Unit Outline (Higher Education)

Institute / School: Institute of Innovation, Science & Sustainability

Unit Title: Security Operations

Unit ID: ITECH3504

Credit Points: 15.00

Prerequisite(s): (ITECH2505)

Co-requisite(s): Nil

Exclusion(s): Nil

ASCED: 020113

Description of the Unit:
This advanced unit delves deep into the dynamic world of Security Operations Centers (SOCs). The students will explore advanced threat detection, incident response, security information and event management (SIEM), and security orchestration, automation, and response (SOAR) technologies. Learn to analyze security data, hunt for threats, investigate incidents, and implement automated workflows to streamline security operations. Through hands-on labs, gain practical experience with leading tools and hone your analytical and problem-solving skills to become a valuable asset in any SOC environment.

Grade Scheme: Graded (HD, D, C, P, MF, F, XF)

Work Experience:

No work experience: Student is not undertaking work experience in industry.

Placement Component: No

Supplementary Assessment: Yes

Where supplementary assessment is available a student must have failed overall in the Unit but gained a final mark of 45 per cent or above, has completed all major assessment tasks (including all sub-components where a task has multiple parts) as specified in the Unit Description and is not eligible for any other form of supplementary assessment

Course Level:

Level of Unit in Course	AQF Level of Course					
	5	6	7	8	9	10
Introductory						

Level of Unit in Course	AQF Level of Course					
	5	6	7	8	9	10
Intermediate						
Advanced			✔			

Learning Outcomes:

Knowledge:

K1. Analyze advanced threat detection methodologies that leverage network traffic analysis, endpoint data analysis, and user behavior analysis.

K2. Critically evaluate security incident response frameworks and best practices for effectively handling security incidents.

K3. Evaluate and compare leading security operations solutions such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) based on their functionalities and organizational needs.

Skills:

S1. Develop security monitoring strategies using advanced threat detection techniques.

S2. Analyze and interpret security data from various sources to support security incident response and threat hunting activities.

Application of knowledge and skills:

A1. Synthesize the unit concepts to create a secure, resilient operational framework for a mock organizational environment.

Unit Content:

Topics may include:

- Introduction to Security Operations Centers (SOCs), Security Operations Life Cycle
- Advanced Threat Detection Techniques (e.g., Network Traffic Analysis, Endpoint Data Analysis, User Behavior Analysis)
- Security incident response frameworks, methodologies, best practices, process & procedure
- Advanced Security Monitoring Strategies & Threat Hunting Concepts
- Introduction to Security Orchestration, Automation, and Response (SOAR)
- SOAR Workflows for Threat Detection & Incident Response
- Integrating SIEM & SOAR for Enhanced Security Operations
- Advanced SOAR Configuration & Optimization
- Future Trends in Security Operations

FEDTASKS

Federation University Federation recognises that students require key transferable employability skills to prepare them for their future workplace and society. FEDTASKS (**T**ransferable **A**ttributes **S**kills and **K**nowledge) provide a targeted focus on five key transferable Attributes, Skills, and Knowledge that are be embedded within curriculum, developed gradually towards successful measures and interlinked with cross-discipline and Co-operative Learning opportunities. *One or more FEDTASK, transferable Attributes, Skills or Knowledge must be evident in the specified learning outcomes and assessment for each FedUni Unit, and all must be directly assessed in each Course.*

FEDTASK attribute and descriptor		Development and acquisition of FEDTASKS in the Unit	
		Learning Outcomes (KSA)	**Assessment task (AT#)**
FEDTASK 1 Interpersonal	Students will demonstrate the ability to effectively communicate, inter-act and work with others both individually and in groups. Students will be required to display skills in-person and/or online in: • Using effective verbal and non-verbal communication • Listening for meaning and influencing via active listening • Showing empathy for others • Negotiating and demonstrating conflict resolution skills • Working respectfully in cross-cultural and diverse teams.	A1	AT4
FEDTASK 2 Leadership	Students will demonstrate the ability to apply professional skills and behaviours in leading others. Students will be required to display skills in: • Creating a collegial environment • Showing self -awareness and the ability to self-reflect • Inspiring and convincing others • Making informed decisions • Displaying initiative	A1	AT4
FEDTASK 3 Critical Thinking and Creativity	Students will demonstrate an ability to work in complexity and ambiguity using the imagination to create new ideas. Students will be required to display skills in: • Reflecting critically • Evaluating ideas, concepts and information • Considering alternative perspectives to refine ideas • Challenging conventional thinking to clarify concepts • Forming creative solutions in problem solving.	K1-K3, S1-S2, A1	AT1-AT4
FEDTASK 4 Digital Literacy	Students will demonstrate the ability to work fluently across a range of tools, platforms and applications to achieve a range of tasks. Students will be required to display skills in: • Finding, evaluating, managing, curating, organising and sharing digital information • Collating, managing, accessing and using digital data securely • Receiving and responding to messages in a range of digital media • Contributing actively to digital teams and working groups • Participating in and benefiting from digital learning opportunities.	S1-S2, A1	AT3-AT4

FEDTASK attribute and descriptor		Development and acquisition of FEDTASKS in the Unit	
		Learning Outcomes (KSA)	Assessment task (AT#)
FEDTASK 5 Sustainable and Ethical Mindset	Students will demonstrate the ability to consider and assess the consequences and impact of ideas and actions in enacting ethical and sustainable decisions. Students will be required to display skills in: • Making informed judgments that consider the impact of devising solutions in global economic environmental and societal contexts • Committing to social responsibility as a professional and a citizen • Evaluating ethical, socially responsible and/or sustainable challenges and generating and articulating responses • Embracing lifelong, life-wide and life-deep learning to be open to diverse others • Implementing required actions to foster sustainability in their professional and personal life.	A1	AT4

Learning Task and Assessment:

Learning Outcomes Assessed	Assessment Tasks	Assessment Type	Weighting
K1-K3	Weekly Quizzes: Short quizzes will assess students' understanding of key concepts.	Quiz	10%-30%
S1-S2	Lab Reports: Lab reports will document hands-on exercises and analysis.	Lab Reports	15%-35%
A1	Project proposal: Students are required to submit an initial project proposal.	Project proposal	10%-30%
A1	Final Project: Students will design a SOAR workflow to automate a specific security incident response task and submit a report.	Final Project	20%-40%

Adopted Reference Style:

IEEE

Refer to the library website for more information

Fed Cite - referencing tool