Blueprint
for the
AlienVault Certified 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.

Deployment Strategy (5-10%)

- Describe the network components and connections to be considered prior to installing and configuring USM Appliance.
- Explain the different methods by which a USM Appliance Sensor can obtain data to generate events.
- Demonstrate adequate planning while preparing to deploy a USM Appliance environment.
- When utilizing network monitoring, explain the differences in methods used to obtain network information.

Basic Configuration (5-10%)

- Explain how OTX is used in USM Appliance.
- Use AlienVault Center to configure selected components in USM Appliance.
- Manage archive and retention methods available inside USM Appliance.
- Describe the manners in which you can verify that your setup is properly configured.
- Describe how USM Appliance works with network flows.

Asset Management (5-10%)

- Explain the different methods for adding or importing assets in USM Appliance.
- Explain the difference between Passive and Active Discovery.
- Explain the significance of internal and external assets.
- Specify the features used to monitor availability of assets.

Threat Determination / Security Capabilities (5-10%)

- Describe the various ways to create notifications from a given circumstance.
- On a USM Appliance Server, identify different use cases when a custom script may be required.
- Describe the impact of multiple policies on data flows.
- Describe risk calculation in USM Appliance.
- Demonstrate the ability to modify directives.
- Demonstrate how options are used in logical correlations.

Analysis (5-10%)

- Given multiple users working together, show different use cases for tagging alarms.
- Explain how to use, change and create report modules from Views in the SIEM console.
- Given a default installation of USM Appliance, describe custom report options for a given scenario.
- Describe the integrity verification process for raw logs.

Reporting (5-10%)

- Describe options available in USM Appliance for customizing reports.
- Given a set of requirements, create a custom report.

Threat Detection (8-13%)

- Demonstrate an understanding of the AlienVault HIDS Log Lifecycle.
- Describe the Syscheck process in AlienVault HIDS.
- Describe the different manners and complications of deploying the AlienVault HIDS agent.
- Describe different ways to deploy AlienVault HIDS agents to different systems.
- Demonstrate an understanding of the rationale behind reviewing or managing vulnerability scan result sets.
- Demonstrate the necessary skills to deploy AlienVault HIDS to non-windows platforms.
- Demonstrate a solid understanding of the log delivery and event capture lifecycle within a USM Appliance deployment.

Behavioral Monitoring (3-8%)

- Identify possible sources of flow data and demonstrate how they can be utilized for analysis.
- Describe how USM Appliance utilizes availability monitoring.

Plugins (5-10%)

- Explain how regular expressions are used in USM Appliance to process logs.
- Compare and contrast the different types of events.
- Explain the available means by which data can be supplied or augmented for plugins.
- Describe the lifecycle of an event as it is received or generated by a USM Appliance Sensor and how it is processed.
- Analyze and describe specific elements of plugins.

Backup and Restore (3-8%)

- Explain various concepts, components and configurations related to backups and restoration.

Update and Maintenance (3-8%)

- Given a notification, demonstrate the ability to troubleshoot the affected component.
- Explain the functionality and value provided by IPMI.

- Demonstrate an ability to upgrade an environment in the appropriate order.

Optimization and Tuning (8-13%)

- Identify system parameters on a USM Appliance device that can be used to narrow down performance problems, and explain what types of problems they may indicate.
- Demonstrate the ability to tune USM Appliance for optimal performance.
- Demonstrate the use of basic Linux commands to troubleshoot and tune AlienVault.
- Identify methods to prevent events from arriving at the server.
- Demonstrate how Rsyslog is used within USM Appliance.
- Demonstrate how AlienVault uses plugins.
- Describe different ways database performance can be impacted on a USM Appliance.

Administrative User Management (3-8%)

- Describe authentication options available in USM Appliance.
- Describe how and why you may configure role based access.
- Demonstrate an understanding of user activity auditing.

Incident Management and Response (3-8%)

- Explain when, how and why USM Appliance ticket modules would be used.
- Explain the virtues of tracking alarms vs tickets as an incident tracking method.

Complex Deployment (3-8%)

- Describe methods for scaling a USM Appliance platform using additional components.
- Demonstrate how to configure and use a remote logger, and why.
- Understand how event forwarding works in USM Appliance and why it would be used.