alialia
CISCO
The bridge to possible

Cisco Stealthwatch Security Instructor-Led Training

Course overview

Cisco Stealthwatch Security is an instructor-led, lab-based, hands-on course offered by the Cisco Stealthwatch Learning Services team. This two-day course focuses on using Cisco Stealthwatch Enterprise from the perspective of a security analyst. The overarching goal of the course is to use the Stealthwatch System to investigate potential security issues and make initial determinations on whether to proceed with a more thorough investigation or to move on to the next potential threat.

This course is intended for individuals who are responsible for using Stealthwatch to monitor security policy, provide feedback on the configuration, and initiate incident response investigations. An entry-level security analyst is the ideal audience for this class.

Course agenda

Day One	
Module: Preface	**60 minutes**
Course Introduction	60 minutes
Module: Introduction	**45 minutes**
Cisco Stealthwatch Security Course Overview	15 minutes
Introduction to Security	30 minutes
Lunch	**60 minutes**
Module: Stealthwatch in the Proactive Mode	**180 minutes**
Using Stealthwatch in the Proactive Mode	30 minutes
Pattern Recognition	45 minutes
Investigation and Detection Using Stealthwatch	30 minutes
Lab: Using Top Reports and Flow Tables for Detection	15 minutes
Lab: Creating and Using Dashboards for Detection	30 minutes
Lab: Creating Custom Security Events	30 minutes

Day Two	
Day One Review	**20 minutes**
Module: Stealthwatch in the Proactive Mode (continued)	**30 minutes**
Lab: Proactive Investigation Practice	30 minutes
Module: Stealthwatch in the Operational Mode	**80 minutes**
Using Stealthwatch in the Operational Mode	15 minutes
Alarms and Alarm Response	15 minutes
Lab: Responding to Alarms	20 minutes
Maps	10 minutes
Lab: Using Maps for Incident Response	20 minutes
Lunch	**60 minutes**

Day Two	
Module: Stealthwatch in the Operational Mode (continued)	**25 minutes**
Host Identification	10 minutes
Lab: Identify Hosts Using Host Snapshot and Host Report	15 minutes
Module: Summary	**90 minutes**
Culminating Scenario: Using Stealthwatch for Insider Threats	60 minutes
Security Best Practices in Stealthwatch	15 minutes
Cisco Stealthwatch Security Course Outcomes	15 minutes
Module: Course Wrap Up	**15 minutes**
Course Conclusion	15 minutes

For more information

Contact the Cisco Stealthwatch Learning Services team at: Stealthwatch-Training@cisco.com

---

Course content is dynamic and subject to change without notice.

C22-3077501-00   07/22