WM3A6-24 Cyber Security Incident Management

20/21

Department
WMG
Level
Undergraduate Level 3
Module leader
Andrew Hood
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

1 - Critically evaluate the operation of a cyber incident response plan.
2 - Investigate digital artefacts against a realistic brief, preserving, analysing, interpreting and reporting significant material.
3 - Critically evaluate the significant characteristics of relevant tools and techniques.

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
Overall forensic process:
Collecting, processing and preserving digital evidence:
Device forensics:
Memory forensics:
Network forensics
Anti-forensic techniques
Forensic report

Learning outcomes

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

- 1 - Critically evaluate the operation of a cyber incident response plan.
- 2 - Investigate digital artefacts against a realistic brief, preserving, analysing, interpreting and reporting significant material.
- 3 - Critically evaluate the significant characterstics of relevant tools and techniques.

Indicative reading list

Luttgens, Jason T., Pepe, Matthew and Mandia, Kevin “Incident Response & Computer Forensics”, 3 Ed, McGraw-Hill (2014)
Poulsen, Kevin, “Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground”, Random House (2012)
Sachowski, Jason, “Implementing Digital Forensic Readiness: From Reactive to Proactive Process”, Syngress (2016)

Subject specific skills

1 - Critically evaluate the operation of a cyber incident response plan.
2 - Investigate digital artefacts against a realistic brief, preserving, analysing, interpreting and reporting significant material.
3 - Critically evaluate the significant characteristics of relevant tools and techniques.

Transferable skills

Critical thinking, problem solving, communication, information literacy

---

Study

Study time

Type	Required
Supervised practical classes	6 sessions of 6 hours (15%)
Private study	68 hours (28%)
Assessment	136 hours (57%)
Total	240 hours

Private study description

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

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Assessment group A

	Weighting	Study time
Coursework	100%	136 hours

The precise composition of the coursework may vary from year to year. It may include two or more sub-components. Where there are two or more sub-components, the weighting of each sub-component towards the overall module grade will be published near the beginning of the module.

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