7907ICT

Workshop Document

**This document is where you write-up the TEN weekly workshop tasks, each one of which is worth 10% of your total marks.**

# How to Approach these workshops (1 - 10)

This document lays out the ten workshop exercises to be completed each week. Either during the workshop session or at another time at your convenience. It contains detail of the task, plus a read-made template to be used when answering the questions.

This is the document that will be submitted for marking in two stages; Part A in week 6 to include workshops 1 through 5. Part B submitted in Week 11 to include weeks 6 to 10.

Key points to note:

* The output of each workshop is a **600-word written report**.
* Write your 600-word report into this workbook, accumulating them until you have completed all ten, then submit it via the Turnitin portal at the bottom of the assignment page of the course website.
* Don’t be tempted to leave doing the workshop write-up until the week the submission. It is a fact that we usually under-estimate the amount of work needed.
* As per university policy, extensions to the allowed time to submit can be granted with the necessary documentation. But please bear in mind that the IT industry is a very deadline driven profession.
* The workshops follow a similar format. Once you become familiar with the process, you should be able to work through the ten workshops over the duration of the course.
* The workshops can be completed individually or in discussions with groups of 2-4 students. Your submission will be an individual one, not a group submission.
* Ensure your report has clear headings for each.
* Try to do one workshop write-up per week.
* Avoid directly copying and pasting information from online sources, including generative language models like ChatGPT or other.

# Module 7: Cyber Forensics and Intelligence Analysis

**<Workshop 7>**

### Introduction

In today’s digital world, data breaches can have severe impacts on organizations, making it crucial to carry out a thorough cyber forensics investigation. As a cybersecurity consultant, my goal is to find the source of the breach, collect potential evidence, and identify the attackers involved. Additionally, I will develop a Cyberthreat Intelligence Program (CIP) to strengthen the company’s security and help prevent future attacks.

#### <cyber forensics investigation>

The investigatory process in cyber forensics includes six main stages. It begins with readiness, where the system is prepared for investigation and ensuring that both the IT team and the investigator understand their roles and know their responsibilities. The next step is evaluation, where the impact of the incident is clearly defined. In the collection stage, evidence is gathered securely, ensuring the admissibility in a court of raw, and conducting interviews to make sure the evidence can be used in court. Then here comes analysis process, where the collected evidence is examined thoroughly, making sure it's accurate and can be repeated if needed. Then, the results are presented in a way that even normal people can understand. The final step is review, where the process is evaluated to find ways to improve for future investigations.

#### <threat intelligence sources>

To gather information about potential threat actors and their tactics, techniques, and procedures (TTPs), several key sources of threat intelligence are used. Signals intelligence (SIGINT) helps by blocking communications and network traffic to spot any suspicious activity. Another important source is open-source intelligence (OSINT), which relies on public data such as social media, reports, and hacker forums to learn more about possible threats. Additionally, technical intelligence (TECHINT) looks at the hardware and software used by attackers to understand their tools and methods. By combining these sources, cybersecurity teams can get a clearer picture of who the attackers are and how they operate, which helps in defending against future attacks.

#### <develop a Cyberthreat Intelligence Program (CIP)>

To establish a Cyberthreat Intelligence Program (CIP) within the company, the process would begin with building both operational and strategic components.

On the operational side, the focus would be on detecting, investigating, and responding to incidents in real-time. This would involve setting up automated systems to collect and analyze network logs, endpoint data, and threat intelligence feeds. A dedicated team would handle incident response, fine-tuning protection and detection processes based on the intelligence gathered.

On the strategic side, the company would prioritize identifying relevant threats based on industry and region, allowing them to focus resources on the most critical risks. This would include setting up continuous improvement loops to regularly update threat detection and response processes.

### Conclusion

In conclusion, having a strong approach to cybersecurity is essential for organizations dealing with data breaches. A thorough cyber forensics investigation helps identify the reasons of data breach, gather evidence that can be used in court, and track down the attackers. By following a well-defined investigation process, companies can enhance their response to future incidents. Additionally, using different threat intelligence sources like SIGINT, OSINT, and TECHINT gives important insights into how attackers operate, which improves overall defense. Finally, setting up a Cyberthreat Intelligence Program (CIP) with both operational and strategic elements ensures that the company can keep improving its defenses and stay ready to handle future threats.

### References

<Use APA referencing style>