Course Outline

Day One

Course Introduction

Cisco Stealthwatch Tuning Course Overview

The Purpose of Tuning

Understanding Security Events and Alarms

Defining Stealthwatch Policies

Classify the System

Lab: Classify Public and Private IP Addresses

Lab: Trusted Internet Hosts

Lab: Classify Undefined Services and Applications

Quiet Noisy Hosts

Lab: Classify Network Scanners with the SMC Web UI

Lab: Reclassify IPs to Reduce Noise

Day Two

Day One Review

Posture the System

Lab: Edit Role Policy

Host Locks and Custom Security Events

Lab: Host Locks and Custom Security Events

Response Management

Tiered Alarms

Lab: Create a Dashboard

Culminating Scenario: Tuning

Tuning Best Practices in Stealthwatch

Cisco Stealthwatch Tuning Course Outcomes

Course Conclusion