NORWICH
UNIVERSITY
Online

Cyber Security and Information Assurance

Continuing Education Courses
Professional Development Courses

online.norwich.edu

NORWICH UNIVERSITY™ *Online*

Course Listing

Norwich University's College of Graduate and Continuing Studies offers the following continuing education courses online in the field of cyber security. Some courses are academic in nature, some are technical, and some are a combination of both. The online training courses include the following:

Professional Development

Conducted in virtual labs to provide hands-on learning, these courses run on an 8-week schedule. Specific tools used in the course include: BackTrack, Nmap, Wireshark, Metasploit, Vistumbler, BurpSuite, Nessus, Cain and Abel, Nikto, Aircrack-ng Suite, John the Ripper, SET (Social Engineer Toolkit). No academic credit is conferred, but Norwich will award Continuing Education Units (CEU) for each course. Registration is open to individuals and groups.

Penetration Testing I

- Intelligence Gathering and Vulnerability Scanning
- Network Vulnerabilities and Analysis
- Windows Vulnerabilities
- Linux Vulnerabilities
- Exploitation
- The Meterpreter
- Client-side Exploits

Penetration Testing II

- Defeating Cryptography
- Social Engineering
- Wireless Attacks
- Web Application Attacks
- Application of Tools
- Pen Test Simulation I
- Pen Test Simulation II

Certificates

Computer Forensic Investigation/
Incident Response Team Management
Computer Security Incident Response Team Management (6 credits)
Computer Forensic Investigation (6 credits)

Vulnerability Management (hands-on learning in a virtual lab)
Vulnerability Management I (6 credits)
Vulnerability Management II (6 credits)

Critical Infrastructure Protection & Cyber Crime
Cyber Crime (6 credits)
Critical Infrastructure Protection (6 credits)

Cyber Law & International Perspectives on Cyberspace
Cyber Law (6 credits)
International Perspectives on Cyberspace (6 credits)

For more information about Norwich's online continuing education courses, call 866.684.7237 or email continuingstudies@norwich.edu

NORWICH UNIVERSITY Online

Certificates
Course Descriptions

Computer Forensic Investigation/Incident Response Team Management

Computer Security Incident Response Team Management (6 credits)
In this course, you will analyze and apply the key points in creating and managing a computer security incident response team (CSIRT), also known as a computer incident response team (CIRT) or a computer emergency response team (CERT). Topics include establishing CSIRTs; responding to computer emergencies; securing the CSIRT; managing the CSIRT with respect to professionalism, setting priorities for triage, and protecting personnel against burnout; and learning from emergencies using the incident postmortem and establishing continuous process improvement within the organization. Students will use their case study to apply their knowledge to real-world situations and will prepare recommendations for the establishment of a new CSIRT or improvement of their existing CSIRT.

Computer Forensic Investigation (6 credits)
This course focuses on the spectrum of tools and techniques used to investigate digital incidents, whether in a civil or criminal environment. The course provides the broad understanding that information assurance professionals must have of the management, investigation, and analysis of digital incidents. It also places that understanding in the context of other information assurance domains. Discussions of digital investigation and forensics cover topics from both technical and management perspectives to increase the information assurance professional's understanding and application of domain-specific knowledge.

Vulnerability Management

Vulnerability Management I (6 credits)
Vulnerability Management I is the first course in a series of two that explores network penetration testing. This course introduces students to penetration testing of computer networks. Students will utilize a virtual lab system and gain hands-on experience through lab exercises. Students will learn to use the well-known open-source Metasploit computer security project to understand security vulnerabilities and how to use this tool for penetration testing, testing the control tools and how to conduct monitoring of an enterprise. In the course students will be introduced to system security and vulnerability analysis, the most common system exploits and vulnerabilities, system "pivoting" and client-side exploits. This course is designed for penetration testers' system security and network administrators.

Vulnerability Management II (6 credits)
Vulnerability Management II is the second course in a series of two that explores network penetration testing and vulnerability management. This course introduces students to advanced open-source tools used to conduct penetration testing of computer networks. Students will learn the rules of engagement and how to conduct legal and ethical security tests and vulnerability assessments. Students will utilize a virtual lab to gain experience through hands-on lab exercises. Students will learn to use well-known open-source tools (Metasaploit, John the Ripper, Wireshark) to understand security vulnerabilities and how to use these tools for penetration testing, testing the control tools and how to conduct monitoring of an enterprise. In the course students will be introduced to system security and vulnerability analysis, the most common system exploits and vulnerabilities, system "pivoting" and client-side exploits.

1819
NORWICH
UNIVERSITY
Online

Certificates
Course Descriptions

Critical Infrastructure Protection & Cyber Crime

Cyber Crime (6 credits)
This course explores the nature of conflict in cyber space while focusing on two major internet-based threats to the U.S. national security: cyber terrorism and cyber crime. The course addresses who is undertaking these cyber activities, what techniques they use, and what countermeasures can be adopted to mitigate their impact. It provides a risk management framework to help information leaders leverage the benefits of internet technologies while minimizing the risks that such technologies pose to their organizations.

Critical Infrastructure Protection (6 credits)
This course examines the security of information in computer and communications networks within infrastructure sectors critical to national security. These include the sectors of banking, securities and commodities markets, industrial supply chain, electrical/smart grid, energy, transportation, communications, water supply and health. Special attention is paid to the risk management of information in critical infrastructure environments through an analysis and synthesis of assets, threats, vulnerabilities, impacts, and countermeasures. Critical consideration is paid to the role of Supervisory Control and Data Acquisition (SCADA) systems in the flow of resources such as electric, water, and fuel.

Cyber Law & International Perspectives on Cyberspace

Cyber Law (6 credits)
This course explores a broad variety of federal statutory, common, and international laws that may impact the information technology professional. Because the overwhelming majority of cyber infrastructure is owned and operated by the private sector, the course focus is on those laws that affect the interaction between government and the private sector information technology industry, including the privacy rights so often implicated in modern data storage systems. The course starts with a look at "cyber law" and whether it is really a distinct legal discipline at all. It then moves into criminal, civil, regulatory, international and common laws with which today's information technology professional may come in contact. Throughout the course we discuss how public policy and other factors impact the development, implementation, and interpretation of the law. Students read, interpret and apply legal authorities and theories, a valuable skill for future information technology leaders if they are to stay in compliance with the ever-growing "cyber" legal framework.

International Perspectives on Cyberspace (6 credits)
This course provides an overview of the issues surrounding transnational cyberspace policies, international investment strategies, and implementation of communication and information technologies that affect the global economy and transforms the flow of information across cultural and geographic boundaries. The course will examine various global governance frameworks, and organizations that shape and transform cyberspace such as the International Telecommunications Union, the World Bank Information and Communications Technology Sector and the U.S. Federal Communications Commission.

1819
NORWICH
UNIVERSITY™
Online

Online Learning

Online Learning at Norwich

Norwich University has built an online learning environment that facilitates individual engagement, deep learning, networking, peer support, and one-on-one contact with faculty and student support staff. The online learning platform offers 24/7 access and support, enabling students to engage with program content and contribute to class discussions at any time from any location each week.

Our curricula incorporate coursework specifically designed to help students succeed in the online learning environment. Classrooms are highly interactive and are linked to extensive online learning resources.

A cyber education at Norwich provides students with the competencies needed to build and defend both private and national cyber-based systems. As one of the early institutions to be recognized by the National Security Agency and Department of Homeland Security as a Center for Academic Excellence in Information Assurance Education, the curricula are continually evolving to keep pace with the current cyber environment and best practices.

Blending Theory and Practice

Our rigorous academics explore the technical theories and methods behind cyber security, best practices in information assurance technology, organizational structure and policy development, the regulatory environment, and management strategies. Key skills fostered throughout the programs include written communications, critical analysis, problem solving, project management, and leadership.

Superb Teacher-Practitioners

Our faculty members have broad industry and research experience that informs and enriches their teaching, providing students with real-world insight and a context for applying their expanded skills and knowledge.

The Norwich Advantage

✓ Flexible online platform allows students to complete classwork around their busy schedules.

✓ High degree of interaction with Norwich faculty and classmates in small online classrooms.

✓ Application of critical thinking, ethical decision-making and leadership throughout the curriculum.

Faculty work closely with students and inspire them to produce their best work, motivate them to reach higher and further than they thought possible, and encourage them to make a difference. The faculty's mission is to teach and mentor the next generation of cyber security leaders.

About Norwich University

Founded in 1819, Norwich University is a small, private, not-for-profit university that offers professional and liberal arts programs. Campus is located in the rural town of Northfield, Vermont and provides education to both military and traditional students. As part of Norwich University, the College of Graduate and Continuing Studies delivers online programs in a rigorous academic environment by building on the nearly 200 years of university tradition. When you enroll in our online programs, you will become a part of Norwich's legacy, which harks back to our founding as the nation's first private military college.

Accreditations/Accolades

Norwich University is regionally accredited by the New England Association of Schools and Colleges, Inc., through its Commission on Institutions of Higher Education.

Norwich University's online bachelor's degree programs are recognized as some of the best in the country by U.S. News & World Report.

Norwich University is recognized as a military friendly school as determined by the Military Friendly Schools Academic Advisory Board Committee Members.

The National Security Agency and Department of Homeland Security have designated Norwich as a Center for Academic Excellence in Cyber Defense.

For more information about Norwich's online continuing education courses, call 866.684.7237 or email continuingstudies@norwich.edu