(9001340) Operational Cybersecurity

Version: 2024

Course Attributes

- **Course Number:** 9001340
- **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

Operational Cybersecurity

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

Parent
9001340 Operational Cybersecurity
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
9001340 Operational Cybersecurity

- **Primary SOC Code**

  151212 - Network and Computer Systems Administrators

- **Secondary SOC Code**

Standards and Benchmarks

National Standards:

9001340 Operational Cybersecurity

This course provides students with insight into the many ways in which computer systems can be secured, countermeasures implemented, and risk assessment performed.

CTE-IT.912.9001340.1 - Demonstrate an understanding of how to configure host systems to guard against cyber intrusion.

Demonstrate an understanding of how to configure host systems to guard against cyber intrusion.

CTE-IT.912.9001340.1.1

Describe the security features and options available for configuring network routers to prevent intrusion.

CTE-IT.912.9001340.1.2

Describe the various types of firewalls (i.e., packet filtering, stateful, application-level gateway, circuit-level gateway) and how each can be used to prevent intrusion.

CTE-IT.912.9001340.1.3

Explain the configuration and operation of a Demilitarized Zone (DMZ) host, including the key services contained within the zone.

CTE-IT.912.9001340.1.4

Describe the role of security zones, content filters, subnets, and trusted zones in configuring a network infrastructure.

CTE-IT.912.9001340.2 - Demonstrate an understanding of authentication methods and strategies.

Demonstrate an understanding of authentication methods and strategies.

CTE-IT.912.9001340.2.1

Describe the strengths, vulnerabilities, and countermeasures related to the use of passwords for authentication.

CTE-IT.912.9001340.2.2

Describe ways in which passwords are compromised and techniques/models for strengthening.

CTE-IT.912.9001340.2.3

Explain token authentication methods (e.g., memory cards, smart cards) and limitations.

CTE-IT.912.9001340.2.4

Discuss the use of biometrics (i.e., facial recognition, fingerprint, hand geometry, retinal pattern, iris, signature, voice) as an authentication strategy, including its advantages, limitations, vulnerabilities, and countermeasures.

CTE-IT.912.9001340.2.5

Describe the challenges associated with remote user authentication, including unique vulnerabilities and corresponding and

effective countermeasures.

CTE-IT.912.9001340.3 - Demonstrate an understanding of methods and strategies for controlling access to computer networks.

Demonstrate an understanding of methods and strategies for controlling access to computer networks.

CTE-IT.912.9001340.3.1

Compare and contrast the three primary categories of access control (i.e., discretionary, mandatory, role-based).

CTE-IT.912.9001340.3.2

Describe the underlying principles of authorization as an access control mechanism applicable to individuals, system services, subjects, and objects.

CTE-IT.912.9001340.3.3

Discuss the key features of an access control system (i.e., reliable input, granularity, least privilege, separation of duty, open/close policies, conflict resolution, administration).

CTE-IT.912.9001340.3.4

Describe the three elements of access control (i.e., subject, object, rights).

CTE-IT.912.9001340.3.5

Describe access rights (i.e., read, write, execute, delete, create, search) and their use in establishing individual and group access control policies.

CTE-IT.912.9001340.3.6

Compare and contrast the use, operation, and limitations of Access Control Matrix (ACM), Access Control Lists (ACLs), and Capability Tickets in a network environment.

CTE-IT.912.9001340.3.7

Describe the UNIX file access control schema.

CTE-IT.912.9001340.3.8

Explain the relationship between security policies and access control.

CTE-IT.912.9001340.3.9

Describe the use and conceptual operation of formal security policy models (e.g., Bell-La Padula (BLP), Chinese Wall Model (CWM), Harrison Ruzzo Ullman (HRU)).

CTE-IT.912.9001340.3.10

Describe the use, strengths, and vulnerabilities of group policies in access control and strategies for ensuring safety.

CTE-IT.912.9001340.3.11

Describe the key entities, relationships, and functions that comprise Role-Based Access Control (RBAC), including privilege management considerations.

CTE-IT.912.9001340.4 - Demonstrate an understanding of key network services, their operation, vulnerabilities, and ways in which they may be secured.

Demonstrate an understanding of key network services, their operation, vulnerabilities, and ways in which they may be secured.

CTE-IT.912.9001340.4.1

Describe the operation of Dynamic Host Configuration Protocol (DHCP), its vulnerabilities, typical cyberattacks, and potential countermeasure strategies.

CTE-IT.912.9001340.4.2

Describe the operation of the Domain Name System (DNS) service, its role in a network environment, its vulnerabilities, typical cyberattacks, and potential countermeasure strategies.

CTE-IT.912.9001340.4.3

Describe the operation of the Simple Mail Transport Protocol (SMTP), its role in a network environment, its vulnerabilities, typical cyberattacks, and potential countermeasure strategies.

CTE-IT.912.9001340.4.4

Describe the operation of the File Transfer Protocol (FTP) and Telnet, their role in a network environment, their vulnerabilities, typical cyberattacks, and potential countermeasure strategies.

CTE-IT.912.9001340.5 - Demonstrate an understanding of the processes involved in hardening a computer system or network.

Demonstrate an understanding of the processes involved in hardening a computer system or network.

CTE-IT.912.9001340.5.1

Describe hardening and some of the general approaches for securing a computer network.

CTE-IT.912.9001340.5.2

Describe and apply the process by which a web server is hardened against their typical cyberattacks.

CTE-IT.912.9001340.5.3

Describe and apply the process by which a mail server is hardened against their typical cyberattacks.

CTE-IT.912.9001340.5.4

Describe and apply the process by which a FTP server is hardened against their typical cyberattacks.

CTE-IT.912.9001340.5.5

Describe and apply the process by which a file/print server is hardened against their typical cyberattacks.

CTE-IT.912.9001340.5.6

Describe and apply the process by which data repositories are hardened against their typical cyberattacks.

CTE-IT.912.9001340.5.7

Describe and apply the process by which Directory Services is hardened against their typical cyberattacks.

CTE-IT.912.9001340.5.8

Describe and apply the process by which various network appliances are hardened against their typical cyberattacks.

CTE-IT.912.9001340.6 - Demonstrate an understanding of Public Key Infrastructure (PKI) management functions, key states, and life cycle/transition considerations.

Demonstrate an understanding of Public Key Infrastructure (PKI) management functions, key states, and life cycle/transition considerations.

CTE-IT.912.9001340.6.1

Compare and contrast the forms, limitations, and vulnerabilities associated with centralized and decentralized key management schemas, including the PKI web of trust model.

CTE-IT.912.9001340.6.2

Describe key escrow, its role in key management, its advantages, and its risks.

CTE-IT.912.9001340.6.3

Differentiate between key backup and key escrow.

CTE-IT.912.9001340.6.4

Explain the role of a key's expiration date, its implications on the key's validity, and its relationship to deactivation.

CTE-IT.912.9001340.6.5

Describe the circumstances under which a key might be revoked, who has authority to revoke a key, and how revocation is communicated.

CTE-IT.912.9001340.6.6

Compare and contrast key suspension and key revocation.

CTE-IT.912.9001340.6.7

Describe ways in which key recovery might be achieved, who is authorized to recover keys, and associated vulnerabilities to attack.

CTE-IT.912.9001340.6.8

Compare and contrast key renewal and key replacement, who is authorized to initiate renewal or replacement, and associated vulnerabilities to attack.

CTE-IT.912.9001340.6.9

Describe the circumstances under which a key might be destroyed, the considerations prior to destruction, and associated vulnerabilities to compromise or attack.

CTE-IT.912.9001340.7 - Demonstrate an understanding of the processes associated with assessing vulnerabilities and risks within an organization.

Demonstrate an understanding of the processes associated with assessing vulnerabilities and risks within an organization.

CTE-IT.912.9001340.7.1

Describe the process of asset identification relative to risk assessment and the considerations or criteria used in identifying assets

requiring protection and understand how to leverage a configuration management database (CMDB) for asset management.

CTE-IT.912.9001340.7.2
Describe the process of threat identification, including identifying the types of threats, asset vulnerabilities, and threat sources.

CTE-IT.912.9001340.7.3
Describe the process of risk assessment, including determination of attack probability, attack consequences, and assignment of risk priorities.

CTE-IT.912.9001340.7.4
Evaluate an existing security posture and identify gaps and vulnerabilities in security.

CTE-IT.912.9001340.7.5
Describe the role of governance, risk, and compliance in achieving a more secure organization.

CTE-IT.912.9001340.7.6
Describe the concepts of Key Performance Indicators and Risk Measurement. (e.g., annualized loss expectancy (ALE), annual rate of occurrence (ARO), single loss expectancy (SLE), Exposure Factor (EF).)

CTE-IT.912.9001340.7.7
Analyze and apply data and measurements to solve business problems and relate it to IT risk and business continuity.

CTE-IT.912.9001340.8 - Demonstrate an understanding of penetration testing, the types of tests and metrics, testing methodologies, and reporting processes.

Demonstrate an understanding of penetration testing, the types of tests and metrics, testing methodologies, and reporting processes.

CTE-IT.912.9001340.8.1
Describe the types of penetration tests (i.e., human, physical, wireless, data networks, telecommunications), the goals of each type, the metrics tested, and the value of their results.

CTE-IT.912.9001340.8.2
Compare and contrast the processes of black box versus white box penetration testing, including their characteristics, limitations, and appropriateness.

CTE-IT.912.9001340.8.3
Define attack vector and explain its relationship and importance to penetration testing.

CTE-IT.912.9001340.8.4
Describe common testing methodologies and standards used in penetration testing.

CTE-IT.912.9001340.8.5
Describe the salient points, structure, detail, and documentation typically addressed in reporting and debriefing the results of penetration testing.

CTE-IT.912.9001340.8.6
Detect malicious and abnormal activities through logs, intrusion detection systems, and other utilities and appliances.

CTE-IT.912.9001340.8.7
Reproduce methods that intruders use to gain unauthorized access to a network system for purposes of compromising information assets.

CTE-IT.912.9001340.8.8
Deploy proprietary and/or open source tools to test known technical vulnerabilities in networked systems.

CTE-IT.912.9001340.8.9
Determine which vulnerabilities are exploitable and estimate the risk and impact of potential exploitations.

CTE-IT.912.9001340.8.10
Recommend appropriate mitigation procedures against discovered vulnerabilities and security gaps.

CTE-IT.912.9001340.8.11
Model the ethics of a licensed Penetration Tester or Computer Security Specialist.

CTE-IT.912.9001340.9 - Demonstrate an understanding of the Incident Response Life Cycle and the activities comprising each phase.

Demonstrate an understanding of the Incident Response Life Cycle and the activities comprising each phase.

CTE-IT.912.9001340.9.1
Describe the activities that make up the Preparation Phase of the Incident Response Life Cycle (e.g., identification of useful tools and resources, setting up a war room, securing communications, creating a governance team, identifying key stakeholders for response activities).

CTE-IT.912.9001340.9.2
Describe the activities that make up the Detection and Analysis Phase of the Incident Response Life Cycle, including identification of indication sources, analysis of resulting signs of an intrusion event, documentation, and notification of the incident.

CTE-IT.912.9001340.9.3
Describe the factors to consider when prioritizing an incident.

CTE-IT.912.9001340.9.4
Describe the activities that make up the Containment, Eradication, and Recovery Phase of the Incident Response Life Cycle, including selecting a containment strategy, collecting and preserving evidence for forensic analysis, identifying the attacker, re-securing the system, and system restoration.

CTE-IT.912.9001340.9.5
Describe the activities that make up the Post Incident Activity Phase of the Incident Response Life Cycle, including identification of lessons learned and evidence retention.

Related CTE Program

0511100315: Applied Cybersecurity

This course provides students with insight into the many ways in which computer systems can be secured, countermeasures implemented, and risk assessment performed.

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.

(9001350) Cybersecurity Planning & Analysis

Version: 2024

Course Attributes

- **Course Number:** 9001350
- **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 Planning & Analysis

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

Parent
9001350 Cybersecurity Planning & Analysis
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
9001350 Cybersecurity Planning & Analysis

- **Primary SOC Code**

  151212 - Network and Computer Systems Administrators

- **Secondary SOC Code**

Standards and Benchmarks

National Standards:

9001350 Cybersecurity Planning & Analysis

This course focuses on the mitigation planning, disaster recovery, business continuity planning, and forensic analysis associated with securing computer environments. Many of the standards covered in this framework are based on or aligned with guidelines published by the Computer Security Division of the National Institute of Standards and Technology (NIST).

CTE-IT.912.9001350.1 - Demonstrate proficiency in cybersecurity risk mitigation planning.
Demonstrate proficiency in cybersecurity risk mitigation planning.

CTE-IT.912.9001350.1.1
Describe the major activities and security controls that are implemented as part of a sound risk management program.

CTE-IT.912.9001350.1.2
Discuss the rationale for executive sponsorship and delineated management responsibilities in successfully implementing a risk management program.

CTE-IT.912.9001350.2 - Demonstrate proficiency in establishing a risk management framework.
Demonstrate proficiency in establishing a risk management framework.

CTE-IT.912.9001350.2.1
Describe the importance of creating a system definition for use in assessing vulnerabilities and risks.

CTE-IT.912.9001350.2.2
Describe the major elements of a system definition.

CTE-IT.912.9001350.2.3
Differentiate among critical assets, cyber assets, and critical cyber assets.

CTE-IT.912.9001350.2.4
Explain why cyber assets are classified as public, restricted, confidential, or private and why this plays a role in creating a risk management framework.

CTE-IT.912.9001350.2.5
Compare and contrast the classes of cyber assets (i.e., public, restricted, confidential, private) and give examples of each.

CTE-IT.912.9001350.2.6
Create a system definition that identifies all cyber assets, their class, and their risk category (e.g., critical).

CTE-IT.912.9001350.2.7
Describe an Electronic Security Perimeter (ESP) and discuss its role in formulating a risk management framework.

CTE-IT.912.9001350.2.8
Describe the process and goals of a vulnerability assessment of ESP access points.

CTE-IT.912.9001350.2.9
Define risk level and explain the variabilities of its components.

CTE-IT.912.9001350.2.10
Describe ways in which system vulnerability may be ranked according to impact (e.g., safety, outage, privacy, monetary).

CTE-IT.912.9001350.2.11
Describe some of the security controls (e.g., access control, training, audit, configuration, maintenance) that come into play when determining the appropriate risk mitigation strategy.

CTE-IT.912.9001350.2.12
Compare and contrast a top-down and a bottoms-up analysis approach for identifying and mitigating risks.

CTE-IT.912.9001350.2.13
Describe the range of testing/evaluation and associated tools used to monitor mitigation control effectiveness.

CTE-IT.912.9001350.2.14
Create a risk management framework.

CTE-IT.912.9001350.3 - Demonstrate proficiency in creating a corporate security policy.
Demonstrate proficiency in creating a corporate security policy.

CTE-IT.912.9001350.3.1
Describe the best practices and security controls that typify a sound corporate security policy.

CTE-IT.912.9001350.3.2
Discuss the elements of a corporate security policy, including policy management, personnel and training, critical asset management, ESP, physical security, incident reporting and response, disaster recovery and business continuity plans.

CTE-IT.912.9001350.3.3
Describe the need for specific implementation and enforcement processes as part of a corporate security policy.

CTE-IT.912.9001350.3.4
Explain the controls required for addressing personnel risks in a corporate security policy (e.g., training, hiring due diligence, enforcement of “least privilege,” access revocation).

CTE-IT.912.9001350.4 - Demonstrate proficiency in addressing process risks.
Demonstrate proficiency in addressing process risks.

CTE-IT.912.9001350.4.1

Describe the best practices and security controls typically implemented for assessing and mitigating operational risks, including.

1. Conduct periodic posture risk assessments.

2. Enforce access control, monitoring, and logging.

3. Perform disposal/redeployment of assets.

4. Enforce change control and configuration management.

5. Conduct vulnerability assessments.

6. Control, monitor, and log all access to assets.

7. Configuration and maintenance.

8. Ensure incident-handling processes.

9. Provide for contingency planning.

CTE-IT.912.9001350.4.2

Create an organized mitigation table that identifies operational or process risks, the potential impact of the risk, and specific actions required to mitigate the risk.

CTE-IT.912.9001350.5 - Demonstrate proficiency in addressing physical security risks.

Demonstrate proficiency in addressing physical security risks.

CTE-IT.912.9001350.5.1

Describe the best practices and security controls that ensure good physical security of critical infrastructure and assets.

CTE-IT.912.9001350.5.2

Discuss the resulting potential for compromise once physical security is breached.

CTE-IT.912.9001350.5.3

Create an organized mitigation table that identifies physical security risks, the potential impact of the risk, and specific actions required to mitigate the risk.

CTE-IT.912.9001350.6 - Demonstrate proficiency in cybersecurity contingency planning.

Demonstrate proficiency in cybersecurity contingency planning.

CTE-IT.912.9001350.6.1

Define resiliency and its relationship to contingency planning.

CTE-IT.912.9001350.6.2

Describe the purpose and scope of an Information Systems Contingency Plan (ISCP).

CTE-IT.912.9001350.6.3

Identify the five main components of a contingency plan (i.e., Supporting Information, Activation and Notification, Recovery,

Reconstitution, Appendices).

CTE-IT.912.9001350.6.4
Describe the contingency planning process and the rationale for each step in the process.

CTE-IT.912.9001350.6.5
Explain the three step process for conducting a business impact analysis (i.e., determine recovery criticality, identify resource requirements, identify recovery priorities).

CTE-IT.912.9001350.6.6
Compare and contrast Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO).

CTE-IT.912.9001350.6.7
Discuss the criteria typically used to activate the contingency plan.

CTE-IT.912.9001350.6.8
Discuss the role of backup and recovery considerations in contingency planning.

CTE-IT.912.9001350.6.9
Create a contingency plan that includes roles and responsibilities, a business impact analysis with contingency strategies/solutions, outage assessment, resource recovery priorities, backup and recovery strategies, and testing/training considerations.

CTE-IT.912.9001350.7 - Demonstrate proficiency in cybersecurity disaster recovery planning.
Demonstrate proficiency in cybersecurity disaster recovery planning.

CTE-IT.912.9001350.7.1
Describe the purpose and scope of a cybersecurity disaster recovery plan.

CTE-IT.912.9001350.7.2
Describe various recovery strategies according to their appropriateness.

CTE-IT.912.9001350.7.3
Explain the key considerations when formalizing a disaster recovery plan.

CTE-IT.912.9001350.7.4
Discuss the role of data collection relative to disaster recovery.

CTE-IT.912.9001350.7.5
Identify the types, purposes, and role of documentation during disaster recovery.

CTE-IT.912.9001350.7.6
Discuss the role of testing in a disaster recovery plan.

CTE-IT.912.9001350.8 - Demonstrate proficiency in cybersecurity business continuity planning.

Demonstrate proficiency in cybersecurity business continuity planning.

CTE-IT.912.9001350.8.1

Describe the purpose and scope of a cybersecurity business continuity plan.

CTE-IT.912.9001350.8.2

Explain the concept of fault tolerance and discuss its role in business continuity planning.

CTE-IT.912.9001350.8.3

Identify and use various utilities employed for the purpose of business continuity.

CTE-IT.912.9001350.8.4

Describe the role of backups for ensuring business continuity.

CTE-IT.912.9001350.9 - Demonstrate proficiency in the essential elements of forensic analysis.

Demonstrate proficiency in the essential elements of forensic analysis.

CTE-IT.912.9001350.9.1

Describe the four phases of forensic analysis and discuss the activities performed in each phase.

CTE-IT.912.9001350.9.2

Describe the forensic and evidentiary considerations when determining containment.

CTE-IT.912.9001350.9.3

Describe the types and sources of data collected for forensic analysis.

CTE-IT.912.9001350.9.4

Explain the various forms of data and associated collection/retrieval tools for the application transport, IP, and link layers.

CTE-IT.912.9001350.9.5

Explain the processes by which data is collected for analysis.

CTE-IT.912.9001350.9.6

Describe the role of system event logs in data collection.

CTE-IT.912.9001350.9.7

Describe the role of the process log in data collection.

CTE-IT.912.9001350.9.8

Describe the processes associated with preserving evidence collected for forensic purposes.

CTE-IT.912.9001350.9.9

Describe how the chain of custody can be maintained for evidence collected during a forensic analysis effort.

Related CTE Program

0511100315: Applied Cybersecurity

This course focuses on the mitigation planning, disaster recovery, business continuity planning, and forensic analysis associated with securing computer environments. Many of the standards covered in this framework are based on or aligned with guidelines published by the Computer Security Division of the National Institute of Standards and Technology (NIST).

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.