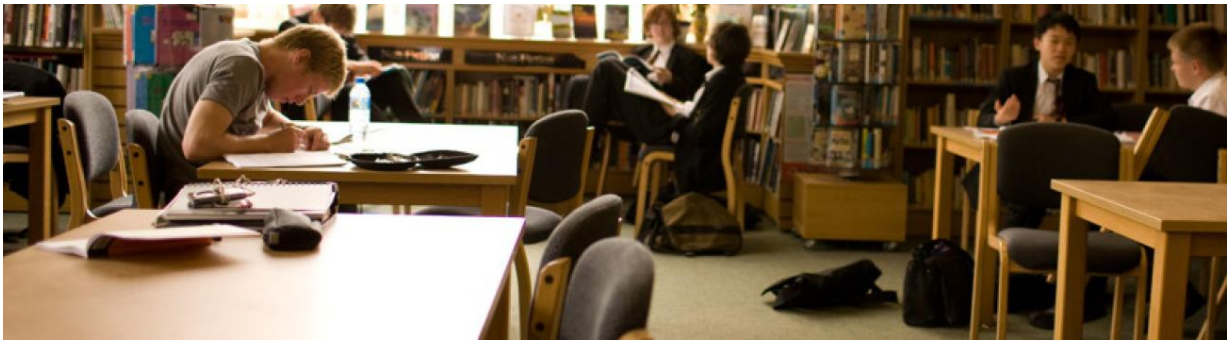
Cisco Stealthwatch Educational Services

Cisco Stealthwatch for Security Operations (SSO)



Cisco Stealthwatch for Security Operations (SSO) is a Virtual Instructor-Led, lab-based, hands-on course offered by the Security Business Unit's Stealthwatch Educational Services team. This course focuses on the proper use of host groups, policies and alarm configuration and the three phases of the Cisco Stealthwatch tuning process.

Cisco Stealthwatch for Security Operations is a lab intensive course that focuses on those who are responsible for using Stealthwatch for monitoring security policy, providing feedback on the configuration, updating and operation of security tools and initiating incident response investigations.

Duration

- Virtual Instructor-Led classroom (VILT): 2 days
- Instructor-Led classroom (ILT): 2 days

Target Audience

This course focuses on new users of Cisco Stealthwatch. This course is intended for customers whose role is to use the Cisco Stealthwatch System for security operations & security monitoring.

Course Objectives

Upon completing this course, you will be able to:

- Explain what Cisco Stealthwatch is and how it works.
- Explain how hosts and host groups are defined in Cisco Stealthwatch.
- Define basic concepts of policy management.
- Identify the three phases of the Cisco Stealthwatch tuning process.
- Complete workflows to identify indicators of compromise in your network.

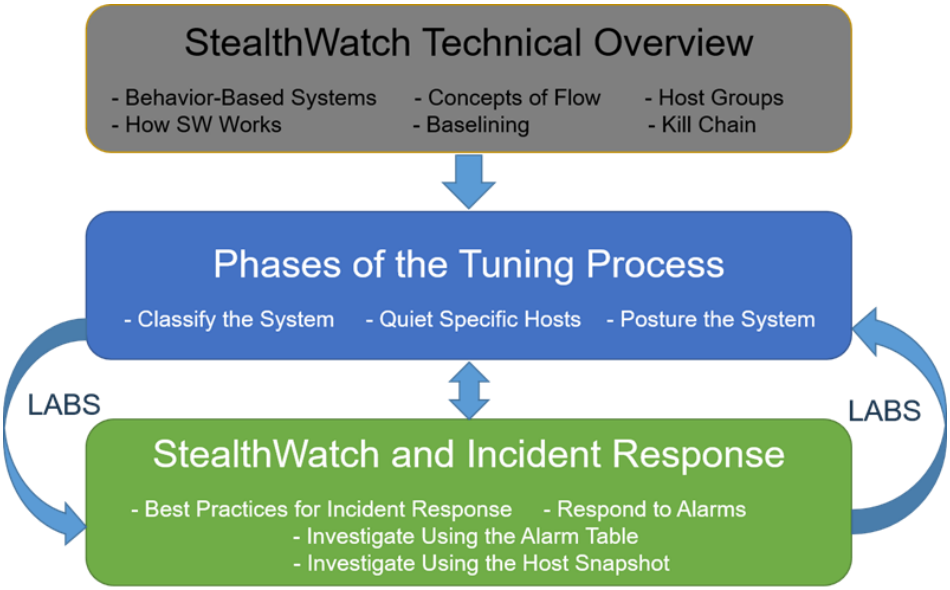
Course Prerequisites and Assumed Knowledge

All students should have completed the following (minimum) prerequisites. These prerequisites are available as eLearning courses found in the Cisco Stealthwatch Customer Training Center (LMS) available through the Customer Community:

- Flow Basics
- Cisco Stealthwatch Overview and Components
- Cisco Stealthwatch SMC Client Interface Overview
- Cisco Stealthwatch Web App Overview

Course Structure

The course can be categorized in the following major concept areas:



Course Outline

Technical Overview

Tuning the System

- Defining Host Groups
- Using Catch All and By Function Host Groups
- Classifying Inside Hosts
- Quieting Noisy Devices
- Posturing the System
- Working with Threshold and Behavioral Alarms
- Understanding / Viewing Traffic
- Defining Services and Applications
- Viewing Traffic from Undefined Sources
- Defining the By Function Host Group
- Reducing False Positives

Incident Response

- Putting Together an Incident Response Process
- Example Workflow for Incident Response

Lab Outline

The course consists of the following labs:

- Lab: Discover and Classify Public IP Addresses
- Lab: Policy and Using By Function Host Groups
- Lab: Classify and Quiet Specific Hosts
- Lab: Maps
- Lab: Host Locking
- Lab: Incident Response
- Lab: Exploring an Advanced Map
- Lab: Copyright Infringement
- Lab: Insider Threats
- Lab: Analysis of an Attack

For More Information

Contact the Customer Success Educational Services team at Stealthwatch-Training@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**