Regional Occupational Program

Cybersecurity 4: CySA+ 2026-2027

COURSE DESCRIPTION

This course prepares students to develop advanced cybersecurity knowledge and skills aligned to current cybersecurity analyst concepts. Students study threat analysis, vulnerability management, security operations, log analysis, incident response, digital evidence, security architecture, ethical hacking concepts, penetration testing concepts, malware, social engineering, denial-of-service attacks, web application threats, wireless and mobile security, intrusion detection, firewalls, and cryptography. Through hands-on labs, simulations, and project-based assignments, students analyze cybersecurity scenarios, identify threats and vulnerabilities, interpret security data, document findings, recommend mitigation strategies, and apply ethical and responsible cybersecurity practices in controlled instructional environments. Students who achieve competency in this course will build skills aligned to CompTIA CySA+ and related cybersecurity analyst pathways.

Course Information:

Course Length:	1 Year
Prerequisite:	Cybersecurity 3: Security+
Course Level:	Capstone
UC:	No
Articulated:	No
Industry Cert.:	CompTIA CySA+
Industry Sector:	Information and Communication Technologies
Pathway:	Information and Support Services
CALPADS:	8112

O*Net SOC Codes:

15-1231	Computer Network Support Specialists
15-1211	Computer Systems Analysts
13-1199.07	Security Management Specialists
15-1212	Information Security Analysts

Legend:

CTE - PS	CTE Pathway Standards
CRP	Career Ready Practices
CTE - AS	CTE Anchor Standards
CCSS	Common Core State Standards
ISTE	International Society for Technology in Education

Includes updates from 25/26 ICT Advisory

Advisory Minutes

Cybersecurity 4: CySA+

Course Orientation

a. Discuss objectives for this course, including competencies, teacher expectations, classroom policies, and procedures.
b. Identify and discuss the acquisition of transferable skills (communication, collaboration, creativity, and critical thinking) and their importance to being college and career ready and for future personal and professional success.
c. Review objectives, competencies, and course syllabus.
d. Discuss student and teacher expectations, including behavior, class rules, appropriate dress, pre-course knowledge, and grading policies, including enrollment and attendance requirements and procedures, and classroom/school safety and disaster procedures.
e. Discuss next steps in course sequence related to the career pathway, the need for reinforcement of basic skills, transferrable skills, and postsecondary and career options.
f. Discuss the Big Six: Career Ready Essentials and the Standards for Career Ready Practice as they relate to this course, all aspects of the industry sector, and being college and career ready.

Big Six: Career Ready Essentials

1. Effective Communication	CTE – PS	CRP	CTE - AS	CCSS	ISTE
a. Demonstrate effective verbal communication and conflict resolution skills. **b. Use the writing process to develop written communication with the appropriate tone, organization, and format for the identified audience.** c. Explain the effect of interpersonal skills on one's ability to communicate effectively and develop relationships. d. Describe the impact of ineffective communication on business relationships. e. Analyze the impact of vocabulary, body language, and tone on verbal communication. f. Demonstrate active listening skills. g. Accurately interpret industry-specific written communication. h. Model responsible and effective use of various communication technologies. i. Identify valid and reliable digital reference and resource materials. j. Gather information from multiple digital sources to compare and contrast, synthesize, and summarize. k. Identify and use appropriate communication and collaboration technologies. l. Utilize technology to problem solve, accomplish tasks, and to produce or publish products.		1 2 11	2 3 4 5 7 8 9 10 11	**LS** 9-10 11-12.6 **SLS** 11-12.2 9-10 11-12.1 11-12.1d **WS** 11-12.7 11-12.6	1b,c 2c 3b,c 5c 6b,c,d

2. Collaboration, Creativity, and Critical Thinking	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Demonstrate critical thinking skills for a variety of purposes and in different settings. **b. Collaborate to reach consensus on an identical objective through the sharing of knowledge, tasks, and learning.** c. Discuss the importance of the critical thinking process to real-world applications. d. Evaluate the impact of creative thinking on problem solving and innovation in real-world applications.		2 4 5 7 9 10	2 3 4 5 7 8	**LS** 9-10 11- 12.6 **SLS** 9-10	1c 3c,d 4a-d 5c,d 6c 7b,c,d

e. Compile work that demonstrates the process used to (elaborate, refine, analyze) evaluate original ideas and maximize creative efforts. f. Apply divergent and convergent thinking to the development of an original idea or solution. g. Examine real-world limits to adopting ideas. h. Demonstrate creative thinking (preparation, insight, evaluation, elaboration, and communication) to create a new idea or concept. i. Assume shared responsibility for collaborative work, and value the individual contributions made by each team member. j. Evaluate evidence, arguments, claims, and beliefs to identify connections. k. Identify bias, prejudice, propaganda, self-deception, distortion, and misinformation. l. Produce intellectual, informational, or material products that serve an authentic purpose. m. Work effectively and respectfully with those from diverse backgrounds or cultures. n. Demonstrate respect, trust, commitment, and the ability to compromise in collaborative projects.		11	9 11	11-12.1 11-12.1d 11-12.2 **WS** 11-12.7 11-12.6	
3. Leaders and Teams: Roles and Responsibilities	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Determine the individual and team members' roles and responsibilities. **b. Demonstrate leadership skills and qualities (i.e., reliability, negotiation skills, initiative, positive reinforcement, recognition of others' efforts, problem-solving skills, conflict resolution, and delegation).** c. Explain the importance of technical, social, and communication skills to team success. d. Compare and contrast leadership styles and their effectiveness in various situations. e. Organize and delegate responsibilities in a team setting to encourage ideas, perspectives, and contributions from all team members. f. Develop a strong sense of team identity by brainstorming solutions, volunteering, assisting others, practicing respect and courtesy, and taking initiative. g. Examine situations in which a follower becomes the leader. h. Describe twenty-first-century skills required across all occupations. i. Identify and discuss the characteristics of a successful team (i.e., leadership, cooperation, and effective decision-making). j. Leverage social and cultural differences to increase innovation and quality of work.		7 8 9	3 7 8 9 11	**SLS** 11-12.2 9-10 11-12.1 11-12.1d **WS** 11-12.6	7a,c
4. Legal, Ethical, and Environmental Considerations	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Demonstrate industry specific ethical and legal practices. **b. Identify eco-friendly industry specific practices and resources.** c. Identify local, state, and federal regulatory agencies, entities, laws, and regulations. d. Identify discrimination based on race, nationality, religion, gender, age, disability, or sexual orientation.		5 7 8 12	3 5 7 8 9	**WS** 11-12.6 11-12.7 **SLS**	2a,b 3a,b 5c 6c

e. Summarize the ethical and legal implications of workplace discrimination and harassment. f. Explain the concept of corporate citizenship. g. Examine an employer's role in protecting the health and welfare of employees, the community, and the environment. h. Analyze current environmental laws and regulations and their impact on industry. i. Compare and contrast both society's and industry's impact on the environment.			11	9-10 11-12.1 11-12.1d 11-12.2	
5. Personal Growth and Career Planning	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Demonstrate continued personal development and growth. **b. Develop and manage a personal growth and career plan.** c. Explain the relationship between sound financial habits and financial security. d. Create and manage a personal financial plan. e. Demonstrate initiative in achieving personal and professional goals. f. Apply time management strategies to meet deadlines. g. Demonstrate a growth mindset through flexibility and a positive attitude. h. Select and demonstrate appropriate job-search and retention techniques. i. Demonstrate strategies to prepare for employment. j. Demonstrate interpersonal skills appropriate for the workplace. k. Elaborate on the importance of perseverance to personal and professional success. l. Discover personal career interests, aptitudes, and skills.		1 2 3 4 6	2 3 4 7 8 11	**LS** 9-10 11-12.6 **SLS** 9-10 11-12.1 11-12.1d 11-12.2 **WS** 11-12.6	1a 3a,c 4d 6a,d 7b
6. Workplace Safety and Personal Wellness	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Demonstrate proper industry specific safe work practices to prevent injury or illness. **b. Assess the potential impact of goal setting on personal and professional success.** c. Describe the role of security and emergency procedures in workplace safety. d. Describe the effect of preventative measures on emergencies in the workplace. e. Identify and describe the causes, prevention, and treatment of common accidents. f. Identify local, state, and federal agencies that regulate workplace safety. g. Explain the role of the California Occupational Safety and Health Administration (Cal-OSHA) and the Environmental Protection Agency (EPA). h. Discuss the basics of system operations. i. Demonstrate the proper use of personal protective equipment (PPE). j. Explain the purpose of and accurately interpret a Safety Data Sheet (SDS). k. Identify hazardous materials and chemicals. l. Demonstrate proper procedures to respond to work-related accidents and injuries. m. Describe how ergonomics, housekeeping, and maintenance are related to accidents and injuries. n. Demonstrate cyber ethics, cyber safety, and cybersecurity.		2 5 6 8 12	2 5 6 7 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.7 11-12.6 **SLS** 9-10 11-12.1 11-12.1d	1a,d 2a,d 5b

o. Assess the potential impact of preventative physical and mental health measures on workplace safety.					

Cybersecurity 4: CySA+ Units of Instruction

7. Assessing Cybersecurity Risk	CTE-PS	CRP	CTE- AS	CCSS	ISTE
a. Explain how systems, networks, applications, data, and users may be at risk of compromise. b. **Explain or recommend strategies to reduce the likelihood and impact of cybersecurity incidents.** c. Identify the strategic value of risk management in the context of information assurance. d. Compare risk assessment methodologies and use them in assessing risk. e. Translate risk assessment into specific strategies for mitigation. f. Develop documentation that supports a risk-management strategy, including findings, mitigation recommendations, and follow-up actions.	A5.1 A5.2 A5.3 A5.4	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	

8. Analyzing the Threat Landscape	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Analyze the nature of cybersecurity threats to better understand how organizations defend systems, networks, applications, data, and users. b. Compare, contrast, and categorize cybersecurity threats and threat profiles. c. Conduct ongoing threat-landscape research using teacher-approved sources to prepare for and support incident response.	A5.0 A5.2	1 4 5 11	1 4 5 10 11	**WS** 11-12.6 11-12.7	

9. Analyzing Reconnaissance Threats to Computing & Network Environments	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. **Identify information an attacker or threat actor may attempt to gather from an organization and explain how that information could be used in planning an attack.** b. Explain or use teacher-approved threat-modeling tools and techniques in a controlled or simulated environment. c. Assess the impact of reconnaissance incidents. d. Assess the impact of social engineering.	A5.0 A5.2 A5.4	1 4 5 11 12	1 4 5 10 11	**WS** 11-12.6 11-12.7	

10. Analyzing Attacks on Computing and Network Environments	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. **Recognize ways malicious activity can compromise an organization and explain the potential operational, technical, financial, and security impacts.** b. Assess the impact of system hacking attacks. c. Assess the impact of threats to web applications, services, and cloud-based resources. d. Assess the impact of malware. e. Assess the impact of hijacking and impersonation attacks.	A5.2	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6	

f. Assess the impact of denial-of-service incidents. g. Assess the impact of threats to mobile infrastructures. h. Assess the impact of threats to cloud infrastructures.				11-12.7	
11. Analyzing Post-Attack Techniques	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain post-compromise activity and strategies used to reduce long-term harm to an organization.** b. Identify and assess defensive indicators of command-and-control techniques. c. Identify and assess defensive indicators of persistence techniques. d. Identify and assess defensive indicators of lateral movement and pivoting techniques. e. Identify and assess defensive indicators of data exfiltration techniques. f. Identify and assess defensive indicators of anti-forensics techniques.	A5.0 A5.2 A5.3 A5.4 A6.0	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
12. Managing Vulnerabilities in the Organization	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Identify vulnerabilities within an organization and explain how vulnerability findings are used to determine risk and recommend remediation or mitigation strategies.** b. Explain or develop components of a vulnerability-management plan, including identification, prioritization, remediation, validation, and documentation. c. Assess common vulnerabilities in the organization. d. Explain or conduct teacher-approved vulnerability scans in a controlled or simulated environment and document findings.	A5.0 A5.2	1 4 5 11 12	1 4 5 10 11	**WS** 11-12.6 11-12.7	
13. Applying Authorized Security Testing and Operational Security	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain how authorized security testing can be used to identify weaknesses and recommend risk mitigation strategies.** b. Explain or conduct teacher-approved, authorized security testing activities in a controlled or simulated environment to evaluate security posture. c. Analyze and report the results of authorized security testing and make mitigation recommendations.	A5.4	1 2 4 5 8 11	1 2 4 5 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7 **SLS** 11-12.1d	
14. Collecting Cybersecurity Intelligence	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain how cybersecurity intelligence is used to monitor threats, vulnerabilities, and risks to support secure systems.** b. Design or evaluate a basic cybersecurity intelligence collection and analysis process using teacher-approved sources and tools.	A5.3 A6.1	1 2 4 5	1 2 4 5	LS 9-10 11-12.6	

c. Collect or interpret data from teacher-approved network-based security intelligence sources. d. Collect or interpret data from teacher-approved host-based security intelligence sources.		8 11	8 10 11	WS 11-12.6 11-12.7 SLS 11-12.1d	
15. Analyzing Log Data	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Analyze log data to identify potential threats, vulnerabilities, indicators of compromise, and actionable security intelligence.** b. Analyze a variety of log data using teacher-approved Windows, Linux, cloud, or security-analysis tools. c. Explain or use a SIEM or log-management system as part of the analysis process. d. Parse log files using searches, filters, queries, or regular expressions to locate meaningful security intelligence.	A7.4	1 4 5 11	1 4 5 10 11	WS 11-12.6 11-12.7	
16. Performing Active Asset and Network Analysis	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain or conduct teacher-approved active asset and network analysis in a controlled or simulated environment to support actionable security intelligence.** b. Analyze incidents using teacher-approved Windows-based or endpoint-analysis tools. c. Analyze incidents using teacher-approved Linux-based or command-line security tools. d. Explain or use teacher-approved malware-analysis methods, tools, or simulations in a controlled environment. e. Analyze common indicators of compromise and document findings.	A5.0 A5.4	1 2 4 5 8 11	1 2 4 5 8 10 11	LS 9-10 11-12.6 WS 11-12.6 11-12.7 SLS 11-12.1d	
17. Responding to Cybersecurity Incidents	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain how timely, structured incident response helps reduce long-term harm to an organization.** b. Design or evaluate components of an incident-response process used to address immediate and potential threats. c. Explain or apply teacher-approved incident-mitigation methods in a controlled or simulated environment. d. Explain the transition from incident response to post-incident review, lessons learned, and forensic investigation when appropriate.	A5.0	1 2 4 5 11	1 2 4 5 10 11	LS 9-10 11-12.6 WS 11-12.6 11-12.7	
18. Investigating Cybersecurity Incidents	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**

a. **Describe the process of collecting and preserving digital evidence to help determine how and why a security incident occurred.** b. Create or evaluate a basic plan for performing a forensic investigation after a cybersecurity incident. c. Explain or demonstrate teacher-approved methods for collecting and analyzing electronic evidence in a secure manner to prevent tampering or compromise. d. Recommend follow-up measures after an investigation, including documentation, reporting, remediation, and lessons learned.	A6.0 A6.2 A6.5	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
19. Addressing Security Architecture Issues	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain how security architecture issues can be identified and addressed to support secure-by-design systems and networks.** b. Identify and recommend remediation for identity and access management issues. c. Explain or apply security practices during the software development lifecycle.	A5.3 A5.4	1 2 4 5 8 11	1 2 4 5 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7 **SLS** 11-12.1d	
20. Introduction to Ethical Hacking and Authorized Security Testing	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain ethical hacking, authorized security testing, and the legal and ethical boundaries required for cybersecurity work.** b. Identify information security threats and attack vectors. c. Identify basic authorized security-testing concepts. d. Identify phases of an attack and explain how defenders use this knowledge to reduce risk. e. Identify types of cyberattacks and related defensive considerations. f. Identify information security controls.	A5.1 A5.2	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
21. Footprinting and Reconnaissance Analysis	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Explain how threat actors gather and refine publicly available or observable information about a target and how defenders can reduce exposure. b. Identify footprinting concepts. c. Identify footprinting threats and related defensive controls. d. Identify footprinting methodologies used in authorized security testing and defensive analysis.		1 2 4 5 8 11	1 2 4 5 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7 **SLS**	

				11-12.1d	
22. Introducing Authorized Network Scanning	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain how authorized network scanning can identify vulnerabilities, open ports, services, operating-system information, and network topology in a controlled or simulated environment.** b. Explain or demonstrate teacher-approved methods to discover live hosts, IP addresses, and open ports in a controlled or simulated environment. c. Explain or demonstrate teacher-approved methods for identifying operating systems and system architecture in a controlled or simulated environment. d. Explain or demonstrate teacher-approved methods for identifying services running on hosts in a controlled or simulated environment. e. Identify or validate vulnerabilities in teacher-approved lab hosts and document findings. f. Identify authorized security-testing report templates and deliverables. g. Identify types of authorized penetration testing and the conditions under which each may be used. h. Identify common authorized security-testing techniques and related ethical responsibilities.	A3.3 A6.0 A6.2 A6.3	1 2 4 5 8 11	1 2 4 5 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7 **SLS** 11-12.1d	
23. Enumeration and Defensive Analysis	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Explain how enumeration can reveal system resources and how defenders use enumeration findings to reduce risk. b. **Conduct a teacher-approved examination of a lab or simulated system to identify exposed information and document defensive findings.** c. Identify enumeration concepts. d. Identify authorized enumeration techniques and related defensive considerations. e. Explain or demonstrate teacher-approved enumeration of a lab or simulated network. f. Explain or demonstrate teacher-approved enumeration of network services or protocols, such as NetBIOS where appropriate, using approved tools.	A6.0 A6.2 A6.3	1 2 4 5 8 11	1 2 4 5 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7 **SLS** 11-12.1d	
24. System Attack Techniques and Defensive Controls	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain common system attack techniques and how defenders detect, prevent, or respond to unauthorized access attempts.** b. Identify password attack techniques and related authentication defenses. c. Identify privilege-escalation concepts, indicators, and defensive controls. d. Identify techniques attackers may use to execute code or conceal activity and explain related detection or prevention methods. e. Identify log-tampering concepts and explain methods used to protect, monitor, and preserve logs.	A4.1	1 2 4 5 8 11	1 2 4 5 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	

				SLS 11-12.1d	
25. Malware	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Explain how malware has evolved and its ability to penetrate and harm networks and systems. b. Identify Trojan concepts. c. Explain how Trojan malware may infect systems and identify prevention, detection, and response strategies. d. Identify types of Trojans. e. Identify techniques to detect Trojans. f. Identify Trojan countermeasures. g. Identify types of viruses and worms. h. Identify indicators of a virus or malware attack. i. Identify basic malware-analysis procedures using teacher-approved tools, examples, or simulations in a controlled environment. j. Identify virus and worm countermeasures.	A5.2	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
26. Sniffing	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain how packet analysis can be used to monitor network traffic, identify suspicious activity, and support defensive actions in a controlled or authorized environment.** b. Explain packet-sniffing and packet-analysis concepts. c. Identify types of sniffing attacks. d. Identify MAC-based attacks and related defensive controls. e. Identify DHCP attacks and related defensive controls. f. Identify spoofing attacks and related defensive controls. g. Identify DNS poisoning and related defensive controls. h. Identify countermeasures to sniffing attacks.	A5.2 A6.2 A6.3	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
27. Social Engineering	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain how social engineering tactics are used to manipulate individuals into disclosing information, granting access, or taking unsafe actions, and identify related prevention strategies.** b. Identify social engineering techniques. c. Identify impersonation and social engineering risks on social media, communication platforms, and other digital environments. d. Identify social engineering countermeasures.	A5.0 A5.3 A5.4	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	

28. Denial of Service	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Describe how Denial of Service (DoS) attacks occur and the measures for preventing them. b. Identify symptoms of a DoS attack. c. Identify the characteristics of a Distributed Denial of Service Attack (DDoS). d. Identify common DoS and DDoS attack methods and related detection or mitigation strategies. e. Identify DoS detection techniques. f. Identify DoS/DDoS countermeasures.	A5.0 A5.3 A5.4	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	

29. Session Hijacking	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. **Explain how session hijacking can occur at the network and application levels and identify techniques used to prevent or detect these attacks.** b. Identify session hijacking techniques. c. Identify network-level session hijacking techniques and related defensive controls. d. Identify protection measures against session hijacking. e. Identify IPsec architecture and its role in protecting network communications.	A5.0 A5.2 A5.3 A5.4	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	

30. Web Server and Web Application Security	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. **Describe how attackers may exploit web servers and web applications and explain defensive practices used to reduce risk.** b. Identify why webservers are compromised. c. Identify common web server attack methods and related defensive controls. d. Identify how to defend against webserver attacks. e. Identify patch management tools. f. Identify authorized security-testing tools used to assess web server and web application security. g. Identify webserver security tools. h. Identify web attack vectors. i. Identify web application threats. j. Identify common web application attack methods and related defensive controls. k. Identify the process of analyzing web infrastructure exposure using authorized and teacher-approved methods. l. Identify common web server compromise techniques and related prevention, detection, and response strategies. m. Identify authorized web application security-testing tools and their appropriate use. n. Identify countermeasures. o. Identify web application security tools.	A5.0 A5.2	1 2 4 5 8 11	1 2 4 5 8 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7 **SLS** 11-12.1d	

p. Explain or demonstrate parameter tampering using teacher-approved examples or simulations in a controlled environment. q. Explain or demonstrate directory traversal using teacher-approved examples or simulations in a controlled environment. r. Explain or demonstrate cross-site scripting (XSS) using teacher-approved examples or simulations in a controlled environment. s. Explain or demonstrate authorized web crawling or web spidering concepts using teacher-approved examples or simulations. t. Explain or demonstrate cookie poisoning and cookie-parameter tampering using teacher-approved examples or simulations in a controlled environment. u. Identify and apply basic practices used to help secure web applications from hijacking and related attacks.					
31. SQL Injections	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Describe how SQL injection attacks can affect applications and data, and explain the importance of secure coding, input validation, detection, and defensive controls. b. Identify SQL injection attacks. c. Identify SQL injection detection. d. Identify types of SQL injection. e. Identify how SQL injection may be used to gather information and explain related detection and prevention strategies. f. Identify teacher-approved SQL injection testing or detection tools and their appropriate use in controlled or simulated environments. g. Identify SQL injection evasion concepts and related defensive detection strategies. h. Identify how to defend against SQL injection attacks. i. Identify SQL injection detection, testing, and prevention tools or techniques.	A5.2 A5.3 A5.4	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
32. Wireless Network Security	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Explain the vulnerability of wireless networks and steps to improve the defense of these networks. b. Identify wireless threats. c. Explain weaknesses in legacy wireless encryption, such as WEP, and identify stronger wireless security practices. d. Identify authorized wireless-network assessment concepts and related defensive controls. e. Identify how unauthorized wireless discovery activities can create privacy and security risks and explain appropriate legal, ethical, and defensive considerations. f. Identify authorized wireless security-assessment tools and their appropriate use in controlled or simulated environments.	A5.4 A6.0	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	

g. Identify practices used to defend against wireless attacks, including secure configuration, encryption, authentication, monitoring, and user awareness. h. Identify wireless monitoring, security, and configuration tools.					
33. Mobile Platform Security	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Explain or demonstrate teacher-approved mobile security assessment concepts in a controlled or simulated environment to identify vulnerabilities and recommend protections. b. Identify mobile attack vectors. c. Identify mobile platform vulnerabilities and risks. d. Identify Android operating-system architecture, common vulnerabilities, and security practices. e. Identify common iOS security risks and related defensive practices. f. Identify mobile-device security risks across current and legacy mobile platforms where appropriate. g. Identify mobile-device security considerations for current and legacy mobile platforms where appropriate. h. Identify guidelines for securing iOS devices. i. Identify guidelines for securing Android devices. j. Identify guidelines for securing current and legacy mobile devices where appropriate. k. Identify guidelines for securing mobile devices, including device configuration, updates, authentication, encryption, application permissions, and mobile device management. l. Identify mobile device management principles. m. Identify mobile security, management, and protection tools.	A5.2	1 2 4 5 8 11	1 2 4 5 8 10 11	LS 9-10 11-12.6 WS 11-12.6 11-12.7 SLS 11-12.1d	
34. Intrusion Detection, Firewalls, Honeypots, and Evasion Awareness	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. **Explain how intrusion detection systems, firewalls, and honeypots are used defensively and how awareness of evasion techniques supports stronger detection and prevention.** b. Identify ways to detect an intrusion. c. Identify types of intrusion detection systems. d. Identify types of firewalls and their architecture. e. Identify firewall-evasion concepts and explain related detection, prevention, and configuration practices. f. Explain the purpose, benefits, risks, and basic setup considerations of honeypots in a controlled or teacher-approved environment. g. Identify intrusion detection, prevention, monitoring, and alerting tools.	A5.2 A5.4	1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	
35. Cryptography	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**

a. Describe the benefits of cryptography to provide data integrity, confidentiality, nonrepudiation, and authentication. b. Identify encryption algorithms. c. Identify cryptography tools. d. Identify cryptographic attack concepts and explain the importance of strong encryption, key management, and secure implementation.		1 2 4 5 11	1 2 4 5 10 11	**LS** 9-10 11-12.6 **WS** 11-12.6 11-12.7	

Standards Alignment

The curricula have been aligned with the CTE Model Curriculum Standards released in 2013. Each industry sector was updated to meet the increased rigor and relevancy requirements of the Common Core State Standards. The curriculum also includes the new Standards for Career Ready Practices.

Standards for Career Ready Practice

1. *Apply appropriate technical skills and academic knowledge.*
2. *Communicate clearly, effectively, and with reason.*
3. *Develop an education and career plan aligned with personal goals.*
4. *Apply technology to enhance productivity.*
5. *Utilize critical thinking to make sense of problems and persevere in solving them.*
6. *Practice personal health and understand financial literacy.*
7. *Act as a responsible citizen in the workplace and the community.*
8. *Model integrity, ethical leadership, and effective management.*
9. *Work productively in teams while integrating cultural and global competence.*
10. *Demonstrate creativity and innovation.*
11. *Employ valid and reliable research strategies.*
12. *Understand the environmental, social, and economic impacts of decisions.*

CTE Anchor Standards—Common Core English Language Arts Alignment

Anchor Standard 1: Academics

Analyze and apply appropriate academic standards required for successful industry sector pathway completion leading to postsecondary education and employment. Refer to the industry sector alignment matrix for identification of standards. Note: alignment listed within each sector.

Anchor Standard 2: Communications

Language Standard: Acquire and accurately use general academic and domain-specific words and phrases sufficient for reading, writing, speaking, and listening at the (career and college) readiness level; demonstrate independence in gathering vocabulary knowledge when considering a word or phrase important to comprehension or expression. LS 9-10, 11-12.6

Anchor Standard 3: Career Planning and Management

Speaking and Listening Standard: Integrate multiple sources of information presented in diverse formats and media (e.g., visually, quantitatively, orally) in order to make informed decisions and solve problems, evaluating the credibility and accuracy of each source and noting any discrepancies among the data. SLS 11-12.2

Anchor Standard 4: Technology

Writing Standard: Use technology, including the Internet, to produce, publish, and update individual or shared writing products in response to ongoing feedback, including new arguments and information.

Anchor Standard 5: Problem Solving and Critical Thinking

Writing Standard: Conduct short as well as more sustained research projects to answer a question (including a self-generated question) or solve a problem, narrow, or broaden the inquiry when appropriate, and synthesize multiple sources on the subject, demonstrating understanding of the subject under investigation. WS 11-12.7

Anchor Standard 6: Health and Safety

Reading Standards for Science and Technical Subjects: Determine the meaning of symbols, keywords, and other domain-specific words and phrases as they are used in a specific scientific or technical context. RSTS 9-10, 11-12.4

Anchor Standard 7: Responsibility and Flexibility

Speaking and Listening Standard: Initiate and participate effectively in a range of collaborative discussions (one-on-one, in groups, and teacher-led) with diverse partners, building on others' ideas and expressing their own clearly and persuasively. SLS 9-10, 11-12.1

Anchor Standard 8: Ethics and Legal Responsibilities

Speaking and Listening Standard: Respond thoughtfully to diverse perspectives; synthesize comments, claims, and evidence made on all sides of an issue; resolve contradictions when possible; and determine what additional information or research is required to deepen the investigation or complete the work. SLS 11-2.1d

Anchor Standard 9: Leadership and Teamwork

Speaking and Listening Standard: Work with peers to promote civil, democratic discussions and decision making; set clear goals and deadlines; and establish individual roles as needed. SLS 11-12.1b

Anchor Standard 10: Technical Knowledge and Skills

Writing Standard: Use technology, including the Internet, to produce, publish, and update individual or shared writing products in response to ongoing feedback, including new arguments or information. WS 11-12.6

Anchor Standard 11: Demonstration and Application

Demonstrate and apply the knowledge and skills contained in the industry-sector anchor standards, pathway standards, and performance indicators in the classroom, laboratory, and workplace settings, and the career technical student organization. Note: no alignment evident for this standard. WS 11-12.6

Information and Communication Technologies

A. Information Support and Services Pathway

A3.3 Recognize where processes are running in a networked environment (e.g., client access, remote access).

A4.1 Use different systems and associated utilities to perform such functions as file management, backup and recovery, and execution of programs.

A5.0 Identify requirements for maintaining secure network systems.

A5.1 Follow laws, regulatory guidelines, policies, and procedures to ensure the security and integrity of information systems.

A5.2 Identify potential attack vectors and security threats.

A5.3 Take preventative measures to reduce security risks (e.g., strong passwords, avoid social engineering ploys, limit account permissions).

A5.4 Use security software and hardware to protect systems from attack and alert of potential threats, anti-malware software, and firewalls.

A6.0 Diagnose and solve software, hardware, networking, and security problems.

A6.1 Use available resources to identify and resolve problems using knowledge bases, forums, and manuals.

A6.2 Use a logical and structured approach to isolate and identify the source of problems and to resolve problems.

A6.3 Use specific problem-solving strategies appropriate to troubleshooting, eliminating possibilities, or guess and check.

A6.5 Evaluate solution methods recognizing the trade-offs of troubleshooting vs. reloading, reimaging, or restoring to factory defaults using a sandbox environment.

A7.4 Document technical support provided such as using a ticketing system.

ISTE Standards for Students

1. Empowered Learner- Students leverage technology to take an active role in choosing, achieving, and demonstrating competency in their learning goals, informed by the learning sciences.

a) Students articulate and set personal learning goals, develop strategies leveraging technology to achieve them, and reflect on the learning process itself to improve learning outcomes.

b) Students build networks and customize their learning environments in ways that support the learning process.

c) Students use technology to seek feedback that informs and improves their practice and to demonstrate their learning in a variety of ways

d) Students understand the fundamental concepts of technology operations, demonstrate the ability to choose, use and troubleshoot current technologies and are able to transfer their knowledge to explore emerging technologies.

2. Digital Citizen- Students recognize the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world, and they act and model in ways that are safe, legal, and ethical.

a) Students cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world.

b) Students engage in positive, safe, legal, and ethical behavior when using technology, including social interactions online or when using networked devices.

c) Students demonstrate an understanding of and respect for the rights and obligations of using and sharing intellectual property.

d) Students manage their personal data to maintain digital privacy and security and are aware of data-collection technology used to track their navigation online.

3.Knowledge Constructor- Students critically curate a variety of resources using digital tools to construct knowledge, produce creative artifacts, and make meaningful learning experiences for themselves and others.

a) Students plan and employ effective research strategies to locate information and other resources for their intellectual or creative pursuits.

b) Students evaluate the accuracy, perspective, credibility, and relevance of information, media, data, or other resources.

c) Students curate information from digital resources using a variety of tools and methods to create collections of artifacts that demonstrate meaningful connections or conclusions.

d) Students build knowledge by actively exploring real-world issues and problems, developing ideas and theories, and pursuing answers and solutions.

4. Innovative Designer- Students use a variety of technologies within a design process to identify and solve problems creating new, useful, or imaginative solutions.

a) Students know and use a deliberate design process for generating ideas, testing theories, creating innovative artifacts, or solving authentic problems.

b) Students select and use digital tools to plan and manage a design process that considers design constraints and calculated risks.

c) Students develop, test, and refine prototypes as part of a cyclical design process.

d) Students exhibit a tolerance for ambiguity, perseverance, and the capacity to work with open-ended problems.

5. Computational Thinker- Students develop and employ strategies for understanding and solving problems in ways that leverage the power of technological methods to develop and test solutions.

a) Students formulate problem definitions suited for technology-assisted methods such as data analysis, abstract models, and algorithmic thinking in exploring and finding solutions.

b) Students collect data or identify relevant data sets, use digital tools to analyze them, and represent data in various ways to facilitate problem-solving and decision-making.

c) Students break problems into component parts, extract key information, and develop descriptive models to understand complex systems or facilitate problem-solving.

d) Students understand how automation works and use algorithmic thinking to develop a sequence of steps to create and test automated solutions.

6. Creative Communicator- Students communicate clearly and express themselves creatively for a variety of purposes using platforms, tools, styles, formats, and digital media appropriate for their goals.

a) Students choose the appropriate platforms and tools for meeting the desired objectives of their creation or communication.

b) Students create original works or responsibly repurpose or remix digital resources into new creations.

c) Students communicate complex ideas clearly and effectively by creating or using a variety of digital objects such as visualizations, models, or simulations.

d) Students publish or present content that customizes the message and medium for their intended audiences.

7. Global Collaborator- Students use digital tools to broaden their perspectives and enrich their learning by collaborating with others and working effectively in teams locally and globally.

a) Students use digital tools to connect with learners from a variety of backgrounds and cultures, engaging with them in ways that broaden mutual understanding and learning.

b) Students use collaborative technologies to work with others, including peers, experts, or community members, to examine issues and problems from multiple viewpoints.

c) Students contribute constructively to project teams, assuming various roles and responsibilities to work effectively toward a common goal.

d) Students explore local and global issues and use collaborative technologies to work with others to investigate solutions.