

Cisco Stealthwatch Security (SSO)

Course Outline:

Day One

- Cisco Stealthwatch Security Course Overview
- Introduction to Security
- Using Stealthwatch in the Proactive Mode
- Pattern Recognition
- Investigation and Detection Using Stealthwatch
- Lab: Using Top Reports and Flow Tables for Detection
- Lab: Creating and Using Dashboards for Detection
- Lab: Creating Custom Security Events
- Lab: Proactive Investigation Practice

Day Two

- Using Stealthwatch in the Operational Mode
- Alarms and Alarm Response
- Lab: Responding to Alarms
- Maps
- Lab: Using Maps for Incident Response
- Host Identification
- Lab: Identify Hosts Using Host Snapshot and Host Report
- Culminating Scenario: Using Stealthwatch for Insider Threats
- Security Best Practices in Stealthwatch
- Cisco Stealthwatch Security Course Outcomes