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

View Full Course Details including Latest Schedule Online

CISCO

CBROPS Understanding Cisco Cybersecurity Operations Fundamentals

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

This 5-day, instructor led Cisco course teaches an understanding of the network infrastructure devices, operations, and vulnerabilities of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. You will learn basic information about security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data used to investigate security incidents. After completing this course, you will have the basic knowledge required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center to strengthen network protocol, protect your devices and increase operational efficiency. This course prepares you for the Cisco Certified CyberOps Associate certification. This course will help you:

- Learn the fundamental skills, techniques, technologies, and the hands-on practice necessary to prevent and defend against cyberattacks as part of a SOC team
- Prepare for the 200-201 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) exam which earns the Cisco Certified CyberOps Associate certification
- Earn 30 Continuing Education Credits toward recertification

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

Refunds and Cancellations

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

Course Objectives

By the end of this course, participants will be able to: • Explain how a Security Operations Center (SOC) operates and describe the different types of services that are performed from a Tier 1 SOC analyst's perspective. • Explain Network Security Monitoring (NSM) tools that are available to the network security analyst. • Explain the data that is available to the network security analyst. • Describe the basic concepts and uses of cryptography. • Describe security flaws in the TCP/IP protocol and how they can be used to attack networks and hosts. • Understand common endpoint security technologies. • Understand the kill chain and the diamond models for incident investigations, and the use of exploit kits by threat actors. • Identify resources for hunting cyber threats. • Explain the need for event data normalization and event correlation. • Identify the common attack vectors. • Identify malicious activities. • Identify patterns of suspicious behaviors. • Conduct security incident investigations. • Explain the use of a typical playbook in the SOC. • Explain the use of SOC metrics to measure the effectiveness of the SOC. • Explain the use of a workflow management system and automation to improve the effectiveness of the SOC. • Describe a typical incident response plan and the functions of a typical Computer Security Incident Response Team (CSIRT). • Explain the use of Vocabulary for Event Recording and Incident Sharing (VERIS) to document security incidents in a standard format.

Course Outline

• Defining the Security Operations Center • Understanding Network Infrastructure and Network Security Monitoring Tools • Exploring Data Type Categories • Understanding Basic Cryptography Concepts • Understanding Common TCP/IP Attacks • Understanding Endpoint Security Technologies • Understanding Incident Analysis in a Threat-Centric SOC • Identifying Resources for Hunting Cyber Threats • Understanding Event Correlation and Normalization • Identifying Common Attack Vectors • Identifying Malicious Activity • Identifying Patterns of Suspicious Behavior • Conducting Security Incident Investigations • Using a Playbook Model to Organize Security Monitoring • Understanding SOC Metrics • Understanding SOC Workflow and Automation • Describing Incident Response • Understanding the Use of VERIS • Understanding Windows Operating System Basics • Understanding Linux Operating System Basics Lab outline • Use NSM Tools to Analyze Data Categories • Explore Cryptographic Technologies • Explore TCP/IP Attacks • Explore Endpoint Security • Investigate Hacker Methodology • Hunt Malicious Traffic • Correlate Event Logs, Packet Captures (PCAPs), and Alerts of an Attack • Investigate Browser-Based Attacks • Analyze Suspicious Domain Name System (DNS) Activity • Explore Security Data for Analysis • Investigate Suspicious Activity Using Security Onion • Investigate Advanced Persistent Threats • Explore

Exam Information

This course will help:

- Prepare for the 200-201 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) exam
- Those in pursuit of the Cisco Certified CyberOps Associate.

Prerequisites Before taking this course, you should have the following knowledge and skills:

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows and Linux operating systems
- Familiarity with basics of networking security concepts
- The following Cisco course can help you gain the knowledge you need to prepare for this course: Implementing and Administering Cisco Solutions (CCNA®)

This course is designed for:

- Students pursuing a technical degree
- Current IT professionals
- Recent college graduates with a technical degree

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

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

Starting at **$4,195**

ATTENTION

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

GSA

Price Match Guarantee

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

10420 Little Patuxent Parkway Suite 500 Columbia, MD 21044