UNSW CANBERRA | Cyber

Cyber Defence

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

Description

This course provides in-depth understanding of the techniques and policy used in computer and network defence. Cyber defenders learn the strategy and technical skills to protect and harden cyber systems, collect appropriate information through logging, detect attempted attacks, and respond to intrusions. Numerous cyber defence technologies and their effectiveness are discussed within this framework. This course will increase the competency of participants in building cyber resilience within an organisation.

Topics covered include:

- Threat modelling
- Network and host-based intrusion detection
- Identifying malicious network and host-based activity
- Linking malicious indicators of compromise to build an intelligence picture
- Classifying intrusion, intent and damage
- NSO theory, methodology and frameworks
- Defensive techniques

Learning Outcomes

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

- Conduct threat modelling.
- Deploy network and host - based intrusion detection systems to identify malicious actors.
- Link malicious indicators of compromise to build an intelligence picture.
- Apply Network Security Operations (NSO) theory, methodology and frameworks to innovate defensive techniques.
- Provide advice and briefings on threats to both technical and non - technical audiences.

Who Should Attend

This course is well suited to experienced IT professionals who wish to further specialise in offensive and defensive tactical cyber operations.

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

Networking and Threat Modelling

Day 1 kicks off with a comprehensive introduction to Cyber Defence, The Information Environment and Network Centric Operations. Students will be introduced to ways of affecting the information environment, approaches to threat modelling, and will be stepped through examples of network attacks.

Topics

Situational awareness, Network Collection Value-Chain, Self-Synchronisation, Hardening, Obfuscation, Threat-Detected Protection, Anomaly Detection, Network Attacks.

Day 2

Protection

This session presents the concept of using protection techniques to proactively prevent or minimise the effect of a compromise or breach. Techniques covered include methods listed in the ASD Essential 8, architectural security design and vulnerability scanning.

Topics

User Application Hardening, Host-Based Hardening, Minimising Attack Surfaces, Linux Firewalls, Network Segmentation, Demilitarised Zones, LUN Masking, Encryption.

Day 3

Collection and Detection

Students will be introduced to collection methods such as the deployment and configuration of sensors, sensor data processing and aggregation for analysis. The session will also cover detection strategies, network and host based intrusion detection and honeypots.

Topics

Network Sensors, Fusion, IOCs and Signatures, Anomaly Detection, Security Onion Architecture, Open Threat Exchange, Honeypots.

Day 4 & Day 5

Incident Response

Day 4 & 5 will give an overview of orientation and investigation techniques. Students will understand how to make sense of observed information to assess the situation, identify indicators of compromise and the extent of threat activity. We will also cover how such indicators initiates incident response plans and look at writing, editing and proper formatting of intelligence reports.

Topics

Orientation, Investigation, Instigation, Association, Incident Response Planning, Intelligence Reporting.

"The course was very good. The practical aspects and real-world scenarios were very helpful."

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