Subject: Career and Technical Education
Grade: 11
Expectations: 61
Breakouts: 115

(a) Introduction.

1. Career and technical education instruction provides content aligned with challenging academic standards, industry relevant technical knowledge, and college and career readiness skills for students to further their education and succeed in current and emerging foundations.

2. The Science, Technology, Engineering, and Mathematics (STEM) Career Cluster focuses on planning, managing, and providing scientific research and professional and technical services such as labora.s hth h tidrehth tunauthorized access. As a field, it has become more sophisticated, so too have the abilities of adversaries looking to penetrate networks and access sensitive information. Cybersecurity professionals prevent, detect, and respond to minimize disruptions to governments, organizations, and individuals.

4.

(C) solve problems and think critically;

(i) solve problems

(ii) think critically

(D) demonstrate leadership skills and function effectively as a team member; and

(i) Page ()-667 aT3 (ma)-26 ()-32.4-a(1d [(Pa)-2 (g)-4.1 (

(D) explain and create a digital signature; and

(i) explain a digital signature

(ii) create a digital signature

(E) illustrate steganography.

(i) illustrate steganography

(7) Cybersecurity skills. The student understands the concept of system defense. The student is expected to:

(A) explain the purpose of establishing system baselines;

(i) explain the purpose of establishing system baselines

(B) evaluate the role of physical security;

(i) evaluate the role of physical security

(C) evaluate the functions of network security devices such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), intrusion detection prevention systems (IDPS), and security information and event management (SIEM) systems;

(i) evaluate the functions of network security devices

(D) analyze log files for anomalies; and

(i) analyze log files for anomalies

(E) develop a plan demonstrating the concept of defense in depth.

(i) develop a plan demonstrating the concept of defense in depth

(8) Cybersecurity skills. The student demonstrates an understanding of secure network design. The student is expected to:

(A) explain the benefits of network segmentation, including sandboxes, air gaps, and virtual local area networks (VLAN);

(i) explain the benefits of network segmentation, including sandboxes

(ii) explain the benefits of network segmentation, including air gaps

(iii) explain the benefits of network segmentation, including virtual local area networks (VLAN)

(B) investigate and discuss the role of software-managed networks, including virtualization and cloud architecture;

(i) investigate the role of software-managed networks, including virtualization

(ii) investigate the role of software-managed networks, including cloud architecture

(iii) discuss the role of software-managed networks, including virtualization

(iv) discuss the role of software-managed networks, including cloud architecture

(C) evaluate the role of honeypots and honeynets in networks; and

(i) evaluate the role of honeypots in networks

(ii) evaluate the role of honeynets in networks

(D) discuss risk response techniques, including accept, transfer, avoid, and mitigate;

(i) discuss risk response techniques, including accept

(ii) discuss risk response techniques, including transfer

(iii) discuss risk response techniques, including avoid

(iv) discuss risk response techniques, including mitigate

(E) develop a plan of preventativeve77 0 TTf0.002 Tc -0.03]T1 0 Td6ques, including ac,.1s(vi)3 kE)e77 0 TTf0.001k 8 (j]T/TT .5 (Tw

(15) Risk assessment. The student investigates the role and effectiveness of environmental controls. The student is expected to:

- (A) explain commonly used physical security controls, including lock types, fences, barricades, security doors, and mantraps; and
  - (i) explain commonly used physical security controls, including lock types
  - (ii) explain commonly used physical security controls, including fences
  - (iii) explain commonly used physical security controls, including barricades
  - (iv) explain commonly used physical security controls, including security doors
  - (v) explain commonly used physical security controls, including mantraps
- (B) describe the role of embedded systems such as fire suppression; heating, ventilation, and air conditioning (HVAC) systems; security alarms; and video monitoring.
  - (i) describe the role of embedded systems