LevelBlue

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

Contents

Module 0: 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 USM Anywhere™ solution. These are the key objectives that you will complete in this module:

- Define security threats
- Identify security challenges in organizations
- Understand the functions and benefits of USM Anywhere

Module 1: Deployment

This module provides an overview of the deployment process of USM Anywhere, and shows how to install and configure additional sensors. These are the key objectives that you will complete in this module:

- Define USM Anywhere
- Explain the USM Anywhere deployment flow
- Understand USM Anywhere deployment models
- Connect a sensor to USM Anywhere
- Connect to USM Anywhere

Module 2: Log Collection

This module explains log collection in USM Anywhere, how to configure log forwarding for Microsoft Windows and Linux assets, and how the data from that log forwarding is turned into events in USM Anywhere. These are the key objectives that you will complete in this module:

- Define USM Anywhere log management
- Configure log forwarding for Linux (rsyslog, osquery) and Windows (NXLog, Sysmon)
- Configure cloud log forwarding (Amazon CloudWatch, [Amazon Web Services] CloudTrail, Amazon Virtual Private Cloud [VPC] Flow Logs)
- Configure a scheduled task
- Understand USM Anywhere BlueApps
- Understand the events page
- Troubleshoot log management

Module 3: Organizing Assets and Asset Groups

This module explains how to add Assets to the USM Anywhere, and how to organize them with Asset Groups. These are the key objectives that you will complete in this module:

- Understand how to add assets to USM Anywhere
- Understand searches and filters
- Understand and create custom asset fields
- Create and modify both static and dynamic asset groups

Module 4: Creating Views and Reports

This module explains how to create and save custom Views to display details about Assets, Asset Groups, Alarms, and Events. These are the key objectives that you will complete in this module:

- Understand Dashboards and their use
- Create and configure saved views
- Export view data as reports

Module 5: Authenticated Scans and Vulnerabilities

This module covers how to configure credentials, perform authenticated scans, and schedule scanning. These are the key objectives that you will complete in this module:

- Define authenticated scans
- Configure credentials for Microsoft Windows Remote Management (WinRM) and Linux (SSH)
- Configure and run authenticated scans
- Schedule recurring asset scan jobs

Module 6: Investigate and Remediate Vulnerabilities

This module explains how to leverage the information provided to prioritize and remediate vulnerabilities. These are the key objectives that you will complete in this module:

- Investigate and remediate vulnerabilities
- Investigate and remediate configuration issues

Module 7: Events and Alarms

This module explains how Alarms are generated from suspicious events. These are the key objectives that you will complete in this module:

- Generate events and alarms
- Investigate how alarms are created
    - Data sources
    - BlueApps
    - Correlation rules
    - LevelBlue Labs Open Threat Exchange® (OTX™)
- Cloud-based alarms

Module 8: Using BlueApps

This module explains the difference between Sensor Apps and BlueApps and how each can be used. These are the key objectives that you will complete in this module:

- Learn about the currently available apps
- Work with the apps

Module 9: Reviewing and Managing your Subscription

This module demonstrates how to monitor a deployment of USM Anywhere and stay aware of any limits, based on the subscription. It teaches how to stay within the monthly limits. These are the key objectives that you will complete in this module:

- Review the subscription
- Reduce event storage through filters

Module 10: Compliance and Reporting

This module covers the different compliance templates that are available. These are the key objectives that you will complete in this module:

- Create reports for ISO 27001 processes:
    - Asset
    - Event

- Alarm

Module 11: Additional Features

This module provides an overview of different features within USM Anywhere, including data management, user management, bookmarks, and messages. These are the key objectives that you will complete in this module:

- Request raw log data
- Manage user accounts
- Set and reference bookmarks
- Check messages and release notes

Module 12: Implementing Rules

The module deep dives into the powerful rules engine in USM Anywhere. It teaches how rules can be leveraged to address noisy events and alarms that may be false positives, or of no interest. It also covers how rules are used to enhance events and alarms by triggering further actions. These are the key objectives that you will complete in this module:

- Understand the rules operators
- Suppress events and alarms through rules
- Create app action rules
- Create multi-level rules
- Understand the rules syntax
- Match the original log line
- Create and use multiple variables to compare dynamic content

Module 13: Rules Best Practice

The module builds on the previous module be teaching the best practice to follow when creating rules in USM Anywhere. It teaches how badly written rules can impact the performance of your environment and explains what errors and warnings can appear as a result. These are the key objectives that you will complete in this module:

- Understand the general best practice for rule creation
- Understand the condition order in rules and why it is important

- Understand the rule operators and which are most appropriate
- Understand how rule performance is evaluated
- Examine the rule history to audit changes
- Modify a badly performing rule to address issues
- Create a rule based on the best practices