Miami Dade College

Course Description

CIS4364 | Intrusion Detection and Incident Response | 4.00 credits

This upper division course addresses the underlying principles and techniques for detecting and responding to current and emerging cybersecurity threats. Students will learn how to handle various types of malware, email, web, network, cloud and internal network incidents, as well as risk assessment methodologies, and policies related to incident handling. Prerequisite: CIS3360.

Course Competencies:

Competency 1: The student will be able to characterize various types of network intrusion incidents by:

1. Describing common information security threats, threat actors, and attack vectors
2. Identifying the critical components of information security
3. Describing the motives, goals, and objectives of information security attacks
4. Describing risk, vulnerability, threat, and exploit and their relation to information security
5. Distinguishing between the major threat categories (network, host, and application)
6. Describing the Defense-in-Depth security
7. strategy and its role in information security

Competency 2: The student will be able to demonstrate a practical understanding of intrusion detection by:

1. Describing the benefits of using security information and event management (SIEM)
2. Listing the significant capabilities of standard SIEM solutions (logging, monitoring, alerting, etc.)
3. Describing the various types of SIEM solutions (in-house, managed, cloud-based) and the advantages/disadvantages of each
4. Describing web authorization techniques and protocols, including Oauth2 and SAML
5. Describing the SIEM architecture and its components (collectors, agents, connectors, etc.)
6. Listing typical vendor SIEM products and their features (ARCSight, Splunk, IBM QRadar)
7. Describe the challenges and recommended practices for a successful SIEM deployment

Competency 3: The student will be able to demonstrate an understanding of cyber threat intelligence and its role in incident response by:

1. Defining and explaining Cyber Threat Intelligence (CTI) and its objectives
2. Describing the significant types of threat intelligence (strategic, tactical, operational)
3. Listing the components of a threat intelligence strategy
4. Describing the types of data collected from Open-Source Intelligence (OSINT)
5. Distinguishing between the types of threat intelligence (human, counter, internal)
6. Describing the Threat Intelligence Lifecycle

Competency 4: The student will be able to demonstrate an understanding of incident response by:

1. Describing the incident handling and response process (IH&R)
2. Explaining the steps within the IH&R process flow
3. Describing the initial incident response steps of preparation, recording and assignment
4. Explaining the steps of incident triage, notification, and containment for incident response
5. Listing the final steps of incident response, including forensic analysis, eradication, recovery
6. and post-incident activities

Competency 5: The student will be able to demonstrate an understanding of forensic readiness and first response by:

1. Describing the role of computer forensics in the incident handling process
2. Explaining the three phases involved in the computer forensics investigation process

3. Describing and listing the benefits of forensic readiness and business continuity
4. Describing and listing the types and characteristics of digital evidence
5. Explaining the principles of digital evidence collection (ACPO, SWGDE)
6. Describing the process of collecting, securing, and analyzing digital evidence
7. Describing the steps for static and volatile evidence collection

Competency 6: The student will be able to demonstrate an understanding of handling network security incidents by:

1. Listing the common types of network security incidents (reconnaissance, DoS, access)
2. Identifying the indications of a network security incident
3. Comparing the various tools used for detecting network security incidents
4. Describing the steps for handling unauthorized access incidents (reconnaissance, sniffing)
5. Listing the indications of inappropriate usage incidents (service, materials, external party)
6. Describing the different types of Denial of Service (DoS) attacks and their impacts
7. Describing the methods and tools for detecting and containing DoS/DDoS attacks
8. Identifying the different types of wireless security incidents (eavesdropping, wardriving)
9. Listing the steps to detect, contain, eradicate, and recover from wireless security incidents

Competency 7: The student will be able to demonstrate an understanding of handling malware incidents by:

1. Identifying the different types of malware attacks and their components
2. Describing the methods of malware propagation (email attachment, removable media, etc.)
3. Explaining the standard techniques used to distribute malware via the Internet
4. Describing the techniques to detect, contain, and eradicate malware
5. Listing the recommended practices for preventing malware incidents

Competency 8: The student will be able to demonstrate an understanding of handling email incidents by:

1. Describe the various forms of email attacks and their impacts on an organization
2. Explaining the types of crimes committed by sending emails (spamming, phishing, etc.)
3. Explaining the types of crimes supported by email (identity theft, cyberstalking)
4. Describe the steps to detect and contain an email attack
5. Describing the steps to eradicate and recover from an email attack

Competency 9: The student will be able to demonstrate an understanding of handling web security incidents by:

1. Listing the causes of web security incidents (configuration errors, insecure coding, etc.)
2. Identifying common web application security risks (SQL injection, XSS, etc.)
3. Describing the steps to detect and analyze web security incidents
4. Describing the steps and tools used to contain and eradicate web application attacks
5. Listing the best practices for securing web
6. applications (secure coding, security testing)

Competency 10: The student will be able to demonstrate an understanding of cloud security incidents by:

1. Describing common cloud security threats and attacks
2. Explaining how to detect and analyze various cloud security incidents
3. Explaining the steps to eradicate and recover from cloud security incidents
4. Describing the best practices to prevent cloud security attacks

Competency 11: The student will be able to demonstrate an understanding of insider threats by:

1. Describing common types of insider threats (disgruntled employees, poorly trained staff)
2. Explaining common motivations for insider attacks (espionage, hacktivism, revenge)

3. Listing some common attacks by insiders (tailgating, theft, eavesdropping)
4. Describing the best practices to detect, contain, eradicate and recover from insider threats

Learning outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Formulate strategies to locate, evaluate, and apply information
- Use computer and emerging technologies effectively