View Full Course Details including Latest Schedule Online

CISCO

SECOPS Certification Training

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

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.

Schedule

Currently, there are no public classes scheduled. Please contact a Phoenix TS Training Consultant to discuss hosting a private class at 301-258-8200.

Program Level

Advanced

Training Delivery Methods

Group Live

Duration

5 Days / 32 hours Training

CPE credits

26 NASBA CPE Credits

Field of Study

Information Technology

Advanced Prep

N/A

Course Registration

Candidates can choose to register for the course by via any of the below methods:

- Email: Sales@phoenixts.com
- Phone: 301-582-8200
- Website: www.phoenixts.com

Upon registration completion candidates are sent an automated course registration email that includes attachments with specific information on the class and location as well as pre-course study and test preparation material approved by the course vendor. The text of the email contains a registration confirmation as well as the location, date, time and contact person of the class.

Online enrolment closes three days before course start date.

On the first day of class, candidates are provided with instructions to register with the exam provider before the exam date.

Complaint Resolution Policy

To view our complete Complaint Resolution Policy policy please click here: Complaint Resolution Policy

PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Refunds and Cancellations

To view our complete Refund and Cancellation policy please click here: Refund and Cancellation Policy

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

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Phoenix TS is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints re-garding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

Starting at **$4,295**

ATTENTION

For GSA pricing or Contractor quotes call 301-258-8200 – Option 2.

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Price Match Guarantee

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