WM3F2-15 Cyber Security Operations

27/28

Department
WMG
Level
Undergraduate Level 3
Module leader
Christo Panchev
Credit value
15
Module duration
10 weeks
Assessment
100% coursework
Study location
University of Warwick main campus, Coventry

Description

Introductory description

This module seeks to introduce the students to current effective and proactive cyber attack deterrents, including tools and techniques that can have long-term benefits to the organisation's security posture and maintain the resilience of its cyber infrastructures.

Module aims

The module focuses on the functions, roles, and operational models of a SOC, including how people, processes, and technology are integrated to provide effective security monitoring and incident response capabilities. It will introduce the students in the fundamental security operations strategies and emerging tools, techniques and approaches to deter orchestrated cyber attacks and mitigate their impact, including cyber infrastructure security monitoring, detection and incident response. The module also seeks to equip students with the technical explication of threat modelling in identifying and ranking threats against a variety of scenarios using industry-led and experimental approaches.

The module equips the participants with an in-depth understanding of the fail-safe capabilities of different systems and mechanisms used to detect and analyse targeted and multi-stage cyber attacks. Students will establish a firm and in-depth knowledge in network and systems security operations, including their design philosophy and their weaknesses exploited by motivated and

resourceful adversaries.

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.

- Security Operations. Security Operations Centre (SOC) structure and processes; Security monitoring, detection and response; Incident Response; Threat hunting.
- Vulnerabilities. Constituent elements of a vulnerability: pre-conditions, pre-condition logic, exploits, post-conditions. Vulnerability inventories, disclosure and mitigation; Standard Security Description references; Cyber mission system development frameworks; Cyber defence measurables & evaluation criteria. Vulnerability and Attack surface management.
- Intelligence gathering for adaptive network defence; Kill-chain model, MITRE and the APTs paradigm; STIX, Threat actors; Cyber threat analytics
- Semantic network and threat modelling techniques. Attack graphs, attack trees and fault trees. The application of attack modelling techniques in aiding attack analysis, event prediction, outlining of mitigation strategies. STRIDE and DREAD, Threat Model Validation & Data Flow Diagrams (DFDs) and Trust Boundaries.
- Cyber incident monitoring, detection and investigation of incidents, and system hardening.

Learning outcomes

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

- Anticipate cyber behaviours, both deliberately adversarial and unintentionally inept, that would undermine an organisation's viability (AHEP4 2.1.3, 2.1.5, C4, C9,)
- Critically evaluate the threat and vulnerabilities of an organisation (AHEP4 2.1.1, 2.1.4, 2.1.5, 2.1.7, 2.1.10, 2.1.11, 2.1.13, 2.2.2, 2.3.2, C4, C9, C12, C14)
- Design cyber defensive solution to maintain an organisation's viability in the face of adversarial or unintentional threats (AHEP4 2.1.1, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.10, 2.1.11, 2.1.12, 2.1.13, 2.3.2, C4, C5, C10, C12, C14)
- Implement proactive cyber security controls in the protection of an organisation's infrastructure. (AHEP4 2.1.1, 2.1.5, 2.1.6, 2.1.7, 2.1.12, C10, C12, C14)

Indicative reading list

Reading lists can be found in Talis

Subject specific skills

Participants will develop an advanced understanding and technical skills in a number of network and computer security principles, strategies, techniques and concepts in cyber security operations

Transferable skills

Critical and analytical thinking, problem solving, communication, professionalism, organise and

manage critical resources such as time, budget and finance

Study

Study time

Type	Required
Lectures	10 sessions of 1 hour (7%)
Supervised practical classes	20 sessions of 1 hour (13%)
Online learning (independent)	10 sessions of 1 hour (7%)
Private study	50 hours (33%)
Assessment	60 hours (40%)
Total	150 hours

Private study description

Additional lab work and research

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
Assessment component			
Practical lab challenges	40%	24 hours	Yes (extension)
Practical lab challenges on incident detection and response.			
Reassessment component is the same			

	Weighting	Study time	Eligible for self-certification
Assessment component			
Coursework	60%	36 hours	Yes (extension)
A report on practical work providing monitoring, detection and/or incident response to complex or multi-stage cyber attacks in a given case study related to security breaches and incidents.			
Reassessment component is the same			

Feedback on assessment

Feedback will be provided on a standard WMG feedback form.

Availability

Courses

This module is Core optional for:

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