UNSW CANBERRA | Cyber

Critical Infrastructure and Control System Security

Location	UNSW Canberra
Duration	5 days
Standard Price	$4,550.00
Defence Price	$4,095.00

Description

This is a technical course, designed to use simulation tools and equipment to replicate the potential threats against Critical Infrastructure Services (CIS) utilising real life SCADA models. The course provides hands on experience with the complexity of modern information technology equipment and the components in control systems and legacy systems, the threat environment and attackers' capabilities as well as techniques for securing these systems.

Topics covered include:

- IT architectures
- Control System architectures
- Security vulnerabilities
- Mitigation strategies
- Nature of attacks
- Defence of SCADA and Industrial Control Systems

*Note: Students should have a basic understanding of Cyber Security gained in the workplace or through the UNSW Canberra Cyber Security Bootcamp or SANS401 or similar. A knowledge of basic networking principles such as OSI/ Internet stack and TCP/IP will also be helpful.

Learning Outcomes

On completion of this course, participants should be able to:

- Understand and evaluate the vulnerabilities of Critical Infrastructure.
- Understand the principles behind the industrial hardware and software of control systems that are used in the operation of Critical Infrastructure.
- Examine technical specifics about the vulnerabilities of critical infrastructure service delivery with an emphasis of those services dependant on control systems reliability and recoverability.
- Develop and implement comprehensive mitigation strategies as well as effective administrative and technical risk management plans to protect and secure process control systems.

Who Should Attend

This course is useful for IT and Engineering graduates in the Cyber Security profession managing or securing Industrial Control Systems or those in intermediate Security roles within Defence and the utility security managing SCADA and other Industrial Control Systems on all types of platforms.

NICE Framework mapping

This course maps to the highlighted work categories:

- Securely Provision
- Oversee & Govern
- Analyse
- Investigate
- Operate & Maintain
- Protect & Defend
- Collect & Operate

To find out more about the NICE Framework go to: niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

Course Day Breakdown

Day 1

Critical Infrastructure (CI)

Day 1 begins with a comprehensive overview of critical infrastructure sectors. Students will gain an understanding of the current threat landscape and will be provided with real world examples of cyber attacks to study and analyse.

Topics

CI in the Economy, Phishing, SQL Injection, Cross-Site Scripting, Malware Attacks, DoS, DDoS.

Day 2

Control Systems

This session will cover the history of control systems, where are they found and how they work. We'll also look at the hardware used in these systems and give an overview of the types of common configurations.

Topics

Control system implementations, Industrialised hardware, Open-loop Control, Closed-loop Control.

Day 3

Components of an Industrial Control System (ICS)

Day 3 starts with an overview of ICS Hardware. We'll look at Unintelligent Field Devices, Intelligence Electronic Devices and Distributed Control Systems. Students will become familiar with the roles and limitations of various components.

Topics

Limit Switches, Sensors, Robotics, Programmable Logic Controller (PLC), Supervisory Control and Data Acquisition (SCADA), IP Addresses, Binary Coded Decimal, Pulse Width Modulation.

Day 4

Cyber Security Fundamentals

This session will provide an overview of cyber threats and attacks. The various stages of cyber attacks will be covered, along with common ICS security vulnerabilities. Students will gain an understanding of cyber security in an Industrial Control System setting.

Topics

Threat Actors and Agents, Threat targets, Attack Vectors, Asymmetric Warfare, Cyber Resiliency.

Day 5

Protection of CI and ICS Forensics

Day 5 consists of a Red team vs. Blue team exercise utilising actual industrial control equipment and the cyber range. Students will gain experience attacking and defending physical real-world type infrastructure scale models that includes traffic management, water supply and electrical supply systems.

Topics

Red teaming, Blue teaming, Cyber physical systems, Cyber offence, Cyber defence, SCADA.

"The facilities, instructional quality and content were all excellent."

Course participant

UNSW Canberra Cyber

UNSW Canberra Cyber is a unique, cutting-edge, interdisciplinary research and teaching centre, working to develop the next generation of cyber security experts and leaders. The centre is based in Canberra at the Australian Defence Force Academy and provides professional, undergraduate and post graduate education in cyber security. Our air-gapped, state of the art cyber range offers a secure environment where we deliver a number of technical and highly specialised learning opportunities. Our courses are designed to give the next generation of cyber security professionals the skill sets needed to thrive in the industry. We can also create bespoke professional education programs tailored to your organisation's needs. Contact us at cyber@adfa.edu.au to discuss how.

Find out more

cyber@adfa.edu.au

unsw.adfa.edu.au/cyber