how to locate log data.

Authenticated scans and Vulnerabilities (1-3%)

- Demonstrate an understanding of an authenticated scan.
- Explain how scans are used in relation to vulnerabilities.

Events, Alarms and Rules (9-11%)

- Demonstrate an understanding of the relationship between Events and Rules.
- Demonstrate an understanding of plugins in relation to Events and Alarms.

Administration (3-5%)

- Understand Messages and Notifications regarding your AlienVault® USM Anywhere™ environment.