Unit 2 Seminar - The Solar Winds Breach Case Study

1. **Create a table that analyses the solar winds exploit using the Cyber Kill Chain. Are there any phases that you cannot identify?**

SolarWinds is a software company specialising in providing system management tools for network and infrastructure monitoring. One of their most popular products is Orion, an IT performance monitoring system that is granted privileged access to IT systems to retrieve log and system performance data. Unfortunately, this made SolarWinds an attractive cyberattack target (Oladimeji & Kerner, 2023).

The SolarWinds hack refers to the supply chain breach that affected the SolarWinds Orion system. It's one of the largest hacks of its kind, affecting over 30,000 organisations, including local, state, and federal agencies. The hackers, known as Nobelium according to Microsoft, were able to infiltrate the networks, systems, and data of SolarWinds customers by distributing backdoor malware as an update to the Orion software (Oladimeji & Kerner, 2023).

Hackerone (N.D.) states that the SolarWinds cyberattack was an APT attributed to APT29, a Russian-state-sponsored group. APTs are highly sophisticated cyber-attacks executed by skilled threat actors, often backed by nation-states or criminal organisations. They infiltrate a network, maintain persistent access, steal valuable data or compromise vital systems. APTs involve complex and multi-vector stages such as reconnaissance, weaponisation, and execution. Attackers employ multiple vectors, including spear phishing and watering hole attacks, and can remain hidden for months to years.

Enterprises can use the intrusion kill chain as a framework for intelligence-driven CND. This approach facilitates the alignment of defensive capabilities with adversary processes, allowing for the measurement of performance and effectiveness.

Furthermore, it enables the development of investment roadmaps to address any capability gaps (Hutchins et al. N.D.).

This is a table that provides an analysis of the SolarWinds exploit using the Cyber Kill Chain based on the ideas of Hutchins et al. (N.D.):

Phase	Description	SolarWinds Exploit
Reconnaissance	The attacker gathers information about the target environment.	Attackers conducted reconnaissance by scanning SolarWinds Orion servers for vulnerabilities.
Weaponisation	The attacker develops or acquires malware or exploits to target the vulnerability.	Attackers developed a backdoor called Sunburst and inserted it into SolarWinds Orion software updates.
Delivery	The attacker delivers the malware or exploits it to the target system.	Attackers had Sunburst to SolarWinds customers through compromised software updates.
Installation	Malware or exploit is installed on the target system.	Sunburst was installed on the target systems through regular software updates.
Command and Control (C2)	The attacker establishes communication with the compromised system to issue commands.	Attackers set up command and control servers to communicate with compromised SolarWinds Orion servers.
Actions on Objective	Attacker achieves their objectives by executing malicious commands.	Attackers used Sunburst to steal sensitive data, elevate privileges, and move laterally within the target networks.

2. Create a list of possible mitigations for each phase. Are there any phases you cannot mitigate?

Effective mitigation of APT requires organisations to implement rigorous security policies, swiftly patch vulnerabilities, continuously monitor for threats, and have a comprehensive incident response plan. Regular user awareness training and engaging with relevant security communities are also essential (Hackerone, N.D.). Below are some ways to reduce the risks associated with each phase mentioned in the previous question:

- For reconnaissance, organisations should implement network segmentation, use firewalls and intrusion detection/prevention systems (IDS/IPS), and educate users on phishing and social engineering.

- For weaponisation, code signing and integrity verification for software updates should be implemented, along with application allowlisting and network traffic monitoring for suspicious activity.

- For delivery, email filtering and anti-malware solutions can be used, along with education on safe browsing practices and restricted access to software updates from untrusted sources.

- For installation, endpoint security solutions, application sandboxing, and prompt software vulnerability patching are recommended.

- For command and control, DNS sinkholing and network traffic analysis, IP reputation filtering, and blocking communication with known malicious domains can be effective.

- Actions on objective can be mitigated by implementing data loss prevention (DLP) solutions, user activity monitoring for suspicious behaviour, and regular security audits.

3. What tools would you utilise in each phase? Give reasons for your answer.

In today's world, traditional network defence tools are not enough to counter Advanced Persistent Threats (APTs). These well-prepared adversaries launch prolonged intrusion campaigns to steal sensitive information. Intelligence-driven computer network defence (CND) techniques can help establish information superiority by creating a feedback loop which enables defenders to stay ahead and decrease the adversary's chances of success. As APTs continue to evolve, it is crucial to adopt an intelligence-based approach to mitigate vulnerability and the threat component of risk (Hutchins et al. N.D.).

According to a report by Vectra (N.D.), the recent SolarWinds attack was carried out with great expertise, successfully bypassing preventive measures such as network sandboxes, endpoint controls, and multifactor authentication (MFA). This was achieved using advanced techniques such as code signing, in-memory dropper, and stolen SAML session signing keys. This incident highlights the importance of using network detection and response as a more effective defence mechanism against such attacks.

SolarWinds (N.D.) emphasises the importance of proactive cybersecurity measures in today's digital age. One effective strategy is vulnerability assessment, which systematically identifies potential security flaws in applications, workstations, and the entire organisational network. This allows security teams to prioritise vulnerabilities based on risk levels for timely remediation - a crucial aspect of IT risk management. Here are the tools I would use for each phase:

- **Reconnaissance:** to identify potential vulnerabilities and threats, I would use network scanners, vulnerability scanners, and threat intelligence feeds (Imperva, 2022).

- **Weaponisation:** to protect against malicious software, I would use code signing certificates, code integrity verification tools, and application allowlisting solutions (Imperva, 2022).

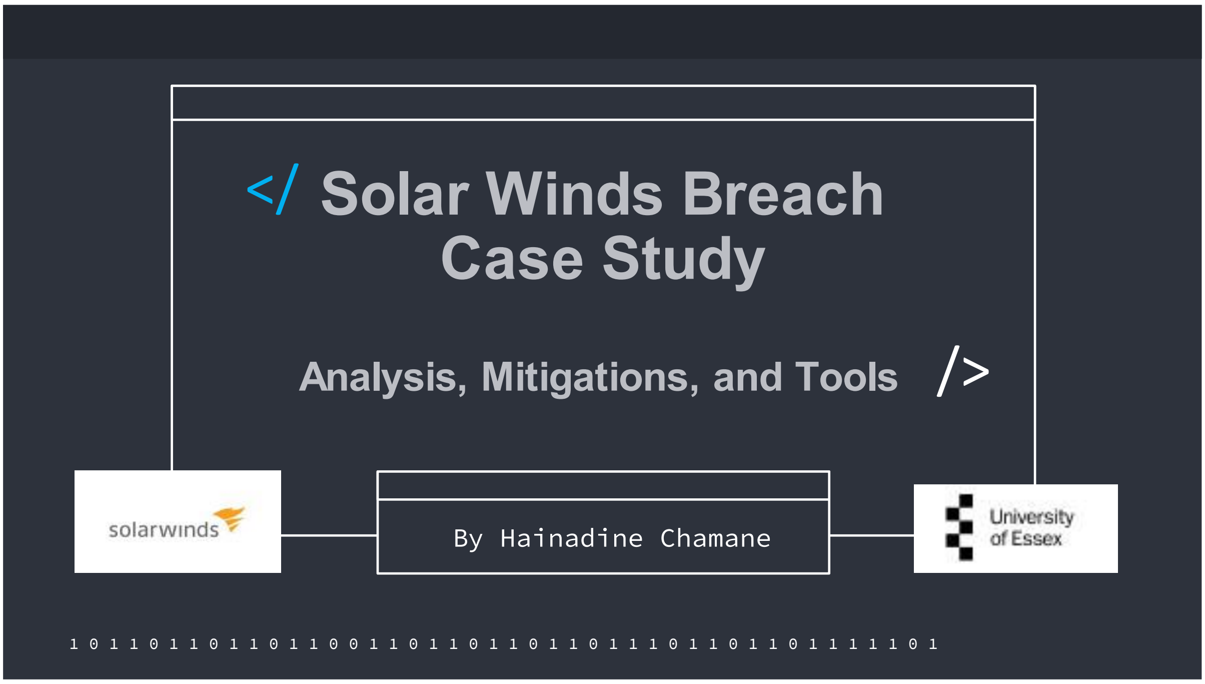
- **Delivery:** to detect and block malicious content, email filtering solutions, anti-malware solutions, and network traffic monitoring tools are necessary (Imperva, 2022).

- **Installation:** to prevent malware installation and identify vulnerabilities, I suggest using endpoint security solutions, application sandboxing tools, and vulnerability scanning tools (Miller, 2022).

- **Command and Control:** to disrupt communication between compromised systems and attackers, DNS sinkholing solutions, network traffic analysis tools, and IP reputation filtering solutions are essential (Gardiner et al. 2014).

- **Actions on Objective:** to detect and prevent data loss and identify suspicious activity, I recommend using data loss prevention (DLP) solutions, security information and event management (SIEM) systems, and security audit tools (IBM, N.D.).

4. **Create a slide deck presentation with up to 4 slides that discuss your solution. Be prepared to present it at the seminar this week.**

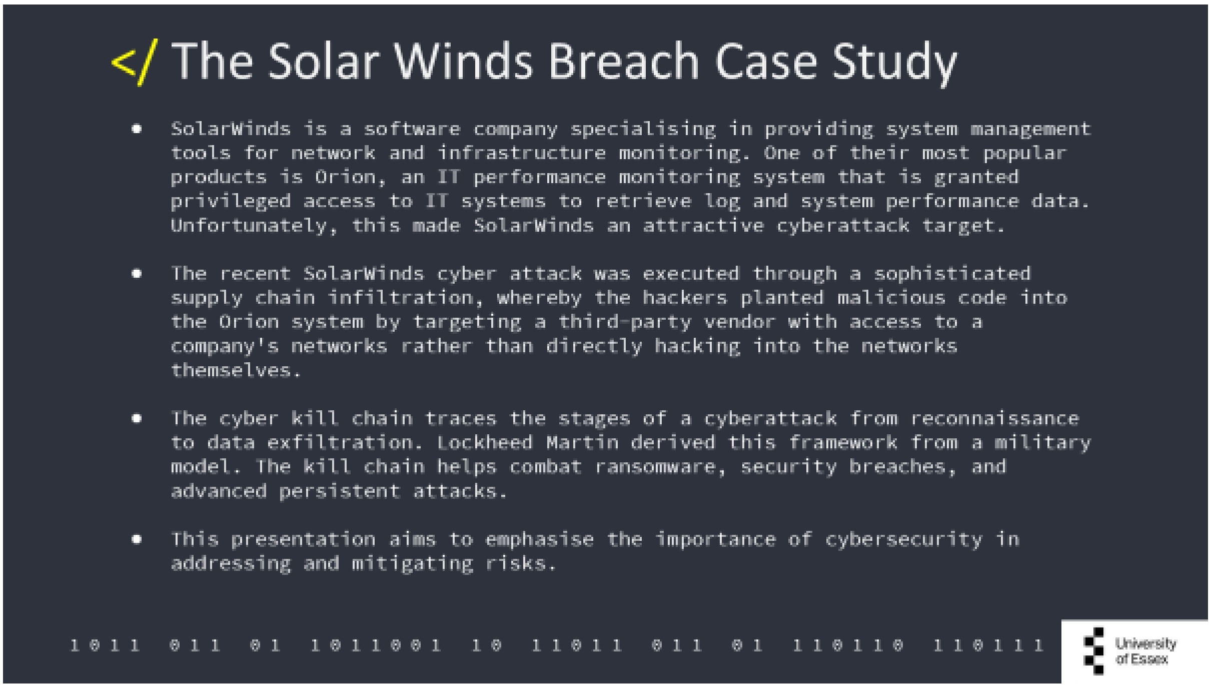


</ Solar Winds Breach Case Study

Analysis, Mitigations, and Tools />

By Hainadine Chamane

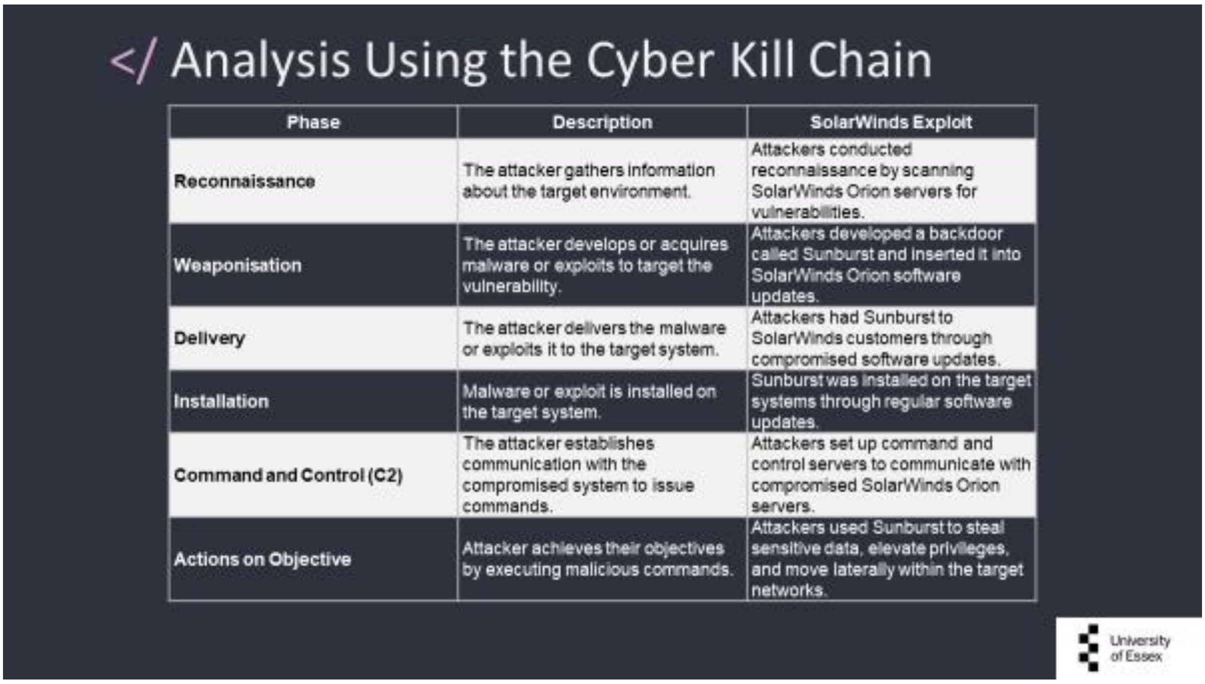
1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1



</ The Solar Winds Breach Case Study

- SolarWinds is a software company specialising in providing system management tools for network and infrastructure monitoring. One of their most popular products is Orion, an IT performance monitoring system that is granted privileged access to IT systems to retrieve log and system performance data. Unfortunately, this made SolarWinds an attractive cyberattack target.
- The recent SolarWinds cyber attack was executed through a sophisticated supply chain infiltration, whereby the hackers planted malicious code into the Orion system by targeting a third-party vendor with access to a company's networks rather than directly hacking into the networks themselves.
- The cyber kill chain traces the stages of a cyberattack from reconnaissance to data exfiltration. Lockheed Martin derived this framework from a military model. The kill chain helps combat ransomware, security breaches, and advanced persistent attacks.
- This presentation aims to emphasise the importance of cybersecurity in addressing and mitigating risks.

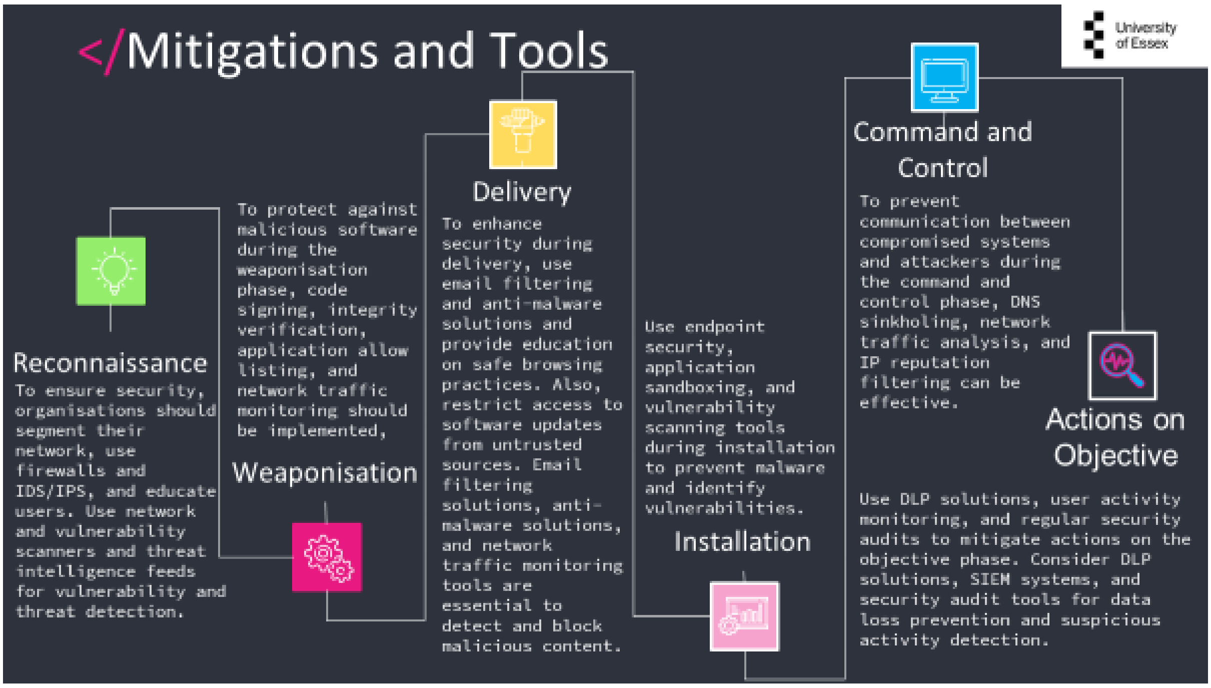
1011 011 01 1011001 10 11011 011 01 110110 110111



</ Analysis Using the Cyber Kill Chain

Phase	Description	SolarWinds Exploit
Reconnaissance	The attacker gathers information about the target environment.	Attackers conducted reconnaissance by scanning SolarWinds Orion servers for vulnerabilities.
Weaponisation	The attacker develops or acquires malware or exploits to target the vulnerability.	Attackers developed a backdoor called Sunburst and inserted it into SolarWinds Orion software updates.
Delivery	The attacker delivers the malware or exploits it to the target system.	Attackers had Sunburst to SolarWinds customers through compromised software updates.
Installation	Malware or exploit is installed on the target system.	Sunburst was installed on the target systems through regular software updates.
Command and Control (C2)	The attacker establishes communication with the compromised system to issue commands.	Attackers set up command and control servers to communicate with compromised SolarWinds Orion servers.
Actions on Objective	Attacker achieves their objectives by executing malicious commands.	Attackers used Sunburst to steal sensitive data, elevate privileges, and move laterally within the target networks.

University of Essex



</Mitigations and Tools

University of Essex

Reconnaissance

To ensure security, organisations should segment their network, use firewalls and IDS/IPS, and educate users. Use network and vulnerability scanners and threat intelligence feeds for vulnerability and threat detection.

Weaponisation

To protect against malicious software during the weaponisation phase, code signing, integrity verification, application allow listing, and network traffic monitoring should be implemented,

Delivery

To enhance security during delivery, use email filtering and anti-malware solutions and provide education on safe browsing practices. Also, restrict access to software updates from untrusted sources. Email filtering solutions, anti-malware solutions, and network traffic monitoring tools are essential to detect and block malicious content.

Installation

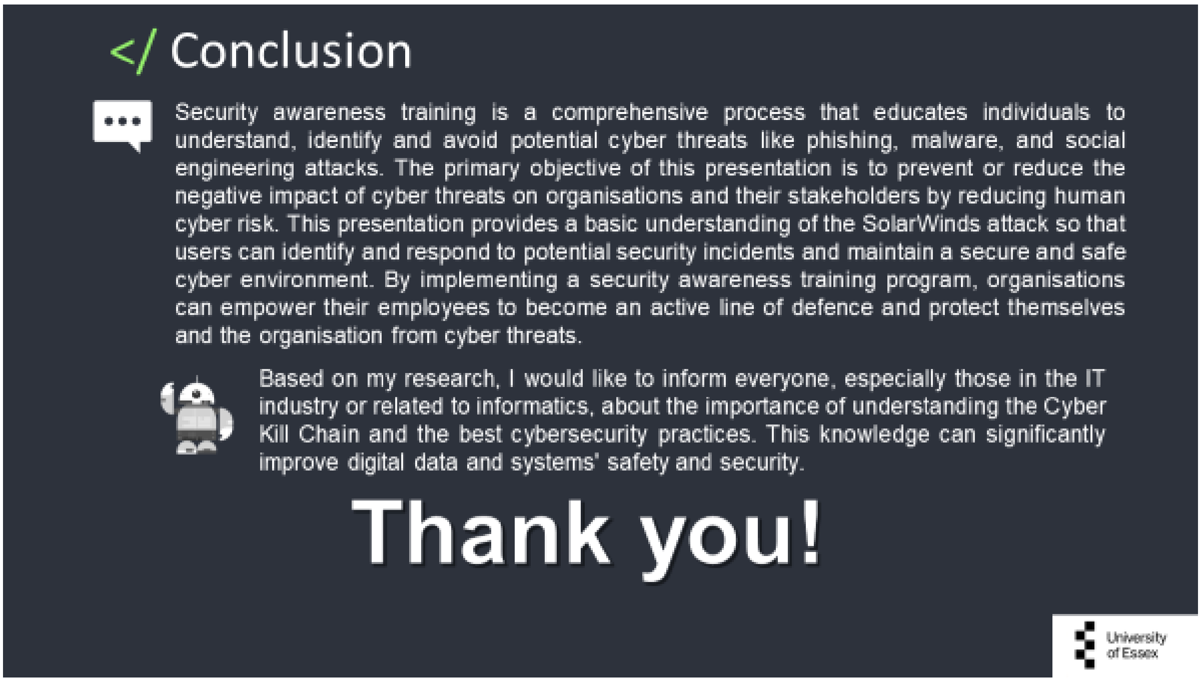
Use endpoint security, application sandboxing, and vulnerability scanning tools during installation to prevent malware and identify vulnerabilities.

Command and Control

To prevent communication between compromised systems and attackers during the command and control phase, DNS sinkholing, network traffic analysis, and IP reputation filtering can be effective.

Actions on Objective

Use DLP solutions, user activity monitoring, and regular security audits to mitigate actions on the objective phase. Consider DLP solutions, SIEM systems, and security audit tools for data loss prevention and suspicious activity detection.



</ Conclusion

Security awareness training is a comprehensive process that educates individuals to understand, identify and avoid potential cyber threats like phishing, malware, and social engineering attacks. The primary objective of this presentation is to prevent or reduce the negative impact of cyber threats on organisations and their stakeholders by reducing human cyber risk. This presentation provides a basic understanding of the SolarWinds attack so that users can identify and respond to potential security incidents and maintain a secure and safe cyber environment. By implementing a security awareness training program, organisations can empower their employees to become an active line of defence and protect themselves and the organisation from cyber threats.

Based on my research, I would like to inform everyone, especially those in the IT industry or related to informatics, about the importance of understanding the Cyber Kill Chain and the best cybersecurity practices. This knowledge can significantly improve digital data and systems' safety and security.

Thank you!

University of Essex

References:

- Oladimeji, S. & Kerner, S.M. (2023). *SolarWinds hack explained: Everything you need to know*. [online] WhatIs.com. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.
- Hackerone (N.D.). *Advanced Persistent Threat: Attack Stages, Examples & Mitigation*. [online] Available at: https://www.hackerone.com/knowledge-center/advanced-persistent-threats-attack-stages-examples-and-mitigation.
- Hutchins, E., Cloppert, M. & Amin, R. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. [online] Available at: http://gauss.ececs.uc.edu/Project4/Documents/kill-chain.pdf.
- Vectra (N.D.). *THREAT DETECTION Breaking down the SolarWinds breach: an inside look at the methods used THREAT REPORT SECURITY THAT THINKS*. [online] Available at: https://content.vectra.ai/hubfs/downloadable-assets/IndustryResearch_BreakingDowntheSolarWindsBreach.pdf [Accessed 16 Nov. 2023].
- SolarWinds (N.D.). *What Is a Vulnerability Assessment? - IT Glossary | SolarWinds*. [online] Available at: https://www.solarwinds.com/resources/it-glossary/vulnerability-assessment.
- Imperva (2022). *What is Vulnerability Assessment | VA Tools and Best Practices | Imperva*. [online] Learning Center. Available at: https://www.imperva.com/learn/application-security/vulnerability-assessment/.

- Miller, E. (2022). *Sifting Through Cybersecurity Solutions: Which Tools do I Really Need?* [online] Available at: https://www.bitlyft.com/resources/sifting-through-cybersecurity-solutions-which-tools-do-i-really-need [Accessed 16 Nov. 2023].
- Gardiner, J., Cova, M. and Nagaraja, S. (2014). *Command & Control Understanding, Denying and Detecting*. [online] *In collaboration with Lastline, Inc*. Available at: https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf.
- IBM (N.D.). *What is data loss prevention (DLP)?* | *IBM*. [online] Available at: https://www.ibm.com/topics/data-loss-prevention.

Reflection

Throughout this unit of study, I have had the opportunity to showcase my interpersonal skills and professional experience as an IT professional. In my ePortfolio, I will be sharing my research findings that answer the questions posed for each content of this unit.

Completing the research and delivering the presentation would have been highly challenging without my interpersonal skills and professional experience. For instance, my professional skills have been instrumental in comprehending crucial cybersecurity information, which I have been able to implement in practice.

When I created a PowerPoint presentation, my interpersonal skills came in handy as I shared it with my colleagues and requested their feedback and comments. This practice helped me improve the quality of my presentation and communication.

Communication skills were crucial in the collaborative discussion. My experiences inside and outside the academic environment have taught me that communication skills are vital in my personal and professional life.

For instance, an individual may possess comprehensive knowledge about a particular field. Still, if they cannot effectively communicate their ideas, knowledge, and feelings, their contribution to the organisation will remain compromised. Therefore, in my opinion, regardless of the industry, area, or type of organisation, communication skills are fundamental to an employee's success and should be considered a mandatory attribute.

My advanced professional experience as an IT professional has been an added advantage in this unit of study.