NterOne REINVENT YOURSELF

SWAT
Cisco Stealthwatch Tuning

Duration: 2 Days

Course Overview:

Cisco Stealthwatch Tuning is a two-day course which provides resources to make the configuration and use of the Cisco Stealthwatch System manageable. The course builds on the content introduced in the Cisco Stealthwatch for Security Operations, Cisco Stealthwatch for Network Operations and Cisco Stealthwatch for System Administrators courses.

Prerequisites:

The knowledge and skills that the learner should have before attending this course are as follows:

- Cisco Stealthwatch for Security Operations
- Cisco Stealthwatch for Network Operations
- Stealthwatch Foundation

Who Should Attend:

The primary audience for this course is as follows:

- Individuals who are responsible for tuning the Stealthwatch System, creating and maintaining policies, monitoring traffic, and obtaining and responding to actionable alarm.

Course Objectives:

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe how the Cisco Stealthwatch Enterprise system provides network visibility through monitoring and detection.
- Define tuning and how it helps the Stealthwatch system create actionable alarms.
- Use the stages of the tuning process to identify workflows and best practices to operationalize Stealthwatch

Course Outline:

Module One

- Course Introduction
- Cisco Stealthwatch Tuning Course Overview
- The Purpose of Tuning
- Understanding Security Events and Alarms
- Defining Stealthwatch Policies

Module Two

- Posture the System
- Host Locks and Custom Security Events
- Response Management
- Tiered Alarms
- Culminating Scenario: Tuning
- Tuning Best Practices in Stealthwatch
- Cisco Stealthwatch Tuning Course Outcomes
- Course Conclusion

Lab Outline:

Lab 1: Classify Public and Private IP Addresses

Lab 2: Trusted Internet Hosts

Lab 3: Classify Undefined Services and Applications

Lab 4: Classify Network Scanners with the SMC Web UI

Lab 5: Reclassify IPs to Reduce Noise

Lab 6: Edit Role Policy

Lab 7: Host Locks and Custom Security Events

Lab 8: Create a Dashboard