**Navneet Kaur (30479221)**

Github Portfolio link: <https://github.com/navneetkaur0920911/Cybersecurity-Portfolio-ITECH1502/tree/main>

# 1. Project Title

**Incident Response Process: A Practical Simulation on TryHackMe**

# 2. Summary

The project illustrates a realistic perception of the incident response process using the TryHackMe platform. The exercise modelled a real-life cybersecurity incident where I played the role of an Incident Response Team (IRT) that was dealing with a breached Windows workstation. The practical work has helped me learn the NIST Incident Response Framework, the stages of which are Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity. In every part, there were practical examples, descriptions, and knowledge assessments. The undertaking of the activity has helped me in improving my understanding of the structured response planning, communication and documentation of cyber incidents. The TryHackMe platform provided a practical, interactive, scenario-based learning format that helped in closing the gap between theoretical knowledge and practical knowledge. Altogether, this activity helped me become more effective in the systematic approach to the security incidents and made me ready to work in the real-life environment in cybersecurity operations and analysis.

# 3. Introduction

The TryHackMe site is an interactive online cybersecurity training platform that aims to train practical skills based on guided labs and scenarios using a cloud-based environment. It offers clients virtual environments that they may use to simulate actual cyberattacks, conduct analysis and implement security designs. I chose TryHackMe to base this project on since it represents an integration of theoretical knowledge with practical tasks that enable learners to complete the challenges in an interactive way and according to the professional cybersecurity processes. The room of incidence response process was selected due to the fact that it connects with the following key unit learning outcomes: using cybersecurity measures (A1) and utilising a case study to detect breaches and recommend mitigation measures (A2). This exercise was an eye-opener on how organisations can handle and bounce back after a cybersecurity incident and continue running their businesses.

# 4. Problem/Challenge

The contemporary organisations have to contend with unceasing cyber threats such as ransomware, phishing, and advanced persistent threats (APTs). When an incident takes place, the response teams should respond with speed to contain the damage to a minimum, bring it back on track and ensure that it does not happen again. The problem that was covered in this activity was to comprehend the way incident response is organised and implemented within a professional environment. The simulation dropped me in the position of an analyst at a Security Operations Centre (SOC) to react to a possible compromise. The task demanded studying alerts, learning response stages, and frameworks, including NIST 800-61r2, which is the set procedure to respond to security incidents.

# 5. Project Goals/Objectives

The main objectives of this project were:

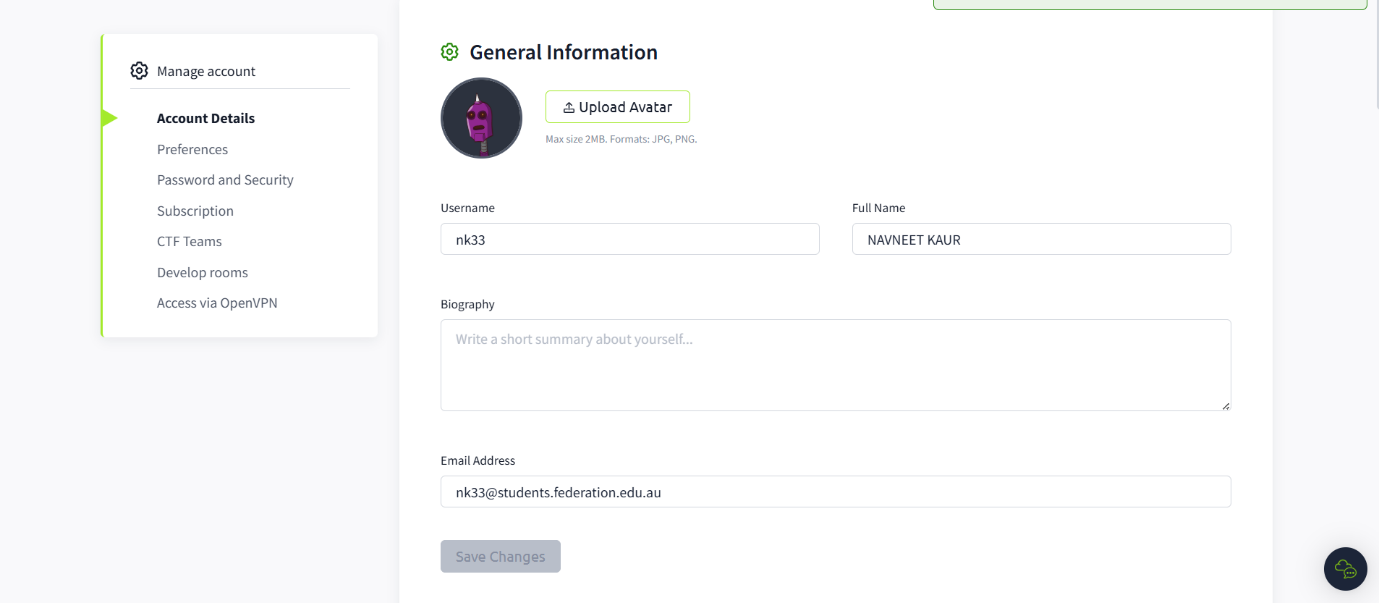
* To interpret and implement the NIST Incident Response Framework to a simulated scenario.
* To determine the purpose and activities in each phase Preparation, Detection, Containment, Eradication, Recovery, and Lessons Learned.
* It enhances analytical thinking and decision making as far as handling an incident is concerned.
* To take into consideration the role of structured response plans to improve the cybersecurity resilience.

# 6. Methodology

The project was conducted using the following step-by-step process:

1. **Platform Registration:**

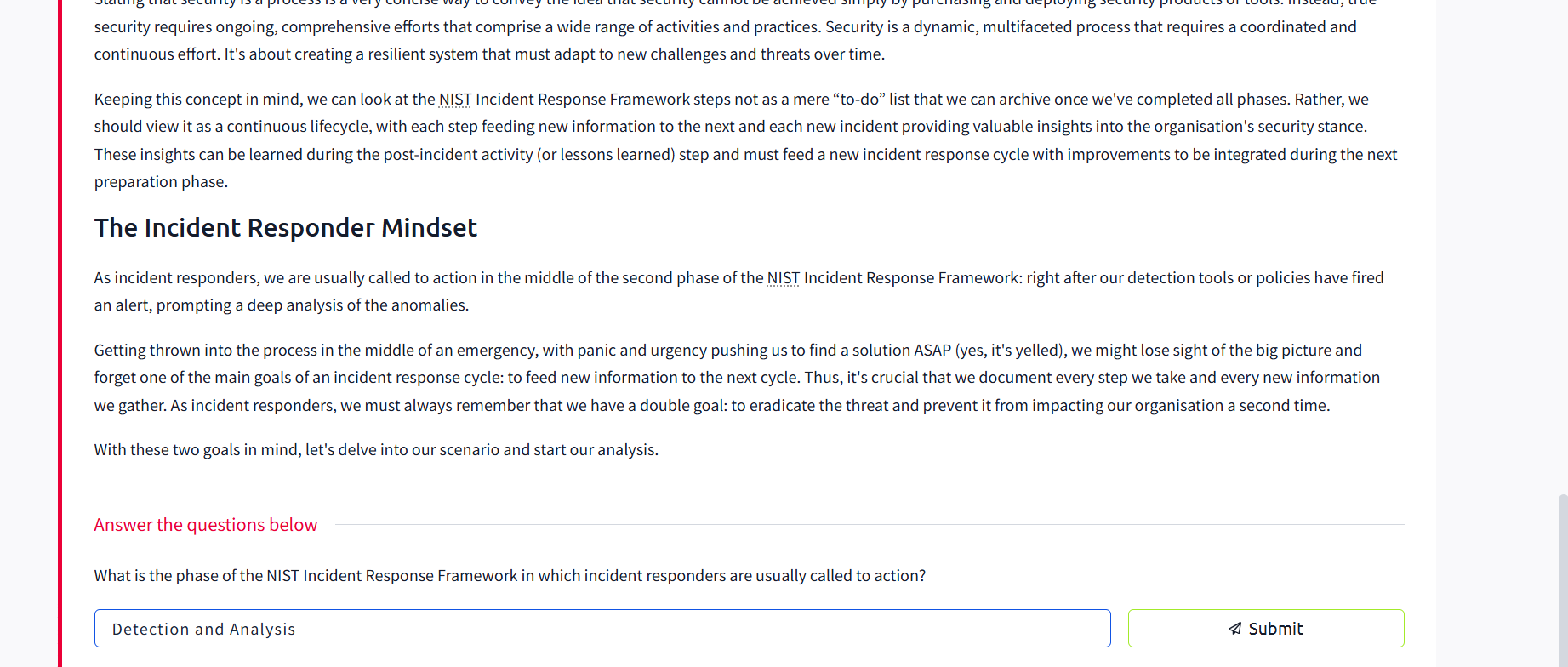
Created an account on TryHackMe using my FedUni email for verification.



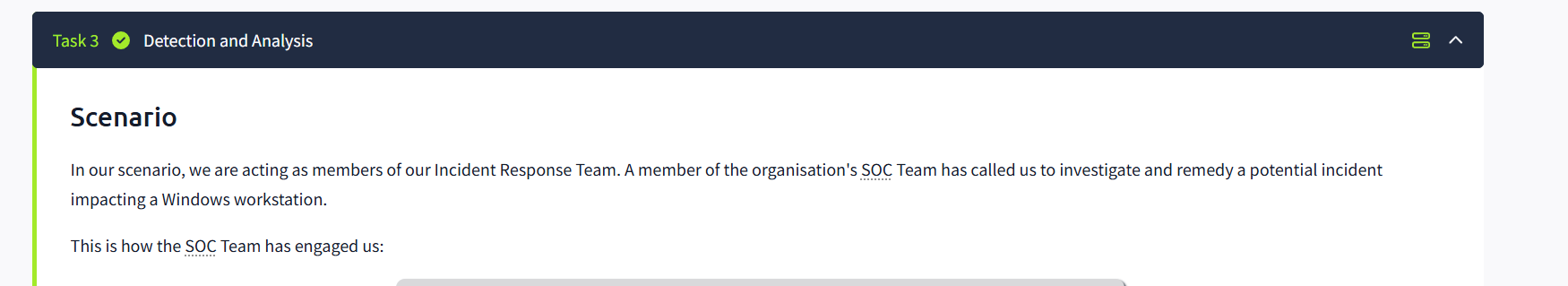
1. **Room Selection:**  
   Enterted the room of the “Incident Response Process” that is dedicated to the conceptualization and implementation of the NIST model.
2. **Task Completion:**

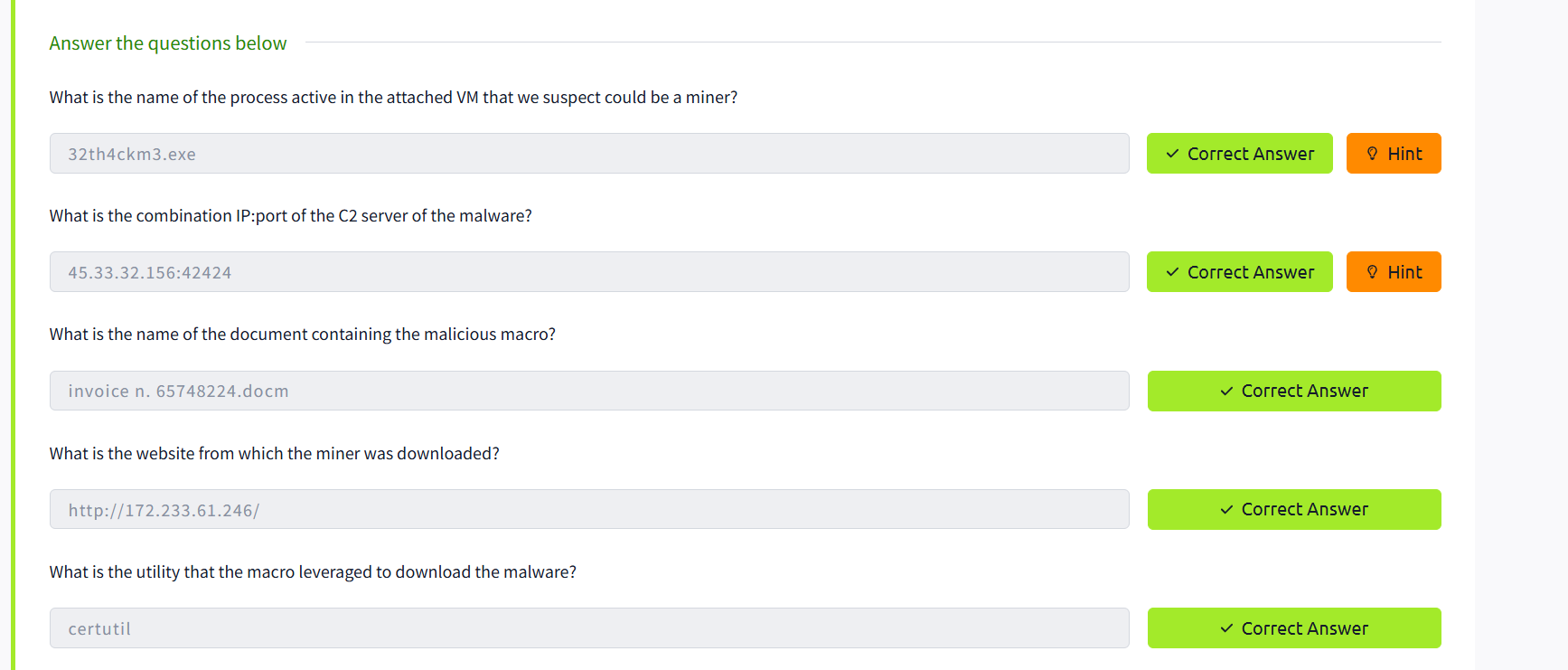
The room was divided into six tasks:

* + *Task 1:* Introduction to Incident Response
  + *Task 2:* Incident Response Lifecycle

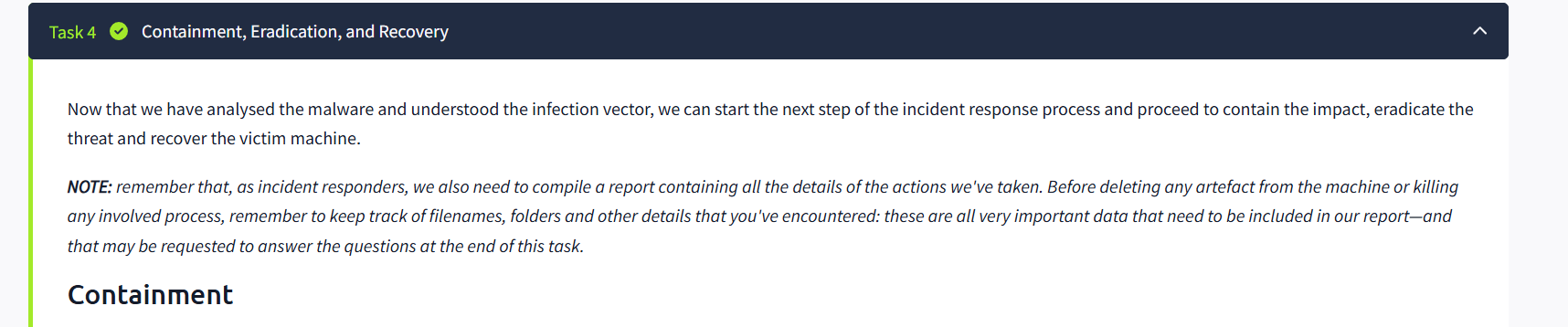


* + *Task 3:* Detection and Analysis



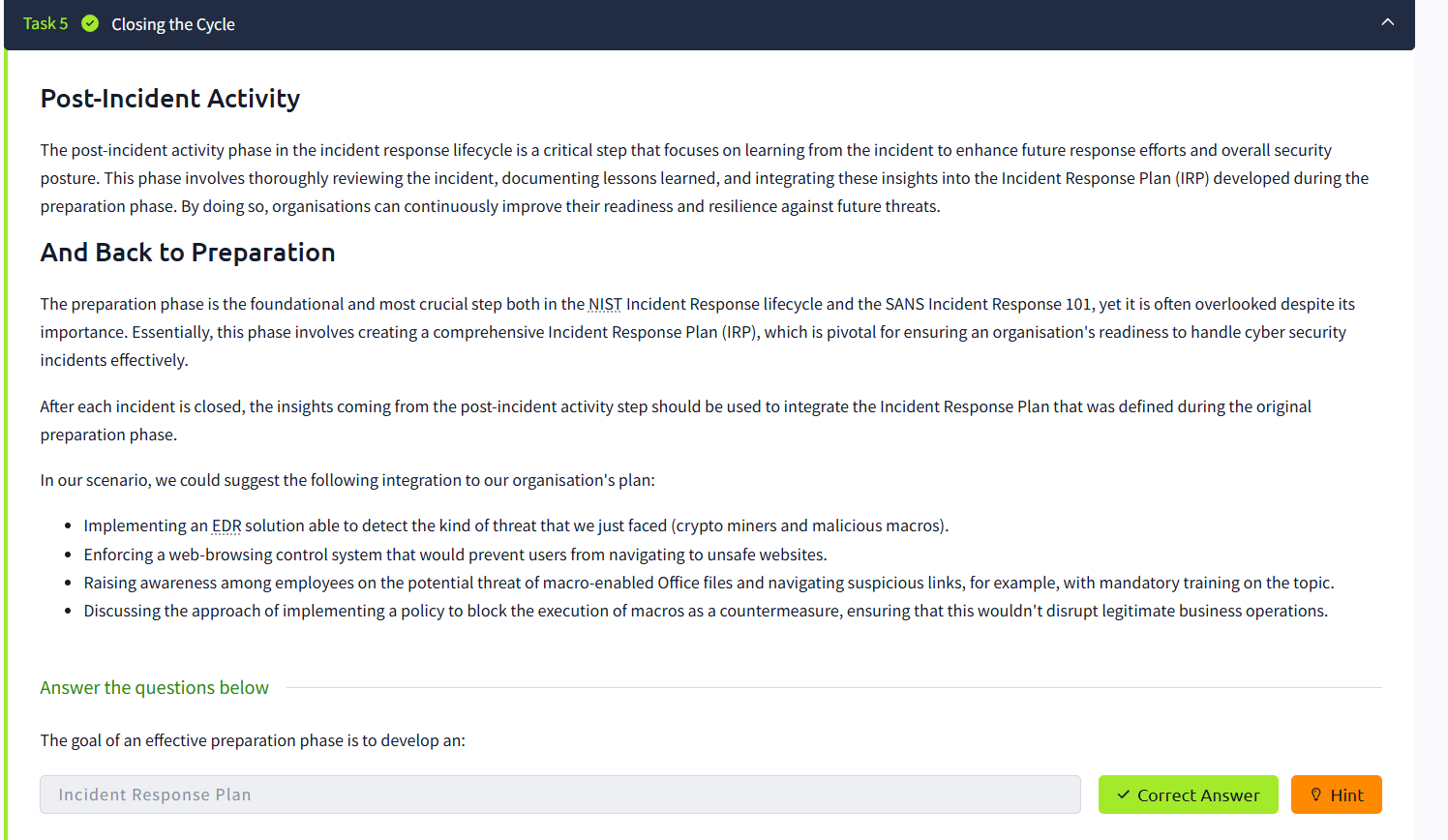


* + *Task 4:* Containment, Eradication, and Recovery





* + *Task 5:* Closing the Cycle



* + *Task 6:* Conclusion

Each task had some reading material, real-life examples, and quizzes to make sure that the understanding was made. The final task consisted of an in-depth overview of all the processes finalised previously, which, once again, proved the idea that incident response is a lifelong learning process. It paid attention to lessons learned reviews, improved documentation, and the implementation of new policies in future preparedness and resilience towards cybercrimes.

1. **Tools Used:**

To show the techniques of the analysis and containment, the tools that are typically utilised in incident response, including SIEM systems, Wireshark, Volatility, and Event Viewer, will be used in the given activity.

# 7. Results/Outcomes

The six tasks were effectively done, as evidenced by the presented screenshot evidence. The simulation has provided me with a hands-on experience of the Incident Response Lifecycle, with its focus on the significance of documentation and the focus on communication when responding to the incident. The outcomes of the activity proved:

* The activity also enhanced my understanding of the four NIST phases and their practical application in real-world scenarios.
* The participants gained an understanding of how to activate detection tools during an incident response.
* One should possess a conscious understanding of how to prevent and eliminate malicious activity.
* The importance of post-incident review to the improvement of the organisation.

**Evidence:**

Screenshots make us see all six tasks done: Introduction, Incident Response Lifecycle, Detection and Analysis, Containment, Eradication and Recovery, Closing the Cycle, and Conclusion, which is the verification of the activities done.

# 8. Reflection

**a. What did you learn about cybersecurity concepts and tools from this exercise?**

I learnt that incident response is a continuous and organized process, which entails setting plans, detection, technical analysis, and recovery. The drill enabled me to better understand how SOC teams collaborate and apply such tools as SIEM and network analysis to detect and respond to threats in an efficient way. It further noted that preparation and communication were also of importance as part of reducing the effect of incidents.

**b. How do you see this experience contributing to your professional growth as a future cybersecurity practitioner?**

This experience supported my theoretical training on cyber defence practices and prepared me to work in the role of a junior analyst or security responder. The working frameworks like NIST have made me understand more clearly how theory can be applied to actual setting of making decisions and how proper documentation is applicable in making organisations resilient and compliant.

**c. Looking back, what would you do differently if you repeated the task?**

If I redo the activity, I would further my study by recreating a live event in LetsDefend or Blue Team Labs to train on the log analysis and handling of evidence. I would also consider trying to use other tools like Volatility or Wireshark on a real virtual machine to have more technical understanding of the aspects of threat containment and forensic investigation.

# 9. Conclusion

The TryHackMe room on Incident Response Process gave me a well-organised and realistic view of the process of responding to cybersecurity incidents in practice. It supported the significance of NIST framework as a lifecycle, instead of a single checklist. The experience has boosted my preparedness to join future operations and incident handover activities of cybersecurity efforts in the real-world workplace.