Administering & Managing Cisco Stealthwatch Operation

Course Objective:

This course focuses on using Cisco Stealthwatch Enterprise from the perspective of a security analyst. The overarching goal of the course is to use Stealthwatch to investigate potential security issues and make initial determinations of whether to proceed with a more thorough investigation or to move on to the next potential threat.

You will learn how to configure fundamental elements of Cisco Stealthwatch Enterprise.

- Describe how the Stealthwatch System provides network visibility through monitoring and detection.
- Describe the goals of using Stealthwatch in the proactive and operational modes.
- Define basic concepts of investigation and detection of potential security issues using the Stealthwatch System.
- Complete workflows to identify indicators of compromise in your network.
- Describe alarm types and alarm notification within Stealthwatch.
- Explain the utility of maps in the Stealthwatch System.
- Describe how the Stealthwatch System contributes to successful incident handling.

Course Delivery and Duration

Delivery method can be Classroom and Online
Duration of Training: **6 Days**

Course Outline

Module 1:- Cisco Stealthwatch for System Administrators (SSA)

- Why Stealthwatch? What is Stealthwatch
- Introduction to Stealthwatch
- Basic Stealthwatch System Installation : Part 1
- Basic Stealthwatch System Installation: Part 2
- SMC Configuration
- The Many User Interfaces of Stealthwatch
- Stealthwatch Application Validation
- Management Console: Basic Setup
- Hosts and Host Groups
- Classify Services and Applications/ Classification of Customer Environment
- Network Devices and the By Function Host Group
- Policy Management: Group Policy
- User and Role Management
- Custom Documents
- Response Management
- Review the Web Application: What's New?

Module 2:- Cisco Stealthwatch for Network

Workflows for Proactive Monitoring

- Validate Exporters
- Proactive with Hosts and Host Groups
- Proactive by Using Maps
- Proactive with Host Locking
- Proactive with Custom Security Events
- Proactive with Policy Management
- Proactive with Response Management
- Proactive with Custom Documents

Reactive Workflows

- Reacting to Overloading Interfaces
- Reactive to Network Issues Where the Host IP is Known
- Reacting to Slow Response
- Reacting to New Devices and Unknown Devices Added to the Network
- Reacting to Reoccurring Issues on the Network
- Documenting Investigations After Resolution

Module 3:- Cisco Stealthwatch for Security

- Introduction to Security
- Using Stealthwatch in the Proactive Mode
- Pattern Recognition
- Investigation and Detection Using Stealthwatch
- Using Top Reports and Flow Tables for Detection
- Creating and Using Dashboards for Detection
- Creating Custom Security Events
- Proactive Investigation Practice
- Using Stealthwatch in the Operational Mode
- Alarms and Alarm Response
- Responding to Alarms
- Maps
- Using Maps for Incident Response
- Host Identification
- Identify Hosts Using Host Snapshot and Host Report
- Culminating Scenario: Using Stealthwatch for Insider Threats
- Security Best Practices in Stealthwatch
- Cisco Stealthwatch Security Course Outcomes

Labs

- Scenario 1. Appliance Setup Tool
- Scenario 2. Appliance Post-Install Configuration & Verification
- Scenario 3. Additional SMC and Central Management Configuration

- Scenario 4. Configure Host Groups
- Scenario 5. Cisco Router NetFlow Configuration and Validation
- Scenario 6. Cisco Router ETA Configuration and Validation
- Scenario 7. Custom Security Events
- Scenario 8. Accessing the Stealthwatch Desktop Client
- Scenario 9. Verify Flow Data and Exporters
- Scenario 10. Classification of Customer Environment
- Scenario 11. Classification of Undefined Services and Application
- Scenario 12. Cisco ISE Integration (Identity Services Engine)
- Scenario 13. Configure the AD LDAP Lookup Feature
- Scenario 14. Creating a Custom Document
- Scenario 15. Response Management
- Scenario 16. Configure Appliance SNMP Agent
- Scenario 17. Determine Estimated FC Database Storage Capacity
- Scenario 18. Create Configuration Backups
- Scenario 19. Stealthwatch Patching - Central Management
- Scenario 21: Health Check - Inventory
- Scenario 22: Health Check - Data Gathering
- Scenario 23: Health Check - UDP Director Log Review
- Scenario 24: Health Check - Flow Collector Log Review
- Scenario 25: Health Check - SMC Log Review
- Scenario 26: Health Check - Flow Sensor Log Review
- Scenario 27: Remediation - Secondary SMC
- Scenario 28: Remediation - Additional FC
- Scenario 29: Remediation - SMC
- Scenario 30: Stealthwatch Apps
- Scenario 31: Remediation - NetFlow Template
- Scenario 32: Advanced NetFlow Configuration
- Scenario 33: NBAR
- Scenario 34: Remediation - Enable ASA NetFlow
- Scenario 35: SIEM Integration
- Scenario 36: NVZ Flow - AnyConnect
- Scenario 37: Tuning - Basic
- Scenario 38: Tuning - Advanced
- Scenario 39: Custom Security Events - ETA
- Scenario 40: Incident Response & Threat Hunting
- Scenario 41: Stealthwatch API
- Scenario 42: Relationship Policy
- Scenario 43: External Lookups
- Scenario 44: Cisco ISE ANC Integration
- Scenario 45: Multiple FC