BOOT CAMPS
ALLEGRO

Presents

Cybersecurity Foundations Bootcamp

Hybrid Format: asynchronous online learning with bi-weekly face-to-face labs

Certificate Awarded by the National CyberWatch Center

10 Week Blended Program

Labs in Philadelphia

In association with:

NATIONAL
CYBERWATCH
CENTER

Introduction

Considering a move to the cybersecurity field? According to a recent Cybersecurity Ventures prediction, "there will be 3.5 million unfilled cybersecurity positions by 2021." Cybersecurity hiring is growing due to a dramatic rise in cybercrime, new government regulation, and privacy concerns. The Allegro Cybersecurity Bootcamp is an effective way to jumpstart a move to the cybersecurity field.

Forecasts for cybersecurity growth have failed to keep pace with the dramatic rise in cybercrime and privacy concerns.
Jobs which require cybersecurity knowledge take longer to fill. The Cyberseek consortium notes that "Jobs requesting public cloud security skills...remain open 79 days on average – longer than almost any other IT skill."

Program Goals

- To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.

- To develop graduates that can plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.

- To develop graduates that can identify, analyze, and remediate computer security breaches.

Program Coverage

Week 1:

Introduction to Information Security, Information Security Trends, Career Exploration, and Professional Certifications

- Current and evolving threat landscape
- Fundamental security concepts (e.g., Confidentiality, Integrity, Availability)

Week 2:

Threats and Vulnerabilities

- Social Engineering (SE)
- Malicious Software (Malware)
- Denial of Service (DoS)/ Distributed DoS
- Software exploitation

Week 3:

Governance, Risk Management, and Compliance (GRC):

- Risk assessment/analysis
- Business Continuity Planning
- Privacy
- Legal (e.g., Criminal/Civil/Admin law)

Week 4:

Identity and Access Management

- Identification
- Authentication
- Authorization
- Accountability

Week 5:

Physical Security

- Secure facility planning
- Physical security access controls

Week 6:

Security Engineering

- Disaster Recovery (DR) planning/implementation
- Secure network design
- Secure application development

Week 7:

Fundamentals of Cryptography

- Classic cryptographic techniques
- Symmetric
- Asymmetric
- Hashing

Week 8:

Public Key Infrastructure (PKI)

- Key Management
- Digital Certificates
- Certificate Authorities (CAs)

Week 9:

Security Testing

- Tests
- Assessments
- Audits

Week 10:

Security Operations

- Categories of computer crime
- Detection
- Incident Management/Response

Blended/Hybrid Format

Rather than passively receiving and reiterating information, you can take an active role in your education and contribute to your own learning. You can work with the faculty members to set learning goals for yourself, and can work toward them through blended learning by combining face-to-face interaction with your faculty through an asynchronous online learning with bi-weekly face-to-face labs.

Program Learning Outcomes

- Analyze and evaluate the cybersecurity needs of an organization.
- Conduct a cybersecurity risk assessment.
- Measure the performance and troubleshoot cybersecurity systems.
- Implement cybersecurity solutions.
- Be able to use cybersecurity, information assurance, and cyber/computer forensics software/tools.
- Identify the key cybersecurity vendors in the marketplace.
- Design and develop a security architecture for an organization.
- Design operational and strategic cybersecurity strategies and policies.

How do you join?

There are limited seats for this batch and selection is based on review of your application and a telephone interview.

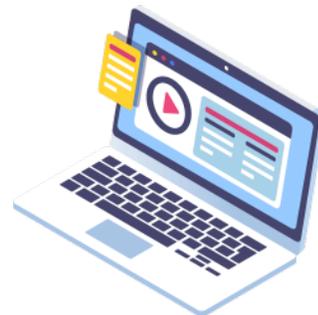| Apply | Wait for Selection | Pay Semester Fee | Register for Courses | Batch Start |

Attend an Information Session

Register to attend an upcoming information session
Contact a Program Counselor @ 717-540-9730 for more information.

About the Faculty

Casey W. O'Brien is the Executive Director and Principal Investigator of the National CyberWatch Center, a cybersecurity education and research consortium focused on advancing cybersecurity education and strengthening the national cybersecurity workforce. Casey has more than 20 years of industry experience in information security and large-scale IT implementation and project management in challenging and cutting-edge environments.

About Allegro

Allegro Learning Solutions partners with educational institutions, subject matter experts, and content providers to re-energize existing educational materials and create new learning experiences that expand educational opportunities for an anytime, anywhere global audience. http://allegrolearnings.com/

About National Cyberwatch Center

Accredited by the Middle States Commission on Higher Education, Harrisburg University is known for their outstanding science and technology-focused degree programs. The institution fosters a diverse community of learners, provides access and support to students who want to pursue a career in science and technology and supports business creation and economic development. http://harrisburgu.edu/