SAN BERNARDINO COUNTY

Regional Occupational Program

Cybersecurity 4: CySA+ 2025-2026

COURSE DESCRIPTION

Threat Analysis and Forensics cover the fundamental principles of using analytic tools to identify, protect, detect, respond, and recover computing systems and digital assets against cyber threats and vulnerabilities. Students can increase their cybersecurity skills by learning ow to apply ethical hacking practices to defend against nefarious activity. Students learn ethical cyber security practices incident response team roles, policies, and procedures of a cybersecurity framework. This course prepares students to take the Cyber Security Analyst plus (CSA+) and Certified Ethical Hacker (CEH) exams which are high demand industry certifications across industry sectors.

Course Information:

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

O*Net SOC Codes:

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

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 24/25 ICT Advisory

Advisory Minutes

Cybersecurity 3: Security+

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 Information Security Risk	CTE-PS	CRP	CTE- AS	CCSS	ISTE
a. Explain how information is at risk of being compromised. **b. Prepare to reduce or eliminate chances of a security incident occurring or the impact it will have on an organization.** 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. Implement sound documentation for your risk management strategy.	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 threats to an organization to better understand how to defend against threats. b. Compare, contrast, and categorize cybersecurity threats and threat profiles. c. Perform ongoing threat landscape research to prepare for incidents.	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 the information an attacker is likely to obtain from an organization in order to better understand what or how they will attack. b. Implement threat modeling tools and tactics. 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 Computer & Network Environments	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Recognize the ways a malicious attack can compromise an organization and the potential effects of such an attack. b. Assess the impact of system hacking attacks. c. Assess the impact of threats to web apps and services. d. Assess the impact of malware. e. Assess the impact of hijacking and impersonation attacks. 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.	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	

11. Analyzing Post-Attack Techniques	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Explain the post-attack phase and how to avoid long lasting harm to an organization. b. Assess command and control techniques. c. Assess persistence techniques. d. Assess lateral movement and pivoting techniques. e. Assess data exfiltration techniques. f. Assess 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 to determine risk and solutions to solve security weaknesses. b. Implement a vulnerability management plan. c. Assess common vulnerabilities in the organization. d. Conduct vulnerability scans.	A5.0 A5.2	1 4 5 11 12	1 4 5 10 11	**WS** 11-12.6 11-12.7	
13. Implementing Compliance and Operational Security	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Demonstrate how to conduct penetration testing to identify weak points and correct and mitigate risks. b. Conduct authorized penetration tests to evaluate the organization's security posture. c. Analyze and report the results of a penetration test 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. Demonstrate how to maintain good intelligence on threats, vulnerabilities, and risks to keep systems secure. b. Design and implement a system of cybersecurity intelligence collection and analysis. c. Collect data from network-based intelligence sources. d. Collect data from host-based security intelligence sources.	A5.3 A6.1	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	

15. Analyzing Log Data	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Analyze log data to identify potential threats and vulnerabilities and actionable intelligence. b. Analyze a wide array of log data by using common Windows and Linux based security tools. c. Incorporate a SIEM system into the analysis process. d. Parse log files by using 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. Demonstrate how to conduct active asset analysis and network analysis to provide more dynamic actionable intelligence. b. Analyze incidents with Windows-based tools. c. Analyze incidents with Linux-based tools. d. Use methods and tools for malware analysis. e. Analyze common indicators of potential compromise.	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 to respond quickly and smartly to a security incident to prevent long-term harm to the organization. b. Design and implement a system to respond to urgent situations by mitigating immediate and potential threats. c. Mitigate incidents using various methods and devices. d. Prepare to move from the incident response phase to the post-mortem forensic investigation phase.	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 evidence and determining how and why a security incident occurred. b. Create a plan for performing forensic investigations after incidents occur. c. Collect and analyze electronic evidence in a secure manner to prevent tampering or compromises. d. Implement measures to follow up on an investigation.	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. Demonstrate how to handle security architecture issues so that an organization can become more secure by design.	A5.3 A5.4	1 2	1 2	**LS** 9-10	

b. Remediate, identify, and access management issues. c. Implement security during the software development lifecycle.		4 5 8 11	4 5 8 10 11	11-12.6 **WS** 11-12.6 11-12.7 **SLS** 11-12.1d	
20. Introduction to Ethical Hacking	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Explain ethical hacking and what skill sets are necessary to perform ethical hacking. b. Identify information security threats and attack vectors. c. Identify basic hacking concepts. d. Identify phases of a hacking attack. e. Identify types of hacking attacks. 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. Foot printing and Reconnaissance	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Describe how to gain and refine initial information on a target to build a profile of the target organization. b. Identify Foot printing concepts. **c.** Identify Foot printing threats. d. Identify the Foot printing methodology.		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. Introduce Scanning Networks	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Explain how to probe a network to search for vulnerabilities, open ports, operating system fingerprinting, and create a network map. b. Demonstrate an ability to discover live hosts, IP addresses, and open ports of live hosts. c. Demonstrate the ability to discover operating systems and system architecture. d. Demonstrate the ability to discover services running on hosts. e. Demonstrate vulnerabilities in live hosts. f. Identify penetration testing deliverable templates. g. Identify types of penetration testing. h. Identify common penetration testing techniques.	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	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Demonstrate how to enumerate resources on a system for later attack. **b. Conduct a deep examination of a system identifying information to have a complete picture of the target.** c. Identify enumeration concepts. d. Identify techniques for enumeration. e. Demonstrate the ability to enumerate a target network. f. Demonstrate the ability to enumerate NetBIOS using the appropriate 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 Hacking	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Demonstrate the process of gaining access to a system using tactics and techniques for actively penetrating a target. b. Identify password cracking techniques. c. Identify the process of privilege escalation and the appropriate tools. d. Identify the process to execute applications and hide files within a system. e. Identify the process to clear system 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. Identify how to infect systems with a Trojan. d. Identify types of Trojans. e. Identify techniques to detect Trojans. f. Identify Trojan countermeasures. g. Identify types of viruses and worms. h. Identify indicates of a virus attack. i. Identify malware analysis procedure. 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. Describe how to conduct packet sniffing to protect networks through defensive actions. b. Understand sniffing concepts. c. Identify types of sniffing attacks.	A5.2 A6.2 A6.3	1 2 4	1 2 4	**LS** 9-10 11-12.6	

d. Identify MAC attacks. e. Identify DHCP attacks f. Identify spoofing attacks. g. Identify DNS poisoning h. Identify countermeasures to sniffing attacks.		5 11	5 10 11	**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 coerce or trick information out of unsuspecting individuals to use this information to gain access to systems and networks. b. Identify social engineering techniques. c. Identify impersonation on social networking sites. 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 DoS attack tools. 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. Tell how session hijacking occurs at both the network level and the application level and the various techniques to prevent these types of attacks. b. Identify session hijacking techniques. c. Identify network level session hijacking techniques. d. Identify protection measures against session hijacking. e. Identify IPsec Architecture.	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. Hacking Webservers and Applications	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Describe how attackers penetrate web servers and web-based applications for the purpose of gaining access to networks and systems. b. Identify why webservers are compromised. c. Identify webserver attack methodology. d. Identify how to defend against webserver attacks. e. Identify patch management tools. f. Identify pen testing 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	

g. Identify webserver security tools. h. Identify web attack vectors. i. Identify web application threats. j. Identify web app attack methodology. k. Identify process of Foot printing web infrastructure. l. Identify hacking web servers. m. Identify web app hacking tools. n. Identify countermeasures. o. Identify web application security tools. p. Demonstrate parameter tampering. q. Demonstrate directory traversals. r. Demonstrate cross-site scripting (XSS). s. Demonstrate web spidering. t. Demonstrate cookie poisoning and cookie parameter tampering. u. Secure web applications from hijacking.				**SLS** 11-12.1d	
31. SQL Injections	**CTE - PS**	**CRP**	**CTE - AS**	**CCSS**	**ISTE**
a. Describe the power and effectiveness of SQL injection attacks and the complexity in defending against such attacks. b. Identify SQL injection attacks. c. Identify SQL injection detection. d. Identify types of SQL injection. e. Identify Network Reconnaissance using SQL injection. f. Identify SQL injection tools. g. Identify evasion techniques. h. Identify how to defend against SQL injection attacks. i. Identify SQL injection detection tools.	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. Hacking Wireless Networks	**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. Identify how to break WEP encryption. d. Identify how to footprint a wireless network. e. Identify how to discover Wi-Fi networks using wardriving. f. Identify wireless hacking tools. g. Identify how to defend against wireless attacks. h. Identify wireless security tools.	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	

33. Hacking Mobile Platforms	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Demonstrate how to conduct penetration testing on mobile devices to detect vulnerabilities. b. Identify mobile attack vectors. c. Identify mobile platform vulnerabilities and risks. d. Identify Android OS architecture and vulnerabilities. e. Identify techniques for hacking iOS devices. f. Identify techniques for hacking windows phones. g. Identify techniques for hacking blackberry devices. h. Identify guidelines for securing iOS devices. i. Identify guidelines for securing Android devices. j. Identify guidelines for securing windows phones. k. Identify guidelines for securing blackberry devices. l. Identify mobile device management principles. m. Identify mobile 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. Evading IDS, Firewalls, and Honeypots	CTE - PS	CRP	CTE - AS	CCSS	ISTE
a. Explain how defense skills are used such as evading intrusion detection systems, circumventing firewalls, and avoiding honeypot traps. b. Identify ways to detect an intrusion. c. Identify types of intrusion detection systems. d. Identify types of firewalls and their architecture. e. Identify how to evade firewalls with appropriate tools. f. Identify how to set up a honeypot. g. Identify intrusion detection 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 code breaking methodologies.		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) Stu 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.