AUSCERT

INTERMEDIATE CYBER SECURITY FOR IT PROFESSIONALS

We rely on the Internet for daily business operations and government service delivery. However, today's threat environment is very different from how it was when many key Internet protocols were designed, resulting in inherent vulnerabilities that require mitigation.

This course is designed to provide participants with awareness of the security issues with a range of Internet oriented technologies and protocols and practical guidance for how participants can secure them.

OUTCOMES

- Enhanced understanding of the security threats and vulnerabilities in key Internet-oriented technologies and mitigation measures
- Understanding of important cyber oriented technologies that would contribute to a cyber security uplift program

DETAILS

Available exclusively to AUSCERT Member organisations.

Delivery Mode

- **Online**: Courses are delivered online via Microsoft Teams , split into two half-day sessions. Participants must attend both sessions to complete the course content.
- **In-person:** On occasion courses may also be conducted face-to-face.

Price

- **Online:** $900 (inc. GST) per person, per training course.
- **In-person:** $1250 (inc. GST) per person, per training course.

REGISTER

Visit our Training page & follow the links: auscert.org.au/training

For any other enquiries please contact: training@auscert.org.au

REQUIRED

Basic knowledge of IT, networking and cyber security knowledge including threats, vulnerabilities and risks.

Having completed AUSCERT's Introduction to Cyber Security for IT Professionals is excellent preparation.

APPROACH

- We describe and discuss how key technologies are abused and bypassed by attackers
- We introduce attendees to the technical and procedural approaches that they can use to thwart attempts to bypass security controls and exploit inherent vulnerabilities
- Incorporating group discussions and interactive learning opportunities
- Reference to and discussion of real-world incidents

CURRICULUM OUTLINE

The curriculum covers key technologies, their inherent weaknesses and the currently available solutions:

- Phishing and Business Email Compromise attacks and the associated email security controls to address them: DKIM, SPF and DMARC
- Domain hijacking, fake web sites, email interception attacks all rely on DNS to be successful. We cover aspects of DNS security that provide important controls to address these threats
- Remote access vulnerabilities and robust configuration choices for Virtual Private Networks (VPNs), including TLS and IPSec security
- TLS security for web sites
- Cryptographic algorithms and protocols – robust options and avoiding weaknesses
- Unix and Linux security – basics of secure system administration
- Introduction to SAN security
- Cloud assurance and due diligence
- BGP hijacking, similar threats, and associated preventative controls