AlienVault USM Appliance for Security Engineers – 5 day course outline

Course Introduction

The Course Introduction provides students with the course objectives and prerequisite learner skills and knowledge for this 5 day course. The Course Introduction presents the course flow diagram and the icons that are used in the course illustrations and figures.

Module 1: Overview

This module provides an overview of the AlienVault® USM Appliance™ solution. Upon completing this module, you will meet these objectives:

- Understand the basic function of AlienVault USM Appliance
- Describe AlienVault USM Appliance Architecture
- Describe AlienVault Labs and the threat intelligence it provides

This module includes these topics:

- AlienVault USM Appliance overview
- USM Appliance Architecture
- AlienVault Labs and OTX

Module 2: AlienVault USM Appliance Basic Configuration and Verifying Operations

This module describes AlienVault USM Appliance installation, basic configuration and verification, and graphical user interface.

Upon completing this module, you will meet these objectives:

- Describe the AlienVault USM Appliance graphical user interface
- Understand how to work with the menus and options available on the graphical user interface
- Verify basic AlienVault USM Appliance operations

This module includes these topics and lab exercises:

- Initial USM Appliance Setup
- AlienVault USM Appliance User Interface
- USM Appliance Settings and Support
- AlienVault USM Appliance Primary Menu
- Environment Snapshot
- Basic Configuration
- Verify Basic Operations
- Lab 2-1: AlienVault USM Appliance Basic Configuration
- Lab 2-2: Verify AlienVault USM Appliance Basic Operations
Module 3: Asset Management

This module describes AlienVault USM Appliance asset management. Upon completing this module, you will meet these objectives:

- Define AlienVault USM Appliance assets
- Describe how AlienVault uses asset management
- Add assets to the USM Appliance asset database
- Configure and schedule asset discovery in the USM Appliance
- Configure and manage assets using asset groups, networks, and asset labels

This module includes these topics and lab exercises:

- Asset Overview
- Navigating the Assets UI
- Managing Assets
- Adding Assets
- Asset Discovery Scans
- Asset Groups
- Networks and Network Groups
- Asset Labels
- Lab 3-1: Manage AlienVault USM Appliance Assets

Module 4: Configuring Data Sources

This module describes AlienVault USM Appliance security intelligence, which uses data source plugins to normalize events from various data sources. It also includes correlation to detect security threats by tracking behavior patterns. Upon completing this module, you will meet these objectives:

- Describe data aggregation and normalization
- Describe data sources and how they work in USM Appliance
- Enable different data sources in USM Appliance
- Understand how events are processed in USM Appliance
- Calculate risk for USM Appliance events
- Correlate events in USM Appliance

This module includes these topics:

- Data Aggregation and Detection
- Data Sources
- Enabling Data Source Plugins
- Working with Events
- Risk Calculation
- Correlation
Module 5: Policies and Actions

This module describes AlienVault USM Appliance policies which are used to influence event processing, and to filter unnecessary events and false positives. The module also describes actions that can be configured as policy consequences. Upon completing this module, you will meet these objectives:

- Navigate the USM Appliance Policies user interface
- Configure USM Appliance actions
- Configure USM Appliance policies for events
- Configure USM Appliance policies for directive events

This module includes these topics and lab exercises:

- USM Appliance Policy UI Overview
- USM Appliance Policies for Events
- USM Appliance Actions
- USM Appliance Policies for Directive Events
- Policy Example Configurations
- Lab 5-1: Configure Policies and Actions

Module 6: Correlation Directives

This module describes how to customize security intelligence in AlienVault USM Appliance system. This module describes how to customize or create new correlation directives. Upon completing this module, you will meet these objectives:

- Understand logical correlation in USM Appliance
- Describe correlation directives
- Create a custom correlation directive

This module includes these topics and lab exercises:

- Logical Correlation
- Correlation Directives
- Custom Correlation Directives
- Create Custom Correlation Directive
- Lab 6-1: Configure a Custom Correlation Directive

Module 7: Threat Detection

This module describes AlienVault USM Appliance threat detection functionalities. The module describes the Intrusion Detection System (IDS) and the AlienVault USM Appliance IDS functionalities: network IDS, and host IDS. The module also describes the AlienVault USM Appliance vulnerability assessment functionality. Upon completing this module, you will meet these objectives:
• Configure AlienVault USM Appliance network IDS
• Configure AlienVault USM Appliance host IDS through the Environment screen
• Configure AlienVault USM Appliance host IDS through the Assets screen
• Configure and perform AlienVault USM Appliance vulnerability assessment

This module includes these topics and lab exercises:
• Network IDS
• Host IDS
• Deploying HIDS — Environment
• Deploying HIDS — Assets
• Vulnerability Assessment
• Lab 7-1: Deploy AlienVault USM Appliance Threat Detection Features

Module 8: Behavioral Monitoring

This module describes AlienVault USM Appliance behavioral monitoring functionalities. The module first (briefly) describes log collection, followed by AlienVault USM Appliance NetFlow collection. The module also explains the AlienVault USM Appliance availability monitoring functionality. Upon completing this module, you will meet these objectives:

• Describe and configure AlienVault USM Appliance log collection
• Describe and configure AlienVault USM Appliance NetFlow collection
• Describe and configure AlienVault USM Appliance availability monitoring

This module includes these topics and lab exercises:
• Log Collection
• NetFlow
• Availability Monitoring
• Lab 8-1: Deploy AlienVault USM Appliance Availability Monitoring

Module 9: OTX

This module describes the Open Threat Exchange (OTX). The module describes OTX and pulses, then how to follow and subscribe to other users and their pulses. Finally, students will create their own pulses. Upon completing this module, you will meet these objectives:

• Describe OTX and its important concepts
• Setting up an OTX account
• Search and subscribe to pulses and follow other OTX users
• Create a pulse for OTX

This module includes these topics and lab exercises:
• Open Threat Exchange
• Setting up an OTX Account
• Searching and Subscribing to Pulses
• Creating a Pulse
• Lab 9-1: Setting up and using OTX

**Module 10: Security Analysis**
This module describes security analysis of alarms and events produced by AlienVault USM Appliance. The module starts with a description of a security analysis process, reviews Dashboards and Alarms, and then provides a detailed breakdown of the steps and tools available during the process of security analysis.

Upon completing this module, you will meet these objectives:
• Describe the Security Analysis Process
• Examine the dashboards
• Remediate the alarms in USM Appliance
• Investigate events in USM Appliance
• Check raw logs for more details
• Examine packet captures for more details about an event
• File tickets to manage event investigation

This module includes these topics and lab exercises:
• Security Analysis Process
• Overview Dashboards
• Remediate Alarms
• Investigate Events
• Check Raw Logs
• Examine Packet Captures
• File Tickets
• Lab 10-1: Perform Security Analysis

**Module 11: System Maintenance**
This module describes AlienVault USM Appliance system maintenance. The module first describes how long AlienVault USM Appliance stores alarms, events, and logs, and how you can modify retention settings. The module also describes how to perform event and full system backup and restore. Upon completing this module, you will meet these objectives:
• Describe AlienVault USM Appliance alarms, events, and logs retention
• Describe how to perform backup and restore of events data
• Describe how to perform backup and restore of configuration data

This module includes these topics and lab exercises:
• Event, Alarm, and Log Retention
Module 12: Administrative User Management

This module describes AlienVault USM Appliance administrative user management. The module first describes the administrative user account that is the default account to manage the web UI in AlienVault USM Appliance. The module continues to describe how to change settings of an administrative user, how to manage administrative user accounts, and how to manage global authentication settings. The module also describes administrative user activity accounting, and how to perform admin user account password recovery. Upon completing this module, you will meet these objectives:

- Describe administrative user management
- Manage user profile
- Manage administrative users
- Describe administrative user accounting
- Manage global authentications settings
- Recover admin user account password

This module includes these topics and lab exercises:

- Administrative User Management
- Configuring an Administrative User
- Manage Global Authentication Settings
- Administrative User Accounting
- Recover Admin Password
- Lab 12-1: Manage Administrative Users

Module 13: AlienVault USM Appliance Deployment

This module describes AlienVault USM Appliance deployment options and explains how to prepare for the deployment. Upon completing this module, you will meet these objectives:

- Understand how to deploy AlienVault USM Appliance components
- Understand various AlienVault USM Appliance deployments
- Understand Correlation Context and Entities
- Describe how to handle other deployment considerations

This module includes these topics:

- Deploying USM Appliance Components
- Deployment Examples
Module 14: Upgrading AlienVault Unified Security Management (USM)

This module describes AlienVault USM Appliance system upgrade process. The module describes how to update the AlienVault USM Appliance system and threat intelligence feeds, and how to perform offline upgrades. Upon completing this module, you will meet these objectives:

- Understand the USM Appliance Upgrade Process
- Upgrading USM Appliance
- Upgrading the threat intelligence, plugins, and reports
- Upgrading the USM Appliance offline

This module includes these topics:

- USM Appliance Upgrade Process
- Upgrading the USM Appliance and the Threat Feed
- Offline Updates for the USM Appliance

Module 15: Reporting

This module describes AlienVault USM Appliance reporting. The module first describes how to generate, view, and schedule reports, and how to customize reports or how to generate custom ones.

Upon completing this module, you will meet these objectives:

- Describe the AlienVault USM Appliance reporting system
- Run, schedule, and view a report
- Create custom reports
- Create custom layouts for your reports
- Create custom modules from security events and logs

This module includes these topics and lab exercises:

- USM Appliance Reporting
- Running Reports
- Creating Custom Reports
- Creating Custom Layouts
- Creating Custom Modules
- Lab 15-1: Run, Schedule, and Customize a Report

Module 16: Custom Plugins

This module describes how to customize security intelligence in AlienVault USM Appliance system. The module first describes the plugins delivered by AlienVault and
then how to customize or create custom data source plugins. Then the module describes how to customize or create new correlation directives. Upon completing this module, you will meet these objectives:

- Understand how to create custom plugins for USM Appliance
- Describe the configuration files for custom plugins
- Understand the role regular expressions play in customizing plugins
- Understand the SQL files for custom plugins
- Enable the new plugin

This module includes these topics and lab exercises:

- AlienVault Plugins
- Customizing Plugins
- Plugin Configuration Files
- Regular Expressions
- SQL Files
- Enabling New Plugins
- Lab 16-1: Creating a Custom Data Source Plugin