AVSE Certification BluePrint

(https://cdn-cybersecurity.att.com/docs/AVSEExamBlueprintOct2018.pdf)

Blueprint for the AlienVault Certified Security Engineer (AVSE) 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™.
    - nmap - Discovery scans & Asset scans
    - jOVAL - Authenticated Asset scans
    - API - AWS/Azure/GCP/VMware/AD
    - HIDS - Syslog/NXLog/Graylog/Agent
    - NIDS - Suricata
    - Security Intelligence - OTX
    - AlienLabs
- Describe how to discover Assets in different environments.
    - AWS
    - Azure
    - GPC
    - Hyper-V
    - VMware
- Explain how to organize Assets using the different types of Asset Groups.
    - Compliance / Static / Dynamic
- Demonstrate when and how to use Asset Scans.
    - Managing Credentials (WinRM port 5985 / SSH port 22)
    - Running Asset Scans
    - Running Authenticated Asset Scans
    - Scheduling Asset Scans
    - Scheduling Authenticated Asset Scans

Tuning (6-8%)

- Explain how and when to use Suppression Rules
    - Suppression Rules from Orchestration Page
    - Suppression Rules from the Alarms Page
    - Suppression Rules from the Events Page

- Demonstrate how and why to use Filter Rules
    - Filtering Rules from the Orchestration Page
    - Filtering Rules from the Events Page
- Describe how to use Orchestration Rules
    - Orchestration Rules
    - Workflow
    - Best Practises

Threat Intelligence (6-8%)

- Demonstrate an understanding of how HIDS and NIDS data is turned into Events using Data Source Plugins
    - HIDS - Host, syslog/nxlog, plugins
    - NIDS - Network, Suricata, plugins
        - (GCP and Azure can't do NIDS)
- Explain the benefits of Open Threat Exchange
    - About OTX
    - Using OTX in USM Anywhere
    - OTX Documentation
    - AlienVault OTX

Detection & Evaluation: (6-8%) - Bonus material

- Demonstrate an understanding of the Kill Chain process including the attacks and stages
    - Defend like an attacker: Applying the cyber kill chain
    - Lockheed Martin Cyber Kill Chain
- Explain Incident Types and how they're represented in AlienVault® USM Anywhere™
    - Alarm Intent
- Explain the information captured in Events and Alarms
    - Alarm Strategy & Method
- AlienVault provide Priority, Description, Recommendation and Community Information.
- Demonstrate an understanding of triage and prioritisation of alarms

Containment & Response (9-11%)

- Discuss Sensor Apps and their capabilities
    - Syslog Server App
    - Graylog App
- 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
    - AlienApp for Forensics and Response
- Demonstrate an understanding of the investigation process
    - Investigations
    - Root Cause Analysis ex.1
    - Root Cause Analysis ex.2
    - Root Cause Analysis ex.3
- 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
    - USM Anywhere Compliance Templates
    - PCI DSS
    - NIST CSF
    - HIPAA
    - ISO27001
- Explain how reports can be customised
    - USM Anywhere Reports
- Identify reporting options available for AlienVault® USM Anywhere™ data
    - Event Type Template
    - Exporting Dashboards

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
    - Asset Administration
- Explain how to assign credentials

        - Managing Credentials in USM Anywhere
        - Assigning Credentials
        - Managing Credentials for your AD Servers
- 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
    - Log Collection from Your Data Sources
    - Managing Jobs in the Scheduler
- 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
    - Events Management
    - Alarms Management
    - Rules Management
- Demonstrate an understanding of plugins in relation to Events and Alarms

Administration (3-5%)

- Understand Messages and Notifications regarding your AlienVault® USM Anywhere™ environment
        - Alarm & Event Notifications
        - Creating Notification Rules from the Events Page
        - Notification Rules from the Orchestration Rules Page
        - Creating Notification Rules from the Alarms Page

AlienVault USM Anywhere: Security Analysis (ANYSA) Syllabus