LevelBlue

USM Anywhere™: Security Analysis (ANYSA) Syllabus

Contents

Course Introduction

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

Module 1: Introduction

This module introduces you to the course by reviewing the security analysis workflow as it applies to USM Anywhere and will also review the setup of the lab environment you will used for hands on experience in the course. These are the key objectives that you will complete in this module:

- Learn about the security analysis workflow
- Become familiar with your lab environment

Module 2: Preparation

This module introduces you to USM Anywhere and discusses the initial steps involved in discovering, organizing, scanning, and monitoring your assets. These are the key objectives that you will complete in this module:

- 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 intrusion detection works in USM Anywhere
- Learn how to send local and cloud security logs to USM Anywhere for analysis

Module 3: 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. These are the key objectives that you will complete in this module:

- Use suppression rules to hide events from view
- Use filter rules to refine events, which saves storage space

- Configure USM Anywhere to alarm on events (false negatives) you are concerned about by using orchestration rules

Module 4: Threat Intelligence

This module describes how the information received by USM Anywhere is transformed into events that are correlated into alarms based on the threat intelligence provided by the LevelBlue SpiderLabs team. These are the key objectives that you will complete in this module:

- Learn about the LevelBlue SpiderLabs team and the work they do
- Learn how data is turned into events using BlueApps
- Learn how alarms are triggered by events using correlation rules
- Learn about the LevelBlue SpiderLabs Open Threat Exchange® (OTX™)

Module 5: Detection and Evaluation

This module explains the Cyber Kill Chain model and defines how it appears on the USM Anywhere web user interface (UI). This module also introduces you to triaging and prioritizing alarms as well has how to manage investigations. These are the key objectives that you will complete in this module:

- Explain the Cyber Kill Chain process
- Review incident types and how they are represented in USM Anywhere
- Investigate information captured in events and alarms
- Triage and prioritization of alarms
- Learn how to track information and evidence in an Investigation

Module 6: Containment and Response

This module discusses how you can respond to an attack on your environment once detected by USM Anywhere. This module introduces Sensor apps and BlueApps, and explains how you can manually or automatically respond to the attack using these apps. These are the key objectives that you will complete in this module:

- Introduce Sensor apps and discuss their capabilities
- Introduce BlueApps and discuss their capabilities
- Describe app actions and how they can be used to respond to attacks

Module 7: Recovery

This module discusses various topics to consider when recovering from an attack that will help you restore your environment and implement measures to prevent future attacks. These are the key objectives that you will complete in this module:

- Restore your environment to full health
- Create orchestration rules to alarm on events

Module 8: Root Cause Analysis

This module examines the investigation of alarms, events and raw logs that have been validated as being part of a security incident. These are the key objectives that you will complete in this module:

- Identify data relevant to an incident
- Describe the investigation process
- Highlight the tools to leverage to aid in investigations
- Prepare root cause analysis incident reports for management

Module 9: Conclusion

This module provides a summary of the entire course and reviews what you have learned in each module. It also provides information about useful LevelBlue resources to help you with your day-to-day work. These are the key points that were discussed in this course and helpful information:

- 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