Cyber Ops 2023-2024 Catalog

[ARCHIVED CATALOG]

CSIA 115 - Cyber Ops

PREREQUISITES/COREQUISITE: SVAD 111 - Linux and Virtualization Tech or CSIA 105 - Introduction to Cyber Security/Information Assurance

PROGRAM: Cyber Security/Information Assurance
CREDIT HOURS MIN: 3
LECTURE HOURS MIN: 2
LAB HOURS MIN: 2
DATE OF LAST REVISION: Fall, 2020

This course introduces the core security concepts and skills needed to monitor, detect, analyze and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application of the skills needed to maintain and ensure security operational readiness of secure networked systems. The skills developed in the curriculum prepares students for a career in the rapidly growing area of cybersecurity operations working in or with a security operations center (SOC) in entry-level job roles such as Security SOC Analyst and Incident Responder.

MAJOR COURSE LEARNING OBJECTIVES: Upon successful completion of this course the student will be expected to:

1. Explain role of Cybersecurity Operations Analyst.
2. Utilize Operating Systems features needed to support cybersecurity analyses.
3. Explain the operation of network infrastructure and classify the various network attacks.
4. Analyze the operation of network protocols and services and use monitoring tools to identify attacks.
5. Use various methods to prevent malicious access to computer hosts and data.
6. Explain the impact of cryptography on network security monitoring.
7. Explain how to investigate and evaluate endpoint vulnerabilities and network security alerts.
8. Use virtual machines to implement, evaluate, and analyze cybersecurity threat events.
9. Analyze network intrusion data to identify compromised hosts and vulnerabilities.
10. Apply incident response models (CSIRSTs and NIST) to manage security incidents.
11. Understand how a SOC team detects and responds to security incidents, and how they protect their organization's information from modern threats.
12. Understand further how modern organizations are dealing with detecting and responding to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing their organizations and their customers.

COURSE CONTENT: Topical areas of study include -

- Cybersecurity and the Security Operations Center
- Protecting the Network
- Windows Operating System
- Cryptography and the Public Key

- Linux Operating System
- Infrastructure
- Network Protocols and Services
- Endpoint Security and Analysis
- Network Infrastructure
- Security Monitoring
- Principles of Network Security
- Incident Response and Handling

Course Addendum - Syllabus (Click to expand)
