WM3A6-24 Cyber Security Incident Management

24/25

Department
WMG
Level
Undergraduate Level 3
Module leader
Olga Angelopoulou
Credit value
24
Module duration
30 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

This module comprises two related but distinct themes: cyber incident response and digital forensics. The cyber incident response theme concentrates on enabling an organisation to support its critical services in the face of a cyber incident. That incident might be something with strong indicators that something is wrong such as a DDOS attack, or it might be something less obvious such as the discovery of a possible data breach from many months ago.
The incident response lifecycle is covered from preparation, through monitoring, detection, containment, eradication, restoration and post incident review.

The digital forensics part of the module is concerned with doing science well. It is about drawing the correct inference from the digital data which pervades modern society.
There are a number of challenges with drawing inference from modern digital data: it is fragile, its quantity may be overwhelming, it may be transient or volatile, it may not be legally accessible, it may not be technically accessible, its structure may be unclear.
Drawing inference from the data is complicated; attributing inference back to an individual or organisation is especially vexed.
Set against these significant challenges is the reality that the digital footprint left by a member of modern society may have been left as a consequence of some wrongdoing.

Digital forensics seeks to overcome the substantial challenges of drawing correct inference from digital data, so that decisions about the identity of the wrongdoer, and the sanctions that follow, may be made with greater confidence from a better informed perspective.
There are a number of principles that have been established by the digital forensics community. From these a range of tools and techniques have been developed for doing standard things in typical circumstances. Analysing the capabilities and limitations of these tools and techniques is an important part of the module.
Representing what has been inferred to a non-specialist audience is also a critical part of any investigation and is practised in the module.

Module aims

This module aims to provide the students with the required skills that will allow them to prepare and manage a cyber security incident and allow them to apply digital forensics principles for the investigation of a cyber security incident.

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 content of this module will be taught from a cyber security perspective.

Planning for cyber incidents

- Incident detection
- Intrusion response: Intrusion management
- Incident handling: Intrusion analysis, monitoring and logging

Digital Forensics

- Collecting, processing and preserving digital evidence
- Host forensics
- Memory forensics
- Network collection and analysis
- Remediation and Reporting

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:

- Critically evaluate the requirements of a standard operating procedure
- Analyse and apply incident response frameworks to effectively manage cyber security incidents
- Demonstrate the ability to establish a forensic investigation technical environment
- Investigate digital artefacts against a realistic brief, preserving, analysing and interpreting significant material

- Conduct comprehensive post-incident analysis and reporting
- Critically evaluate the significant characteristics of relevant tools and techniques

Indicative reading list

Johansen, G., 2022. Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response.

Joakim, Kavrestad, 2020. Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications. Springer

View reading list on Talis Aspire

Subject specific skills

1. Incident response lifecycle and practices
2. Investigation principles
3. Evaluation of a cyber security incident
4. Evidence management, interpretation, and critique skills
5. Host based analysis
6. Network based analysis

Transferable skills

1. Critical thinking
2. Problem solving
3. Communication
4. Information literacy
5. Analytical Reasoning
6. Research skills

Study

Study time

Type	Required
Lectures	18 sessions of 1 hour (8%)
Supervised practical classes	18 sessions of 1 hour (8%)
Online learning (independent)	30 sessions of 1 hour (12%)
Other activity	6 hours (2%)
Private study	40 hours (17%)
Assessment	128 hours (53%)
Total	240 hours

Private study description

Independent activity between workshops, following up on activities initiated in previous workshops or preparing for upcoming workshops.

Other activity description

Face to face learning support and guidance to support the technical elements of the module.

Costs

No further costs have been identified for this module.

Assessment

You must pass all assessment components to pass the module.

Assessment group A3

	Weighting	Study time
Proposal of a cyber incident standard operating procedure	40%	50 hours
Proposal of a cyber incident Standard Operating Procedure in response to a given case study.		
Investigation of a cyber incident	60%	78 hours
Apply investigation techniques on a given cyber incident scenario and produce a technical report that responds to relevant findings.		

Feedback on assessment

Written feedback for each assignment
Verbal feedback during tutorial sessions
Solutions provided to selected tutorial questions
Summative feedback on assignments

Availability

Courses

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
    - Year 3 of H651 Cyber Security
    - Year 3 of H651 Cyber Security
    - Year 3 of H651 Cyber Security