CRICOS Provider No. 00103D | RTO Code 4909 | TEQSA No. PRV12151 (Australian University)

## ITECH1502 Cybersecurity Fundamentals

## Week 2 Lab Activities

# Understanding Modern Cyber Threat Landscape and the role of AI

**Lab Overview:**

This week’s practical labs are designed to deepen your understanding of the evolving cyber threat landscape, evaluate the use of AI-powered tools in cyber defense, and help you plan a cybersecurity career aligned with real-world roles. Each lab task is structured to provide hands-on, research-based, and reflective learning experiences essential for becoming cybersecurity professionals.

**Learning Outcomes Assessed:**

1. Critically investigate and classify recent cyberattacks by identifying threat actors, exploited vulnerabilities, and organizational weaknesses using foundational cybersecurity concepts and reflection on incident response strategies.
2. Evaluate the capabilities and limitations of AI-powered cybersecurity tools by comparing open-source and commercial platforms in terms of threat detection, automation, and response time, while reflecting on their ethical and operational implications.
3. Design a personalized cybersecurity career plan by analyzing industry job roles, required competencies, and relevant certifications, while aligning academic learning with professional growth and employability goals.

**🔐 Lab Task 1: Cyber Threat Analysis of a Real-World Incident (1 Mark)**

You are required to investigate **any one major real-world cybersecurity incident** from the **past three years (2021–2024)** and complete a structured analysis using the provided table and critical reflection prompts.

You may choose from high-profile cases such as:

* MOVEit Exploit (2023)
* Medibank Data Breach (2022)
* Latitude Financial Hack (2023)
* Optus Data Breach (2022)
* Colonial Pipeline Attack (Follow-up) (2021–2022)
* LastPass Credential Theft (2022)
* Any other publicly reported cyber incident

### ****📊 A. Cyber Threat Analysis Table****

|  |  |
| --- | --- |
| **Component** | **Your Case Study Details** |
| Incident Name & Year | **Medibank Data Breach (2022)** |
| Type of Attack | **Ransomware and data extortion** |
| Threat Actor Type | **Cybercriminal group** |
| Motivation | **Financial gain via ransom demands and public data release** |
| Vulnerability Exploited | **Poor access controls , poor security** |
| Targeted Asset(s) | **Personal and health records of customers** |
| Risk Realized | **Massive data leak, reputational damage, legal scrutiny, and customer trust loss** |
| Scope of Exposure | **Over 9.7 million individuals affected across Australia** |
| Safeguards Lacking | **No multi-factor authentication** |
| Post-Incident Action | **Public breach disclosure, refusal to pay ransom, strengthened cyber controls, government investigation** |

### ****🧠 B. Critical Reflection (250–300 words)****

Respond to the following reflection prompts based on your analysis:

1. **What were the key failures (technical, administrative, human, or vendor-related) that contributed to the success of the attack?**

**Administrative gaps included insufficient internal oversight and delayed detection, while human factors, such as lack of security training and awareness, compounded the problem which was the key failures which contributed for a successful attack.**

1. **How did the affected organization respond, and what could have been improved in their response strategy?**

**Medibank chose transparency by disclosing the breach and refusing to pay ransom and even though that shows some trust their initial communication lacked clarity and timeliness, causing customer to be anxiety and have gain less trust in the organization**.

1. **What proactive or AI-enhanced defense mechanisms could have prevented or minimized this attack? A Ai powered threat detection which is a machine learning models can flag anomalies like unusual login times or data access patterns in real time.**

**🤖 Lab Task 2: Investigating AI-Powered Cyber Defense Tools (1 Mark)**

You are required to investigate **two cybersecurity tools/platforms** — one **open-source** and one **commercial** — that incorporate Artificial Intelligence (AI) or Machine Learning (ML) in their threat detection and response mechanisms.

### ****A. Tool Analysis Table****

Choose **one tool from each category**:

* **Open Source Tools** (examples):
  + Wazuh
  + Snort + ML plugins
  + Zeek (with ML extensions)
  + ELK Stack (integrated with ML models)
* **Commercial Tools** (examples):
  + IBM QRadar Advisor with Watson
  + Palo Alto Cortex XSOAR
  + Darktrace
  + Microsoft Defender for Endpoint
  + CrowdStrike Falcon

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool Type** | **Tool Name** | **Threats Detected** | **AI/ML Capabilities** | **How it Reduces Incident Response Time** |
| Open Source | **Wazuh** | **File integrity changes**  **unauthorized access,** | **Basic ML driven rule classification, log analysis, and correlation** | **Automates threat detection and alerting across endpoints and logs** |
| Commercial | **Darktrace** | **Insider threats,**  **zero-day attacks** | **Advanced self-learning AI, anomaly detection** | **Detects unknown threats quickly and autonomously responds to contain incidents** |

🔍 Tip: Refer to vendor documentation, whitepapers, or analyst reports to fill in the table accurately.

### ****B. Critical Reflection (250–300 words)****

Answer the following questions based on your analysis:

1. **Which tool (open-source or commercial) do you think is more effective for a medium-sized organization and why?**

**Wazuh offers the best as Its cost-effectiveness, scalability, and modular design make it ideal for teams with limited resources.**

1. **What are the ethical or operational challenges in using AI for automated decision-making in cybersecurity?  
    Ai powered anomaly detection is a system that identifies unusual behaviors such as sudden spikes in outbound data , access to sensitive files during usual hours which could be a challenge as an attacker can breach in a time that seems usual for the ai**
2. **How might your chosen tools have helped reduce impact or detection time in a recent high-profile cyberattack (e.g., MOVEit, SolarWinds, Medibank)?**

**Wazuh can be a great tool for the Medibank incidents that happen in 2022 because this tool can detect file integrity changes, unauthorized access which detect the cybercriminal I the incident**

**💼 Lab Task 3: Designing Your Cybersecurity Career Pathway [1 Mark]**

You are required to explore real-world cybersecurity job opportunities and create a **personalized career pathway** aligned with your interests and current skills.

### ****Step-by-Step Instructions****

#### ****1. Select a Cybersecurity Role:** Search for a cybersecurity job of interest using any of the following platforms:**

* Seek.com.au
* [LinkedIn Jobs](https://www.linkedin.com/jobs/)
* Indeed.com.au
* Government or industry-specific portals (e.g., cyber.gov.au, apsjobs.gov.au)

🎯 Choose a **realistic entry- or mid-level cybersecurity role**, such as:

* Security Analyst
* SOC Analyst
* Cybersecurity Consultant
* Penetration Tester
* Cloud Security Engineer
* GRC Analyst
* Digital Forensics Investigator

#### ****2. Extract Role Details:**** Fill in the following table based on the job posting

|  |  |
| --- | --- |
| **Job Title** | **Security Analyst** |
| Job Link / Source | **Seek.com.au** |
| Required Skills | * **Network protocols, firewalls, intrusion detection systems.** * **Familiarity with tools like Splunk, Wireshark, or CrowdStrike.** * **Analytical thinking and incident documentation** |
| Preferred Qualifications | **Bachelor’s degree in Cybersecurity** |
| Relevant Certifications | **CompTIA Security+, CySA+** |
| Key Responsibilities | **Monitor Security Information and Event Management (SIEM) systems.**  **Perform threat hunting and vulnerability scanning.**  **Investigate alerts and escalate incidents.**  **Maintain logs and create security reports.** |
| Industry Sector (e.g., gov, finance) |  |

#### ****3. Plan Your Career Pathway:**** Based on the job requirements, design a realistic **career development plan**

* **Short-Term Goals (Next 12 Months):**  
  Courses to complete, certifications **CEH, OSCP, GPEN**
* **Mid-Term Goals (1–3 Years):**  
  Work experience, internship, volunteer roles, portfolio development.
* **Long-Term Goals (3+ Years):**  
  Target roles, advanced certifications (e.g., CISSP, CISM), career specialization.

You may present this plan as:

* A timeline or roadmap
* A table or flowchart
* A step-by-step list with milestones

|  |  |  |
| --- | --- | --- |
| Stage | Plan |  |
| **Short-Term Goals (Next 12 Months)** | CEH/OSCP prep, tool mastery |  |
| **Mid-Term Goals (1–3 Years):** | Volunteer/intern, SIEM workflows |  |
| **Long-Term Goals (3+ Years** | Analyst role, CISSP/CISM, specialization |  |

### ✍️ ****Reflection Questions (200–300 words)****

1. **Why did you choose this role and how does it align with your background or interest area (e.g., IT, healthcare, engineering)?**

**I chose security analyst cause I find it very interested and is the job that I want to do in the future after ive done my course and the responsibility of the jobs fits with my interest**

1. **What challenges might you face in achieving this pathway, and how can you overcome them?**
2. **Challenges I might find hard is the software there use such as splunk , wireshark and crowd strike which is what I need to learn more**
3. **How does understanding cybersecurity roles help shape your academic and practical learning in this unit? This task in understanding cybersecurity roles helps us student to shape our future and goals and to know what we need to achieve to earn this role in ou future and also allows to understand the requirements of the task**

## Lab Submission Guidelines

1. Students might use AI tools. However, they must have to demonstrate their understanding of contents through oral questions or presentation.
2. All students are required to submit their completed **Week 2 Lab** tasks via **Moodle** by **Sunday, 3 August 2025** 23:59 (local time). Late submissions are not accepted.
3. Navigate to **Week 2 > Active Learning** in Moodle to access the submission link.