THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Doctor of Engineering in Cybersecurity Analytics (Online, DC4)

Introduction

The School of Engineering and Applied Science Online Programs offers the Doctor of Engineering (D.Eng.) degree in Cybersecurity Analytics. Classes are held on Saturdays, starting in Spring 2023 with a target graduation date of Fall 2024. Applicants should normally hold a master's degree in engineering, applied science, mathematics, computer science, information technology, or related field from an accredited institution.

The Doctor of Engineering in Cybersecurity Analytics

The D.Eng. in Cybersecurity Analytics addresses the widespread need for practitioners who can apply advanced knowledge from the program of study to address real-world cybersecurity challenges, whereas a PhD in cybersecurity contributes to fundamental research.

The D.Eng. in Cybersecurity Analytics empowers the student to plan and implement security measures to protect an organization's network and systems, implement strategies to track threats and monitor networks for security breaches, build secure and resilient computer systems with subject matter expertise in cybersecurity analytics, advanced tools and techniques for ensuring confidentiality, integrity, and availability of an organization's data and systems.

Curriculum

The curriculum comprises 45 credit hours of graduate level courses and a research phase during which the student writes and defends a praxis paper. The research phase requires a minimum of 15 credit hours.

Proposed Courses

CSCI 6015	Cyber Forensics (3 credits)
CSCI 6016	Applied Network Defense (3 credits)
ECE 6160	Secure Computer Architecture (3 credits)
SEAS 6800A	ST: Challenges in Cybersecurity (3 credits)
SEAS 6800B	ST: Cybersecurity Architectures (3 credits)
SEAS 6800C	ST: Python Applications in Cyber Analytics (3 credits)
SEAS 8410	Security Data Analysis & Visualization (3 credits)
SEAS 8414	Analytical Tools for Cyber Analytics (3 credits)
SEAS 8415	Applied Cryptography and Data Protection (3 credits)
SEAS 8499	Praxis Development for Cybersecurity (3 credits)
SEAS 8199	Praxis Research for Doctor of Engineering (15 credits)

Course work culminates in the praxis proposal, a research report that proposes a practice-based solution to a problem in cybersecurity of the student's own choosing—that could be used by cybersecurity practitioners.

Classroom Phase Schedule

Course sessions last 10 weeks. Classes meet Saturday mornings from 9:00 am-12:00 pm and afternoons from 1:00-4:00 pm (all times Eastern). This program is taught in an accelerated, cohort format in which students take all courses in lock step. Classes cannot be taken out of sequence, attendance at all class meetings is expected, and students must remain continuously enrolled; i.e., leaves of absence are permitted only in medical or family emergency, or in case of deployment to active military duty.

Session	#Courses	#Credit Hours	Session Dates
Spring-1 2023	2	6	January 7 — March 11, 2023
Spring-2 2023	2	6	March 18 — May 20, 2023
Summer 2023	2	6	June 3 — August 5, 2023
Fall-1 2023	2	6	August 12 – October 14, 2023
Fall-2 2023	2	6	October 21 — January 13, 2024

No classes on Memorial Day, Thanksgiving, Christmas, and New Year Weekends

Research Phase (Min. 15 Credit Hours)

In order to be successfully awarded the D.Eng. degree, students must earn a grade point average of at least 3.2 in the 10 classroom courses, and no grade below B-. Upon completion of the classroom phase, students are registered for a minimum of 15 credit hours (ch) of SEAS 8199 Praxis Research: 6 ch in Spring 2024, 3 ch in Summer 2024, and 6 ch in Fall 2024. Throughout the research phase, the student develops the praxis on an advisor-approved topic related to cybersecurity. Faculty research director(s) meet with students at least once per month, who are expected to attend each meeting.

Research Areas for Praxis

With the advisor's consent, the student may elect to focus on an area within the Cybersecurity field. Below, find sample areas of research:

- Addressing the Cybersecurity Malicious Insider threat
- Exploring Cybersecurity Requirements in the Defense Acquisition Process
- Internet of Things Device Cybersecurity
- Cybersecurity of Networked Home Medical Devices
- Cybersecurity Challenges in Healthcare Industries

Cost

All classes meet live online through synchronous distance learning technologies. Classes are recorded for future viewing. Tuition is billed at $1625 per credit hour for the 2022-2023 year. A non-refundable tuition deposit of $995, which is applied to tuition in the first semester, is required when the student accepts admission.

Course Descriptions

See also http://bulletin.gwu.edu/courses

CSCI 6015 Cyber Forensics. Acquiring, preserving and analyzing digitally stored information while ensuring that this information is admissible as evidence in a court of law. Principles and techniques for cyber forensics investigations using industry-standard forensic process.

CSCI 6016 Applied Network Defense. Computer security: protection aspects of the Internet. Cryptographic tools to provide security, such as shared key encryption (DES, 3DES, RC and more), public key encryption, key exchange, and digital signature. Internet protocols and applications.

ECE 6160 Secure Computer Architecture. Building blocks of secure hardware and systems: trusted execution environment, security engines; side and covert channels in computing systems; hardware trojans; physically unclonable functions and challenges; obfuscation strategies.

SEAS 6800A ST: Challenges in Cybersecurity. Introduction to most common types of attacks, e.g., ransomware attacks, IoT attacks, cloud attacks, phishing attacks, blockchain and cryptocurrency attacks, software vulnerabilities, BYOD policies, and insider attacks, as well as analytical techniques of their mitigation.

SEAS 6800B ST: Cybersecurity Architectures. Introduction to traditional network-centric cybersecurity (i.e., Defense in Depth) and emerging cybersecurity architecture models including DevSecOps, Cloud-native, and risk adaptive (Zero Trust Architecture) structures. Discussion of the benefits and challenges of these models, alignment with MITRE frameworks, and how they support the business/mission outcomes of an organization.

SEAS 6800C ST: Python Applications in Cyber Analytics. Introduction to programming with Python; Developing python scripts to automate data cleaning; Introduction to machine learning with Python including text mining and time series analysis; Performing cyber security tasks such as anomaly detection, DoS attack detection, and spam detection using Python.

SEAS 8410. Security Data Analysis & Visualization. Visualization aspect of security data, including study of data analytics and scaling up information security, security metrics and security monitoring techniques focusing on industry applications. Tools for security data visualization and analytics.

SEAS 8414 Analytical Tools for Cyber Analytics. This course is designed to provide students with the basic foundations for application of deterministic, probabilistic, and statistical models to address problems in cyber analytics.

SEAS 8415 Applied Cryptography and Data Protection: Introduction to cryptographic techniques, case studies for real-life applications of modern cryptographic solutions, classical cryptographical algorithms (AES, RSA, RC4) and techniques (symmetric, asymmetric-public key cryptography, hash functions), digital signatures, key management and distribution. Advanced topics such as zero-knowledge proofs and zero-trust architectures.

SEAS 8499 Praxis Development for Cybersecurity. Overview of research methods. Aims and purpose of the praxis. Development of praxis research strategies, formulation and defense of a praxis proposal. Praxis proposal defense must be passed before the student is admitted to degree candidacy to undertake praxis work. Restricted to students who have completed all required coursework for the D.Eng. in the field of Cybersecurity Analytics.

SEAS 8199 Praxis Research for Doctor of Engineering. Independent applied research in cybersecurity culminating in the final praxis report and final examination for the degree of Doctor of Engineering. May be repeated for credit. Restricted to students in the D.Eng. in the field of Cybersecurity Analytics.

The University reserves the right to adjust course offerings, schedules, and tuition rates.