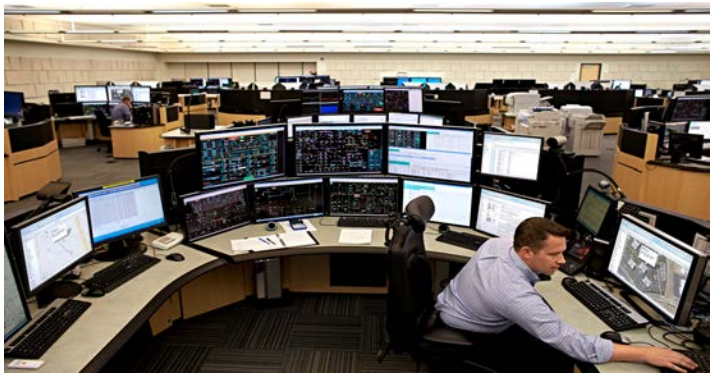
CCNA Cybersecurity Operations At-A-Glance



Today, emboldened cybercriminals are tapping into legitimate online resources. They leach server capacity, steal data, and demand ransoms from online victims whose information they hold hostage. The explosive growth in Internet traffic-driven largely by faster mobile speeds and the proliferation of online devices- works in their favor by helping to expand the attack surface. 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.

Gain Career Ready Cyber Security Skills

"Demand for cybersecurity professionals is expected to rise to 6 million globally by 2019." (*One Million Cybersecurity Job Openings in 2016, Forbes)*. Students can get ready for this in-demand job market by gaining career ready cyber security knowledge and skills from the CCNA Cybersecurity Operations curriculum.

The CCNA Cybersecurity Operations curriculum provides a 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. The curriculum helps prepare students for entry-level cybersecurity career opportunities and is aligned to the Understanding Cisco Cybersecurity Fundamentals exam (210-250 SECFND) and Implementing Cisco Cybersecurity Operations exam (210-255 SECOPS) leading to the Cisco CCNA Cybersecurity Operations certification.

The course provides practical, relevant and job-ready skills aligned closely with the specific tasks expected of SOC professionals through the following components:

- Interactive, multimedia content
- Activities, virtual hands-on lab, Packet Tracer activities that reinforce learning
- Links to articles and websites for enhanced learning on specific topics
- Quizzes and exams to check students understanding of the information covered

Cyber Security Careers

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. Such jobs are 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.

CCNA Cybersecurity Operations is delivered through the Cisco NetAcad.com learning environment. Instructors can enroll students and teach the course through the same process used for other NetAcad™ courses.

Module	Learning Objectives
Chapter 1. Cybersecurity and the Security Operations Center	• Explain the role of the Cybersecurity Operations Analyst in the enterprise. • Explain why networks and data are attacked. • Explain how to prepare for a career in Cybersecurity operations.
Chapter 2. Windows Operating System	• Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses. • Explain the operation of the Windows Operating System. • Explain how to secure Windows endpoints.
Chapter 3. Linux Operating System	• Explain the features and characteristics of the Linux Operating System. • Perform basic operations in the Linux shell. • Perform basic Linux administration tasks.
Chapter 4. Network Protocols and Services	• Analyze the operation of network protocols and services. • Explain how the Ethernet and IP protocols support network communications and operations • Explain how network services enable network functionality.
Chapter 5. Network Infrastructure	• Explain network topologies and the operation of the network infrastructure. • Explain how network devices enable wired and wireless network communication.

Module	Learning Objectives
	• Explain how devices and services are used to enhance network security.
Chapter 6. Principles of Network Security	• Classify the various types of network attacks. • Explain how networks are attacked. • Explain the various types of threats and attacks.
Chapter 7. Network Attacks: A Deeper Look	• Use network monitoring tools to identify attacks against network protocols and services. • Explain network traffic monitoring. • Explain how TCP/IP vulnerabilities enable network attacks. • Explain how common network applications and services are vulnerable to attack.
Chapter 8. Protecting the Network	• Use various methods to prevent malicious access to computer networks, hosts, and data. • Explain approaches to network security defense. • Use various intelligence sources to locate current security threats.
Chapter 9. Cryptography and the Public Key Infrastructure	• Explain the impacts of cryptography on network security monitoring. • Use tools to encrypt and decrypt data. • Explain how the public key infrastructure (PKI) supports network security.
Chapter 10. Endpoint Security and Analysis	• Explain endpoint vulnerabilities and attacks investigation process. • Use tools to generate a malware analysis report. • Classify endpoint vulnerability assessment information.
Chapter 11. Security Monitoring	• Evaluate network security alerts. • Explain how security technologies affect security monitoring. • Explain the types of log files used in security monitoring.
Chapter 12. Intrusion Data Analysis	• Analyze network intrusion data to identify compromised hosts and vulnerabilities • Explain how security-related data is collected. • Analyze intrusion data to determine the source of an attack.
Chapter 13. Incident Response and Handling	• Explain how network security incidents are handled by CSIRTs. • Apply incident response models, such as NIST 800-61r2 to a security incident. • Use a set of logs to isolate threat actors and recommend an incident response plan.