Cybersecurity Modular (CYBERSECURITY-501)

Program Length: 28 Lessons
Duration: Self-paced, expected 30 weeks
Instructional Type: Online, self-paced
Class Schedule: Self-paced with one 45-minute 1-on-1 mentor session every week
Credential awarded: Certificate of Completion

In addition to the 45 minutes of mentoring session every week, students are expected to dedicate on average at least 9.25 hours each week to independent study and project work for an overall average commitment of 10 hours per week.

Program Description:
The Cybersecurity Modular program equips students to learn the skills needed to fulfill roles within the cybersecurity ecosystem. Through various experiential learning opportunities, students complete hands-on digital exercises using industry-standard tools and strategies. At the conclusion of this program, students will be prepared for roles focused on securing and defending data and information within a modern network and infrastructure.

Program Objectives:
The program covers 13 high-level objectives, each of which is broken down into a set of core competencies.

Objective 1: Identify and describe components of systems, software and networking fundamentals and apply best practice configurations to these components.
● Identify, describe, and access common graphical user and command line interface tools found in the Windows OS.
● Identify and describe the layers of the Open Systems Interconnection (OSI) and transmission control protocol/Internet protocol (TCP/IP) Models.
● Configure the appropriate settings to connect to a local area network.
Objective 2: Apply foundational principles of cybersecurity to different types of technology and threats.
● Use proper Authentication, Authorization, and Accounting (AAA) combinations to common technology for secure access control.
● Identify the different types of threat actors and apply common behaviors to each group.
● Analyze information to identify classes of cyber-attacks and top-level attack methods and techniques.
● Identify and describe common malware categories.
Objective 3: Describe and apply fundamental cryptography concepts, including the role cryptography plays in cybersecurity.
● Describe the role cryptography plays in cybersecurity
● Apply fundamental cryptography concepts, including symmetric and asymmetric encryption
Objective 4: Describe and apply fundamental secure networking concepts to network configuration and design.
● Describe the role of network devices in security.
● Apply concepts of common security devices and technologies.
● Identify and describe fundamental network segmentation concepts.
● Identify and describe fundamental concepts of wireless security.

Objective 5: Apply best practice secure configuration to endpoint devices and conduct endpoint log analysis.
● Distinguish between subcategories of security within an organization's environment and identify common strategies used in endpoint security.
● Apply Windows native anti-malware and common commercial anti-malware tools to endpoint protection.
● Locate and analyze log alerts found on a Windows 10 computer system.
Objective 6: Apply identity and access management best practices, models, and protocols to secure identity and access configuration.
● Apply industry-recognized identity and access standards to an organization's Identity and Access Management (IAM) process.
● Apply Windows Active Directory (AD) best practices to secure access configuration and conduct an identity and access audit using Windows AD.
● Identify and apply lifecycle management best practices to user digital identities.
● Describe and apply the principles of zero trust to identity and access management secure configuration to networks and devices.
Objective 7: Identify and describe secure application development concepts, attacks, and countermeasures.
● Identify and describe secure application development concepts.
● Identify and describe application attacks along with associated countermeasures.
Objective 8: Apply common risk mitigation techniques, including data classification and vendor risk assessments.
● Apply common risk mitigation techniques to situations requiring cyber mitigation decisions.
● Conduct a cyber third-party risk assessment on a potential company vendor.
● Apply data classification labels to the correct type of data.
Objective 9: Apply vulnerability management best practices to scanning and patch management operations and conduct basic penetration testing techniques.
● Identify the role of vulnerability management within security operations and organizational risk management.
● Apply common industry vulnerability management principles to vulnerability management processes.
● Conduct basic penetration testing techniques.
Objective 10: Apply industry-recognized best practices to security governance, user awareness training and disaster recovery to security planning operations.
● Create a security awareness training program.
● Plan and conduct a disaster recovery and continuity tabletop exercise.
● Identify US Federal laws, privacy laws, and industry regulations and apply to cybersecurity concepts.
Objective 11: Demonstrate the use of tools and techniques common to the role of a cybersecurity analyst.
● Demonstrate the use of common command line tools.
● Use common tools for footprinting and enumeration.
● Capture and analyze network traffic.
● Analyze various types of log files.
Objective 12: Apply industry best practices to incident response operations, digital forensics, eDiscovery and threat intelligence analysis.

● Apply the incident response lifecycle to incident response procedures.
● Apply incident response best practices to events in cloud, mobile, and hybrid environments.
● Write an incident report following incident response operations.
● Apply digital forensics best practices to incident response operations.
● Conduct secure data acquisition in accordance with industry best practices.
● Apply cyber threat models to threat intelligence analysis.
Objective 13: Prepare for internal career growth in cybersecurity
● Identify internal career growth opportunities within your organization.
● Build a career path plan.
● Create personal branding assets and job application materials.
● Practice interviewing strategies.

Program Outline:

Course code	Course Title	Number of Lessons	Expected # weeks to complete
CS501-1	IT Security Professional	8	9
CS501-2	Security Analyst	12	12
CS501-3	Security Specialist	8	9
	Total Lessons	**28**	30

COURSE DESCRIPTIONS

CS501-1 IT Security Professional
This course introduces students to data and information and the components of modern IT systems, which they will be learning to protect and defend throughout this program. A significant portion of this course is dedicated to computer networking concepts and focuses on identifying proper function, placement, and configuration of networking devices and components within common network architectures. By the conclusion of this offering, students will be able to describe and demonstrate fundamental concepts of working with network addressing, ports, protocols, and services.

CS501-2 Security Analyst
In this course, students learn the core knowledge and skills necessary to begin a career in the role of a cybersecurity analyst. Students train to develop the core competencies needed to use information collected from a variety of sources to identify, analyze, and report events that occur within an enterprise to protect network and information systems from cyber threats. Students will develop communication, critical thinking, and problem-solving skills necessary to approach real world problems in cybersecurity.

CS501-3 Security Specialist
This course will dive deeper into concepts that have been introduced throughout the program and pair them with advanced tools, techniques, and strategies for analyzing data and conduct penetration testing operations. Students will strengthen knowledge and skills needed to use information collected from a variety of sources to identify, analyze, and report events that occur

to protect network and information systems from cyber threats. At the conclusion of this course, students will be able to plan and apply appropriate incident procedures to a given attack scenario, apply digital forensics techniques, and author post-incident reports with remediation recommendations for an organization.