MODULE 7: CYBER FORENSICS AND INTELLIGENCE ANALYSIS

Instructions:

Imagine you are a cybersecurity consultant hired by a company that recently experienced a data breach. Your task is to conduct a cyber forensics investigation and gather threat intelligence to understand the nature of the breach and the potential actors involved.

1. Cyber Forensics Investigation (15 minutes):

- Outline the key steps you would follow in conducting a cyber forensics investigation, considering the legal aspects and admissibility of evidence.
- Describe the different stages of the forensics process, from readiness and evaluation to collection, analysis, presentation, and review.
- Discuss the potential countermeasures that criminals might employ to obfuscate or conceal their activities, and how you would address them.

2. Threat Intelligence Analysis (15 minutes):

- Identify at least three primary sources of cyber intelligence (e.g., SIGINT, OSINT, TECHINT) that you would leverage to gather information about the potential threat actors and their tactics, techniques, and procedures (TTPs).
- Explain how you would establish a Cyberthreat Intelligence Program (CIP) within the company, considering the operational and strategic components.
- Discuss the importance of collaborating with external entities, such as information sharing and analysis centres (ISACs) and threat intelligence communities, in gathering and sharing relevant threat intelligence.

Output:

After completing the exercise, you should provide a written answer of approximately 600 words, addressing the following:

1. A summary of the cyber forensics investigation process, highlighting the legal considerations and admissibility of evidence.
2. An overview of the threat intelligence sources and methods they would employ to gather information about the potential threat actors and their TTPs.

3. A brief outline of how they would establish a Cyberthreat Intelligence Program (CIP) within the company, including operational and strategic components, as well as external collaborations.

This exercise aims to reinforce the concepts of cyber forensics, threat intelligence gathering, and the establishment of a Cyberthreat Intelligence Program (CIP). It encourages you to think critically about the practical application of these concepts in a simulated scenario, while also considering legal aspects and collaboration with external entities.