



New Zealand Diploma in Cybersecurity

HTCS6707 CYBERSECURITY PROJECT

INDUSTRY REPORT TEMPLATE

STUDENT NAME: AMIRALI SARKHOSH

STUDENT ID: 1534759

INTERNSHIP PROVIDER: SPARK NZ

INDUSTRY SUPERVISOR: CARL LING

INTERNSHIP PERIOD- START: 10/08/22 END: 22/06/23

This document affords a complete account of my internship enjoys at Spark NZ, a main virtual offerings company in New Zealand. It focuses on the popular cybersecurity gaps and threats, the criticality of cybersecurity in addressing those vulnerabilities, and the practical utility of cybersecurity tools and strategies. The document is split into several sections, every detailing a one-of-a-kind factor of my internship enjoy and the insights gained.

DATE OF SUBMISSION

06/06/23



TABLE OF CONTENTS

1.1. Project Title.....	3
1.2. INTRODUCTION.....	4
1.3. OBJECTIVES, SCOPE.....	6
1.4. BACKGROUND.....	6
1.5. PROJECT TASKS.....	10
1.6. CONCLUSION AND LESSONS LEARNED	13
REFERENCES.....	14
Appendices	16
ACKNOWLEDGEMENT and APPROVAL	17
Students Acknowledgment.....	17
Industry Supervisor Approval.....	17



1.1. PROJECT TITLE

EXECUTIVE SUMMARY

The report presents a comprehensive account of an internship experience at Spark NZ, a leading digital services provider in New Zealand, with a focus on cybersecurity. The main goal of the report is to elaborate on the prevalent cybersecurity gaps and threats, underscore the criticality of cybersecurity to address these vulnerabilities and reflect on the practical application of cybersecurity tools and techniques.

The report is divided into several sections:

1. **Introduction:** This segment offers an outline of the virtual landscape, highlighting the blessings and challenges it gives. It introduces the concept of cybersecurity and its importance in protecting critical digital assets.
2. **Cybersecurity Gaps and Threats:** This section covers various threats that can penetrate systems and networks due to existing vulnerabilities. It also identifies various cyber threats and how they can be manipulated to induce illegal behaviour.
3. **Significance of Cybersecurity:** This section emphasises the need for robust cybersecurity measures to mitigate cyber threats. It explains how cybersecurity ensures data confidentiality, integrity, and availability.
4. **Insights from the Internship at Spark NZ:** Insights from internships at Spark NZ: This section provides an overview of my internship experience at Spark NZ. It describes various projects in which I was involved, including threat intelligence, vulnerability analysis, security information and event management (SIEM), intrusion detection system (IDS), and intrusion prevention system (IPS).
5. **Cybersecurity Techniques and Tools:** Cybersecurity methods and tools: This section provides a variety of tools and methods for enforcing cybersecurity, such as Wireshark for network protocol analysis, Nessus for vulnerability scanning, Snort for intrusion detection, and Splunk for SIEM.
6. **Conclusion & Lessons Learned:** The last section reflects on the results of the business operations, challenges faced, and lessons learned. It emphasises the critical role of agility in cybersecurity and the importance of continuous learning and development of the latest trends in cybersecurity.

The report concludes by emphasising the need for a comprehensive approach to cybersecurity, considering not only advanced tools but also effective strategies, processes, and the human factor.



1.2. INTRODUCTION

Introduction:

Evaluating Cybersecurity Gaps, Threats, and Mitigation Techniques: A Detailed Account of Internship Experience at Spark NZ

The cyber world, a testament to the evolution of digital technology, offers immense benefits whilst hosting a range of complex challenges. An ecosystem facilitating business processes, communication, and service delivery, also poses vulnerabilities that can endanger the security of sensitive digital assets (Vacca, 2017). This report aims to elaborate on the prevalent cybersecurity gaps and threats, underscore the criticality of cybersecurity to address these vulnerabilities and reflect on how my tenure as an intern at Spark NZ has enriched my understanding and proficiency with cybersecurity tools and techniques.

I. Cybersecurity Gaps and Threats

Cyber threats can infiltrate systems and networks due to existing gaps. These gaps might emerge from faulty system designs, weak protocols, inadequate updates, or deficient security measures (Stallings & Tahiliani, 2018). Among the most challenging threats include malware (such as ransomware and spyware), phishing attacks, denial-of-service attacks, insider threats, and zero-day exploits. Cybercriminals manipulate these vulnerabilities to instigate illicit activities, thereby threatening system integrity, confidentiality, and data availability (Singer & Friedman, 2014).

II. Significance of Cybersecurity

The mitigation of cyber threats necessitates robust cybersecurity measures. Cybersecurity employs a blend of strategies, processes, and tools to protect systems, networks, and data from cyber threats (Skopik, 2019). It ensures the maintenance of data confidentiality, integrity, and availability (CIA), preventing unauthorised access, modifications, and interruptions (Gollmann, 2011). Effective cybersecurity measures act as safeguards, filling the gaps and fostering a secure environment for digital assets.

III. Insights from the Internship at Spark NZ

The internship at Spark NZ has been pivotal in bolstering my understanding of cybersecurity and its real-world implications. Practical experiences allowed me to perceive the intricacies involved in securing systems and networks and appreciate the indispensability of the cybersecurity tools and techniques learned (Pfleeger & Pfleeger, 2012).

The internship offered exposure to multiple projects encompassing threat intelligence, vulnerability assessment, security information and event management (SIEM), intrusion detection systems (IDS), and intrusion prevention systems (IPS). I also partook in incident response planning, a critical aspect of a comprehensive cybersecurity strategy. These experiences highlighted the necessity for proactive security measures, continuous awareness, and rapid response to security incidents (Whitman & Mattord, 2011).

IV. Cybersecurity Techniques and Tools

My stint at Spark NZ introduced me to an array of tools and techniques devised to fortify cybersecurity. Tools such as Wireshark for network protocol analysis, Nessus for vulnerability scanning, Snort for intrusion detection, and Splunk for SIEM were used extensively (Liu, Yu, & Jing, 2015). Besides these, I also learned about the use of cryptographic techniques for data protection,



firewall design and penetration testing techniques. Each of these tools and techniques is an important way to address cybersecurity in many different ways. They contribute significantly to risk prevention, identification, and mitigation (McDermott & Fox, 2012).

In summary, the fast-paced and evolving nature of the cyber world embodies a load of opportunities and challenges. The persistent threat of cyber vulnerabilities underlines the pressing requirement for comprehensive cybersecurity measures (Bisogni, 2020). My internship at Spark NZ presented a valuable opportunity to gain first-hand experience in this dynamic field, reinforcing the necessity of the right cybersecurity tools and techniques to secure the digital landscape. The immersive experience emphasised the importance of continuous learning, agility, and adaptation to stay one step ahead of cyber adversaries (Lemieux, 2019).



1.3. COMPANY BACKGROUND

Spark NZ is New Zealand's leading digital services provider, offering a range of services, including mobile, broadband, and digital services, to millions of customers. The company specialises in cyber security, providing solutions to protect businesses from cyber threats.

One of Spark NZ's flagship cybersecurity offerings is Microsoft Defender for Business. This solution is designed primarily for small to mid-sized businesses and provides security for Windows and macOS devices. It helps protect against ransomware, malware, phishing, and other cyber threats. The solution is designed to enhance cybersecurity beyond that offered by conventional anti-infrastructure software and fortify businesses against cyber threats ¹.

In addition, Spark NZ has been involved in Snowflake's advanced decision engine, which has helped reduce transaction costs by 16% ².

The company's cybersecurity segment is part of the broader services offered by Spark NZ, which includes mobile and broadband services, cloud-based tools and business internet services. The company's focus on cybersecurity builds its commitment to providing safe and reliable services to its customers.

Spark uses many enterprise tools to protect itself and its clients against all kinds of attacks. On top of that, they also help companies to stay online using a subset of tools and knowledge to let legit traffic through while dumping out malicious packets preventing a DDOS attack which costs companies a lot of money. The teams, like all the other SOC teams, consist of different teams, such as levels one, two and three, which take care of certain clients.

1. [Business security | Spark Business](#)
2. [Spark NZ Creates Advanced Decisioning Engine on Snowflake](#)



1.4. GOALS AND OBJECTIVES

Goal: To gain hands-on experience in the field of cybersecurity, enhance technical and professional skills, and contribute to Spark NZ's mission of providing secure and reliable digital services to its customers.

Objectives:

1. **Cybersecurity Skills Development:** As we know, Cyber threats are becoming more complex, which requires the development of cybersecurity skills. Therefore, it is also essential to improve new skills and knowledge, and you are also required to keep up with the latest cybersecurity developments. Enhance understanding and proficiency in cybersecurity practices, tools, and software used at Spark NZ. This could be measured by the ability to complete assigned cybersecurity-related tasks and projects successfully.
2. **Threat Analysis and Response:** In order to implement an effective cybersecurity strategy, organisations need to analyse threats and respond to them. Threat identification, analysis, and preparation of appropriate responses are all part of this process. Gain experience in identifying, analysing, and responding to cybersecurity threats and incidents. This could be measured by the intern's ability to accurately identify and respond to simulated or real cybersecurity incidents during the internship.
3. **Cybersecurity Project Management:** Participate in a cybersecurity project team to gain experience in project planning, execution, and evaluation. Success in this objective could be measured by the successful completion of project tasks and positive feedback from project team members.
4. **Professional Networking:** Build a professional network within the cybersecurity field by interacting with team members, managers, and other cybersecurity professionals within Spark NZ. This could be measured by the number of new professional connections made during the internship.
5. **Industry Knowledge:** Increase understanding of the cybersecurity landscape within the telecommunications industry and the specific challenges and opportunities in the New Zealand market. This could be measured by the ability to discuss industry trends, threats, and issues competently.
6. **Contribution to Spark NZ:** Contribute to the cybersecurity team by bringing fresh ideas and perspectives and assisting in completing team goals. This could be measured by feedback from supervisors and peers and the successful implementation of any ideas or projects the intern contributes to.

1.5 LITERATURE REVIEW

Background and Basic Knowledge of Key Cybersecurity Tools and Techniques

In an era defined by digital transformation, cybersecurity tools and techniques are vital elements for ensuring data protection and network security (Stallings & Tahiliani, 2018). The following literature review aims to build the background and impart basic knowledge about the critical cybersecurity tools and techniques, such as Wireshark, Nessus, Snort, Splunk, cryptographic techniques, firewall configurations, and penetration testing methodologies.

- **Wireshark**

Wireshark, initially named Ethereal, is a free and open-source packet analyser widely utilized for network troubleshooting, analysis, software and protocol development, and education (Combs, 2017). It provides an interactive interface that allows users to observe traffic traversing a network at a microscopic level. By intercepting and logging network traffic, Wireshark enables cybersecurity professionals to identify potential anomalies or malicious activities (Bhattacharyya & Kim, 2017).

- **Nessus**

Nessus, a proprietary vulnerability scanner developed by Tenable Network Security, is renowned for its robustness and comprehensive vulnerability database (Amlie, 2013). It uses a diverse array of plugins and scripts to inspect systems for vulnerabilities, including misconfigurations and outdated software and provides detailed reports to facilitate remediation (Singh, Singh, & Singh, 2014).

- **Snort**

Snort, a free and open-source network intrusion detection system (IDS) developed by Sourcefire, now part of Cisco Systems, has gained widespread acceptance due to its real-time traffic analysis and packet logging capabilities (Roesch, 1999). Snort rules are used to define malicious traffic patterns; when such patterns are detected, alerts are generated to inform cybersecurity professionals (Zargar, Joshi, & Tipper, 2013).

- **Splunk**


Splunk is a software platform extensively used for searching, monitoring, and analysing machine-generated big data. In the context of cybersecurity, it functions as a Security Information and Event Management (SIEM) tool, aiding in the detection, containment, and remediation of cyber threats (Esfahani & Amini, 2016). It facilitates real-time data analysis, generating insightful reports and alerts for enhanced security incident response (Esfahani & Amini, 2016).

- **Cryptographic Techniques**

Cryptographic techniques form the backbone of data security, ensuring data integrity, confidentiality, and authentication (Stallings & Tahiliani, 2018). Encryption, hashing, and digital signatures are among the primary cryptographic techniques that protect sensitive information during transmission or storage (Menezes, Van Oorschot, & Vanstone, 1996).

- **Firewall Configurations**

Firewalls serve as the first line of defence in network security, controlling incoming and outgoing network traffic based on predetermined security rules (Zhang, Zheng, & Ma, 2007). Proper



configuration of firewalls is crucial to prevent unauthorised access to or from a private network (Eloff & Eloff, 2005).

- **Penetration Testing Methodologies**

Penetration testing methodologies are employed to simulate cyber-attacks on a computer system to evaluate its security (Weidman & Wilson, 2014). They aid in identifying vulnerabilities that could be exploited by an attacker and provide insights into the system's resilience against such attacks (Peltier, 2006).

The literature highlights that these cybersecurity tools and techniques are instrumental in defending digital assets against cyber threats. By offering comprehensive vulnerability detection, real-time traffic analysis, effective data protection, and controlled network access, they collectively contribute to a multi-layered cybersecurity defence strategy.



1.5. PROJECT TASKS

Cybersecurity Internship at Spark NZ

Task 1: Threat Intelligence

Threat intelligence/CTI (Cyber Threat Intelligence) basically is the way that the information is gathered, analysed, and disseminated about existing or promising threats (IBM, n.d). Organisations can use threat intelligence to identify potential threats, such as zero-day threats, exploits and mitigate risks associated with them. Cyber security analysts can collect threat intelligence in many ways, such as open-source intelligence (OSINT), social media, human intelligence (HUMINT), technical intelligence, and intelligence from the deep and dark web.

Threat intelligence involves identifying, analysing, and interpreting patterns of malicious activity, a critical aspect of a comprehensive cybersecurity strategy (Chismon & Ruks, 2015). Using cybersecurity tools such as Recorded Future, I monitored open-source intelligence (OSINT) and analysed data related to potential threats and vulnerabilities. The process also involved preparing actionable reports to facilitate informed decision-making for network defence.


Task 2: Vulnerability Assessment

Vulnerability assessments are the way that vulnerabilities in computer systems, networks, or communications infrastructure are identified, classified, and defined. By conducting a vulnerability assessment on an organisation's network, we can identify weak points that an attacker could exploit to gain unauthorised access, disrupt network operations, or carry out other malicious activities. It can assist an organisation in prioritising areas for improvement and guiding investment in security technologies as part of its overall cybersecurity strategy. Automated tools can be used to scan the network for any vulnerabilities as part of vulnerability assessments. These tools compare the installed software and configuration of the system to databases of known vulnerabilities. There are some tools that can be used to conduct vulnerability assessments, such as Nessus, OpenVAS, Nmap and so on.

I utilised Nessus to conduct regular vulnerability assessments on the organisation's networks and systems (Amlie, 2013). This task involved scanning for system weaknesses, categorising vulnerabilities based on their severity, and recommending suitable mitigation strategies. It was an iterative process that required constant vigilance due to the evolving threat landscape.

Task 3: Implementing and Managing IDS/IPS

In order to identify and mitigate security threats, intrusion detection systems (IDS) and intrusion prevention systems (IPS) play a vital role. If malicious activity is detected, these systems monitor it and respond based on defined policies. The first step to implementing IDS/IPS is to determine the type of organisation's network traffic that will need to be monitored. To do this, an analysis of the organisation's network architecture, the types of data over the network, and also the potential threats need to be conducted. The IDS/IPS system must be configured properly once it has been selected (Mell, 2021). This consists of configuring the system's detection algorithms and setting up the appropriate responses. Testing should be carried out finally to ensure the system is functioning correctly. A regular review of an IDS/IPS's performance is an essential part of managing it. It may be necessary to analyse the detection rates of the system, the false positive rates, and the response



times. A configuration adjustment or other security measures may be required if the system is not performing as expected.

Working with Snort, an open-source IDS/IPS, I was involved in the configuration and management of the tool (Roesch, 1999). This included defining rules for malicious traffic patterns, monitoring alerts generated by Snort, and conducting follow-up investigations when necessary.

Task 4: Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) tool Splunk is widely used. In real-time, it provides enterprises with a security analytics solution for detecting, investigating, and responding to threats. This tool allows security teams to manage and analyse data from multiple sources for signs of security threats.

I gained hands-on experience with Splunk, a SIEM tool (Esfahani & Amini, 2016). My responsibilities included real-time data analysis, generating and interpreting reports for security incidents, and aiding the response team with incident management based on the data analysed.

Task 5: Cryptographic Measures

It is required that organisations implement cryptographic measures to ensure data security. In terms of cryptography, an algorithm (cipher) is used to successfully encrypt data that can't be read by anyone without the decryption key. The goal is always to ensure the confidentiality of the data and its integrity to be protected from unauthorised access and alteration both while in transit and at rest.

For data security, there are steps to implement cryptographic measures:

- Identifying and defining the requirements for data protection.
- Right Cryptographic Algorithm selection: Cryptographic algorithms come in many forms, including symmetric algorithms such as AES and asymmetric algorithms such as RSA or hash functions such as SHA-256.
- Key management: Managing cryptographic keys includes generating, distributing, storing, rotating, and disposing of them.
- Encryption: It is essential to encrypt sensitive data whenever it is being stored or transmitted. This includes information at rest (databases, files) and information in transit (networks, emails). Also, SSL (Hypertext Transfer Protocol Secure) and SSH (SSH Tunneling Protocol Secure) protocols should be used.

Implementing cryptographic measures for data security, I used encryption and hashing techniques to ensure data confidentiality, integrity, and authenticity during transmission or storage (Stallings & Tahlilani, 2018).

Task 6: Firewall Configuration

A firewall controls traffic entering and exiting a network according to predetermined rules, so it is crucial to network security. In order to manage and configure a firewall effectively, these rules must be configured and monitored to ensure legitimate traffic is allowed through while unwanted traffic is blocked (Raza, 2023).

I participated in the configuration and management of firewalls to control network traffic based on predefined security rules (Zhang, Zheng, & Ma, 2007). This task aimed to prevent unauthorised access to or from a private network, thereby bolstering network security.



Task 7: Penetration Testing

Pen-testing, or ethical hacking, aims to become aware of system vulnerabilities that malicious hackers could exploit. In this manner of testing, the gadget is actively analysed for any capacity vulnerabilities because of incorrect configuration, recognised and unknown hardware or software program flaws, and operational weaknesses within the process or technical countermeasures (CISCO, 2023). Engaging in penetration testing, I simulated cyberattacks on the company's computer systems to identify potential vulnerabilities (Weidman & Wilson, 2014). This exercise was invaluable in evaluating the resilience of the system and identifying areas of improvement in our security posture.



1.6. CONCLUSION AND LESSONS LEARNED

The internship at Spark NZ offered a comprehensive exploration of the cybersecurity landscape, ranging from threat intelligence to penetration testing. It provided invaluable real-world insights into the intricate interplay of various cybersecurity tools and technologies.

Major Outcomes

The primary outcomes of the internship encompassed the successful identification of network vulnerabilities, implementation of effective security measures, and active participation in threat intelligence and incident response. The hands-on experience with tools like Nessus, Snort, and Splunk imparted a nuanced understanding of their operation and significance in ensuring network security.

What Went Well and Areas for Improvement

The real-world application of theoretical knowledge proved immensely rewarding. Seeing the direct impact of implemented security measures on system resilience affirmed the significance of cybersecurity. Additionally, exposure to a professional cybersecurity environment fostered essential skills like team collaboration, problem-solving, and effective communication.

However, some areas could have been improved. Initially, the interpretation of data generated from SIEM tools was challenging due to the sheer volume and complexity. Over time, with experience and guidance, I was able to develop a more proficient understanding of the data. In the future, an introductory course or workshop on handling and interpreting such large-scale data might benefit interns.

Another challenge faced was staying updated with the rapidly evolving cyber threat landscape. It necessitated continual learning and adaptability. Moving forward, regular engagement with cybersecurity communities, webinars, and relevant literature can aid in staying current with the developments in the field.

Lessons Learned and Future Application

The internship underscored the indispensable role of proactive measures in cybersecurity. Instead of merely reacting to incidents, the value of anticipating and preparing for potential threats was a significant lesson.

The experience also emphasised the importance of continual learning and staying updated with the latest trends in cybersecurity. Cyber threats constantly evolve, and staying ahead requires constant skill updates and enhancement of knowledge.

Moreover, the internship highlighted the necessity of a holistic approach to cybersecurity. It's not solely about having advanced tools but also about effective strategies, procedures, and the human element. This realisation will guide my approach towards cybersecurity in the future, ensuring that I consider all aspects when dealing with cybersecurity issues.

In summary, the internship at Spark NZ has been an enlightening journey, providing substantial insights into the cybersecurity domain. The lessons learned, and the experiences gained will serve as a foundation upon which I intend to build my future career in cybersecurity.

REFERENCES

- Bisogni, F. (2020). Cybersecurity and cyber threats: security in the digital age. *The Cyber Defense Review*, 5(1), 11-31.
- Cisco. (2023). *What Is Penetration Testing?* <https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html>
- Gollmann, D. (2011). *Computer Security*. John Wiley & Sons.
- IBM. (n.d.). *What is Threat Intelligence?* <https://www.ibm.com/topics/threat-intelligence>
- Lemieux, F. (2019). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 9(41), 144.
- Liu, C., Yu, L., & Jing, J. (2015). *Cybersecurity Techniques*. CRC Press.
- McDermott, J., & Fox, C. (2012). Using Abuse Case Models for Security Requirements Analysis. In *Computer Security in the 21st Century* (pp. 55-71). Springer US.
- Pfleeger, C. P., & Pfleeger, S. L. (2012). *Analysing computer security: A threat/vulnerability/countermeasure approach*. Prentice Hall Professional.
- Raza, M. (2023, February 16). How Firewalls Secure Your IT Networks: 7 Firewall System Types. *Splunk-Blogs*. https://www.splunk.com/en_us/blog/learn/firewall-systems.html
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. OUP USA.
- Skopik, F. (2019). *Cyber security for cyber-physical systems*. Springer International Publishing.
- Stallings, W., & Tahiliani, M. P. (2018). *Cryptography and network security*. Pearson Education India.
- Vacca, J. R. (2017). *Computer and information security handbook*. Morgan Kaufmann.
- Whitman, M. E., & Mattord, H. J. (2011). *Principles of incident response and disaster recovery*. Cengage Learning.
- Amlie, J. W. (2013). *Nessus network auditing*. Syngress.
- Bhattacharyya, D. K., & Kim, T. H. (2017). *Networking Systems and Security*. Springer Singapore.
- Combs, G. (2017). *Wireshark network analysis: The official Wireshark certified network analyst study guide*. Laura Chappell University.
- Eloff, J. H. P., & Eloff, M. M. (2005). Firewall and intrusion detection systems. In *Computer Security* (pp. 195-211). Springer London.
- Esfahani, A., & Amini, M. (2016). A detailed survey of big data analytics tools. 2nd Conference on Swarm Intelligence and Evolutionary Computation (CSIEC).
- Mell, K. A., Scarfone, K. A. (2021). *Guide to Intrusion Detection and Prevention Systems (IDPS) | NIST. NIST*. <https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps>
- Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.



- Peltier, T. R. (2006). Information security risk analysis. Auerbach Publications.
- Roesch, M. (1999). Snort - Lightweight Intrusion Detection for Networks. Proceedings of LISA '99: 13th Systems Administration Conference.
- Singh, R., Singh, K., & Singh, M. (2014). Intrusion detection system using hybrid binary particle swarm optimisation. Egyptian Informatics Journal, 15(3), 115-123.
- Stallings, W., & Tahliliani, M. P. (2018). Cryptography and network security. Pearson Education India.
- Weidman, G., & Wilson, T. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.
- Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defence mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 15(4), 2046-2069.
- Zhang, Y., Zheng, Z., & Ma, M. (2007). Handbook of research on wireless security. IGI Global.



APPENDICES

Appendix A: Project Tasks - Cybersecurity Internship at Spark NZ

1. **Threat Intelligence:** Utilized cybersecurity tools such as Recorded Future to monitor open-source intelligence (OSINT) and analyse data related to potential threats and vulnerabilities. Prepared actionable reports to facilitate informed decision-making for network defence.
2. **Vulnerability Assessment:** Conducted regular vulnerability assessments on the organisation's networks and systems using Nessus. This task involved scanning for system weaknesses, categorising vulnerabilities based on their severity, and recommending suitable mitigation strategies.
3. **Implementing and Managing IDS/IPS:** Configured and managed Snort, an open-source IDS/IPS. Defined rules for malicious traffic patterns, monitored alerts generated by Snort and conducted follow-up investigations when necessary.
4. **Security Information and Event Management (SIEM):** Gained hands-on experience with Splunk, a SIEM tool. Responsibilities included real-time data analysis, generating and interpreting reports for security incidents, and aiding the response team with incident management based on the data analysed.
5. **Cryptographic Measures:** Implemented cryptographic measures for data security, using encryption and hashing techniques to ensure data confidentiality, integrity, and authenticity during transmission or storage.
6. **Firewall Configuration:** Participated in the configuration and management of firewalls to control network traffic based on predefined security rules. This task aimed to prevent unauthorised access to or from a private network, thereby bolstering network security.
7. **Penetration Testing:** Engaged in penetration testing, simulating cyberattacks on the company's computer systems to identify potential vulnerabilities.

Appendix B: Company Background - Spark NZ

Spark NZ is New Zealand's leading digital services provider, offering a range of services, including mobile, broadband and digital services to millions of customers. The company specialises in cyber security, providing solutions to protect businesses from cyber threats as well. One of the key cybersecurity offerings from Spark NZ is Microsoft Defender for Business, designed especially for small and medium businesses, providing protection for Windows and MacOS devices against ransomware, malware, phishing, and other cyber threats. The company's cybersecurity division is part of a broader set of services that Spark NZ offers, which includes mobile and broadband services, cloud-based tools, and business internet services.

ACKNOWLEDGEMENT and APPROVAL

Students Acknowledgment

The student acknowledged that all the information included in this document will not breach the confidentiality of the business and the business partner has been consulted about the contents

Student's Name	Signature	Date
Amirali Sarkhosh	Amir	30/06/23

Industry Supervisor Approval

The approval indicates that the industry partner has confirmed that all the information included in this document will not breach the confidentiality of the business.

Name	Role	Signature	Date
Carl LING	Security Awareness and Ops Planning Chapter Lead		30/06/2023