SWAT (CISCO STEALTHWATCH TUNING) 1.0

Objetivo

After taking this course, you should be able to: * Describe how Stealthwatch 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.

PÃºblico Alvo

This course is intended for professionals want to tuning the Stealthwatch System, creating and maintaining policies, monitoring traffic, and obtaining and responding to actionable alarms.

PrÃ©-Requisitos

It is strongly recommended to complete the Stealthwatch Foundations training prior to taking this training. ItÂ´s recommended the learning participated on the following trainings: * Cisco Stealthwatch for Security Operations; * Cisco Stealthwatch for Network Operations.

Carga HorÃ¡ria

16 horas (2 dias).

ConteÃºdo ProgramÃ¡tico

Course Introductions
Course Outline
Course Goal & Objectives

Part 1
Cisco Stealthwatch Tuning Course Overview
The Purpose of Tuning
Understanding Security Events and Alarms
Defining Stealthwatch Policies
Classify the System
Lab 1: Classify Public and Private IP Addresses
Lab 2: Trusted Internet Hosts
Lab 3: Classify Undefined Services and Applications
Quiet Noisy Hosts
Lab 4: Classify Network Scanners with the SMC Web UI
Lab 5: Reclassify IPs to Reduce Noise

Part 2

Day One Review
Posture the System
Lab 6: Edit Role Policy
Host Locks and Custom Security Events
Lab 7: Host Locks and Custom Security Events
Response Management
Tiered Alarms
Lab 8: Create a Dashboard
Culminating Scenario: Tuning
Tuning Best Practices in Stealthwatch
Cisco Stealthwatch Tuning Course Outcomes
Course Conclusion