CISCO TRAINING

Performing CyberOps Using Cisco Security Technologies

Perform CyberOps with Cisco Security Technologies. Learn to detect, analyze, and respond to cyber threats effectively.

DURATION
2 hours

LEVEL
Intermediate

FORMAT
Instructor-Led

- Globally Recognized Certification
- Expert-Led Hands-On Training
- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

This intermediate-level course, "Performing CyberOps Using Cisco Security Technologies," is meticulously designed for IT professionals seeking to master the operational aspects of cybersecurity within a modern network environment. You will delve into the critical processes and technologies required to effectively monitor, detect, analyze, and respond to cyber threats. The curriculum emphasizes practical application, equipping you with the skills to defend organizational assets against an evolving landscape of cyberattacks. This course is ideal for individuals looking to enhance their capabilities in a Security Operations Center (SOC) or any role involving active cybersecurity defense. It solidifies your understanding of foundational security principles while providing hands-on experience with industry-leading Cisco security tools and methodologies.

Upon completion, participants will possess a robust skill set crucial for maintaining a strong security posture. You will learn to interpret security alerts, analyze network traffic for suspicious activity, understand common attack vectors, and implement effective incident response procedures using a Cisco-centric approach. The professional benefits extend beyond technical proficiency, preparing you for recognized cybersecurity roles and boosting your value in the competitive IT job market by demonstrating expertise in critical security operations leveraging renowned Cisco technologies. This training is your gateway to becoming a more effective and indispensable cybersecurity defender.

Duration	2 hours
Level	Intermediate
Vendor	Cisco

COURSE CURRICULUM

01 Module 1: Introduction to Cyber Operations

- The Role of CyberOps in Enterprise Security
- Understanding the Threat Landscape and Attack Vectors
- Security Operations Center (SOC) Models and Functions
- Key Security Concepts: Confidentiality, Integrity, Availability
- Overview of Cybersecurity Frameworks and Compliance

02 Module 2: Network Fundamentals for Security Operations

- TCP/IP Review and Network Architectures
- Common Network Protocols and Services (DNS, HTTP, SMTP)
- Network Devices and Their Security Implications (Routers, Switches, Firewalls)
- Understanding Network Topologies and Segmentation
- Packet Analysis and Traffic Capture Tools

03 Module 3: Security Monitoring and Threat Detection

- Log Management and SIEM (Security Information and Event Management) Concepts
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Endpoint Detection and Response (EDR) Basics
- Analyzing Security Alerts and Incidents
- Using Threat Intelligence Feeds and Platforms

04 Module 4: Attack Methodologies and Vulnerability Assessment

- Common Malware Types and Their Characteristics

- Web Application Attacks (SQL Injection, XSS)
- Social Engineering and Phishing Techniques
- Introduction to Vulnerability Scanning and Penetration Testing
- Understanding Exploit Kits and Command-and-Control (C2) Channels

05 Module 5: Incident Response and Management Using Cisco Technologies

- The Incident Response Lifecycle (Preparation, Identification, Containment, Eradication, Recovery, Post-Incident Analysis)
- Cisco Security Products for Threat Detection (e.g., Cisco Firepower, Stealthwatch, Umbrella)
- Analyzing Security Incidents with Cisco Talos Intelligence
- Forensic Readiness and Data Collection Techniques
- Developing and Implementing Response Playbooks

06 Module 6: Advanced Cisco Security Operations

- Implementing Network Segmentation with Cisco Solutions
- Advanced Malware Protection (AMP) and Threat Grid Integration
- Cloud Security Operations with Cisco Products
- Automating Security Operations with Cisco Orchestration Tools
- Best Practices for Securing Endpoints and Cloud Environments

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Cybersecurity Operations Analyst (Tier 1/2)**

> **Incident Response and Handler Specialist**

> **Security Monitoring and Threat Detection Engineer**

FREQUENTLY ASKED QUESTIONS

Q: What foundational knowledge or certifications are recommended before enrolling in 'Performing CyberOps Using Cisco Security Technologies'?

While this course is designed for an intermediate audience, a foundational understanding of networking concepts (e.g., CompTIA Network+ or CCNA equivalent knowledge) and basic cybersecurity principles (e.g., CompTIA Security+ or CCNA CyberOps Associate equivalent knowledge) is highly recommended. Familiarity with command-line interfaces and operating system fundamentals will also be beneficial for maximizing your learning experience.

Q: How will this course specifically enhance my ability to perform incident response and threat analysis using Cisco's security portfolio?

This course provides targeted training on utilizing key Cisco security technologies for real-world cyber operations. You will gain practical skills in interpreting alerts from Cisco Firepower, analyzing network flows with Cisco Stealthwatch, leveraging Cisco Umbrella for DNS-layer security, and utilizing Cisco Talos intelligence for threat hunting and incident enrichment. This vendor-specific focus ensures you are proficient in the tools commonly deployed in enterprise SOCs that rely on Cisco solutions, directly translating to enhanced incident response and threat analysis capabilities.

Q: Beyond general CyberOps roles, what specific advantages does proficiency in Cisco Security Technologies offer for my cybersecurity career progression?

Proficiency in Cisco Security Technologies provides a significant advantage by making you a highly desirable candidate for organizations that have invested in Cisco's comprehensive security ecosystem. It enables you to seamlessly integrate into environments using Cisco Firewalls, IPS/IDS, SIEMs, and cloud security offerings. This specialized knowledge can lead to roles such as a Cisco Security Administrator, Network Security Engineer focusing on Cisco products, or a dedicated SOC Analyst in a Cisco-centric security posture, potentially opening doors to higher-level positions and increased earning potential due to specialized vendor expertise.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+	10,000+	50+
Years of Excellence	Professionals Trained	Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location
1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email
info@computer-pride.co.ke

Phone
+254 705 900 900

www.computer-pride.co.ke