AlienVault® USM Appliance™: Security Analysis (AUSA) Syllabus

Course Introduction

The AlienVault® USM Appliance™: Security Analysis 2-day course provides security analysts with the knowledge and skills to fully leverage USM Appliance to perform analyst duties to identify and remediate known and emerging threats.

Module 1: Overview: Get to Know the USM Appliance™

In this module, your CISO makes you the Security Analyst for E.T.&T. You must discover the capabilities of the USM Appliance and begin to discover, organize, scan and monitor your company assets to identify and neutralize threats. You will perform daily security tasks and initiate your Incident Response plan when needed.

- Tour the USM Appliance Web UI primary and secondary menu features and functions
- Understand the five essential capabilities delivered by AlienVault® USM Appliance™
- Run an asset scan to discover assets and organize with asset groups
- Discuss and enable availability monitoring for assets

Module 2: Preparation: Know your Environment

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

- Learn security analysis and incident response concepts
- Run a vulnerability scan to discover asset vulnerabilities
- Triage alarms and events to differentiate noise & false positives from threats and compromises

Module 3: Tuning: Policies and Directives

This module teaches you to set a baseline for your environment in USM Appliance to cut out the noise & false positives, highlighting alarms and events that are critical.

- Understand Host Intrusion Detection (HIDS) and Network Intrusion Detection (NIDS)
- Hide unimportant events with policies
- Configure USM Appliance to alarm on certain false negatives through policies and directives

Module 4: Attacks, Threat Intelligence and Penetration Testing

This module describes how HIDS and NIDS information received by USM Appliance is transformed into events which in turn are correlated into alarms based on the threat intelligence provided by the AlienVault Labs team.

- Introduce the value and function of Open Threat Exchange® (OTX™)
- Discover how data source plugins convert HIDS and NIDS data into events
- Understand how alarms are triggered by event(s) using correlation directives

AlienVault, AlienApp, AlienApps, AlienVault OSSIM, Open Threat Exchange, OTX, OTX Endpoint Security, Unified Security Management, USM, USM Anywhere, USM Appliance, and USM Central, are trademarks of AlienVault and/or its affiliates. Other names may be trademarks of their respective owners.

- Learn how attackers identify vulnerabilities and exploit them to penetrate networks and hosts

Module 5: Detection and Evaluation
This module explains the kill chain taxonomy and defines how it appears on the USM Appliance User Interface (UI). You will also be introduced to triaging and prioritizing alarms.

- Introduces the AlienVault Labs team and describes the work they do
- Explain the kill chain as it appears in USM Appliance
- Review incident types and how they are represented in USM Appliance
- Investigates the helpful information captured in events and alarms
- Additional triage and prioritization of alarms

Module 6: Containment and Response
This module covers how to respond to an attack on your environment once detected by USM Appliance. We will introduce the knowledge base and other resources to support containment, eradication and recovery. We will discuss and practice how to manually or automatically respond to the attack using these capabilities.

- Introduce the USM Appliance knowledge base and use it to research threat
- Discuss common attack vectors and strategies to contain them
- Determine appropriate incident response based on the types of attack and goals

Module 7: 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 the investigation process
- Highlight the tools to leverage to aid in investigation
- Prepare root cause analysis incident reports for management

Module 8: Recovery from Compromise
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.

- Patch vulnerabilities and confirm resolution
- Restoring your environment to full health
- Documenting the triage and recovery steps in tickets, then closing alarms and tickets
- Creating Policies or Directives to alarm on critical events in the future

Module 9: Communication & Reporting
This module reviews all the reporting capabilities that are available in USM Appliance, where they can be run from and how they can be customized to meet your needs.

AlienVault, AlienApp, AlienApps, AlienVault OSSIM, Open Threat Exchange, OTX, OTX Endpoint Security, Unified Security Management, USM, USM Anywhere, USM Appliance, and USM Central, are trademarks of AlienVault and/or its affiliates. Other names may be trademarks of their respective owners.

- Discuss communication and reporting requirements / strategies
- Identify the reporting options available for USM Appliance data
- Learn how USM Appliance facilitates reporting and how reports can be customized

Module 10: Post Mortem & Conclusion
This module provides a recap of the course and review of key knowledge and skills. You will also receive information about useful AlienVault resources to help you with your day to day work.

- Summary and review of course modules
- Importance of incident response team post mortems and acting on recommendations
- Details on USM Appliance documentation and obtaining support
- Information about AlienVault forums and how to get an OTX account

AlienVault, AlienApp, AlienApps, AlienVault OSSIM, Open Threat Exchange, OTX, OTX Endpoint Security, Unified Security Management, USM, USM Anywhere, USM Appliance, and USM Central, are trademarks of AlienVault and/or its affiliates. Other names may be trademarks of their respective owners.