Villanova University’s cybersecurity graduate courses are taught in the evening (2 ½ hours once a week), onsite at the Navy Yard in Philadelphia making them convenient and accessible. When traveling for work, students can access class recordings and materials from anywhere, available 24/7. Students also have the option to stream classes live, depending on their schedules.

GRADUATE CERTIFICATE COURSE OUTLINE – You’re only five courses away from earning a graduate certificate in cybersecurity!

Fall 2016 | ECE 8484 – Cybersecurity Threats and Defense

Course description: Malware and cyber threats: computer network defense; software for Data Protection and Privacy, Security Information and Event Management (SIEM), Governance, Risk and Compliance (GRC); trusted computer systems and secure applications; identity and access management including biometrics; next generation security concepts.

Spring 2017 | ECE 8476 – Cryptography & Network Security

Course description: Theory and practice of computer communications security, including cryptography, authentication, and secure electronic mail. Topics include secret and public key cryptography; message digests; password-based, address-based, and cryptographic authentication; privacy and authentication in email; PEM, PGP, and S/MIME. Use of various algorithms.

Summer 2017 | ECE 8485 – Critical Infrastructure Control Systems Security

Course description: Security risks of critical infrastructure systems such as electrical, pipelines, water, and transportation. Design and setup of Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controller (PLC) systems. Security challenges and defense-in-depth methodology. Hands-on lab experiments.

Fall 2017 | ECE 8486 – Ethical Hacking

Course description: Quantifying security in an unambiguous way using the Trusted System Evaluation Criteria. "Hacking" a system, developing and implementing countermeasures and threat removal, techniques for Access control, confidentiality, etc. Secure the network, web, enterprise and database, the Cloud and the Semantic Web.

Spring 2018 | ECE 8498 – Designing and Securing Cyber-Physical Systems

Course description: Today's modern Industrial Control Systems including those supporting the nation's critical infrastructure blend information and control technology. They are examples from the wider landscape of Cyber-Physical Systems (CPS) that include consumer technologies, which are bringing the world to a deeply connected Internet of Things and People. Examples include home automation and protection, connected vehicles, connected medical devices, drones, and Smart Buildings and Cities. Secure engineering practices in these examples are often not applied with sufficient rigor. This course will cover the spectrum of application areas where secure engineering can lead to a safer and more secure connected environment that also respects the privacy of people connected to and with these systems. It will also consider how security can be improved once systems are deployed and operational. Strategies for risk mitigation and the adoption of emerging standards such as the NIST Draft Framework for Cyber-Physical Systems will be considered throughout the course. Prerequisites: ECE 8485*

*Note: This is the only prerequisite in the Graduate Certificate Cyber-Physical & Control Systems Security (C2S2) program, and is scheduled to be offered in the summer of 2017.

Villanova University’s graduate certificate programs are often used as a pathway to a graduate degree program. Credit earned in this certificate can be counted toward the master's degree in cybersecurity.