(9001330) Cybersecurity Essentials

Version: 2024

Course Attributes

- **Course Number:** 9001330
- **Grade Level:** 3
- **Course Length:** 1 Hours
- **SOC Codes:**

  Program Primary SOC: 151212 - Network and Computer Systems Administrators

  Additional SOCs: *Refer to the Related Careers (SOC Codes) section*

Course Structure

Cybersecurity Essentials

The outline below shows the structure of this Course, including all its requirements and optional components.

Parent
9001330 Cybersecurity Essentials
0 Child Components - 0 Required

Related Careers (SOC Codes)

The career titles and SOC codes listed below are based on the 2018 Standard Occupational Classification (SOC) system, which is a federal statistical standard used by federal agencies to classify workers into occupational categories for the purpose of collecting, calculating, or disseminating data. Students completing this program, including required and optional program components, will learn valuable concepts and skills related to the following career(s).

Parent
9001330 Cybersecurity Essentials

- **Primary SOC Code**

  151212 - Network and Computer Systems Administrators

- **Secondary SOC Code**

Standards and Benchmarks

National Standards:

9001330 Cybersecurity Essentials

This course provides students with insight into the many variations of vulnerabilities, attack mechanisms, intrusion detection systems, and some methods to mitigate cybersecurity risks, including certificate services and cryptographic systems.

CTE-IT.912.9001330.1 - Demonstrate an understanding of the technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges.

Demonstrate an understanding of the technical underpinnings of cybersecurity and its taxonomy, terminology, and challenges.

CTE-IT.912.9001330.1.1

Explain the various elements that make up the security taxonomy used by the U.S. Computer Emergency Readiness Team (CERT).

CTE-IT.912.9001330.1.2

Describe the challenges associated with achieving and maintaining computer security.

CTE-IT.912.9001330.1.3

Discuss the range of potential consequences of various forms of security breaches.

CTE-IT.912.9001330.1.4

Describe various defense mechanisms, techniques, and methodologies (e.g., antivirus, anti-malware, protocol analyzers and scans, analyzing email headers, patch management).

CTE-IT.912.9001330.1.5

Compare and contrast mechanisms employed in passive and active cyberattacks.

CTE-IT.912.9001330.1.6

Describe vulnerabilities associated with each element of the CIA Triad.

CTE-IT.912.9001330.1.7

Explain the differences between hardware, software, data, and network assets susceptible to cyber-attack.

CTE-IT.912.9001330.1.8

Describe the tools and technologies used in cybersecurity.

CTE-IT.912.9001330.1.9

Define intrusion detection and discuss its role in cybersecurity (e.g., HIDS and NIDS).

CTE-IT.912.9001330.1.10

Explain what is meant by the term countermeasures (e.g., NIPS and HIPS).

CTE-IT.912.9001330.1.11

Describe the role recovery plays in cybersecurity (e.g., Business Continuity Plan).

CTE-IT.912.9001330.2 - Demonstrate an understanding of common information and computer system security vulnerabilities.

Demonstrate an understanding of common information and computer system security vulnerabilities.

CTE-IT.912.9001330.2.1

Describe the basic categories of vulnerabilities associated with cybersecurity (i.e., hardware, software, network, human, physical, and organizational).

CTE-IT.912.9001330.2.2

Describe the ways in which various social networks are cybersecurity targets.

CTE-IT.912.9001330.2.3

Describe footprinting and explain how it is used to reveal system vulnerabilities.

CTE-IT.912.9001330.2.4

Explain why default values and technical controls are points of vulnerability and describe the hardening efforts being taken by government and industry.

CTE-IT.912.9001330.2.5

Describe the process of port scanning and explain why it is so prevalent in cybersecurity.

CTE-IT.912.9001330.2.6

Describe what is meant by password strength and explain its relationship to vulnerability.

CTE-IT.912.9001330.2.7

Distinguish between a weak and a strong password.

CTE-IT.912.9001330.2.8

Describe some of the ways in which intruders can cover their tracks.

CTE-IT.912.9001330.2.9

Describe the circumstances under which a computer system is vulnerable to a denial of service attack.

CTE-IT.912.9001330.3 - Demonstrate an understanding of common cyberattack mechanisms, their consequences, and motivation for their use.

Demonstrate an understanding of common cyberattack mechanisms, their consequences, and motivation for their use.

CTE-IT.912.9001330.3.1

Describe spoofing as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.2
Describe the introduction of malware or spyware as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.3
Describe the use of grayware as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.4
Describe the use of computer viruses or worms as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.5
Describe Logic Bombs as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.6
Describe botnet and rootkit as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.7
Describe the introduction of a Trojan horse as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.8
Describe DNS poisoning as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.9
Describe buffer overflow as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.3.10
Understand the risk associated with a zero-day exploit.

CTE-IT.912.9001330.3.11
Understand risks associated with P2P networking including the Gnutella protocol and Torrents.

CTE-IT.912.9001330.3.12
Describe the use of ransomware as an attack mechanism and discuss its consequences and common motivating factors for its use.

CTE-IT.912.9001330.4 - Be able to identify and explain the following different kinds of cryptographic algorithms.

Be able to identify and explain the following different kinds of cryptographic algorithms.

CTE-IT.912.9001330.4.1
Demonstrate the use and purpose of hashing functions.

CTE-IT.912.9001330.4.2
Demonstrate the use and purpose of symmetric keys.

CTE-IT.912.9001330.4.3
Demonstrate the use and purpose of asymmetric keys.

CTE-IT.912.9001330.5 - Demonstrate an understanding of the following kinds of steganographic techniques and their use in cybersecurity.
Demonstrate an understanding of the following kinds of steganographic techniques and their use in cybersecurity.

CTE-IT.912.9001330.5.1
Network steganographic methods (e.g., WLAN).

CTE-IT.912.9001330.5.2
Digital steganographic methods (e.g., image encryption, audio, mimic functions, video, packet manipulation).

CTE-IT.912.9001330.5.3
Understand how steganographic methods are used in malware.

CTE-IT.912.9001330.6 - Understand how cryptography and digital signatures address the following security concepts.
Understand how cryptography and digital signatures address the following security concepts.

CTE-IT.912.9001330.6.1
Provide examples of confidentiality.

CTE-IT.912.9001330.6.2
Provide examples of integrity.

CTE-IT.912.9001330.6.3
Provide examples of authentication.

CTE-IT.912.9001330.6.4
Provide examples of non-repudiation.

CTE-IT.912.9001330.6.5
Provide examples of access control.

CTE-IT.912.9001330.7 - Understand and be able to explain the following concepts of PKI (Public Key Infrastructure).
Understand and be able to explain the following concepts of PKI (Public Key Infrastructure).

CTE-IT.912.9001330.7.1
Provide examples of certificates (e.g., policies, practice statements).

CTE-IT.912.9001330.7.2
Provide examples of revocation.

CTE-IT.912.9001330.7.3
Provide examples of trust models.

CTE-IT.912.9001330.8 - Demonstrate an understanding of certificates and their role in cybersecurity.

Demonstrate an understanding of certificates and their role in cybersecurity.

CTE-IT.912.9001330.8.1
Describe the role of a Certificate Authority (CA).

CTE-IT.912.9001330.8.2
Describe Registration Authority (RA) and its relevance to security certificates.

CTE-IT.912.9001330.8.3
Compare and contrast SSL/TSL X.509-compliant certificates with PGP-compliant certificates.

CTE-IT.912.9001330.8.4
Describe the events that make up the lifecycle of a certificate.

CTE-IT.912.9001330.8.5
Describe how root certificate distribution works.

CTE-IT.912.9001330.8.6
Describe the role of a Certificate Revocation List (CRL).

CTE-IT.912.9001330.8.7
Describe the role of the Online Certificate Status Protocol (OCSP).

CTE-IT.912.9001330.9 - Demonstrate an understanding of intrusion, the types of intruders, their techniques, and their motivation.

Demonstrate an understanding of intrusion, the types of intruders, their techniques, and their motivation.

CTE-IT.912.9001330.9.1
Define intrusion.

CTE-IT.912.9001330.9.2
Describe the classes of intruders (i.e., masquerader, misfeasor, clandestine user).

CTE-IT.912.9001330.9.3
Describe what is meant by a hacker and discuss their role in cybersecurity.

CTE-IT.912.9001330.9.4
Compare and contrast the “black hat”, “white hat”, “blue hat”, and “grey hat” hacker cultures (i.e., computer criminal versus

computer security expert).

CTE-IT.912.9001330.9.5
Describe various techniques used by hackers to achieve intrusion.

CTE-IT.912.9001330.9.6
Describe the difference between an inside and an outside attack.

CTE-IT.912.9001330.10 - Demonstrate an understanding of Intrusion Detection Systems (IDS).
Demonstrate an understanding of Intrusion Detection Systems (IDS).

CTE-IT.912.9001330.10.1
Describe the three logical components of IDS (i.e., sensors, analyzers, user interface).

CTE-IT.912.9001330.10.2
Explain how user behavior relates to the detection of an intruder.

CTE-IT.912.9001330.10.3
Describe the essential requirements for any IDS.

CTE-IT.912.9001330.11 - Describe host-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
Describe host-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).

CTE-IT.912.9001330.11.1
Describe anomaly detection, specifically threshold and profile-based approaches.

CTE-IT.912.9001330.11.2
Describe the types of audit records employed in intrusion detection (i.e., native, detection-specific).

CTE-IT.912.9001330.11.3
Describe signature detection, specifically rule-based anomaly and penetration identification approaches.

CTE-IT.912.9001330.12 - Describe network-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).
Describe network-based IDS, its capabilities, and its approaches to detection (i.e., anomaly, signature).

CTE-IT.912.9001330.12.1
Describe the primary approach for intrusion detection in a network.

CTE-IT.912.9001330.12.2
Compare and contrast inline and passive sensors.

CTE-IT.912.9001330.12.3
Discuss typical placement of sensors in a network-based IDS environment and explain the rationale for each.

CTE-IT.912.9001330.13 - Demonstrate an understanding of IDS applications.

Demonstrate an understanding of IDS applications.

CTE-IT.912.9001330.13.1

Describe the operation, typical activities, and outputs of an intrusion detection system.

CTE-IT.912.9001330.13.2

Describe some of the limitations of intrusion detection systems.

CTE-IT.912.9001330.13.3

Differentiate between an intrusion detection system (passive) and an intrusion prevention (reactive) system.

CTE-IT.912.9001330.13.4

Compare and contrast several of the intrusion detection systems available on the current market.

CTE-IT.912.9001330.14 - Demonstrate an understanding of port scanning and network traffic monitoring employed as intrusion detection techniques.

Demonstrate an understanding of port scanning and network traffic monitoring employed as intrusion detection techniques.

CTE-IT.912.9001330.14.1

Describe the process of monitoring/detecting port scanning attacks and associated patterns.

CTE-IT.912.9001330.14.2

Explain how the monitoring and analysis of network traffic can be used to detect intrusion.

CTE-IT.912.9001330.14.3

Utilize network monitoring and analysis tools to detect intrusion and anomalies.

CTE-IT.912.9001330.15 - Demonstrate an understanding of firewalls and other means of intrusion prevention.

Demonstrate an understanding of firewalls and other means of intrusion prevention.

CTE-IT.912.9001330.15.1

Describe the purpose and limitations of firewalls.

CTE-IT.912.9001330.15.2

Describe the four types of firewalls (i.e., packet filtering, stateful inspection, application-level gateway, circuit-level gateway).

CTE-IT.912.9001330.15.3

Describe the use of honeypots as an intrusion prevention technique.

CTE-IT.912.9001330.15.4

Explain how security policies are used to prevent intruders.

CTE-IT.912.9001330.15.5

Explain how Access Control Lists (ACLs) are used to prevent intrusion.

CTE-IT.912.9001330.16 - Demonstrate an understanding of vulnerabilities unique to virtual computing environments.

Demonstrate an understanding of vulnerabilities unique to virtual computing environments.

CTE-IT.912.9001330.16.1

Describe the limitations of traffic monitoring within virtual networks.

CTE-IT.912.9001330.16.2

Discuss the primary vulnerability of virtual operating systems.

CTE-IT.912.9001330.16.3

Describe the “hypervisor” and explain its role in securing a virtual environment.

CTE-IT.912.9001330.17 - Demonstrate an understanding of social engineering and its implications to cybersecurity.

Demonstrate an understanding of social engineering and its implications to cybersecurity.

CTE-IT.912.9001330.17.1

Define social engineering and describe its role in cybersecurity.

CTE-IT.912.9001330.17.2

Discuss common mechanisms that constitute social engineering (e.g., phishing, baiting, quid pro quo, pretexting).

CTE-IT.912.9001330.17.3

Describe the variety of attacks targeting the human element.

CTE-IT.912.9001330.17.4

Describe countermeasures that can be used to counter social engineering attacks.

CTE-IT.912.9001330.18 - Demonstrate an understanding of fundamental security design principles and their role in limiting points of vulnerability.

Demonstrate an understanding of fundamental security design principles and their role in limiting points of vulnerability.

CTE-IT.912.9001330.18.1

Discuss the three over-arching security design principles (i.e., only necessary, simple, ease of use).

CTE-IT.912.9001330.18.2

Describe the principle of least privilege as it relates to computer security.

CTE-IT.912.9001330.18.3

Describe the principle of separation of duties as it relates to computer security.

CTE-IT.912.9001330.18.4
Describe the principle of defense in depth as it relates to computer security.

CTE-IT.912.9001330.18.5
Describe the principle of fail secure or fail safe and false positive or false negative as it relates to computer security.

CTE-IT.912.9001330.18.6
Describe the principle of economy of mechanism as it relates to computer security.

CTE-IT.912.9001330.18.7
Describe the principle of complete mediation as it relates to computer security.

CTE-IT.912.9001330.18.8
Describe the principle of open design as it relates to computer security.

CTE-IT.912.9001330.18.9
Describe the principle of least common mechanism as it relates to computer security.

CTE-IT.912.9001330.18.10
Describe the principle of psychological acceptability as it relates to computer security.

CTE-IT.912.9001330.18.11
Describe the principle of leveraging existing components as it relates to computer security.

CTE-IT.912.9001330.18.12
Describe the principle of weakest link as it relates to computer security.

CTE-IT.912.9001330.18.13
Describe the principle of single point of failure as it relates to computer security.

CTE-IT.912.9001330.19 - Demonstrate the importance of health, safety, and environmental management systems in organizations and their importance to organizational performance and regulatory compliance.

Demonstrate the importance of health, safety, and environmental management systems in organizations and their importance to organizational performance and regulatory compliance.

CTE-IT.912.9001330.19.1
Describe personal and jobsite safety rules and regulations that maintain safe and healthy work environments.

CTE-IT.912.9001330.19.2
Explain emergency procedures to follow in response to workplace accidents.

CTE-IT.912.9001330.19.3
Create a disaster and/or emergency response plan.

CTE-IT.912.9001330.20 - Demonstrate leadership and teamwork skills needed to accomplish team goals and objectives.

Demonstrate leadership and teamwork skills needed to accomplish team goals and objectives.

CTE-IT.912.9001330.20.1

Employ leadership skills to accomplish organizational goals and objectives.

CTE-IT.912.9001330.20.2

Establish and maintain effective working relationships with others in order to accomplish objectives and tasks.

CTE-IT.912.9001330.20.3

Conduct and participate in meetings to accomplish work tasks.

CTE-IT.912.9001330.20.4

Employ mentoring skills to inspire and teach others.

CTE-IT.912.9001330.21 - Explain the importance of employability skill and entrepreneurship skills.

Explain the importance of employability skill and entrepreneurship skills.

CTE-IT.912.9001330.21.1

Identify and demonstrate positive work behaviors needed to be employable.

CTE-IT.912.9001330.21.2

Develop personal career plan that includes goals, objectives, and strategies.

CTE-IT.912.9001330.21.3

Examine licensing, certification, and industry credentialing requirements.

CTE-IT.912.9001330.21.4

Maintain a career portfolio to document knowledge, skills, and experience.

CTE-IT.912.9001330.21.5

Evaluate and compare employment opportunities that match career goals.

CTE-IT.912.9001330.21.6

Identify and exhibit traits for retaining employment.

CTE-IT.912.9001330.21.7

Identify opportunities and research requirements for career advancement.

CTE-IT.912.9001330.21.8

Research the benefits of ongoing professional development.

CTE-IT.912.9001330.21.9

Examine and describe entrepreneurship opportunities as a career planning option.

Related CTE Program

0511100315: Applied Cybersecurity

This course provides students with insight into the many variations of vulnerabilities, attack mechanisms, intrusion detection systems, and some methods to mitigate cybersecurity risks, including certificate services and cryptographic systems.

State Adopted Instructional Materials

[Author(s)], ([Copyright]), [Title] ([Edition] ed.), [Publisher].

CPALMS Educational Resources

Click HERE to access more than [XXXX] CPALMS-approved educational resources aligned to the standards and benchmarks in this CTE program.

(9001320) Computer & Network Security Fundamentals

Version: 2024

Course Attributes

- **Course Number:** 9001320
- **Grade Level:** 3
- **Course Length:** 1 Hours
- **SOC Codes:**

  Program Primary SOC: 151212 - Network and Computer Systems Administrators

  Additional SOCs: *Refer to the Related Careers (SOC Codes) section*

Course Structure

Computer & Network Security Fundamentals

The outline below shows the structure of this Course, including all its requirements and optional components.

Parent
9001320 Computer & Network Security Fundamentals
0 Child Components - 0 Required

Related Careers (SOC Codes)

The career titles and SOC codes listed below are based on the 2018 Standard Occupational Classification (SOC) system, which is a federal statistical standard used by federal agencies to classify workers into occupational categories for the purpose of collecting, calculating, or disseminating data. Students completing this program, including required and optional program components, will learn valuable concepts and skills related to the following career(s).

Parent
9001320 Computer & Network Security Fundamentals

- **Primary SOC Code**

  151212 - Network and Computer Systems Administrators

- **Secondary SOC Code**

Standards and Benchmarks

National Standards:

9001320 Computer & Network Security Fundamentals

This course introduces students to cybersecurity and provides them with essential computer and networking knowledge and skills, particularly those related to cybersecurity.

CTE-IT.912.9001320.1 - Demonstrate an understanding of cybersecurity, including its origins, trends, culture, and legal implications.

Demonstrate an understanding of cybersecurity, including its origins, trends, culture, and legal implications.

CTE-IT.912.9001320.1.1

Define cybersecurity.

CTE-IT.912.9001320.1.2

Describe how information security evolved into cybersecurity and the impact of the Internet on the pace and nature of the evolution.

CTE-IT.912.9001320.1.3

Describe the individual elements that comprise the CIA triad (i.e., Confidentiality, Integrity, Availability).

CTE-IT.912.9001320.1.4

Define and explain the various types of hackers and the role each plays in cybersecurity.

CTE-IT.912.9001320.1.5

Describe various methodologies used by hackers and the basis for their employment.

CTE-IT.912.9001320.1.6

Describe the individual elements of the AAA model (Authentication, Authorization and Accounting).

CTE-IT.912.9001320.2 - Describe the national agencies and supporting initiatives involved in cybersecurity.

Describe the national agencies and supporting initiatives involved in cybersecurity.

CTE-IT.912.9001320.2.1

Describe the role of the National Security Agency.

CTE-IT.912.9001320.2.2

Describe current trends in cyberattacks and strategies for combating them.

CTE-IT.912.9001320.2.3

Describe the legal implications of computer hacking and other forms of cyberattacks.

CTE-IT.912.9001320.2.4
Understand the importance of the weekly bulletins distributed by the United States Computer Emergency Readiness Team (US-CERT).

CTE-IT.912.9001320.2.5
Determine if any software or hardware on a given network has vulnerabilities outlined in the most recent US-CERT bulletin.

CTE-IT.912.9001320.3 - Discuss the underlying concepts of terms used in cybersecurity.

Discuss the underlying concepts of terms used in cybersecurity.

CTE-IT.912.9001320.3.1
Differentiate between cybersecurity and information assurance.

CTE-IT.912.9001320.3.2
Define confidentiality and give examples of security breaches.

CTE-IT.912.9001320.3.3
Define integrity and give examples of security breaches.

CTE-IT.912.9001320.3.4
Define authenticity and give examples of security breaches.

CTE-IT.912.9001320.3.5
Define accountability (non-repudiation) and give examples of security breaches.

CTE-IT.912.9001320.4 - Demonstrate an understanding of basic computer components, their functions, and their operation.

Demonstrate an understanding of basic computer components, their functions, and their operation.

CTE-IT.912.9001320.4.1
Describe the internal components of a computer (e.g., power supply, hard drive, mother board, I/O cards/ports, cabling).

CTE-IT.912.9001320.4.2
Demonstrate and understanding of common computer and programming terminology.

CTE-IT.912.9001320.4.3
Explain the physical and logical architecture of a microcomputer system.

CTE-IT.912.9001320.4.4
Describe the file types used in the operation of a computer.

CTE-IT.912.9001320.4.5
Compare and contrast memory technologies (e.g., RAM, ROM, virtual memory, memory management).

CTE-IT.912.9001320.5 - Demonstrate knowledge of different operating systems.

Demonstrate knowledge of different operating systems.

CTE-IT.912.9001320.5.1

Compare operating system file naming conventions.

CTE-IT.912.9001320.5.2

Describe the common elements that comprise the architecture of an operating system (e.g., kernel, file manager, memory manager, device manager, network manager).

CTE-IT.912.9001320.5.3

Demonstrate proficiency with file management and structure (e.g., folder creation, file creation, backup, copy, delete, open, save).

CTE-IT.912.9001320.5.4

Demonstrate a working knowledge of standard file formats.

CTE-IT.912.9001320.5.5

Describe the purpose of various operating systems (e.g., Windows, Mac, iOS, Android and Linux).

CTE-IT.912.9001320.5.6

Describe the difference between client and network operating systems.

CTE-IT.912.9001320.5.7

Differentiate between different operating systems and applications and Macros.

CTE-IT.912.9001320.5.8

Explain the basics of boot sequences, methods and startup utilities.

CTE-IT.912.9001320.5.9

Compare and contrast open source and proprietary software.

CTE-IT.912.9001320.5.10

Describe common system utilities used in performing computer maintenance.

CTE-IT.912.9001320.6 - Demonstrate an understanding of the Open Systems Interconnection (OSI) model.

Demonstrate an understanding of the Open Systems Interconnection (OSI) model.

CTE-IT.912.9001320.6.1

Explain the interrelations of the seven layers of the Open Systems Interconnection (OSI) as it relates to hardware and software.

CTE-IT.912.9001320.6.2

Describe the purpose of the OSI model and each of its layers.

CTE-IT.912.9001320.6.3
Explain specific functions belonging to each OSI model layer.

CTE-IT.912.9001320.6.4
Understand how two network nodes communicate through the OSI model.

CTE-IT.912.9001320.6.5
Discuss the structure and purpose of data packets and frames.

CTE-IT.912.9001320.6.6
Describe the two types of addressing covered by the OSI model.

CTE-IT.912.9001320.7 - Demonstrate an understanding of the TCP/IP model.

Demonstrate an understanding of the TCP/IP model.

CTE-IT.912.9001320.7.1
Explain the interrelations of the four layers of the TCP/IP model as it relates to hardware and software.

CTE-IT.912.9001320.7.2
Describe the purpose of the TCP/IP model and each of its layers.

CTE-IT.912.9001320.7.3
Explain specific functions belonging to each TCP/IP model layer.

CTE-IT.912.9001320.7.4
Understand how two network nodes communicate through the TCP/IP model.

CTE-IT.912.9001320.7.5
Describe the two types of addressing covered by the TCP/IP model.

CTE-IT.912.9001320.8 - Describe the services and protocols that operate in the application, transport, network, and data link layers of the OSI Model.

Describe the services and protocols that operate in the application, transport, network, and data link layers of the OSI Model.

CTE-IT.912.9001320.8.1
Describe the services and protocols used in the OSI Application Layer (i.e., DHCP, DNS, FTP, HTTP, SMTP, Telnet, IMAP).

CTE-IT.912.9001320.8.2
Describe the services and protocols used in the OSI Transport Layer (i.e., TCP, TLS/SSL, UDP).

CTE-IT.912.9001320.8.3
Describe the services and protocols used in the OSI Network Layer (i.e., IP, ICMP, IGMP, IPsec).

CTE-IT.912.9001320.8.4
Describe the services and protocols used in the OSI Data Link Layer (i.e., ARP, OSPF, L2TP, PPP).

CTE-IT.912.9001320.9 - Demonstrate proficiency using computer networks.

Demonstrate proficiency using computer networks.

CTE-IT.912.9001320.9.1
Define networking and describe the purpose of a network.

CTE-IT.912.9001320.9.2
Describe the conceptual background of digital networks and cloud computing including terminology and basics.

CTE-IT.912.9001320.9.3
Describe various types of networks and the advantages and disadvantages of each (e.g., peer to peer, client/server, server/thin client, ROI).

CTE-IT.912.9001320.9.4
Describe the use, advantages, and disadvantages of various network media (e.g. coaxial, twisted pair, fiber optics).

CTE-IT.912.9001320.9.5
Describe the function of various network devices (e.g., managed switch, switched hub or switch, router, bridge, gateway, access points, modem).

CTE-IT.912.9001320.9.6
Describe how network devices are identified (i.e., IP addressing).

CTE-IT.912.9001320.9.7
Explain the protocols commonly used in a network environment.

CTE-IT.912.9001320.9.8
Differentiate between public and private IP addresses.

CTE-IT.912.9001320.9.9
Describe the common ports and corresponding protocols used in a network.

CTE-IT.912.9001320.9.10
Describe the difference between the Internet and intranet.

CTE-IT.912.9001320.9.11
Compare and contrast IPv4 and IPv6.

CTE-IT.912.9001320.9.12
Compare and contrast the different methods for network connectivity (e.g., broadband, wireless, Bluetooth, cellular).

CTE-IT.912.9001320.9.13

Discuss the differences between Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Virtual Local Area Network (VLAN), and Virtual Private Network (VPN).

CTE-IT.912.9001320.10 - Describe and differentiate between serial, digital subscriber line (DSL), Metro Ethernet, and cable modem WAN connections.

Describe and differentiate between serial, digital subscriber line (DSL), Metro Ethernet, and cable modem WAN connections.

CTE-IT.912.9001320.10.1

Describe the various types of cloud computing (IaaS, PaaS, SaaS) and modes of delivery (Public, Private, Community, Hybrid).

CTE-IT.912.9001320.10.2

Describe practices that aid in protecting the Hybrid cloud model.

CTE-IT.912.9001320.10.3

Describe the challenges and solutions associated with securing embedded devices.

CTE-IT.912.9001320.11 - Demonstrate an understanding of basic security concepts.

Demonstrate an understanding of basic security concepts.

CTE-IT.912.9001320.11.1

Distinguish between vulnerability and a threat.

CTE-IT.912.9001320.11.2

Discuss the different types of attacks (e.g., active, passive).

CTE-IT.912.9001320.11.3

Define security policy and explain its role in cybersecurity.

CTE-IT.912.9001320.11.4

Describe the basic methods of authentication (e.g., password, biometrics, smart cards. two-factor authentication, multifactor authentication).

CTE-IT.912.9001320.11.5

Describe the various forms of encryption methodologies (e.g., symmetric, asymmetric, block cipher, stream cipher).

CTE-IT.912.9001320.11.6

Describe hash functions and their role in authentication.

CTE-IT.912.9001320.11.7

Describe various method of access control used in computer security (e.g., policies, groups, Access Control List (ACL)).

CTE-IT.912.9001320.11.8

Understand the concept of malware (i.e., ransomware, worms, viruses, adware) and how attackers use it to steal sensitive or

confidential information.

CTE-IT.912.9001320.12 - Demonstrate an understanding of legal and ethical issues in cybersecurity.

Demonstrate an understanding of legal and ethical issues in cybersecurity.

CTE-IT.912.9001320.12.1

Define cybercrime and discuss the challenges facing law enforcement.

CTE-IT.912.9001320.12.2

Identify the key legislative acts that impact cybersecurity.

CTE-IT.912.9001320.12.3

Describe the Federal criminal code related to computers and give examples of cybercrimes and penalties, particularly those involving inappropriate access.

CTE-IT.912.9001320.12.4

Discuss the concept of digital forensics and its place in cybercrime investigations and incident response.

CTE-IT.912.9001320.12.5

Distinguish among the Intellectual Property Rights of trademark, patent, and copyright.

CTE-IT.912.9001320.12.6

Explain digital rights management and the implications of the Digital Millennium Copyright Act (DMCA).

CTE-IT.912.9001320.12.7

Describe the implications of various social media on the safeguarding of personal or sensitive information.

CTE-IT.912.9001320.12.8

Describe various safeguards that can be employed to help ensure that sensitive or confidential information is not inadvertently divulged or obtained.

CTE-IT.912.9001320.13 - Demonstrate an understanding of virtualization technology.

Demonstrate an understanding of virtualization technology.

CTE-IT.912.9001320.13.1

Define virtual computing.

CTE-IT.912.9001320.13.2

Explain the benefits of virtual computing.

CTE-IT.912.9001320.13.3

Differentiate between guest and host operating systems.

CTE-IT.912.9001320.13.4
Install desktop virtualization software.

CTE-IT.912.9001320.13.5
Describe the role of the hypervisor.

CTE-IT.912.9001320.13.6
Create and upgrade a virtual machine.

CTE-IT.912.9001320.13.7
Optimize the performance of a virtual machine.

CTE-IT.912.9001320.13.8
Preserve the state of a virtual machine.

CTE-IT.912.9001320.13.9
Clone, move and share virtual machines.

CTE-IT.912.9001320.13.10
Use basic (static) and dynamic virtual disks and disk drives.

CTE-IT.912.9001320.13.11
Configure a virtual network.

CTE-IT.912.9001320.13.12
Connect devices to a virtual machine.

CTE-IT.912.9001320.13.13
Enable security settings on a virtual machine.

CTE-IT.912.9001320.14 - Recognize and understand the administration of remote access technologies.

Recognize and understand the administration of remote access technologies.

CTE-IT.912.9001320.14.1
Configure 802.1x authentication for a given scenario.

CTE-IT.912.9001320.14.2
Connect clients to a VPN.

CTE-IT.912.9001320.14.3
Understand Authentication, Authorization and Accounting (AAA) management.

CTE-IT.912.9001320.14.4
Differentiate between TACACS+ (Terminal Access Controller Access Control System) and RADIUS.

CTE-IT.912.9001320.14.5
Differentiate between Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) protocols as they apply to VPN options.

CTE-IT.912.9001320.14.6
Implement the use of SSH (Secure Shell).

CTE-IT.912.9001320.14.7
Implement the use of IPsec (Internet Protocol Security).

CTE-IT.912.9001320.14.8
Identify vulnerabilities associated with authentication.

CTE-IT.912.9001320.14.9
Understand ways to implement VoIP technologies.

CTE-IT.912.9001320.14.10
Demonstrate the use and purpose of Kerberos.

CTE-IT.912.9001320.15 - Understand the application of concepts of physical security.
Understand the application of concepts of physical security.

CTE-IT.912.9001320.15.1
Configure access controls including biometric devices, keypads and security tokens.

CTE-IT.912.9001320.15.2
Recognize social engineering attempts.

CTE-IT.912.9001320.15.3
Evaluate environmental controls (e.g., EMI shielding, temperature, humidity and fire suppression).

CTE-IT.912.9001320.15.4
Develop a method of training users to recognize, report, and avoid social engineering attempts.

CTE-IT.912.9001320.15.5
Identify components of physical security, including mantraps, motion detection, alarm systems, locks, video surveillance, and fences/barricades.

CTE-IT.912.9001320.15.6
Install a camera for a video surveillance system.

CTE-IT.912.9001320.15.7
Configure an alarm system including a keypad and motion detector.

CTE-IT.912.9001320.15.8
Recognize vulnerabilities associated with physical security.

CTE-IT.912.9001320.15.9
Explain how a mantrap is used as a counter measure against tailgating.

CTE-IT.912.9001320.16 - Securely configure and maintain the following types of devices.

Securely configure and maintain the following types of devices.

CTE-IT.912.9001320.16.1
Configure and maintain software and hardware firewalls.

CTE-IT.912.9001320.16.2
Configure and secure routers.

CTE-IT.912.9001320.16.3
Apply security settings to switches.

CTE-IT.912.9001320.16.4
Configure and secure wireless devices.

CTE-IT.912.9001320.16.5
Secure a LAN connected to a DSL/cable modem.

CTE-IT.912.9001320.16.6
Configure a RAS (Remote Access Server) for remote connectivity.

CTE-IT.912.9001320.16.7
Securely deploy a PBX (Private Branch Exchange).

CTE-IT.912.9001320.16.8
Explain the benefits of implementing a VPN (Virtual Private Network).

CTE-IT.912.9001320.16.9
Deploy IDS (intrusion detection system) and IPS (intrusion prevention systems).

CTE-IT.912.9001320.16.10
Analyze the performance, efficiency and security of the network based on network monitoring and diagnostic software.

CTE-IT.912.9001320.16.11
Employ techniques used to lock down workstations.

CTE-IT.912.9001320.16.12
Configure and secure servers for a given scenario.

CTE-IT.912.9001320.16.13
Understand and assess the security of mobile devices including but not limited to those using the Android, iOS and Windows platforms.

CTE-IT.912.9001320.17 - Understand the societal and security challenges of emerging technologies.

Understand the societal and security challenges of emerging technologies.

CTE-IT.912.9001320.17.1
Explain the security implications of the Internet of Things (IoT) (i.e., understand the efforts to address authentication and updates to IoT devices).

CTE-IT.912.9001320.17.2
Explain societal and security challenges associated with robotics.

CTE-IT.912.9001320.17.3
Explain security challenges associated with serverless computing.

CTE-IT.912.9001320.17.4
Explain societal and security challenges associated with the implementation of 5G.

CTE-IT.912.9001320.17.5
Describe and explain the security challenges of Autonomous vehicles (i.e., the significance of vehicular cybersecurity and its relation to: computer vision, artificial intelligence, machine learning and deep learning).

CTE-IT.912.9001320.18 - Recognize and be able to differentiate and explain access control models.

Recognize and be able to differentiate and explain access control models.

CTE-IT.912.9001320.18.1
Understand access control as it applies to MAC (Mandatory Access Control).

CTE-IT.912.9001320.18.2
Understand access control as it applies to DAC (Discretionary Access Control).

CTE-IT.912.9001320.18.3
Understand access control as it applies to RBAC (Role Based Access Control).

CTE-IT.912.9001320.19 - Understand the security concerns for media.

Understand the security concerns for media.

CTE-IT.912.9001320.19.1
Understand and identify security concerns with the use of Coaxial Cable.

CTE-IT.912.9001320.19.2
The student should be able to identify and understand security concerns for UTP/STP (Unshielded Twisted Pair / Shielded Twisted Pair).

CTE-IT.912.9001320.19.3
Identify and understand security concerns fiber optic cable.

CTE-IT.912.9001320.19.4
Identify security concerns associated with removable media.

CTE-IT.912.9001320.19.5
Address pitfalls associated with tape backups.

CTE-IT.912.9001320.19.6
Apply drive encryption to hard drives.

CTE-IT.912.9001320.19.7
Secure flash drives.

CTE-IT.912.9001320.19.8
Smartcards and secure USB memory.

CTE-IT.912.9001320.20 - Explain the following security topologies as they relate to cybersecurity.
Explain the following security topologies as they relate to cybersecurity.

CTE-IT.912.9001320.20.1
Determine Security Zones.

CTE-IT.912.9001320.20.2
Point out vulnerabilities on a DMZ (Demilitarized Zone).

CTE-IT.912.9001320.20.3
Explain the security benefits of using an intranet.

CTE-IT.912.9001320.20.4
Explain the security benefits of using an extranet.

CTE-IT.912.9001320.20.5
Secure a VLAN (Virtual Local Area Network).

CTE-IT.912.9001320.20.6
Describe the security benefits associated with NAT (Network Address Translation).

CTE-IT.912.9001320.20.7
Justify the implementation of tunneling, for security purpose.

CTE-IT.912.9001320.21 - Use oral and written communication skills in creating, expressing and interpreting information and ideas.

Use oral and written communication skills in creating, expressing and interpreting information and ideas.

CTE-IT.912.9001320.21.1
Select and employ appropriate communication concepts and strategies to enhance oral and written communication in the workplace.

CTE-IT.912.9001320.21.2
Locate, organize and reference written information from various sources.

CTE-IT.912.9001320.21.3
Design, develop and deliver formal and informal presentations using appropriate media to engage and inform diverse audiences.

CTE-IT.912.9001320.21.4
Interpret verbal and nonverbal cues/behaviors that enhance communication.

CTE-IT.912.9001320.21.5
Apply active listening skills to obtain and clarify information.

CTE-IT.912.9001320.21.6
Develop and interpret tables and charts to support written and oral communications.

CTE-IT.912.9001320.21.7
Exhibit public relations skills that aid in achieving customer satisfaction.

CTE-IT.912.9001320.22 - Solve problems using critical thinking skills, creativity and innovation.

Solve problems using critical thinking skills, creativity and innovation.

CTE-IT.912.9001320.22.1
Employ critical thinking skills independently and in teams to solve problems and make decisions.

CTE-IT.912.9001320.22.2
Employ critical thinking and interpersonal skills to resolve conflicts.

CTE-IT.912.9001320.22.3
Identify and document workplace performance goals and monitor progress toward those goals.

CTE-IT.912.9001320.22.4
Conduct technical research to gather information necessary for decision-making.

CTE-IT.912.9001320.23 - Use information technology tools.

Use information technology tools.

CTE-IT.912.9001320.23.1
Use personal information management (PIM) applications to increase workplace efficiency.

CTE-IT.912.9001320.23.2
Employ technological tools to expedite workflow including word processing, databases, reports, spreadsheets, multimedia presentations, electronic calendar, contacts, email, and internet applications.

CTE-IT.912.9001320.23.3
Employ computer operations applications to access, create, manage, integrate, and store information.

CTE-IT.912.9001320.23.4
Employ collaborative/groupware applications to facilitate group work.

CTE-IT.912.9001320.24 - Describe the roles within teams, work units, departments, organizations, inter-organizational systems, and the larger environment.

Describe the roles within teams, work units, departments, organizations, inter-organizational systems, and the larger environment.

CTE-IT.912.9001320.24.1
Describe the nature and types of business organizations.

CTE-IT.912.9001320.24.2
Explain the effect of key organizational systems on performance and quality.

CTE-IT.912.9001320.24.3
List and describe quality control systems and/or practices common to the workplace.

CTE-IT.912.9001320.24.4
Explain the impact of the global economy on business organizations.

CTE-IT.912.9001320.25 - Describe the importance of professional ethics and legal responsibilities.

Describe the importance of professional ethics and legal responsibilities.

CTE-IT.912.9001320.25.1
Evaluate and justify decisions based on ethical reasoning.

CTE-IT.912.9001320.25.2
Evaluate alternative responses to workplace situations based on personal, professional, ethical, legal responsibilities, and employer policies.

CTE-IT.912.9001320.25.3

Identify and explain personal and long-term consequences of unethical or illegal behaviors in the workplace.

CTE-IT.912.9001320.25.4

Interpret and explain written organizational policies and procedures.

CTE-IT.912.9001320.25.5

Display proficiency in using team-oriented collaboration and video teleconferencing software (e.g. Teams, Zoom).

Related CTE Program

0511100315: Applied Cybersecurity

This course introduces students to cybersecurity and provides them with essential computer and networking knowledge and skills, particularly those related to cybersecurity.

State Adopted Instructional Materials

[Author(s)], ([Copyright]), [Title] ([Edition] ed.), [Publisher].

CPALMS Educational Resources

Click HERE to access more than [XXXX] CPALMS-approved educational resources aligned to the standards and benchmarks in this CTE program.