LAUSD UNIFIED **Division of Adult and Career Education**

Career Technical Education (CTE) Course Outline

Course Title:	CyberOps Associate
Course Number:	77-65-85
Date:	July 2025
Industry Sector:	Information and Communication Technologies
Pathway:	Networking
CBEDS Title:	Network Engineering
CBEDS Code:	4646
CalPADS	8121
Credits:	10

Hours:

Total
140

Course Description:

This competency-based course is designed to prepare students to pass the Cisco CCNA CyberOps certification examination. This is the second course in a sequence of three courses of the cybersecurity pathway. Technical instruction includes an introduction, safety, network and data attacks, cybersecurity operations careers, Windows Operating System, Linux overview, network protocols, Ethernet & Internet protocol, principals of network security, address resolution protocol, the transport layer, network services, network communication devices, network security infrastructure, attackers and their tools, common threats and attacks, observing network operation, TCP/IP vulnerabilities, network applications and service vulnerabilities, network security defense, access control, threat intelligence, cryptography, endpoint protection, endpoint vulnerability assessment, technologies and protocols, network security data, evaluating alerts, working with network security data, digital forensics and incident analysis and response, and employability skills and resume preparation. The competencies in this course are aligned with the California Common Core Standards and the California Career Technical Education Model Curriculum Standards.

Prerequisites:	Enrollment requires a 6.0 reading level as measured by the CASAS GOALS test, successful completion (or demonstrate competency) of Algebra 1, successful completion of Cybersecurity Essentials CCST (77-65-75).
NOTE:	For Perkins purposes this course has been designated as a **concentrator** course. This course **cannot** be repeated once a student receives a Certificate of Completion.
A-G Approval	N/A
Methods of Instruction:	Lecture and discussion, demonstration and participation, multimedia presentations, individualized instruction, peer teaching, role-playing, guest speakers, field trips and field study experiences, projects
Student Evaluation:	Summative: End of section assessments
Industry Certification:	Cisco Certified CyberOps Associate (CBROPS) certification.
Recommended Texts:	Santos, Omar. Cisco Cybersecurity Operations Fundamentals CBROPS 200-201 Official Cert Guide (Certification Guide) 1st Edition, Cisco Press, December 2020
Link to Resource Folder	https://bit.ly/CyberOpsResources

COMPETENCY AREAS AND STATEMENTS	MINIMAL COMPETENCIES	STANDARDS
A. INTRODUCTION Understand, apply, and evaluate classroom and workplace policies and procedures. (2 hours)	1. Describe the scope and purpose of the course. 2. Discuss and demonstrate Zoom, Schoology, and basic computer skills. 3. Identify classroom policies and procedures. 4. Discuss, identify, research, and draw conclusions about different career paths, occupations, employment outlook, and career advancements in the Information and Communications Technologies industry sector which impact cybersecurity. 5. Describe opportunities available for promoting gender equity and the representation of non-traditional populations in the Information and Communications Technologies industry sector. 6. Explain and recognize the importance of customer-oriented service, ethics, teamwork, respect of individual and cultural differences, and diversity in the workplace.	**Career Ready Practice:** 1, 2, 3, 4, 8, 9, 10, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5, 2.8 Career Planning & Management: 3.1, 3.3, 3.4, 3.5 Technology: 4.2 Ethics & Legal Responsibilities: 8.4 Leadership & Teamwork: 9.3, 9.6 Demonstration & Application: 11.1 **CTE Pathway:** B2.2
B. SAFETY Understand safety procedures and	1. Discuss classroom and workplace first aid, emergency procedures, and accidents or injury prevention.	**Career Ready Practice:** 1, 2, 10, 12

techniques in the Information and Communication Technologies Industry Sector. (2 hours)	2. Discuss the California Occupational Safety and Health Administration (Cal/OSHA) workplace requirements for cybersecurity technicians to maintain a safe and healthy working environment. 3. Discuss the use of the Safety Data Sheet (SDS) as it applies to the Information and Communication Technologies industry sector. 4. Practice personal safety when lifting, bending, or moving equipment and supplies. 5. Explain how each of the following insures a safe workplace: a. employees' rights as they apply to job safety b. employers' obligations as they apply to safety c. safety laws applying to electrical tools 6. Explain and sign the LAUSD Responsible Use Policy (RUP). 7. Pass the Safety Test with 100% accuracy.	**CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5, 2.6 Health & Safety: 6.1, 6.2, 6.3, 6.4, 6.7 Demonstration & Application: 11.1 **CTE Pathway:** B2.2
C. THE DANGER Identify and explain why networks and data are attacked. (2 hours)	1. Explain why networks and data are attacked. 2. Outline features of cybersecurity incidents. 3. Explain the motivations of the threat actors behind specific security incidents. 4. Discuss the potential impact of network security attacks. 5. Pass The Danger assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.3 Problem Solving & Critical Thinking: 5.2, 5.3, 5.4 Technical Knowledge & Skills: 10.1 **CTE Pathway:** B8.1, B8.4

D. FIGHTERS IN THE WAR AGAINST CYBERCRIME Explain how to prepare for a career in cybersecurity operations. (2 hours)	1. Research the various careers in cybersecurity to make informed decisions. 2. Explain the mission of the Security Operations Center (SOC). 3. Describe resources available to prepare for a career in cybersecurity operations. 4. Describe the current entry level cybersecurity certifications. 5. Pass a Fighters in the War Against Cybercrime assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 3, 4, 5, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Career Planning & Management: 3.1, 3.4 Technology: 4.2, 4.5 Problem Solving & Critical Thinking: 5.4 Technical Knowledge & Skills: 10.1, 10.5 **CTE Pathway:** B4.1, B4.6, B8.2
E. WINDOWS OPERATING SYSTEM Explain the security features of the Windows operating system.	1. Discuss security features (e.g., passwords, user rights, updates, etc.) of the Windows Operating System. 2. Discuss the history of the Windows Operating System. 3. Explain the architecture of Windows and its operation of: a. Hardware Abstraction Layer (HAL) b. user mode c. kernel mode 4. Explain and demonstrate how to configure and monitor Windows. 5. Explain how Windows can be kept secure. 6. Pass a Windows Operating System assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2

(6 hours)		Problem Solving & Critical Thinking: 5.3, 5.6, 5.7, 5.10 Technical Knowledge & Skills: 10.1, 10.5, 10.8, 10.10 Demonstration & Application: 11.1 **CTE Pathway:** B4.2, B6.1, B8.2
F. LINUX OVERVIEW Explain how to implement basic Linux security. (6 hours)	1. Demonstrate how to implement basic Linux security (e.g., passwords, user rights, updates, etc.). 2. Discuss why Linux skills are essential for network security monitoring and investigation. 3. Use the Linux shell to manipulate text files. 4. Explain how client-server networks function. 5. Explain and demonstrate how a Linux administrator locates and manipulates security log files. 6. Manage the Linux file system and permissions. 7. Explain the basic components of the Linux GUI. 8. Use tools to detect malware on a Linux host. 9. Pass a Linux Overview assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.3, 5.6, 5.7, 5.10 Technical Knowledge & Skills: 10.1, 10.5, 10.8, 10.10 Demonstration & Application: 11.1 **CTE Pathway:**

		B4.2, B6.1, B8.2
G. NETWORK PROTOCOLS Explain how protocols enable network operations. (6 hours)	1. Define and explain network operations. 2. Explain, demonstrate, and compare the basic operations of the following data networked communications: a. unicast b. multicast c. broadcast 3. Explain how protocols enable network operations: a. message encoding b. message formatting c. message size d. message timing e. message delivery options 4. Explain how data encapsulation allows data to be transported across the network: a. Open Systems Interconnection (OSI) model b. TCP/IP model 5. Pass a Network Protocols assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.3 Technical Knowledge & Skills: 10.1, 10.5, 10.6 Demonstration & Application: 11.1 **CTE Pathway:** B1.2, B4.3
H. **ETHERNET & INTERNET PROTOCOL (IP)** Explain how the ethernet and IP protocols support network communications.	1. Explain how the Ethernet supports network communication. 2. Discuss how the IPv4 and IPv6 protocols support network communications. 3. Describe how IP addresses enable network communication. 4. Identify the types of IPv4 addresses that enable network communication. 5. Describe and demonstrate how the default gateway enables network communication. 6. Pass an Ethernet and Internet Protocol assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.3 Problem Solving & Critical Thinking:

(6 hours)		5.3 Technical Knowledge & Skills: 10.1, 10.2, 10.5 Demonstration & Application: 11.1 **CTE Pathway:** B1.2, B1.5, B3.5
I. PRINCIPLES OF NETWORK SECURITY Explain how ICMP is used to test network connectivity. (4 hours)	1. Define and discuss how the Internet Control Message Protocol (ICMP) is used to test network connectivity. 2. Demonstrate and use Windows tools, ping, and trace route to verify network connectivity. 3. Pass a Principles of Network Security assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.5, 5.7 Technical Knowledge & Skills: 10.1, 10.5 Demonstration & Application: 11.1 **CTE Pathway:** B1.2, B3.4, B4.1
	1. Compare the roles of the Media Access Control	

J. ADDRESS RESOLUTION PROTOCOL (ARP) Analyze address resolution protocol PDUs on a network. (6 hours)	(MAC) address and the IP address. 2. Define and analyze Address Resolution Protocol (ARP) by examining Ethernet frames and: a. demonstrate use of software to capture and analyze frames b. explain ARP poisoning 3. Explain how ARP requests impact network and host performance. 4. Pass an ARP assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10, 11 **CTE Anchor:** Academics: 1.0 Communications : 2.1, 2.3, 2.5 Technology: 4.2, 4.3 Problem Solving & Critical Thinking: 5.1, 5.3, 5.7 Technical Knowledge & Skills: 10.1 Demonstration & Application: 11.1 **CTE Pathway:** B1.1, B8.2
K. THE TRANSPORT LAYER Explain how transport layer protocols support network functionality.	1. Explain how the following transport layer protocols support network communication: a. User Datagram Protocol (UDP) b. Transmission Control Protocol (TCP) 2. Describe and demonstrate how the transport layer establishes communication sessions using the TCP three-way handshake. 3. Identify how the transport layer establishes reliable communications using acknowledgements. 4. Pass a Transport Layer assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 10 **CTE Anchor:** Academics: 1.0 Communications : 2.1, 2.3, 2.5 Technology: 4.2

(6 hours)		Technical Knowledge & Skills: 10.1 Demonstration & Application: 11.1 **CTE Pathway:** B1.1, B1.2
L. NETWORK SERVICES Explain how network services enable network functionality. (6 hours)	1. Explain how the following services enable network functionality: a. Dynamic Host Configuration Protocol (DHCP) b. Domain Name Service (DNS) c. Network Address Translation (NAT) d. File Transfer Protocol (FTP) e. Simple Mail Transfer Protocol (SMTP) f. Post Office Protocol (POP) g. Internet Message Access Protocol (IMAP) h. Hypertext Transfer Protocol (HTTP) 2. Pass a Network Services assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Technical Knowledge & Skills: 10.1 **CTE Pathway:** B1.1, B1.2
M. NETWORK COMMUNICATION DEVICES Explain how network devices enable wired and wireless network communication.	1. Describe and compare how the following network devices enable network communication: a. switch b. access point c. router 2. Discuss how the following wireless devices enable network communication: a. Service Set Identifier (SSID) b. wireless encryption c. passive vs. active mode d. authentication	**Career Ready Practice:** 1, 2, 4, 5, 11 **CTE Anchor:** Academics: 1.0 Communications:

(6 hours)	3. Research solutions to common connectivity issues. 4. Pass a Network Communication Devices assessment with an 80% score or higher.	2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.3, 5.6, 5.9 Technical Knowledge & Skills: 10.1, 10.5 **CTE Pathway:** B3.6
N. NETWORK SECURITY INFRASTRUCTURE Explain how network devices and services are used to enhance network security.	1. Explain and analyze how network designs influence the flow of traffic through the network to make informed decisions. 2. Describe and demonstrate how the following specialized devices are used to enhance network security: a. packet filtering firewalls b. stateful firewalls c. application gateway firewalls d. next generation firewalls e. Intrusion Detection System (IDS) f. Intrusion Protection System (IPS) g. Advanced Malware Protection (AMP) h. Web Security Appliance (WSA) i. Email Security Appliance (ESA) 3. Understand how the following network services enhance network security: a. Simple Network Management Protocol (SNMP) b. Netflow c. port mirroring d. Syslog e. Network Time Protocol (NTP) f. Authentication Authorization Accounting (AAA) g. Virtual Private Network (VPN) 4. Pass a Network Security Infrastructure assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.3, 5.4 Technical Knowledge & Skills: 10.1 Demonstration & Application: 11.1 **CTE Pathway:**

(6 hours)		B1.1, B1.5, B3.1, B4.3, B8.2
O. ATTACKERS AND THEIR TOOLS Explain how networks are attacked. (4 hours)	1. Differentiate types of security threats in a network, how they have evolved, and continue to evolve. 2. Explain the various types of attack tools, past and present, used by Threat Actors. 3. Pass an Attackers and Their Tools assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.5 Technical Knowledge & Skills: 10.1 **CTE Pathway:** B8.1, B8.4
P. COMMON THREATS AND ATTACKS Explain the various types of threats and attacks.	1. Describe the following types of malwares: a. viruses b. trojan horses c. worms d. ransomware 2. Define reconnaissance, access, and social engineering attacks. 3. Explain denial of service, buffer overflow, and evasion attacks. 4. Pass a Common Threats and Attacks assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Technical Knowledge & Skills: 10.1, 10.8

(4 hours)		**CTE Pathway:** B1.1, B8.1, B8.4
Q. OBSERVING NETWORK OPERATION Explain network traffic monitoring. (4 hours)	1. Explain the importance of network monitoring. 2. Explain and demonstrate how network monitoring is conducted to include: a. network taps b. traffic or port mirroring c. Security Information and Event Management System (SIEM) d. Security Orchestration Automation and Response (SOAR) 3. Pass an Observing Network Operation assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Technical Knowledge & Skills: 10.1 Demonstration & Application: 11.1 **CTE Pathway:** B4.1, B8.2
R. ATTACKING THE FOUNDATION Explain how TCP/IP vulnerabilities enable network attacks.	1. Explain and demonstrate the IPv4 and IPv6 header structures. 2. Describe and discuss how the following IP vulnerabilities enable network attacks: a. ICMP attacks b. amplification and reflection attacks c. address spoofing attacks 3. Explain how TCP and UDP vulnerabilities enable the following network attacks: a. TCP synchronization attack b. TCP reset attack c. UDP flood attack 4. Pass an Attacking the Foundation assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.1, 4.2

(6 hours)		Problem Solving & Critical Thinking: 5.1 Technical Knowledge & Skills: 10.8, 10.12 Demonstration & Application: 11.1 **CTE Pathway:** B1.4, B3.4, B4.1, B4.5, B8.2, B8.4
S. ATTACKING WHAT WE DO Explain and discuss how common network applications and services are vulnerable to attack. (4 hours)	1. Discuss IP service vulnerabilities and mitigation techniques including: a. ARP vulnerabilities b. ARP poisoning c. DNS attacks d. DNS tunneling e. DHCP attacks 2. Explain how the following network application vulnerabilities enable network attacks: a. common HTTP exploits b. Email c. web-exposed databases d. client-size scripting 3. Pass an Attacking What We Do assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5 **CTE Anchor:** Academics: 1.0 Communications : 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.1 Technical Knowledge & Skills: 10.1, 10.8 **CTE Pathway:** B3.7, B4.1, B4.5, B4.9, B8.1, B8.4, B8.5

T. UNDERSTANDING DEFENSE Explain approaches to network security defense. (4 hours)	1. Discuss how the defense-in-depth strategy is used to protect networks: a. identify assets b. identify vulnerabilities c. identify threats d. describe the security onion and the security artichoke 2. Practice developing security policies, regulations, and research industry standards listed below: a. business policies b. security policies c. Bring Your Own Device (BYOD) policies 3. Pass an Understanding Defense assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 9, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.1, 4.2, 4.5 Problem Solving & Critical Thinking: 5.4, 5.6 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1, 10.2, 10.14 **CTE Pathway:** B4.2, B6.1
U. ACCESS CONTROL Explain access control as a method of protecting a network.	1. Discuss and demonstrate how access control protects network data. 2. Explain the Confidentiality Integrity & Availability (CIA) Triad. 3. Define the concept of zero trust. 4. Describe and interpret access control models. 5. Demonstrate how Authentication, Authorization & Accounting (AAA) is used to control network access. 6. Pass an Access Control assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2

(6 hours)		Problem Solving & Critical Thinking: 5.4 Technical Knowledge & Skills: 10.1, 10.8, 10.10 Demonstration & Application: 11.1 **CTE Pathway:** B1.1
V. THREAT INTELLIGENCE Use various intelligence sources to locate current security threats. (4 hours)	1. Work in teams to research and analyze information sources used to communicate emerging network security threats. 2. Identify various threat intelligence services. 3. List various threat intelligence government organizations and communities. 4. Pass a Threat Intelligence assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 9, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.1, 4.2, 4.3, 4.5 Problem Solving & Critical Thinking: 5.1, 5.4, 5.6 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1, 10.4, 10.13, 10.14

		CTE Pathway: B4.6, B8.2, B8.3
W. CRYPTOGRAPHY Explain how the public key infrastructure supports network security. (6 hours)	1. Define and explain the role of cryptography to ensure the integrity and authenticity data. 2. Discuss how cryptographic approaches enhance data confidentiality. 3. Define and provide examples of public key cryptography. 4. Demonstrate how the Public Key Infrastructure (PKI) functions. 5. Identify and analyze how the use of cryptography affects cybersecurity operations. 6. Pass a Cryptography assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.3 Problem Solving & Critical Thinking: 5.6, 5.8 Technical Knowledge & Skills: 10.1, 10.8 Demonstration & Application: 11.1 **CTE Pathway:** B1.1, B1.4, B8.2
X. ENDPOINT PROTECTION Explain how a malware analysis website generates a malware analysis report.	1. Identify methods of mitigating malware. 2. Describe and differentiate between host-based Intrusion Prevention System and Intrusion Detection System (IPS/IDS) log entries. 3. Work in teams to explain how sandbox is used to analyze malware. 4. Pass an Endpoint Protection assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 9 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5

(4 hours)		Technology: 4.1, 4.2 Problem Solving & Critical Thinking: 5.1, 5.3, 5.6 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1, 10.5, 10.9 **CTE Pathway:** B1.1, B1.5, B3.1, B4.1, B4.5, B8.2, B8.4
Y. ENDPOINT VULNERABILITY ASSESSMENT Explain how endpoint vulnerabilities are assessed and managed.	1. Explain the importance of value of network and server profiling. 2. Work in teams, discuss and demonstrate how Common Vulnerability Scoring System (CVSS) reports are used to describe security vulnerabilities. 3. Identify and research how secure device management techniques are used to protect data and assets. 4. Illustrate how information security management systems are used to protect assets. 5. Define common cybersecurity frameworks. 6. Pass an Endpoint Vulnerability assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 9, 10, 11 **CTE Anchor:** Academics: 1.0 Communications : 2.1, 2.3, 2.5 Technology: 4.1, 4.2 Problem Solving & Critical Thinking: 5.1, 5.10 Leadership & Teamwork: 9.7 Technical Knowledge & Skills:

(4 hours)		10.1, 10.2, 10.3 Demonstration & Application: 11.1 **CTE Pathway:** B1.1, B4.1, B4.4, B4.7, B8.2, B8.3, B8.4
Z. TECHNOLOGIES & PROTOCOLS Explain how security technologies affect security monitoring. (4 hours)	1. Research and characterize the behavior of common network protocols in the context of security monitoring. 2. Work in teams to demonstrate how security technologies affect the ability to monitor common network protocols. 3. Pass a Technologies and Protocols assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 9, 10, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.1, 4.2 Problem Solving & Critical Thinking: 5.1, 5.3 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1 Demonstration & Application: 11.1 **CTE Pathway:** B1.1, B1.2, B3.7, B4.3, B4.5, B8.2, B8.4

AA. NETWORK SECURITY DATA Explain the types of network security data used in security monitoring. (4 hours)	1. Discuss the types of data used in security monitoring. 2. Compare and contrast the elements of: a. an end device log file b. a network device log file 3. Pass a Network Security Data assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.3 Problem Solving & Critical Thinking: 5.3 Technical Knowledge & Skills: 10.1, 10.12, 10.13 **CTE Pathway:** B1.1, B4.1, B8.2, B8.3
BB. EVALUATING ALERTS Explain the process of evaluating alerts.	1. Identify the structure and the source of alerts. 2. Work in teams and compare how alerts are classified. 3. Pass an Evaluating Alerts assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 9, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.3 Problem Solving & Critical Thinking:

(4 hours)		5.6 Leadership and Teamwork: 9.7 Technical Knowledge & Skills: 10.1, 10.8 **CTE Pathway:** B1.1, B4.1, B8.4
CC. WORKING WITH NETWORK SECURITY DATA Interpret data to determine the source of an alert. (4 hours)	1. Explain how data is prepared for use in Network Security Monitoring (NSM) system. 2. Use Security Onion tools to investigate network security events. 3. Describe the Elasticsearch Logstash Kibana (ELK). 4. Discuss the network monitoring tools that enhance workflow management. 5. Pass a Working with Network Security Data assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 10 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.1, 5.4 Technical Knowledge & Skills: 10.1, 10.8, 10.12, 10.13 Demonstration & Application: 11.1 **CTE Pathway:** B1.1, B4.1, B8.1, B8.2, B8.4

DD. DIGITAL FORENSICS & INCIDENT ANALYSIS & RESPONSE Explain how the CyberOps Associate responds to cybersecurity incidents. (4 hours)	1. Explain the role of digital forensic processes. 2. Identify the steps in the Cyber Kill Chain. 3. Classify an intrusion event using the Diamond Model. 4. Apply the National Institute of Standards and Technology Guide (NIST 800-61r2) Incident handling procedures to a given incident scenario. 5. Pass a Digital Forensics and Incident Analysis and Response assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.1, 4.2 Problem Solving & Critical Thinking: 5.2, 5.4 Technical Knowledge & Skills: 10.1, 10.2 **CTE Pathway:** B4.2, B7.1, B8.1, B8.3, 8.5
EE. EMPLOYABILITY SKILLS AND RESUME PREPARATION Understand, apply, and evaluate the employability skills and résumé preparation desired of cybersecurity technicians.	1. Understand and define employer requirements for soft skills to include: a. attitude toward work b. communication and collaboration c. critical thinking, problem solving, and decision-making d. customer service e. diversity in the workplace f. flexibility and adaptability g. interpersonal skills h. leadership and responsibility i. punctuality and attendance j. quality of work k. respect, cultural and diversity differences	**Career Ready Practice:** 1, 2, 3, 4, 5, 7, 8, 9, 10, 11 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.4. 2.5 Career Planning & Management:

(4 hours)	l. teamwork m. time management n. trust and ethical behavior o. work ethic 2. Develop a career plan that reflects career interests, pathways, and post-secondary options. 3. Create/revise a résumé, cover letter, and/or portfolio. 4. Demonstrate, analyze, research, and review the role of online job searching platforms and career websites to make informed decisions. 5. Understand the importance of assessing social media account content for professionalism. 6. Demonstrate and complete and/or review an on-line job application. 7. Understand and demonstrate interview skills to get the job to include: a. do's and don'ts for job interviews b. how to dress for the job 8. Demonstrate and create sample follow-up letters. 9. Understand the importance of the continuous upgrading of job skills as it relates to: a. certification, licensure, and/or renewal b. professional organizations/events c. industry associations and/or organized labor	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.8, 3.9 Technology: 4.1, 4.2, 4.3, 4.5 Problem Solving & Critical Thinking: 5.1, 5.4 Responsibility & Flexibility: 7.2, 7.3, 7.4, 7.7 Ethics & Legal Responsibilities: 8.3, 8.4, 8.5 Leadership & Teamwork: 9.1, 9.2, 9.3, 9.4, 9.6, 9.7 Technical Knowledge & Skills: 10.1, 10.3, 10.12 Demonstration & Application: 11.1, 11.2, 11.5 **CTE Pathway:** B4.7

ACKNOWLEDGEMENTS

Thanks to the following individuals for their contributions in developing and editing this curriculum:

Ana Martinez, Trung Le, Silvia Quijada, and Robert Yorgason

Approved by: Renny L. Neyra, Executive Director