STRANDS AND STANDARDS

PRINCIPLES OF CYBER DEFENSE AND ETHICS

Course Description

This course will provide a comprehensive view of Cybersecurity across an organization. You will learn how to use features of modern operating systems to enhance an organization's security, understand inherent weaknesses in wireless and wired networks, and be better equipped to protect your employer's and your own information. As a prerequisite to advanced topics in ethical hacking, incident response and digital forensics, you will also learn about Cybersecurity career paths and how to further develop your skills in these areas.

Intended Grade Level	10-12
Units of Credit	0.5
Core Code	35.01.00.00.036
Concurrent Enrollment Core Code	N/A
Prerequisite	Digital Literacy
Skill Certification Test Number	Coming Soon
Test Weight	N/A
License Type	CTE and/or Secondary Education 6-12
Required Endorsement(s)	
Endorsement 1	Cybersecurity
Endorsement 2	Information Technology Systems
Endorsement 3	Programming & Software Development

STRAND 1

Understanding Security Layers.

Standard 1

Understand core security principles.

- Understand the concepts of confidentiality, integrity, availability.
- Understand how threat and risk impact principles; principles of least privilege; social engineering; and attack surface.

Standard 2

Understand physical security.

- Understand site security, computer security, removable devices and drives, access control, mobile device security, disable Log On Locally, and keyloggers.

Standard 3

Understand Internet security.

- Understand browser settings, zones, and secure websites.

Standard 4

Understand wireless security.

- Understand advantages and disadvantages of specific security types; keys, SSID, and MAC filters.

STRAND 2

Understanding Operating System Security.

Standard 1

Understand user authentication.

- Understand multifactor, smart cards, RADIUS, and Public Key Infrastructure (PKI).
- Understand the certificate chain, biometrics, Kerberos, and time skew using Run As to perform administrative tasks and password reset procedures.

Standard 2

Understand permissions.

- Understand the following: file; share; registry; Active Directory; NTFS vs. FAT; enabling or disabling inheritance; behavior when copying or moving files within the same disk or onto another disk; multiple groups with different permissions; basic permissions and advanced permissions; take ownership; and delegation.

Standard 3

Understand password policies.

- Understand the following: password complexity; account lockout; password length; password history; time between password changes; enforce by using group policies; and common attach methods.

Standard 4

Understand audit policies.

- Understand the following: types of auditing; what can be audited; enabling auditing; what to audit for specific purposes; where to save audit information; and how to secure audit information.

Standard 5

Understand encryption.

- Understand the following: EFS; how EFS-encrypted folders impact moving and copying files; Bitlocker (ToGo); Trusted Platform Module (TPM); software-based encryption; MAIL encryption and signing and other uses; VON; public key and private key; encryption algorithms; certificate properties; certificate services; PKI/ certificate services infrastructure; and token devices.

Standard 6

Understand malware.

- Understand the following: buffer overflow; worms; Trojans; and spyware.

STRAND 3

Understanding Network Security.

Standard 1

Understand dedicated firewalls.

- Understand the types of hardware firewalls and their characteristics.
- Understand when to use a hardware firewall instead of a software firewall and stateful vs. stateless inspection.

Standard 2

Understand Network Access Protection (NAP).

- Understand the purpose of NAP and the requirements for NAP.

Standard 3

Understand network isolation.

- Understand the following: VLANs; routing; honeypot; DMZ; NAT; VPN; IPsec; and Server and Domain Isolation.

Standard 4

Understand protocol security.

- Understand the following: protocol spoofing; IPsec; tunneling; DNSsec; network sniffing; and common attack methods.

STRAND 4

Understand Security Software.

Standard 1

Understand client protection.

- Understand the following: anti-virus; User Account Control (UAC); keeping client operating system and software updated; encrypting offline folders; software restriction policies.

Standard 2

Understand e-mail protection.

- Understand the following: anti-spam; anti-virus; spoofing; phishing and pharming; client vs. server protection; SPF records; and PTR records.

Standard 3

Understand server protection.

- Understand the following: separation of services; hardening; keeping server updated; secure dynamic DNS updates; disabling unsecure authentication protocols; Read-Only Domain Controllers; separate management VLAN; Microsoft Baseline Security Analyzer (SBA}.

STRAND 5

Understand Security Careers and Ethics.

Standard 1

- Identify careers in Cybersecurity.
- Identify education and/or certifications needed to work in the Cybersecurity field.
- Identify Cybersecurity professional organizations.

Workplace Skills

- Problem Solving
- Critical Thinking
- Legal Requirements/Expectations

Skill Certificate Test Points by Strand

CTE Skill Certificate Test in Development