THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

DOCTOR OF ENGINEERING IN CYBERSECURITY ANALYTICS ONLINE

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 Fall 2023 with a target graduation date of Summer 2025. 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 24 credit hours of graduate level courses and a minimum of 24 credit hours of research during which the student writes and defends a praxis paper.

Proposed Program

CSCI 6015	Cyber Forensics (3 credits)
CSCI 6016	Applied Network Defense (3 credits)
SEAS 8400	Challenges in Cybersecurity (3 credits)
SEAS 8405	Cybersecurity Architectures (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 8188	Praxis Research for DEng in Cyber Analytics (24 credits minimum)

Classroom Phase Schedule

Classroom courses last 10 weeks each and 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. Courses 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 the case of medical or family emergency, or deployment to active military duty.

Session	#Courses	#Credit Hours	Session Dates
Fall-1 2023	2	6	August 12 — October 14, 2023
Fall-2 2023	2	6	October 28 — January 20, 2024
Spring-1 2024	2	6	February 3 — April 6, 2024
Spring-2 2024	2	6	April 20 – June 29, 2024

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

Research Phase Schedule (Min. 24 Credit Hours)

In order to proceed to the research phase, students must earn a grade point average of at least 3.2 in the 8 classroom courses, and no grade below B-. Upon successful completion of the classroom phase, students are registered for a minimum of 24 credit hours (ch) of SEAS 8188 Praxis Research: 3 ch in Summer 2024, 9 ch in Fall 2024, 9 ch in Spring 2025, and 3 ch Summer 2025. Throughout the research phase, the student develops the praxis under the guidance of a designated faculty advisor. Faculty research advisors meet individually with students every two weeks.

Selected Research Areas for Praxis

With the advisor's consent, the student focuses their research on an area within the Cybersecurity field. Some sample areas include:

- 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

Tuition

All classes meet live online through synchronous distance learning technologies. Classes are recorded for future viewing. Tuition is $1625 per credit hour for the 2023-2024 year and is billed at the beginning of each semester for the courses registered during that semester. A non-refundable tuition deposit of $995, which is applied to tuition due the first semester, is required when the applicant 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.

SEAS 8400 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 8405 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 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. Survey of analytical tools for analyzing cyber security data with particular attention to the use of data analytics procedures in supporting appropriate cyber security policy decisions

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 8188 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.