CyberOps Associate (CA) v1.0
Scope and Sequence

Last updated July 29, 2020

Introduction

Today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOCs) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity exploits and threats. CyberOps Associate prepares candidates to begin a career working as associate-level cybersecurity analysts within security operations centers.

Target Audience

The CyberOps Associate course is designed for Cisco Networking Academy® students who are seeking career-oriented, entry-level security analyst skills. Target students include individuals enrolled in technology degree programs at institutions of higher education and IT professionals who want to pursue a career in the Security Operation Center (SOC). Learners in this course are exposed to all of the foundational knowledge required to detect, analyze, and escalate basic cybersecurity threats using common open-source tools.

Prerequisites

CyberOps Associate students should have the following skills and knowledge:

- PC and internet navigation skills
- Basic Windows and Linux system concepts
- Basic understanding of computer networks
- Binary and Hexadecimal understanding
- Familiarity with Cisco Packet Tracer

Target Certification

This course aligns with the Cisco Certified CyberOps Associate (CBROPS) certification. Candidates need to pass the 200-201 CBROPS exam to achieve the Cisco Certified CyberOps Associate certification. The CBROPS exam tests a candidate's knowledge and skills related to security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

Course Description

The course has many features to help students understand these concepts:

- The course is comprised of twenty-eight (28) modules. Each module is comprised of topics.
- Modules emphasize critical thinking, problem solving, collaboration, and the practical application of skills.
- Each module contains some way to practice and assess understanding, such as a lab or a Packet Tracer activity. These module-level activities provide feedback and are designed to indicate learner's mastery of the

skills needed for the course. Learners can ensure their level of understanding well before taking a graded quiz or exam.

- Some topics may contain a Check Your Understanding interactive quiz, or some other way to assess understanding, such as a lab or a Packet Tracer. These topic-level assessments are designed to tell learners if they have a good grasp of the topic content, or if they need to review before continuing. Learners can ensure their level of understanding well before taking a graded quiz or exam. Check Your Understanding quizzes do not affect the learner's overall grade.
- Rich multimedia content, including interactive activities, videos, and quizzes, addresses a variety of learning styles and helps stimulate learning and increase knowledge retention.
- Virtual environments simulate real-world cybersecurity threat scenarios and create opportunities for security monitoring, analysis, and resolution.
- Hands-on labs help students develop critical thinking and complex problem solving skills.
- Innovative assessments provide immediate feedback to support the evaluation of knowledge and acquired skills.
- Technical concepts are explained using language that works well for learners at all levels and embedded interactive activities break up reading of the content and help reinforce understanding.
- The curriculum encourages students to consider additional IT education, but also emphasizes applied skills and hands-on experience.
- Cisco Packet Tracer activities are designed for use with Packet Tracer 7.3.0 or later.

Course Objectives

CyberOps Associate v1.0 covers knowledge and skills needed to successfully handle the tasks, duties, and responsibilities of an associate-level Cybersecurity Analyst working in a Security Operations Center (SOC).

Upon completion of the *CyberOps Associate v1.0* course, students will be able to perform the following tasks:

- Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
- Explain the features and characteristics of the Linux Operating System.
- Analyze the operation of network protocols and services.
- Explain the operation of the network infrastructure.
- Classify the various types of network attacks.
- Use network monitoring tools to identify attacks against network protocols and services.
- Explain how to prevent malicious access to computer networks, hosts, and data.
- Explain the impacts of cryptography on network security monitoring.
- Explain how to investigate endpoint vulnerabilities and attacks.
- Evaluate network security alerts.
- Analyze network intrusion data to identify compromised hosts.

- Apply incident response models to manage network security incidents.

Lab Equipment Requirements

This course requires no physical equipment other than the student's lab PC. It uses several Virtual Machines (VMs) to create the lab experience.

Baseline Equipment Bundle:

- PCs - minimum system requirements
  - CPU: Intel Pentium 4, 2.53 GHz or equivalent with virtualization support
  - Operating Systems, such as Microsoft Windows, Linux, and Mac OS
  - 64-bit processor
  - RAM: 8 GB
  - Storage: 40 GB of free disk space
  - Display resolution: 1024 x 768
  - Language fonts supporting Unicode encoding (if viewing in languages other than English)
  - Latest video card drivers and operating system updates
- Internet connection for lab and student PCs

Student PC Software:

- Oracle VM VirtualBox Manager (version 6.1 or later)
- CyberOps Workstation VM
  - Downloadable from the Course
  - Requires 1 GB RAM, 20 GB Disk Space
- Security Onion VM
  - Downloadable from the Course
  - Requires 4 GB RAM (minimum), 8GB RAM (highly recommended), 20 GB Disk Space

CyberOps Associate Outline

Listed below are the current set of modules and their associated competencies outlined for this course. Each module is an integrated unit of learning that consists of content, activities and assessments that target a specific set of competencies. The size of the module will depend on the depth of knowledge and skill needed to master the competency. Some modules are considered foundational, in that the artifacts presented, while not assessed, enable learning of concepts that are covered on the CBROPS certification exam.

Table 1. CyberOps Associate v1.0 Course Outline

Module/Topics	Goals/Objectives
Module 1. The Danger	**Explain why networks and data are attacked.**
1.0 Introduction	A brief introduction to the course and the first module.
1.1 War Stories	Outline features of cybersecurity incidents.
1.2 Threat Actors	Explain the motivations of the threat actors behind specific security incidents.

Module/Topics	Goals/Objectives
1.3 Threat Impact	Explain the potential impact of network security attacks.
1.4 The Danger Summary	A brief summary and the module quiz.
Module 2. Fighters in the War Against Cybercrime	**Explain how to prepare for a career in cybersecurity operations.**
2.0 Introduction	An introduction to the module.
2.1 The Modern Security Operations Center	Explain the mission of the security operations center.
2.2 Becoming a Defender	Describe resources available to prepare for a career in cybersecurity operations.
2.3 Fighters in the War Against Cybercrime Summary	A brief summary and the module quiz.
Module 3. The Windows Operating System	**Explain the security features of the Windows operating system.**
3.0 Introduction	An introduction to the module.
3.1 Windows History	Describe the history of the Windows Operating System.
3.2 Windows Architecture and Operations	Explain the architecture of Windows and its operation.
3.3 Windows Configuration and Monitoring	Explain how to configure and monitor Windows.
3.4 Windows Security	Explain how Windows can be kept secure.
3.5 The Windows Operating System Summary	A brief summary and the module quiz.
Module 4. Linux Overview	**Implement basic Linux security.**
4.0 Introduction	An introduction to the module.
4.1 Linux Basics	Explain why Linux skills are essential for network security monitoring and investigation.
4.2 Working in the Linux Shell	Use the Linux shell to manipulate text files.
4.3 Linux Servers and Clients	Explain how client-server networks function.
4.4 Basic Server Administration	Explain how a Linux administrator locates and manipulates security log files.
4.5 The Linux File System	Manage the Linux file system and permissions.
4.6 Working with the Linux GUI	Explain the basic components of the Linux GUI.
4.7 Working on a Linux Host	Use tools to detect malware on a Linux host.
4.8 Linux Basics Summary	A brief summary and the module quiz.
Module 5. Network Protocols	**Explain how protocols enable network operations.**
5.0 Introduction	An introduction to the module.
5.1 Network Communication Process	Explain the basic operations of data networked communications.

Module/Topics	Goals/Objectives
5.2 Communication Protocols	Explain how protocols enable network operations.
5.3 Data Encapsulation	Explain how data encapsulation allows data to be transported across the network.
5.4 Network Protocols Summary	A brief summary and the module quiz.
Module 6. Ethernet and Internet Protocol (IP)	**Explain how the ethernet and IP protocols support network communications.**
6.0 Introduction	An introduction to the module.
6.1 Ethernet	Explain how Ethernet supports network communication.
6.2 IPv4	Explain how the IPv4 protocol supports network communications.
6.3 IP Addressing Basics	Explain how IP addresses enable network communication.
6.4 Types of IPv4 Addresses	Explain the types of IPv4 addresses that enable network communication.
6.5 The Default Gateway	Explain how the default gateway enables network communication.
6.6 IPv6 Prefix Length	Explain how the IPv6 protocol supports network communications.
6.7 Ethernet and IP Protocol Summary	A brief summary and the module quiz.
Module 7. Principles of Network Security	**Connectivity Verification**
7.0 Introduction	An introduction to the module.
7.1 ICMP	Explain how ICMP is used to test network connectivity.
7.2 Ping and Traceroute Utilities	Use Windows tools, ping, and traceroute to verify network connectivity.
7.3 Connectivity Verification Summary	A brief summary and the module quiz.
Module 8. Address Resolution Protocol	**Analyze address resolution protocol PDUs on a network.**
8.0 Introduction	An introduction to the module.
8.1 MAC and IP	Compare the roles of the MAC address and the IP address.
8.2 ARP	Analyze ARP by examining Ethernet frames.
8.3 ARP Issues	Explain how ARP requests impact network and host performance.
8.4 Address Resolution Protocol Summary	A brief summary and the module quiz.
Module 9. The Transport Layer	**Explain how transport layer protocols support network functionality.**
9.0 Introduction	An introduction to the module.
9.1 Transport Layer Characteristics	Explain how transport layer protocols support network communication.

Module/Topics	Goals/Objectives
9.2 Transport Layer Session Establishment	Explain how the transport layer establishes communication sessions.
9.3 Transport Layer Reliability	Explain how the transport layer establishes reliable communications.
9.4 The Transport Layer Summary	A brief summary and the module quiz.
Module 10. Network Services	**Explain how network services enable network functionality.**
10.0 Introduction	An introduction to the module.
10.1 DHCP	Explain how DHCP services enable network functionality.
10.2 DNS	Explain how DNS services enable network functionality.
10.3 NAT	Explain how NAT services enable network functionality.
10.4 File Transfer and Sharing Services	Explain how file transfer services enable network functionality.
10.5 Email	Explain how email services enable network functionality.
10.6 HTTP	Explain how HTTP services enable network functionality.
10.7 Network Services Summary	A brief summary and the module quiz.
Module 11. Network Communication Devices	**Explain how network devices enable wired and wireless network communication.**
11.0 Introduction	An introduction to the module.
11.1 Network Devices	Explain how network devices enable network communication.
11.2 Wireless Communications	Explain how wireless devices enable network communication.
11.3 Network Communication Devices Summary	A brief summary and the module quiz.
Module 12. Network Security Infrastructure	**Explain how network devices and services are used to enhance network security.**
12.0 Introduction	An introduction to the module.
12.1 Network Topologies	Explain how network designs influence the flow of traffic through the network.
12.2 Security Devices	Explain how specialized devices are used to enhance network security.
12.3 Security Services	Explain how network services enhance network security.
12.4 Network Security Infrastructure Summary	A brief summary of this module.
Module 13. Attackers and Their Tools	**Explain how networks are attacked.**
13.0 Introduction	An introduction to the module.
13.1 Who is Attacking Our Network?	Explain how network threats have evolved.

Module/Topics	Goals/Objectives
13.2 Threat Actor Tools	Describe the various types of attack tools used by Threat Actors.
13.3 Attackers and Their Tools Summary	A brief summary and the module quiz.
Module 14. Common Threats and Attacks	**Explain the various types of threats and attacks.**
14.0 Introduction	An introduction to the module.
14.1 Malware	Describe types of malware.
14.2 Common Network Attacks – Reconnaissance, Access, and Social Engineering	Explain reconnaissance, access, and social engineering attacks.
14.3 Network Attacks – Denial of Service, Buffer Overflows, and Evasion	Explain denial of service, buffer overflow, and evasion attacks.
14.4 Common Threats and Attacks Summary	A brief summary and the module quiz.
Module 15. Observing Network Operation	**Explain network traffic monitoring.**
15.0 Introduction	An introduction to the module.
15.1 Introduction to Network Monitoring	Explain the importance of network monitoring
15.2 Introduction to Network Monitoring Tools	Explain how network monitoring is conducted.
15.3 Network Monitoring and Tools Summary	A brief summary and the module quiz.
Module 16. Attacking the Foundation	**Explain how TCP/IP vulnerabilities enable network attacks.**
16.0 Introduction	An introduction to the module.
16.1 IP PDU Details	Explain the IPv4 and IPv6 header structure.
16.2 IP Vulnerabilities	Explain how IP vulnerabilities enable network attacks.
16.3 TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities enable network attacks.
16.4 Attacking the Foundation Summary	A brief summary and the module quiz.
Module 17. Attacking What We Do	**Explain how common network applications and services are vulnerable to attack.**
17.0 Introduction	An introduction to the module.
17.1 IP Services	Explain IP service vulnerabilities.
17.2 Enterprise Services	Explain how network application vulnerabilities enable network attacks.
17.3 Attacking What We Do Summary	A brief summary and the module quiz.
Module 18. Understanding Defense	**Explain approaches to network security defense.**
18.0 Introduction	An introduction to the module.

Module/Topics	Goals/Objectives
18.1 Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
18.2 Security Policies, Regulations, and Standards	Explain security policies, regulations, and standards.
18.3 Understanding Defense Summary	A brief summary and the module quiz.
Module 19. Access Control	**Explain access control as a method of protecting a network.**
19.0 Introduction	An introduction to the module.
19.1 Access Control Concepts	Explain how access control protects network data.
19.2 AAA usage and operation	Explain how AAA is used to control network access.
19.3 Access Control Summary	A brief summary and the module quiz.
Module 20. Threat Intelligence	**Use various intelligence sources to locate current security threats.**
20.0 Introduction	An introduction to the module.
20.1 Information Sources	Describe information sources used to communicate emerging network security threats.
20.2 Threat Intelligence Services	Describe various threat intelligence services.
20.3 Threat Intelligence Summary	A brief summary and the module quiz.
Module 21. Cryptography	**Explain how the public key infrastructure supports network security.**
21.0 Introduction	An introduction to the module.
21.1 Integrity and Authenticity	Explain the role of cryptography in ensuring the integrity and authenticity data.
21.2 Confidentiality	Explain how cryptographic approaches enhance data confidentiality.
21.3 Public Key Cryptography	Explain public key cryptography.
21.4 Authorities and the PKI Trust System	Explain how the public key infrastructure functions.
21.5 Applications and Impacts of Cryptography	Explain how the use of cryptography affects cybersecurity operations.
21.6 Cryptography Summary	A brief summary of this module.
Module 22. Endpoint Protection	**Explain how a malware analysis website generates a malware analysis report.**
22.0 Introduction	An introduction to the module.
22.1 Antimalware Protection	Explain methods of mitigating malware.
22.2 Host-based Intrusion Prevention	Explain host-based IPS/IDS log entries.
22.3 Application Security	Explain how sandbox is used to analyze malware.

Module/Topics	Goals/Objectives
22.4 Endpoint Protection Summary	A brief summary and the module quiz.
Module 23. Endpoint Vulnerability Assessment	**Explain how endpoint vulnerabilities are assessed and managed.**
23.0 Introduction	An introduction to the module.
23.1 Network and Server Profiling	Explain the value of network and server profiling.
23.2 Common Vulnerability Scoring System (CVSS)	Explain how CVSS reports are used to describe security vulnerabilities.
23.3 Secure Device Management	Explain how secure device management techniques are used to protect data and assets.
23.4 Information Security Management Systems	Explain how information security management systems are used to protect assets.
23.5 Endpoint Vulnerability Assessment Summary	A brief summary and the module quiz.
Module 24. Technologies and Protocols	**Explain how security technologies affect security monitoring.**
24.0 Introduction	An introduction to the module.
24.1 Monitoring Common Protocols	Explain the behavior of common network protocols in the context of security monitoring.
24.2 Security Technologies	Explain how security technologies affect the ability to monitor common network protocols.
24.3 Technologies and Protocols Summary	A brief summary and the module quiz.
Module 25. Network Security Data	**Explain the types of network security data used in security monitoring.**
25.0 Introduction	An introduction to the module.
25.1 Types of Security Data	Describe the types of data used in security monitoring.
25.2 End Device Logs	Describe the elements of an end device log file.
25.3 Network Logs	Describe the elements of a network device log file.
25.4 Network Security Data Summary	A brief summary and the module quiz.
Module 26. Evaluating Alerts	**Explain the process of evaluating alerts.**
26.0 Introduction	An introduction to the module.
26.1 Source of Alerts	Identify the structure of alerts.
26.2 Overview of Alert Evaluation	Explain how alerts are classified.
26.3 Evaluating Alerts Summary	A brief summary and the module quiz.
Module 27. Working with Network Security Data	**Interpret data to determine the source of an alert.**

Module/Topics	Goals/Objectives
27.0 Introduction	An introduction to the module.
27.1 A Common Data Platform	Explain how data is prepared for use in Network Security Monitoring (NSM) system.
27.2 Investigating Network Data	Use Security Onion tools to investigate network security events.
27.3 Enhancing the Work of the Cybersecurity Analyst	Describe network monitoring tools that enhance workflow management.
27.4 Working with Network Security Data Summary	A brief summary and the module quiz.
Module 28. Digital Forensics and Incident Analysis and Response	**Explain how the CyberOps Associate responds to cybersecurity incidents.**
28.0 Introduction	An introduction to the module.
28.1 Evidence Handling and Attack Attribution	Explain the role of digital forensic processes.
28.2 The Cyber Kill Chain	Identify the steps in the Cyber Kill Chain.
28.3 The Diamond Model of Intrusion Analysis	Classify an intrusion event using the Diamond Model.
28.4 Incident Response	Apply the NIST 800-61r2 incident handling procedures to a given incident scenario.
28.5 Digital Forensics and Incident Analysis and Response Summary	A brief summary of this module.
28.6 Prepare for Your Exam and Launch Your Career!	Certification preparation, discount vouchers, and other career resources.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**