AlienVault® USM Anywhere™: Security Analysis (ANYSA) Syllabus

Course Introduction

The AlienVault® USM Anywhere™: Security Analysis 2-day course provides security analysts with the knowledge and tools to fully leverage USM Anywhere to perform analyst duties.

Module 1: Preparation

This module introduces you to USM Anywhere and discusses the initial steps involved in discovering, organizing, scanning and monitoring your Assets.

- Learn about the five essential tools provided as part of USM Anywhere
- Discover Assets in different environments
- Organize Assets using the different Asset Group types
- Configure Authenticated Asset Scans to identify Vulnerabilities
- Understand how Host Intrusion Detection (HIDS) and Network Intrusion Detection (NIDS) works in USM Anywhere

Module 2: Tuning

This module describes how to set a baseline for your environment in USM Anywhere so that you can cut out the noise (false positives) and focus on the Events and Alarms you are concerned about.

- Hide Events from view through Suppression Rules
- Filter Events to save on storage through Filter Rules
- Configure USM Anywhere to Alarm on Events (false negatives) you are concerned about through Orchestration Rules

Module 3: Threat Intelligence

This module describes how the HIDS and NIDS information revived by USM Anywhere is transformed into Events which in turn are correlated into Alarms based on the Threat Intelligence provided by the AlienVault Labs team.

- Introduces the AlienVault Labs team and describes the work they do
- Describes how HIDS and NIDS data is turned into Events using Data Source Plugins
- Describes how Alarms are triggered by Event(s) using Correlation Rules
- Learn about the Open Threat Exchange® (OTX™)

Module 4: Detection and Evaluation

This module explains the Kill Chain Taxonomy and defines how it appears on the USM Anywhere User Interface (UI). You will also be introduced to triaging and prioritizing Alarms.

- Explain the Kill Chain process
- Review Incident Types and how they are represented in USM Anywhere
- Investigates the helpful information captured in Events and Alarms
- Triage and prioritization of Alarms

Module 5: Containment and Response
This module discusses how you can respond to an attack on your environment once detected by USM Anywhere. We will introduce Sensor Apps and AlienApps, and speak about how you can manually or automatically respond to the attack using these apps.

- Introduce Sensor Apps and discuss their capabilities
- Introduce AlienApps and discuss their capabilities
- Describe App Actions and how they can be used to respond to attacks

Module 6: Root Cause Analysis
This module will deep dive into the investigation of Alarms, Events and Raw Logs that have been validated as being part of a security incident.

- Identify data relevant to an incident
- Describe investigation process
- Highlight the tools to leverage to aid in investigation
- Prepare Root Cause Analysis incident reports for management

Module 7: Recovery
This module discusses the various topics to consider when recovering from an attack to restore your environment and put measures in place to prevent such an attack in the future.

- Restoring your environment to full health
- Create Orchestration Rules to Alarm on Events in the future
- Patch Vulnerabilities and confirm resolution

Module 8: Reporting
This module reviews all the reporting capabilities that are available in USM Anywhere, where they can be run from and how they can be customized to meet your needs.

- Review compliance reports available and how they are generated
- Identify the reporting options available for USM Anywhere data
- Learn how reports can be created and customized

Module 9: Conclusion
This module will provide a recap of the entire course and review what you have learned in each module. You will also receive information about useful AlienVault resources to help you with your day to day work.

- Summary of course modules and how they connect
- Details on USM Anywhere documentation
- Details on how to obtain support
- Information about our forums
- Details on how to obtain an OTX account