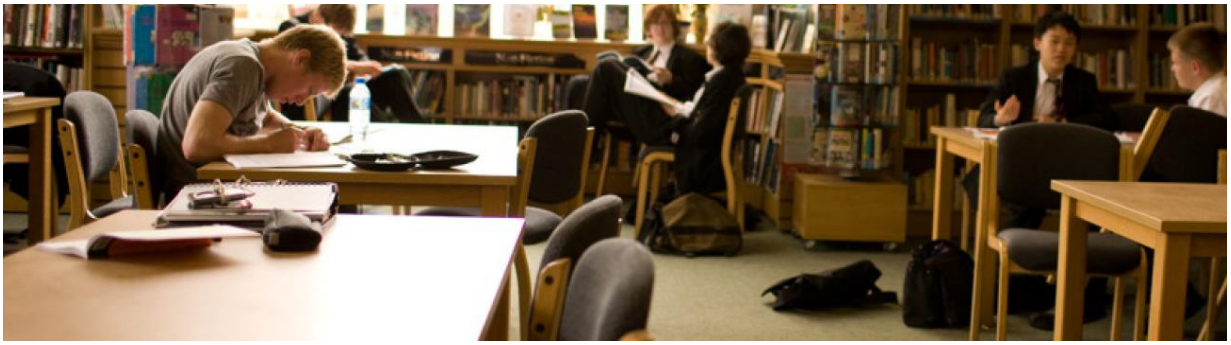
Cisco Stealthwatch Educational Services

Cisco Stealthwatch Tuning (SWAT)



Cisco Stealthwatch Tuning (SWAT) is a Virtual Instructor-Led, hands-on course offered by the Security Business Unit's Stealthwatch Educational Services team. This course provides resources to make the configuration and use of the Cisco Stealthwatch System manageable.

To help make our customers successful, we provide resources to make the configuration and use of the Cisco Stealthwatch System manageable. This one-day Cisco Stealthwatch Advanced Tuning course is designed for Cisco Stealthwatch administrators and analysts who are familiar with the basics of tuning the Cisco Stealthwatch System.

The course builds on the content introduced in the Cisco Stealthwatch for Security Operations, Cisco Stealthwatch for Network Operations and Cisco Stealthwatch for System Administrators courses.

Duration

- Virtual Instructor-Led classroom (VILT): 1 day
- Instructor-Led classroom (ILT): 1 day

Course Objectives

Upon completing this course, you will be able to:

- Create summary views of all alarms in the system.
- Explain how summary views can help prioritize the tuning strategy.
- Develop tuning recommendations based on security events and alarm summary.
- Identify workflows for tuning specific security events.
- Test tuning strategies and recommendations.

Target Audience

This course is designed for the installed based of new and existing Cisco Stealthwatch customers.

Course Prerequisites and Assumed Knowledge

It assumes that the customer has either taken these courses or feels comfortable with concepts such as creating and modifying host groups, classifying scanners, servers, services and applications, editing default/host/role policies, creating custom events, posturing the Cisco Stealthwatch System and identifying the bad hosts in the system.

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

- Cisco Stealthwatch for Security Operations
- Cisco Stealthwatch for Network Operations

Course Outline

The course consists of the following lessons:

- Summarizing alarms with your SIEM
- Working with large numbers of alarms
- Strategy for summarizing alarms
- Understanding the value of summarizing alarms and security event data

Tuning Recommendations for Specific Security Events

- Discussions around specific security events
- Using knowledge of specific security for tuning and posture
- Workflows for tuning specific security events
- Workflows for investigating specific security events

Testing Your Tuning Recommendations

- Presenting your tuning recommendations
- Monitoring your system posture
- Testing your tuning recommendations

Lab Outline

- Lab: Create Pivot Tables Based on Alarm Summaries
- Lab: Create and Customize Security Events, Define Stealthwatch Applications and Schedule Reports
- Lab: Host Locking and Custom Security Events
- Lab: Discover Security Events and Create New Policy
- Lab: Proactive Tune and Confirm Applied Policy
- Lab: Alternate Tuning Methods for Scanning Events
- Lab: Trust an Outsider with Policy or Services
- Investigate Alarm Traffic

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.**