CISCO TRAINING

Understanding Cisco Cybersecurity Operations Fundamentals

Master Cisco cybersecurity operations fundamentals. Learn to detect, analyze, and respond to cyber threats effectively.

DURATION
2 hours

LEVEL
Foundation

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

The "Understanding Cisco Cybersecurity Operations Fundamentals" course at Computer Pride provides a robust entry point into the dynamic world of cybersecurity. This foundational program is meticulously designed to introduce learners to the core concepts and practices of cybersecurity operations, with a specific emphasis on the principles and methodologies embraced by Cisco, a global leader in networking and security solutions. Participants will gain a comprehensive understanding of the modern threat landscape, including common attack vectors, vulnerabilities, and the adversaries behind them.

Throughout this engaging 2-hour course, you will delve into essential topics such as network security monitoring, endpoint protection, basic threat intelligence, and the fundamentals of incident response. We explore how Security Operations Centers (SOCs) function, the roles within them, and the crucial skills required to detect, analyze, and respond to security incidents. The curriculum is structured to provide practical insights into securing networks and systems, leveraging foundational concepts that are applicable across various IT environments.

Completing this course will empower you with critical foundational knowledge, preparing you for entry-level roles in cybersecurity and serving as an excellent stepping stone for further specialized training and certifications. It instills a security-first mindset and equips you with the initial competencies necessary to contribute effectively to an organization's security posture, enhancing your professional value in an increasingly digital and threat-laden world.

Duration	2 hours
Level	Foundation
Vendor	Cisco

COURSE CURRICULUM

01 Module 1: Introduction to Cybersecurity Operations

- The Evolving Cybersecurity Landscape
- Key Security Principles (Confidentiality, Integrity, Availability)
- Roles and Responsibilities in a Security Operations Center (SOC)
- Understanding Threats, Vulnerabilities, and Attacks
- Overview of Cybersecurity Frameworks and Standards

02 Module 2: Network Security Fundamentals

- Network Devices and Security Zones
- Introduction to Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS)
- Basic Network Traffic Analysis and Packet Capture Concepts
- Common Network Attacks (e.g., DoS, Spoofing) and Defenses
- Secure Network Protocols (e.g., VPN, SSL/TLS basics)

03 Module 3: Endpoint Security Concepts

- Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR)
- Understanding Malware Types and Characteristics
- Host-Based Security: OS Hardening and Patch Management
- User Account Management and Authentication Basics
- Data Loss Prevention (DLP) Fundamentals

04 Module 4: Threat Intelligence and Analysis

- Sources and Types of Threat Intelligence
- Understanding Indicators of Compromise (IoCs)
- Introduction to Security Information and Event Management (SIEM) Systems
- Basic Log Analysis and Correlation for Security Events
- Vulnerability Scanning and Management Overview

05 Module 5: Incident Response and Management Basics

- Introduction to the Incident Response Lifecycle (NIST Framework)
- Detection and Analysis Phase Activities
- Containment, Eradication, and Recovery Strategies
- Post-Incident Activities and Reporting
- Business Continuity and Disaster Recovery Concepts

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Entry-Level Security Operations Center (SOC) Analyst**

> **Junior Cybersecurity Technician**

> **Network Security Monitoring Specialist**

FREQUENTLY ASKED QUESTIONS

Q: What foundational skills will I acquire to contribute effectively to a Security Operations Center (SOC) environment after completing this Cisco Cybersecurity Operations Fundamentals course?

This course equips you with essential skills for an entry-level SOC role, including understanding the modern threat landscape, identifying common network and endpoint attacks, performing basic log analysis, recognizing Indicators of Compromise (IoCs), and grasping the initial phases of incident response. You'll learn how to interpret security alerts and contribute to the detection and analysis of security incidents within a typical SOC framework, building a solid foundation for further specialization in cybersecurity operations.

Q: Does this course specifically prepare me for any Cisco certification, or is it purely for foundational knowledge?

While "Understanding Cisco Cybersecurity Operations Fundamentals" provides critical foundational knowledge, it is designed as a preparatory step. It lays a solid groundwork for more advanced Cisco security certifications, such as the Cisco Certified CyberOps Associate. This course helps build the core concepts and terminology necessary to succeed in those higher-level, industry-recognized certifications focused on cybersecurity operations, making your subsequent certification journey more effective.

Q: How does understanding Cisco's approach to cybersecurity operations specifically benefit my career compared to a vendor-neutral introductory course?

Learning cybersecurity operations through a Cisco lens offers a significant advantage as Cisco is a dominant player in enterprise networking and security solutions globally. This course introduces you to the concepts and principles often implemented using Cisco security technologies, providing practical context that is directly applicable in many corporate

environments. It gives you a head start in understanding security solutions from a major vendor, which can be highly beneficial when working with diverse network infrastructures and seeking employment with organizations leveraging Cisco technology.

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