



## How You Benefit

- Begin a career in the rapidly growing area of cybersecurity operations at the Associate level, working in or with a security operations center (SOC)
- Gain the foundational knowledge and skills to prepare for more advanced job roles in Cybersecurity Operations, working with Security Operations team
- Gain a basic understanding of how a SOC team detects and responds to security incidents, and how they protect their organization's information from modern threats
- Understand further how modern organizations are dealing with detecting and responding to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing their organizations and their customers

## Demand for Trained and Experienced Cybersecurity Operations Professionals

Cybersecurity operations jobs play a key part of securing information systems through the monitoring, detecting, investigating, analyzing, and responding to security events, thus protecting systems from cybersecurity risks, threats, and vulnerabilities.

Cybersecurity operations jobs are also among the fastest-growing roles in IT, as organizations set up security operations centers (SOCs), and establish teams to monitor and respond to security incidents.

Industry studies show that the average time to detect a cybersecurity breach is measured in months, even as the number and cost of security breaches continue to rise, as do regulatory penalties for organizations suffering a data breach. Facing mounting challenges from cybercrime, cyberespionage, insider threats, and advanced persistent threats, organizations are establishing SOC teams of security professionals who can monitor, detect, and respond rapidly to security incidents before they cause damage.

The CCNA Cyber Ops certification program provides a valuable first step in acquiring the knowledge and skills needed to work with a SOC team, and can be a valuable part of beginning a career in the exciting and growing field of cybersecurity operations.

Because static/fixed security controls cannot catch 100 percent of cybersecurity threats and issues, SOC teams provide a critical part of an organization's protection—investigating information security threats, and detecting and responding to incidents in real-time. Due to the increased number of cybersecurity related jobs, organizations continue to struggle with finding or developing cybersecurity talent, and are paying a premium for qualified individuals who can fill those roles.

The program includes:

- **Skills Building:** Instructor-led Training is available to help you learn best practices and gain hands-on experience.
- **Skills Validation:** Assess Cisco Cyber Ops practical skills and knowledge in cybersecurity operations, how to detect and respond to security incidents and protect their organization’s information from modern threats.
- **Skills Reinforcement:** Build confidence in your ability to identify and react to security threats.

## Gain Job-Ready Practical Skills

The Cisco CCNA Cyber Ops certification program provides practical, relevant, and job-ready certification curricula aligned closely with the specific tasks expected of these in-demand professionals. Cisco realizes that Security Operations Center (SOC) Analyst increasingly must focus on design, configuration, and support responsibilities as the technical consultant and device specialist or expert on a security team. Therefore, the Cisco Security curriculum is specific to the best practices of network security administrators, engineers, and experts using the latest Cisco equipment, devices, and appliances.

### Curriculum Overview

CYBER OPS: **CCNA** ▾

Cisco Certified Network Associate Cybersecurity Operations (CCNA Cyber Ops)		
Earn the CCNA Cyber Ops certification to gain the skills and knowledge needed to begin a career in cybersecurity operations, addressing cybersecurity threats that enterprises are faced with on a daily basis. Candidates will learn how to detect and respond to security threats using the latest technology.		
Pre-requisite(s)	Basic knowledge of computer operating systems, such as Windows and Linux	
Topic Focus	<ul style="list-style-type: none"> <li>· Network Concepts</li> <li>· Security Concepts</li> <li>· Cryptography</li> <li>· Host-based Security Analysis</li> <li>· Security Monitoring</li> <li>· Attack Methods</li> </ul>	<ul style="list-style-type: none"> <li>· Endpoint Threat Analysis and Computer Forensics</li> <li>· Network Intrusion Analysis</li> <li>· Incident Response</li> <li>· Data and Event Analysis</li> <li>· Incident Handling</li> </ul>
Job Role(s)	<ul style="list-style-type: none"> <li>· Security Operations Center (SOC) Analyst (Associate/Beginning Level)</li> <li>· Job roles requiring knowledge of basic cybersecurity technologies and principles</li> </ul>	
Experience Level (Years)	One to three years	
Required Exam(s)	210-250 SECFND	210-255 SECOPS
Recommended Training	Understanding Cisco Cybersecurity Fundamentals (SECFND) v1.0	Implementing Cisco Cybersecurity Operations (SECOPS) v1.0

[www.cisco.com/go/ccnacyberops](http://www.cisco.com/go/ccnacyberops)

