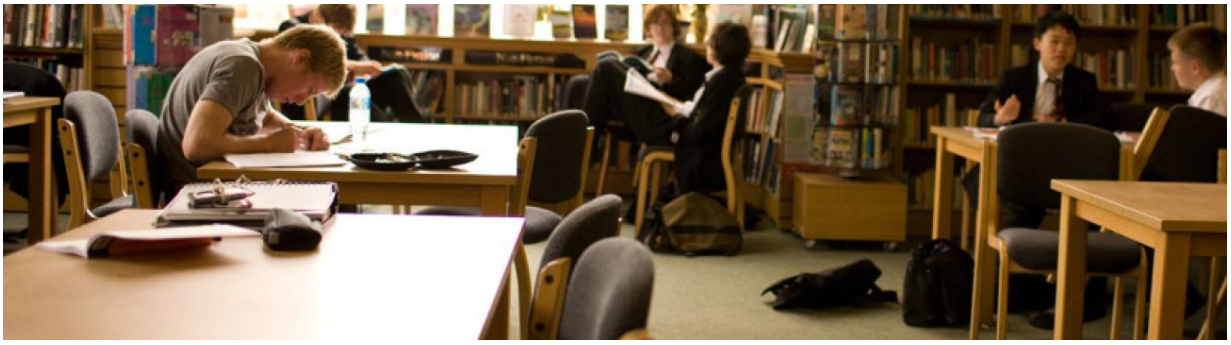
Cisco Stealthwatch Educational Services

Cisco Stealthwatch Proactive Hunting and Detection (PHD)



Cisco Stealthwatch Proactive Hunting and Detection (PHD) is a Virtual Instructor-led, hands-on course offered by the Security Business Unit's Stealthwatch Educational Services team. This course focuses on proactively monitoring the network and actively identify suspicious behavior on the network.

In previous Cisco Stealthwatch training courses, students received instruction on basic use of the Cisco Stealthwatch System. This course provides advanced instruction for organizations that have developed a mature use of Cisco Stealthwatch alarms and policies. Using Cisco Stealthwatch to proactively search for abnormal behavior requires a solid understanding of host groups, tuning and familiarity with Cisco Stealthwatch alarms and policies. Before beginning this course, learners should know how to triage relevant alarms and investigate specific indicators of compromise.

Duration

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

Course Objectives

Upon completing this course, you will be able to:

- Use patterns and context to detect network anomalies.
- Detect hosts using known services over non-standard ports.

- Detect specific DNS issues including rogue DNS servers, suspicious DNS services based on their graphical representation and potential amplification attacks against improperly configured DNS servers.
- Identify NTP traffic destined to the internet but NOT sourcing from a known internal NTP server.
- Use Top Conversation reports to identify misconfigured endpoints.
- Complete security assessment workflows related to protecting assets and data, enhancing defenses and identifying rogue servers, zone transfers and users bypassing proxy services and more.

Target Audience

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

Course Prerequisites and Assumed Knowledge

While the course does not have formal prerequisites, it is strongly recommended that 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 available through the Stealthwatch Customer Community:

- Cisco Stealthwatch for Security Operations
- Cisco Stealthwatch Advanced Tuning

Course Outline

The course consists of the following lessons:

Lesson 1: Detection Requirements

- Explain the importance of using the concepts that you have already learned
- Use by-function host groups, network classification, categorizing traffic
- Understand what alarms are important to your organizational policies and how to triage them
- Use Cisco Stealthwatch in investigative, reactive and proactive interactions
- Understand the necessity of access to employees that are extremely knowledge about the current network

Lesson 2: Pattern Recognition

- The importance of recognizing patterns in your system
- Identifying and working with traffic patterns
- Identifying traffic spikes
- Alarm patterns using specific hosts, host groups, target host, target host groups
- Recognizing suspicious traffic based on when traffic occurs

- Detecting patterns in DNS and NTP traffic

Lesson 3: Context

- The importance of understanding context
- Using context in working with dashboards and reports
- Using context to identify related alarms and security events
- Using context in the identification of red flags in investigating alarms, traffic, Top X reports, flow data and other resources available in Cisco Stealthwatch

Lesson 4: Workflows Around Concerning Traffic Patterns

- Identify notable but not necessarily malicious traffic with the internet as a source or destination
- Identifying suspicious traffic patterns in combination with suspicious flow conversations
- Identifying odd traffic patterns based on one-day, two-day and seven-day historical analysis
- Identifying the appropriate values to drill into after detecting suspicious flows

Lesson 5: Workflows Around Known Traffic with Unknown Ports

- The role of the Flow Sensor when working with unknown ports
- Identifying hosts using services on non-standard ports
- Identifying hosts attempting to circumvent IDS or business policy
- Using the new Fake Application Detected security event

Lesson 6: Workflows Around Unsanctioned Services

- Identifying DNS and NTP traffic destined to the internet from suspicious source
- Identifying hosts with configuration issues
- Identifying hosts attempting to bypass IDS/business policy

Lesson 7: Workflows Around User-to-User Traffic

- Detecting user to using traffic

Lesson 8: Security Assessment Workflows

- Workflow to protect assets and data
- Workflow working with behavioral analytics
- Workflow using DNS analytics
- Workflow related to rogue servers, zone transfers users bypassing proxy services

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.**