View Full Course Details including Latest Schedule Online

CISCO

SECOPS Certification Training

Due to Covid-19 safety restrictions PhoenixTS will temporarily be unable to provide food to our students who attend class at our Training Center; however, our Break Areas are **currently open** where students will find a constant supply of Coffee, Tea and Water. Students may bring their own lunch and snacks to eat in our breakrooms or at their seat in the classroom or eat out at one of the many nearby restaurants.

Course Overview

Our 5- day, instructor-led SECOPS (Implementing Cisco Cybersecurity Operations) training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online is intended to teach the introductory-level skills and knowledge required for success in a Security Operations Center (SOC) . It will teach you the fundamental skills required to begin a career working as an associate-level cybersecurity analyst in a security operations center.

This course will prepare you for the associate level 210-255® Certification exam.

Course Outline

Module 1: SOC Overview

Lesson 1: Defining the Security Operations Center

- Types of Security Operations Centers
- SOC Analyst Tools
- Data Analytics
- Hybrid Installations: Automated Reports, Anomaly Alerts
- Sufficient Staffing Necessary for an Effective Incident Response Team
- Roles in a Security Operations Center
- Develop Key Relationships with External Resources

- Challenge

Lesson 2: Understanding NSM Tools and Data

- Introduction
- NSM Tools
- NSM Data
- Security Onion
- Full Packet Capture
- Session Data
- Transaction Data
- Alert Data
- Other Data Types
- Correlating NSM Data
- Challenge

Lesson 3: Understanding Incident Analysis in a Threat-Centric SOC

- Classic Kill Chain Model Overview
- Kill Chain Phase 1: Reconnaissance
- Kill Chain Phase 2: Weaponization
- Kill Chain Phase 3: Delivery
- Kill Chain Phase 4: Exploitation
- Kill Chain Phase 5: Installation
- Kill Chain Phase 6: Command-and-Control
- Kill Chain Phase 7: Actions on Objectives
- Applying the Kill Chain Model
- Diamond Model Overview
- Applying the Diamond Model
- Exploit Kits
- Challenge

Lesson 4: Identifying Resources for Hunting Cyber Threats

- Cyber-Threat Hunting Concepts
- Hunting Maturity Model
- Cyber-Threat Hunting Cycle
- Common Vulnerability Scoring System
- CVSS v3.0 Scoring
- CVSS v3.0 Example
- Hot Threat Dashboard

- Publicly Available Threat Awareness Resources
- Other External Threat Intelligence Sources and Feeds Reference
- Challenge

Module 2: Security Incident Investigations

Lesson 1: Understanding Event Correlation and Normalization

- Event Sources
- Evidence
- Security Data Normalization
- Event Correlation
- Other Security Data Manipulation
- Challenge

Lesson 2: Identifying Common Attack Vectors

- Obfuscated JavaScript
- Shellcode and Exploits
- Common Metasploit Payloads
- Directory Traversal
- SQL Injection Cross-Site Scripting
- Punycode
- DNS Tunneling
- Pivoting
- Challenge

Lesson 3: Identifying Malicious Activity

- Understanding the Network Design
- Identifying Possible Threat Actors
- Log Data Search
- NetFlow as a Security Tool
- DNS Risk and Mitigation Tool
- Challenge

Lesson 4: Identifying Patterns of Suspicious Behavior

- Network Baselining

- Identify Anomalies and Suspicious Behaviors
- PCAP Analysis
- Delivery
- Challenge

Lesson 5: Conducting Security Incident Investigations

- Security Incident Investigation Procedures
- Threat Investigation Example: China Chopper Remote Access Trojan
- Challenge

Module 3: SOC Operations

Lesson 1: Describing the SOC Playbook

- Security Analytics
- Playbook Definition
- What Is In a Play?
- Playbook Management System
- Challenge

Lesson 2: Understanding the SOC Metrics

- Security Data Aggregation
- Time to Detection
- Security Controls Detection Effectiveness
- SOC Metrics
- Challenge

Lesson 3: Understanding the SOC WMS and Automation

- SOC WMS Concepts
- Incident Response Workflow
- SOC WMS Integration
- SOC Workflow Automation Example
- Challenge

Lesson 4: Describing the Incident Response Plan

- Incident Response Planning
- Incident Response Life Cycle
- Incident Response Policy Elements
- Incident Attack Categories
- Reference: US-CERT Incident Categories
- Regulatory Compliance Incident Response Requirements
- Challenge

Exam Information

Students can elect to take the associate-level 210-255 Implementing Cisco Cybersecurity Operations (SECOPS) Exam.

SECOPS Certification Exam 210-255 Details:

- Number of Questions: 60-70
- Passing Score: 80%
- Test Duration: 90 minutes
- Test Format: Multiple Choice, Multiple Answer, Drag and drop, Testlets, Simlets, Router & Switch Simulations
- Test Delivery: Pearson VUE

SECOPS Certification Exam Domains:

This exam tests candidates on the following domains:

- Endpoint Threat Analysis and Computer Forensics
- Network Intrusion Analysis
- Incident Response
- Data and Event Analysis
- Incident Handling

Due to Covid-19 safety restrictions PhoenixTS will temporarily be unable to provide food to our students who attend class at our Training Center; however, our Break Areas are **currently open** where students will find a constant supply of Coffee, Tea and Water. Students may bring their own

lunch and snacks to eat in our breakrooms or at their seat in the classroom or eat out at one of the many nearby restaurants.

Starting at **$4,295**

ATTENTION

For GSA pricing or Contractor quotes call

240.667.7757

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.