SWAT

Cisco Stealthwatch Tuning

16 horas | Security & Cybersecurity | Cisco

INTRODUÇÃO

The Cisco Stealthwatch Tuning (SWAT) v7.1 course focuses on the tuning process in Cisco Stealthwatch Enterprise system, to gain visibility across your enterprise and detect actionable threats. This course covers all essential aspects of the tuning process, including tuning best practices, which will optimize the Stealthwatch System.

This course will help you:
* Understand how the system generates events and alarms;
* Configure policies and adjust system events and alarms;
* Understand the importance of hosts and host groups.

OBJETIVO DO CURSO

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.

PÚBLICO-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.

PRÉ-REQUISITOS

It is strongly recommended to complete the Stealthwatch Foundations training prior to taking this training.

It´s recommended the learning participated on the following trainings:
* Cisco Stealthwatch for Security Operations;
* Cisco Stealthwatch for Network Operations.

CONTEÚDO PROGRAMÁTICO

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