Cybersecurity Certificate

Why Valley Forge Military College (VFMC) Cybersecurity Certificate?

Cybersecurity has emerged as one of the leading creators of jobs and opportunity for all economic sectors. Technology providers, policy makers, legal expertise, banking, insurance, devices, and educational programs are evolving to deal with Cybersecurity issues. VFMC offers students a four course Cybersecurity sequence that can be taken as electives within their existing selected programs since Cybersecurity crosses and impacts all disciplines of study. Students can take advantage of this opportunity to graduate with an Associate's degree in their desired major with an additional Cybersecurity Certificate credential on their transcript.

What will you learn?

VFMC Cybersecurity studies focuses on the eleven (11) knowledge units (KU) required by National Centers of Academic Excellence in Information Assurance/Cyber Defense for Two-Year Education (CAE2Y).

1. Basic Data Analysis: provide basic abilities to manipulate data into meaningful information
2. Basic Scripting: provide ability to create simple scripts that automate & perform simple operations
3. Cyber Defense: provide basic awareness of options to mitigate threats
4. Cyber Threats: provide basic information about cyber threats
5. Fundamental Security Design Principles: provide basic security design fundamentals
6. IA Fundamentals: provide basic IA concepts
7. Intro to Cryptography: provide basic ability to understand where & how cryptography is used
8. IT Systems Components: provide understanding of basic components in IT system & roles in system operation
9. Networking Concepts: provide basic understanding of network components & how they interact
10. Policy, Legal, Ethics & Compliance: provide rules & guidelines controlling IA
11. System Administration: provide skills to perform basic operations

Why is Cybersecurity a great potential career field?

The increasing number of news reports on the increasing numbers of identity thefts and other online security breaches requires a stronger Cybersecurity workforce. Statistics point to the demand for Cybersecurity professionals growing 3.5 times faster than the overall IT job market, and 12 times faster than the total labor market. This demand has lead the US federal government to create the National Cybersecurity Workforce Framework describing the vast landscape of Cybersecurity related jobs with common expectations of the required KSA.

Course Descriptions

Introduction to Computer Information Systems: This course is an introduction to computer information systems concepts, hardware, software applications, network communications, and security and privacy issues surrounding computers and information systems. This course focuses on Basic Data Analysis; Cyber Threats; Fundamental Security Design Principles for Usability; IA Fundamentals; Intro to Symmetric & Public Key Cryptography; IT Systems Components; and Policy, Legal, Ethics & Compliance KUs required in CAE2Y. The course is also centered on the use and integration of computer technology and software applications to improve human task completion efficiency.

The use of information systems and computer technologies to organize, coordinate, and inform human activities are the focus of this introductory course. Coverage includes an overview of current hardware and software technologies and issues, networks and communications, and information systems basics and trends. The objective of the course is to understand the process of digital information manipulation and to develop critical information management and computer technology skills necessary in an information age workplace and society. Social, cultural, and ethical aspects of security and privacy and related issues surrounding digital information and computer technology are discussed.

Data Management & Security: This course covers database terms & concepts, ethics & privacy, data security and security metadata, and organizational data management strategies. This course focuses on Intro to Cryptography; IA Fundamentals for Data Security at rest & in processing; Databases; Database Management Systems; Structured Query Language (SQL) Scripting; and Database System Administration KUs required in CAE2Y.

Major emphasis is placed on understanding the various data management functions needed by organizations and Basic Data Analysis providing basic abilities to manipulate data into meaningful information. Topics include types of data models and database management systems, data definition and manipulation, database system administration and management including database security covering availability, integrity & confidentiality. Data management fundamentals and technologies that support database security, error recovery, concurrency control, and distributed database systems are also studied. Students become prepared to recommend data management technologies and security solutions, and also analyze organizational data management needs.

Network Communications & Security: This course focuses on fundamental principles of computer and communication networking with a specific emphasis on network security. This course focuses on IA Fundamentals for Data Security in transit; Network & Security IT Systems Components; Networking Concepts; Basic Scripting; and System Administration KUs required in CAE2Y.

Fundamental network concepts and current networking technologies provides basic understanding of network components and how they interact, and enables students to understand communication protocol principles and usage in network design; understand network design issues addressing performance considerations and risk management in security cost- benefit tradeoff analysis. Students develop understanding on how the Internet works, how to securely integrate and manage distributed data services across networks, and how to design, specify, and justify secure networking solutions.

Information Systems Security: This course covers planning, development, and implementation of a comprehensive information security program in an organization covering authentication and access control, integrity and confidentiality of information, and risk management and business continuity planning. This course focuses on Cyber Threats; Fundamental Security Design Principles; Cyber Defense (CD); and Information Assurance (IA) KUs required in CAE2Y. These KUs provide information about cyber threats, basic security design fundamentals, IA concepts, and awareness of options to mitigate threats. Additional KUs addressed in this course provide focus on Security Policy Development & Compliance covering Cybersecurity Planning & Security Program Management; IA Architectures, Standards & Compliance; Life-Cycle Security; Security Risk Analysis; and Supply Chain Security.

Topics examine information systems security from program management and systems development perspectives by investigating security models and frameworks using National Institute of Standards and Technology (NIST) security publications and risk assessment framework to establish security processes, recommend organizational security policies and practices, and develop business continuity plans. The business continuity planning will be integrated in with college VFMC emergency response plans to test and recommend improvements to the business continuity plan developed in the course.