LAUSD UNIFIED Division of Adult and Career Education

Career Technical Education (CTE) Course Outline

Course Title:	Cybersecurity Essentials CCST
Course Number:	77-65-75
Date:	July 2025
Industry Sector:	Information and Communication Technologies
Pathway:	Networking
CBEDS Title:	Network Engineering
CBEDS Code:	4646
CalPADS	8120
Credits:	5

Hours:

Total
80

Course Description:

This competency-based course is designed to prepare students to pass the Cisco Certified Support Technician (CCST) Cybersecurity certification examination. This is the first course in a sequence of three courses of the cybersecurity pathway. Technical instruction includes an introduction, safety, cybersecurity threats, vulnerabilities and attacks, securing networks, TCP/IP vulnerabilities, mitigating threats, wireless network communication devices, network security infrastructure, the Windows Operating System, Linux overview, system and endpoint protection, cybersecurity principles, practices, and processes, network security defense, system and network defense, access control, access control lists, firewall technologies, zone-based policy firewalls, cloud security, cryptography, technologies and protocols, network security data, evaluating alerts, governance and compliance, network security testing, threat intelligence, endpoint vulnerability assessment, risk management and security controls, 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 Computer Essentials (75-50-70) and Introduction to IT Support Technician (79-30-65) or Networking 1 (74-65-51) course or equivalent experience in the field as verified by the instructor.
NOTE:	For Perkins purposes this course has been designated as an **introductory** 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 Support Technician (CCST) Cybersecurity certification.
Recommended Texts:	Sexton, Shane & Lacoste Raymond. Cisco Certified Support Technician (CCST) Cybersecurity 100-160 Official Cert Guide, 1st Edition, Cisco Press, 2024.
Link to Resource Folder	https://bit.ly/CyberEssentialsResources

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	1. Discuss classroom and workplace first aid, emergency procedures, and accidents or injury prevention.	**Career Ready Practice:** 1, 2, 10, 12

Understand safety procedures and 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 network 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 ensures 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. CYBERSECURITY THREATS, VULNERABILITIES & ATTACKS Explain how threat actors execute the most common types of cyber-attacks. (3 hours)	1. Explain the threats, vulnerabilities, and attacks that occur in various domains. 2. Identify different deception methods used by attackers to deceive their victims. 3. Describe common types of network attacks: a. Denial of Service (DOS) b. Domain Name System (DNS) c. Man-in-the Middle (MitM) 4. Describe common types of wireless and mobile device attacks. 5. Describe types of application attacks. 6. Pass a Cybersecurity Threats, Vulnerabilities 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 **CTE Pathway:** B1.1, B8.1, B8.4

D. SECURING NETWORKS Explain network security principles. (2 hours)	1. Describe the current network security landscape. 2. Explain how network threats have evolved. 3. Pass a Securing Networks 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, 4.5 Problem Solving & Critical Thinking: 5.3 Technical Knowledge & Skills: 10.1, 10.5 **CTE Pathway:** B1.1, B2.1, B3.3, B8.1
E. 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 the following TCP and UDP vulnerabilities enable 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 Problem Solving & Critical Thinking:

(3 hours)		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
F. ATTACKING WHAT WE DO Recommend measures to mitigate threats. (3 hours)	1. Discuss the following IP service vulnerabilities and mitigation techniques: a. ARP vulnerabilities b. ARP poisoning c. DNS attacks d. DNS tunneling e. DHCP attacks 2. Explain how network application vulnerabilities enable network attacks. 3. Recommend basic threat mitigation measures. 4. 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

G. WIRELESS NETWORK COMMUNICATION DEVICES Explain how to troubleshoot a wireless network. (2 hours)	1. Explain how wireless devices enable network communication. 2. Describe threats to WLANs. 3. Work in teams to troubleshoot a wireless connection. 4. Pass a Wireless Network Communication Devices 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 Technology: 4.2 Problem Solving & Critical Thinking: 5.1, 5.2, 5.5, 5.6 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1 **CTE Pathway:** B1.1, B1.5, B2.3, B3.1, B3.5, B3.6, B4.1
H. **NETWORK SECURITY INFRASTRUCTURE** Explain how devices and services are used to enhance network security.	1. Explain how specialized devices are used to enhance network security 2. Demonstrate how services enhance network security. 3. 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:

(2 hours)		4.2 Problem Solving & Critical Thinking: 5.3, 5.4 Technical Knowledge & Skills: 10.1 Demonstration & Application: 11.1 **CTE Pathway:** B1.1, B1.5, B3.1, B4.3, B8.2
I. THE WINDOWS OPERATING SYSTEM Explain how to use Windows administrative tools.	1. Discuss the history of the Windows Operating System. 2. Explain the architecture of Windows and its operation including: a. Hardware Abstraction Layer (HAL) b. user mode c. kernel mode 3. Use Windows administrative tools to configure, monitor, and manage system resources. 4. Explain how Windows can be kept secure. 5. Pass the 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 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:

(4 hours)		11.1 **CTE Pathway:** B4.2, B6.1, B8.2
J. LINUX OVERVIEW Implement basic Linux security. (4 hours)	1. Discuss why Linux skills are essential for network security monitoring and investigation. 2. Use the Linux shell to manipulate text files. 3. Use the Linux command line to identify servers that are running on a computer. 4. Use commands to locate and monitor log files. 5. Use commands to manage the Linux file system and permissions. 6. Explain the basic components of the Linux GUI. 7. Use tools to detect malware on a Linux host. 8. 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
K. SYSTEM & ENDPOINT PROTECTION Evaluate endpoint protection and the impacts of malware.	1. Demonstrate how to use processes and procedures to protect systems. 2. Explain methods of mitigating malware. 3. Recommend endpoint security measures. 4. Work in teams and use malware investigation tools to learn malware features. 5. Pass a System & Endpoint Protection assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 9, 10, 11 **CTE Anchor:** Academics: 1.0

(2 hours)		Communications: 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.1, 5.3, 5.6 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1, 10.5 Demonstration & Application: 11.1 **CTE Pathway:** B4.1, B4.5, B8.1, B8.4
L. CYBERSECURITY PRINCIPLES, PRACTICES, & PROCESSES User cybersecurity best practices to improve confidentiality, integrity, and availability.	1. Demonstrate how to use hashes to verify the integrity of files. 2. Compare the three states of data. 3. Compare the types of cybersecurity countermeasures. 4. Pass a Cybersecurity Principles, Practices & Processes 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: 5.4, 5.6

(2 hours)		Technical Knowledge & Skills: 10.1, 10.8, 10.12 Demonstration & Application: 11.1 **CTE Pathway:** B1.4, B8.2
M. UNDERSTANDING DEFENSE Explain approaches to network security defense. (2 hours)	1. Discuss how the defense in-depth strategy is used to protect networks including: a. identify assets b. identify vulnerabilities c. identify threats d. describe the security onion and the security artichoke 2. Explain how an organization monitors cybersecurity threats. 3. Practice developing the following security policies, regulations, and research industry standards: a. business policies b. security policies c. Bring Your Own Device (BYOD) policies 4. Pass an Understanding Defense assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 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 Technical Knowledge & Skills: 10.1, 10.2, 10.14 **CTE Pathway:** B4.2, B6.1
N. SYSTEM & NETWORK DEFENSE	1. Demonstrate how physical security measures are implemented to protect network equipment. 2. Describe how to apply application security measures. 3. Demonstrate how to harden network services and protocols.	**Career Ready Practice:** 1, 2, 4, 5, 9, 10 **CTE Anchor:**

Implement the various aspects of system and network defense. (4 hours)	4. Explain how network segmentation can help you harden the network. 5. Work in teams to configure wireless router hardening and security. 6. Explain physical security with Internet of Things (IoT) devices. 7. Implement physical security with IoT devices. 8. Pass a System & Network Defense assessment with an 80% score or higher.	Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2, 4.4 Problem Solving & Critical Thinking: 5.1, 5.3, 5.4 Leadership & Teamwork: 9.7 Technical Knowledge & Skills: 10.1, 10.8 Demonstration & Application: 11.1 **CTE Pathway:** B2.1, B3.1, B4.5, B8.2, B8.4
O. ACCESS CONTROL Configure local and server-based access controls.	1. Configure secure access on a host. 2. Discuss and demonstrate how access control protects network data. 3. Explain the need for account management and access control strategies. 4. Discuss the configuration of server-based authentication with TACACS+ and RADIUS (Terminal Access Controller Access-Control System + Remote Authentication Dial-In User Service). 5. 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

(2 hours)		Technical Knowledge & Skills: 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
BB. RISK MANAGEMENT & SECURITY CONTROLS Select security controls based on risk assessment outcomes.	1. Explain risk management and assessment methodology. 2. Discuss evaluating security controls to mitigate risk. 3. Pass a Risk Management & Security Controls assessment with an 80% score or higher.	**Career Ready Practice:** 1, 2, 4, 5, 8 **CTE Anchor:** Academics: 1.0 Communications: 2.1, 2.3, 2.5 Technology: 4.2 Problem Solving & Critical Thinking: 5.1, 5.3, 5.4 Ethics & Legal Responsibilities: 8.5 Technical Knowledge & Skills: 10.1, 10.2, 10.8 **CTE Pathway:**

(2 hours)		B1.1, B4.5, B6.2, B7.1, B8.1, B8.2, B8.4
CC. DIGITAL FORENSICS & INCIDENT ANALYSIS & RESPONSE Use incident response models and forensic techniques to investigate security incidents. (2 hours)	1. Explain the role of digital forensic processes. 2. Identify the steps in the Cyber Kill Chain. 3. Use the Diamond Model of Intrusion Analysis to classify intrusion events. 4. Apply the National Institute of Standards and Technology Guide (NIST 800-61r2) incident handling procedures to a given incident scenario. 5. Discuss backup solutions and restoring operations. 6. Pass a Digital Forensics & Incident Analysis & 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
DD. EMPLOYABILITY SKILLS AND RESUME PREPARATION Understand, apply, and evaluate the employability skills and résumé preparation desired of networking 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	**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

(4 hours)	j. quality of work k. respect, cultural and diversity differences 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	Career Planning & Management: 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