Miami Dade College

Course Description

CTS2317 | Advanced Network Security | 4.00 credits

This advanced network course covers the CISSP domains for security professionals. The student will learn security and risk management; asset security; security architecture and engineering; communication and network security; identity and access management; security assessment and testing; security operations; and software development security. Prerequisite: CTS1120.

Course Competencies

Competency 1: The student will demonstrate an understanding of security and risk management by:

1. Describing the data security concepts of confidentiality, integrity and availability.
2. Describing security governance principles, including: security functions in the enterprise; organizational processes; roles and responsibilities; security control frameworks; due diligence; and compliance requirements.
3. Describing legal, regulatory and compliance requirements that pertain to the information security of an enterprise.
4. Describing and modeling the ethics and standards of a security professional.
5. Drafting a security policy, standards, procedures, and guidelines for a given business organization.
6. Describing Business Continuity (BC) requirements and performing a Business Impact Analysis (BIA).
7. Preparing a security policy for a given organization, including: personnel procedures; identification of threats and vulnerabilities; risk assessment and analysis; enumerated countermeasures, controls, and responses; asset valuation, reporting requirements; and security frameworks.
8. Describing threat modeling concepts and methodologies.
9. Describing risk-based management concepts relating to hardware and software services, and vendors.
10. Drafting a security awareness, education, and training program.

Competency 2: The student will demonstrate an understanding of asset security by:

1. Describing and classifying information and assets.
2. Describing methods of determining and maintaining information and asset ownership.
3. Describing methods of privacy protection.
4. Describing methods of ensuring asset retention.
5. Describing data security controls and protection methods.
6. Describing secure information and asset handling requirements.

Competency 3: The student will demonstrate an understanding of security architecture and engineering by:

1. Describing methods of implementing and managing system architecture and engineering processes using secure design principles.
2. Describing the fundamental concepts of security models.
3. Describing the selection of controls based upon systems security requirements.
4. Describing the security capabilities of information systems, including memory protection, Trusted Platform Module (TPM), encryption and decryption.
5. Describing methods to assess and mitigate the vulnerabilities of security architectures, designs, and solution elements, including: client-based and server-based systems, databases, cryptographic systems, Industrial Control Systems (ICS), Cloud-based systems, and Internet of Things (IoT).
6. Describing the best practices for mitigating vulnerabilities in web-based systems, mobile systems, and embedded devices.
7. Describing the types and uses of cryptography, including: key management and algorithm selection; cryptographic methods; Public Key Infrastructure; digital signatures; and hashing.

8. Assessing an organization and recommending security controls for site and facility design.…

Competency 4: The student will demonstrate an understanding of communications and network security by:

1. Describing the vulnerabilities in the Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models.
2. Describing the best practices for secure network design, including: perimeter protection, defense in depth, firewalls, proxies, honeypots, intrusion detection systems, network address translation, system monitoring, encryption and encapsulation, endpoint security, etc.
3. Describing the vulnerabilities of wireless networks and performing a reconnaissance of a wireless network.
4. Securing a wireless network by performing a site survey, securing the service set identifier and wireless access points, deploying encryption and network access control, determining antenna placement and adjusting power levels, etc.
5. Describing the management of email security, including goals, issues and solutions.
6. Describing remote access security management, including protocols, authentication and security mechanisms.
7. Describing virtual private network management, including protocols, encryption, authentication and security monitoring.
8. Describing the various forms of network attack and the defensive methods and countermeasures for prevention and mitigation.
9. Describing methods of securing network components.
10. Describing methods of securing communication channels according to design.
11. Designing and implementing a secure local area network, including network access control, intrusion prevention and detection systems, proxies, firewalls, honeypots, etc.

Competency 5: The student will demonstrate an understanding of identity and access management by:

1. Describing methods for controlling physical and logical access to assets.
2. Describing methods for managing identification and authentication of people, devices, and services.
3. Identifying methods of integrating identity as a third-party service.
4. Describing the use of authorization mechanisms, including Role Based Access Control; Rule-based access control; Mandatory Access Control; Discretionary Access Control; and Attribute Based Access Control.
5. Describing the management of the identity and access
6. provisioning lifecycle, including provisioning, user and system account review, and deprovisioning.

Competency 6: The student will demonstrate an understanding of security assessment and testing by:

1. Describing design and validation assessment, testing and audit strategies.
2. Describing methods of security control testing, including: vulnerability assessment, penetration testing, log reviews, synthetic transactions, code review and testing, test coverage analysis, and interface testing.
3. Performing security data collection for technical and administrative purposes, including: management review and approval, key performance and risk indicators, backup verification data, training and awareness, disaster recovery and business continuity.
4. Analyzing test output and generating a report.
5. Performing a security assessment and audit.

Competency 7: The student will demonstrate an understanding of security operations by:

1. Describing the process of a security investigation, including: evidence collection and handling, reporting and documentation, investigative techniques, digital forensics tools, tactics, and procedures.
2. Describing the requirements for different investigation types, including: administrative, criminal, civil, regulatory, and industry standards.
3. Performing logging and monitoring activities, including: intrusion detection and prevention; security information and event management; continuous monitoring; and egress monitoring.
4. Describing methods of securely provisioning resources, including asset inventory; asset management; and configuration management.
5. Describing foundational security operations concepts, including: need-to-know/least privileges; separation

of duties and responsibilities; privileged account management; job rotation; information lifecycle; and service level agreements.

6. Describing resource protection techniques.
7. Performing incident handling for a given event, including: detection; response; mitigation; reporting; recovery; remediation; and lessons learned.
8. Performing detective and preventative measures, including: firewalls; intrusion detection and prevention systems; whitelisting/blacklisting; third-party provided security services; sandboxing; honeypots/honeynets; and anti- malware.
9. Performing patch and vulnerability management.
10. Describing the change management process for controlling transitions, including: review, authorization, test, implementation, and release of changed resource.
11. Describing recovery strategies, including: backup storage strategies; recovery site strategies; multiple processing sites; system resilience, high availability, quality of service, and fault tolerance.
12. Describing Disaster Recovery (DR) processes, including: response; personnel; communications; assessment; restoration; training and awareness.
13. Describing Disaster Recovery Plans and their implementation.
14. Describing Business Continuity (BC) planning and exercises.
15. Describing physical security management and control.
16. Describing personnel safety and security concerns, including travel; security training and awareness; emergency management; and duress.

Competency 8: The student will demonstrate an understanding of software development security by:

1. Describing the security process in the Software Development Life Cycle (SDLC).
2. Identifying security controls in development environments.
3. Assessing the effectiveness of software security.
4. Assessing the security impact of acquired software.
5. Defining secure coding guidelines and standards.

Competency 9: The student will demonstrate an understanding of workplace skills and professionalism by:

1. Describing the roles of the network security professional in a business enterprise.
2. Presenting and following oral and written instructions.
3. Demonstrating self-motivation and responsibility to complete an assigned task.
4. Choosing appropriate actions in situations requiring effective time management.
5. Applying principles and techniques for being a productive, contributing member of a team.
6. Identifying and discussing intellectual property rights and licensing issues.
7. Identifying and discussing issues contained within professional codes of conduct.
8. Using appropriate communication skills, courtesy, manners, and dress in the workplace.
9. Documenting problems and solutions in service reports and maintaining support records.
10. Explaining the methods and best practices of interviewing end users to determine the symptoms and probable causes of system problems.

Learning Outcomes:

1. Communication
2. Computer / Technology Usage
3. Critical Thinking
4. Ethical Issues
5. Information Literacy
6. Numbers / Data
7. Social Responsibility

Updated: Fall 2024