WM9PE-15 Cyber Incident Management

24/25

Department
WMG
Level
Taught Postgraduate Level
Module leader
Paul Stephens
Credit value
15
Module duration
4 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

A cyber security incident can have a significant impact on the operational efficiency of a business. There are essential mechanisms and skillset that can be utilised to allow a potential attack against infrastructure to be effectively identified, managed and mitigated in a timely manner.
This module aspires to equip students with these skills and consists of two main parts. First, it explores the principles of responding to a cyber security incident and the incident response lifecycle. Second, it focuses on familiarising the students with the scientific techniques utilised for the technical analysis of the systems involved in a cyber security incident.

Module aims

This module aims to provide the students with a detailed understanding of the principles of managing a cyber security incident and allow them to apply advanced technical concepts and practices in cyber investigations.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

The module follows the incident response lifecycle:

- Preparation for responding to a cyber security incident and forensic readiness
- Understanding a threat - threat hunting
- Identification of a cyber security incident - detection methods, first response and management
- Intrusion analysis, monitoring and logging
- Digital forensics process in incident response - collection and preservation
- Investigation techniques
- Host forensics
- Network collection and analysis - log analysis
- Malware handling
- Cyber security incident remediation

This is an indicative module outline and actual sessions held may differ.

Learning outcomes

By the end of the module, students should be able to:

- comprehensively identify the different phases comprising the incident response lifecycle
- critically evaluate the principles of cyber incident management across diverse scenarios
- demonstrate the ability to analyse an individual approach of responding to a cyber security incident with the application of relevant techniques
- evaluate and provide sound reasoning for suitable responses to identified cyber security incidents

Indicative reading list

- Joseph Muniz, Aamir Lakhani, Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer, Cisco Press, 2018
- Luttgens, Jason T., Pepe, Matthew and Mandia, Kevin, Incident Response & Computer Forensics, 3 Ed, McGraw-Hill, 2014
- Sachowski, Jason, Implementing Digital Forensic Readiness: From Reactive to Proactive Process, 2 Ed, Syngress, 2019
- Gogolin Greg, Digital forensics explained, 2 Ed, CRC Press, 2021

Research element

- Current themes in cyber incident management research.
- Current and future trends on techniques related to cyber incident response.

Interdisciplinary

There is some interdisciplinary element relevant to the nature of the digital forensics part of the module. It involves relevant law elements.

Subject specific skills

Incident response lifecycle and practices, investigation principles, evaluation of a cyber security incident, host based analysis, network based analysis

Transferable skills

Problem solving, critical thinking, decision making, communication, technical literacy

---

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Seminars	5 sessions of 1 hour (3%)
Supervised practical classes	15 sessions of 1 hour (10%)
Private study	60 hours (40%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Studying textbooks, lecture notes and other resources provided. It may also involve preparation tasks before a seminar and coursework preparation.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time	Eligible for self-certification
Managing a cyber security incident	100%	60 hours	Yes (extension)

The portfolio may consist of multiple small pieces of work. It may include a proposal of an incident response plan, a small practical task, an in-class assessment and a short report outlining the findings or a short research paper.

This assignment requires approximately 50% practical and technical input. The word count has been reduced from the 100%x15CAT=4,000 words to 3000 to compensate the practical work required to complete the assessment.

Assessment group R

	Weighting	Study time	Eligible for self-certification
Reflection on the portfolio	100%		Yes (extension)

An individual critical evaluation and reflection on the portfolio submission.

Feedback on assessment

Summative feedback will be provided on the assignment.
Verbal feedback will be offered during practical sessions.

Availability

There is currently no information about the courses for which this module is core or optional.