AlienVault® USM Anywhere™: Deploy, Configure, Manage (ANYDC) Syllabus

Module 1: Orientation
This Orientation provides an overview of the security landscape, the challenges in detecting threats in an organization's environment, and an overview of the AlienVault® USM Anywhere™ solution.

- Define Security Threats
- Identify Security Challenges in Organizations
- Understand the functions and benefits of USM Anywhere

Module 2: Deployment
This module provides an overview of the deployment process of USM Anywhere, and shows how to install and configure additional sensors.

- Define USM Anywhere
- Explain the USM Anywhere Deployment Flow
- Understand USM Anywhere Deployment Models
- Install and Configure an On Premises Sensor
- Configure an Installed Sensor in the USM Anywhere Web Console
- Edit Sensor Settings in the USM Anywhere Web Console

Module 3: Asset Management
This module explains how to add Assets to the USM Anywhere, and how to organize them with Asset Groups.

- Understand how to add assets to USM Anywhere
- Understand Searches and Filters
- Create and Configure Saved Views
- Export View Data as Reports
- Understand and Create Custom Asset Fields
- Create and Modify both Static and Dynamic Asset Groups

Module 4: Log Collection
This module explains Log Collection in USM Anywhere, how to configure log forwarding for Windows and Linux Assets, and how the data from that log forwarding is turned into Events via the USM Anywhere Plugins.

- Define USM Anywhere Log Management
- Configure Log Forwarding for Linux (rsyslog, osquery) and Windows (NXLog, Sysmon)
- Understand USM Anywhere Plugins
- Introduce Events Page
- Troubleshoot Log Management

Module 5: Authenticated Scans and Vulnerabilities
This module covers how to configure credentials, perform authenticated scans, and schedule scanning.

- Define Authenticated Scans
- Configure Credentials for Windows (WinRM) and ssh
- Configure and run Authenticated Scans
- Schedule recurring Asset Scan Jobs
- Investigate and Remediate Vulnerabilities

Module 6: Events, Alarms, and Rules
This module explains how Rules work with Events and Alarms within the USM Anywhere system, and how to create and configure Rules to customize your USM Anywhere Instance.

- Introduce Sensor Apps and AlienApps
- Define Events and Alarms
- Understand Event and Alarm Actions
- Understand Rules and Rule Types
    - Correlation
    - Orchestration
    - Suppression
    - Filtering

Module 7: Administration
This module provides an overview of different administrative and reporting tools within USM Anywhere, including Dashboards, Data Management, User Management, Bookmarks and Messages.

- Navigate the Dashboards
- Navigate the Subscription Page
- Request Raw Log Data
- Understand and Leverage Filtering Rules
- Manage User Accounts
- Set and Reference Bookmarks
- Check Messages and Release Notes

Module 8: Resources
This module provides an overview of different documentation, support, and community resources to assist students in fully utilizing the USM Anywhere product.

- Locate USM Anywhere Documentation Resources
- Locate USM Anywhere Status and Updates (Release Notes)
- Locate AlienVault Support and Community Resources