Report On

TECH OPERATION INTERN OF MeghOps Ltd.

By

Maria Tasnim Shifa
21301711

An Internship submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
BRAC University
October 2025

Declaration

It is hereby declared that

1. The report submitted is my/our own original work while completing degree at Brac University.
2. The report does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The report does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Maria Tasnim Shifa
21301711

Approval

The Internship titled "Tech Operation Intern of MeghOps Ltd. " submitted by

1. Maria Tasnim Shifa (21301711)

of Summer , 2025 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science in 10 October, 2025.

Examining Committee:

Supervisor:
(Member)

Mr. Tamkin Mahmud Tan
Lecturer
Department of Computer Science Engineering
BRAC University

Thesis Coordinator:
(Member)

Dr. Md. Golam Rabiul Alam, PhD
Professor
Department of Computer Science Engineering
BRAC University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD
Chairperson and Associate Professor
Department of Computer Science and Engineering
BRAC University

Abstract

During my internship at MeghOps Ltd., I had the opportunity to observe and assist with various technical and operational tasks within the cybersecurity field. My role primarily involved supporting day-to-day activities such as preparing technical documents, troubleshooting issues, and learning about security processes like vulnerability assessments and penetration testing. While much of my work was observationbased, I faced several challenges that tested my adaptability and problem-solving skills.

Some of these challenges included working with tools and processes that were completely new to me, understanding technical workflows without much prior guidance, and learning how to coordinate effectively with team members. At times, I struggled to find the right approach to certain problems due to limited practical knowledge, which required me to do extra research and think critically. Managing deadlines while balancing learning curves was another challenge that made me grow professionally. These experiences taught me perseverance and the importance of continuous learning.

Through these challenges, I realized that hands-on problem-solving is one of the most important skills a student can develop. I believe that if students are taught more practical techniques in class to deal with real-life problems, adapting to workplace challenges would be much easier and more efficient. In general, the internship was a beneficial experience, as it allowed me to close the gap between theory and practice, as well as to enhance my technical performance, collaboration, communication, and flexibility.

Dedication

I put all my efforts and struggle in my education process in my beloved parents whose love, support, and encouragement have been my most important strength. My success would be meaningless without them. I am very thankful for their guidance and sacrifices which moulded my character to the present day.

I would also like to dedicate this internship report to the respectable supervisor, Tamkin Mahmud Tan, who helped and mentored me during this internship. I have benefited significantly by his wise guidance, motivation, and support to work on my abilities and become a better and confident professional.

Acknowledgement

To begin with, it is all praise to the Almighty Allah that I was in a position to accomplish my internship amicably. I am also very grateful to have had a supervisor Tamkin Mahmud Tan, who guided and supported me during my time as an intern. Finally, I express my heartfelt gratitude to my parents for their constant encouragement and prayers, which have brought me to the verge of graduation.

Company Vetting System

MeghOps

House 63, Road 25/A, Banani,
Dhaka-1213, Bangladesh.

Date 01.10.2025

Company Vetting Statement

This is to certify that MeghOps Ltd. has reviewed and vetted the internship report submitted by Maria Tasnim Shifa, an intern in the Tech Operation Department.

The report does not contain any confidential or internal information related to MeghOps Ltd. and does not compromise the company's security or operational integrity in any way.

MeghOps Ltd.

Rifat Hassan
Chairman, MeghOps.

P: +880 17 9800 0055 M: reachus@meghops.io W: www.meghops.io

Innovating Cyber Horizons

Figure 1: An image of a Vetting System

Table of Contents

Chapter 1

1.1 Overview of Internship

1.1.1 Student Information

- **Name:** Maria Tasnim Shifa
- **ID:** 21301711
- **Program:** Bachelor of Computer Science and Engineering (CSE)
- **Major:** Computer Science and Engineering (CSE)

1.1.2 Internship Information

- **Period:** 1st September 2024-31st March 2025
- **Company Name:** MeghOps Ltd.
- **Department:** Tech Operation
- **Address:** House 63, Road 25/A, Banani, Dhaka-1213, Bangladesh

1.2 Preamble

University education provides a strong foundation of theoretical knowledge, but internships give students the chance to experience real-world professional environments. They allow students to apply what they have learned in the classroom to practical tasks, develop technical and interpersonal skills, and better understand workplace dynamics. Such experiences also help in building confidence and preparing for future careers.

I had a chance to do my internship in MeghOps Ltd. and was guided by my industry supervisor Rifat Hassan, who was the Chairman of MeghOps. I am lucky to be able to work in such a professional setting and to be exposed to real projects. Tamkin Mahmud Tan, my university supervisor, helped me with my internship and was ok

with it provided that it fitted my academic objectives.

This BRAC University internship was to offer students practical working experience in the workplace, assist the students in relating their academic knowledge to practical issues, and furnishing them with future professional challenges and career development.

Generally, this internship was a priceless experience that enabled me to develop both, technically and professionally and provided me with a better picture of how I can use my education in a practical setting [**In case of internship**] Introduce the Product

1.3 Objective

It is a report, which was written after an internship experience in MeghOps Ltd. and the report has been submitted as a part of Computer Science and Engineering course in BRAC University. The ultimate objective of this report is to fulfil the academic requirement of the completion of the internship program.

Besides, the report will also aim to provide a general overview of MeghOps Ltd., Work environment, projects and operation. It is as well a reflection of my personal learning process, my challenges, the competencies and the professional development which I gained during the internship. The paper can also serve as a decent source of information to anyone seeking to have a brief understanding of MeghOps Ltd. and my contributions in the internship period.

1.4 Information Sources

The details contained in this report have been primarily collected through observation and experience during my internship at meghops Ltd. and the interaction with people. The company official resources were also used to gather additional information.

1.5 Document Overview

This report has brought to focus my internship experience at MeghOps Ltd. wherein I have been able to highlight the activities that I was engaged in, some of the challenges that I encountered, and how I managed to overcome them. It also looks back at the skills that I had gained within the internship period, both in terms of technical and professional. Overall, the paper will include a description of MeghOps Ltd. and include the information about my individual accomplishments and personal development during the internship.

Chapter 2

2.1 Company Overview

MeghOps Ltd. [4] is one of the most renowned cybersecurity firms in Bangladesh, and it offers the finest digital security services to the firms of other sectors. The company, through its platform Axiler [5], provides advanced cyber defense solutions. Some of the services offered by the company include Web Application Firewalls (WAF), and Vulnerability assessment and penetration testing (VAPT) services as well as Cloud Security and cybersecurity advisory services. It aims at assisting organizations to secure their digital resources, make themselves more robust against cyber attacks, and carry out business operations without hustles.

MeghOps liaises with the business, financial and technology agencies to develop custom security systems that address the needs of each. The company has acquired technical and operational knowledge fronts and is therefore not only concerned with system protection, but also performance and efficiency is being boosted with the provision of secure solutions to the workplace.

To continue being competitive in the fast changing digital world, MeghOps invests in innovation development, research and modern technology implementation. It also uses other global services such as Google, Microsoft, and AWS in an attempt to enhance its services. MeghOps will also allow its customers to comfortably transact business in the contemporary globalized world through the delivery of innovative tools and a great culture of security consciousness.

Figure 2.1: MeghOps Ltd. Company Overview

2.2 First day of joining

My internship in MeghOps Ltd. commenced with an orientation into the company atmosphere and culture of work. I was invited to join the Tech Operations group on the first day, and given an introduction to the industry supervisor, Mr. Rifat Hassan, who was the Chairman of the MeghOps Ltd. My scope of apparently doing the internship and the kind of work I would be watching and facilitating in the course of the program was also briefed to me.

To provide the background on the HR and the technical team, I was offered the overview of the services of the company, and their focus on the cybersecurity solutions, including the vulnerability assessment, penetration testing, and web application firewalls. I was also exposed to some of the internal tools that were employed in the management and documentation of tasks, and they allowed me to comprehend the workflow at the company.

Though the orientation and learning of the basics were dominated during the first day, I had a clear idea of what was ahead of me regarding the working environment. My experience of learning more about my work mate and how work was cooperative in the workplace also helped me feel comfortable and encouraged me to take the first steps as an intern in Tech Operations.

Figure 2.2: First Day at MeghOps Ltd.

2.3 Products And Customers Overview

MeghOps Ltd. is a company that provides a variety of cybersecurity products and services aimed at protecting business organizations against cyber threats and improving their efficiency at work. Their major products are:

- **Cloud Security Suite** - Incorporates visibility, tracking, and safety of the cloud conditions against threats.

- **Cloud Cost Optimizer** - This is an artificial intelligence tool that assists organizations in saving on redundant cloud costs and maximizes cloud resources.

- **MeghEye Attack Surface Monitoring** - This gives the eye of a hacker perspective to act on the vulnerabilities before they come in.

- **MeghOps Web Application Firewall (WAF)** - Prevents application attacks such as SQL injection, XSS, and CSRF.

- **Dedicated Log Analyzer** - Monitors the logs of the system in real time to identify anomalies and malicious activities.

- **Server Health Monitoring** - Continuous servers monitor performance of servers and notifies about the possible failures.

Besides these products, MeghOps offers professional services like Vulnerability Assessment and Penetration Testing (VAPT), cloud migration and security testing, compliance testing, cybersecurity advisory, and security training courses.
Meghops has a wide range of clients that consists of enterprises, financial institutions, startups, as well as tech-driven firms. Among the esteemed customers and partners, the company will have DIVC, GitHub, iFarmer, aamarPay, SkilledIn Green, Ostad, and DITECH. In addition, the company has international relationships with such programs as Google for Startups, Microsoft for Startups, and AWS Startup Programs, which reinforce its service platform.

MeghOps has positioned itself as a reliable ally to those organizations that seek to safeguard their digital resources and achieve sustainable business development in a highly dynamic environment in the field of cybersecurity by its innovative products and customer-oriented services.

Chapter 3

3.1 Workplace Details

3.1.1 Company Responsibilities

Company Responsibilities The Tech Operations department of Meghops Ltd. is the heart of the company and which offers the appropriate maintenance of the cybersecurity solutions and the internal business affairs of the company. The team will be involved with the daily technical task, reliability of the systems and will contribute to the delivery of safe services to the customers.The key roles include:

- **Daily Process Management:** t is the management of the daily processes to ensure there are no disruptions in the work processes as well as all the technical operation to ensure the operations run smoothly.

- **Technical Documentation:**Keep the system configurations, software updates and standard processes well maintained and up-to-date to ensure that the required information is easily accessible to anyone whenever needed.

- **System Monitoring and Troubleshooting:** The performance of the system should be monitored every now and then, and any form of anomaly in the system should be identified and the anomaly corrected to keep the system running smoothly.

- **Software Deployment and Maintenance:** This will assist in software rollouts, software upgrades and monitoring systems that have been installed and that all is flowing well.

- **Task and Project Coordination:** Help in organizing the current activities and projects, tracking of the progress, and meeting the deadline in time.

- **Technical Support:** This is supposed to offer timely assistance to team members should they have minor hardware or software problems, and hence there will be minimal downtime

- **Internal Tools and Database Maintenance:** This is supposed to offer timely assistance to team members should they have minor hardware or software problems, and hence there will be minimal downtime.

- **Cybersecurity Operations:** PInvolvement in this type of activities as vulnerability testing, penetration testing, and Web Application Firewall (WAF) system management to improve the security system at large.

These roles will allow the Tech Operations team to confirm that Meghops will continue to operate effectively, will be in a position to provide its services to its clients, and its commitment to provide high-quality and dependable cybersecurity services.

3.1.2 Organization Core Value

In MeghOps, the values are the basis of our belief in developing a safe and solid digital ecosystem. In our opinion, cybersecurity is not a service but a duty to secure the businesses, persons, and organizations against the constantly increasing cyber threats. Our core values guarantee that we provide the best security solutions and create trust, innovation and excellence in all our actions. Security First Approach All our activities are based on cybersecurity. We specialize in the security of digital assets, in which case, businesses can do business in a world that is increasingly dependent and intricate. We are proactive as far as the security is concerned and make sure that the threats do not evolve into the vulnerabilities endangering life.

Innovation Continuous Improvement

The digital menace environment is dynamic and so are we. MeghOps has been determined to undertake research and development and implementation of the new technologies to stay up to date with the cybercriminals. We should offer high security solutions to businesses through our innovation to the ever changing needs.

Trust Integrity

We operate on the principle of security being rooted in trust and our services at MeghOps seek to provide assurance that the utmost ethical convictions are respected. We also believe in transparency, honesty and accountability whereby our clients can leave the most valuable digital assets with us without losing it.

Client-Centric Solutions

Business is also unique and so are its security requirements. Our tailor made cyber security offerings are consistent with client objectives, business structure and the issues that are pertinent to the business industry. We will be collaborative through our own way and ensure that we fulfill the need of security and at the same time facilitate business advancement and business productiveness.

Reliability Resilience

The modern world is a digitized one and requires that companies must be hard on cyber attacks. We have also developed the capacity of developing good security solutions that are robust and scaled and have high quality, which ensure that there is sustainability in security. We are experts in cloud security, the experience of which presupposes that companies should use such kinds of resources as Amazon AWS, Google Cloud, and Microsoft Azure and can work without failures.

Knowledge Sharing and Empowering

It is not only that cybersecurity is the question of system protection but it is also the question of education and empowerment of the organizations to create PR of security awareness. We trust in making knowledge and tools available to business so that we could be capable of establishing the dangers and active security measures. These values are the key attributes of our mission of offering the best-in-cycle cybersecurity solutions at MeghOps. We assist the firms to protect their IT assets, and easily maneuver through the intricacies of cybersecurity by being proactive in threats, inventive, and of high integrity.

3.1.3 Products Services

MeghOps is a provider of comprehensive cybersecurity solutions and products that would prevent any business organisation in the world against cyber threats, streamline its business operations, and meet the industry regulations and standards. In an extremely digitalized world, our cyber security can offer services that are of interest to detecting, suppressing and deterring cyber threats by businesses.

Products

- Cloud Security Suite - The Cloud Security Suite provides a good visibility and control of the cloud environments of organisations. It also applies advanced tracking and threat-detection solutions to identify security threats, mitigate weaknesses and offer a safe cloud infrastructure in advance.

Figure 3.1: Organization Core Values

- Cloud Cost Optimizer - This AI-powered service can help enterprises to save on the clouds and identify spots of inefficiencies and eliminate redundant spending. It enables organizations to manage their investments in the cloud effectively to be able to have cost effective and scalable cloud operations.

- MeghEye Attack Surface Monitoring - MeghEye is an innovative cloud security that gives the hackers the perspective of your attack surface. It is also proactive as opposed to the traditional alert based systems because it goes out of its way to identify vulnerabilities and weaknesses within its systems by emulating real life attacks such that the business is able to further strengthen its security measures before the cybercriminals can even exploit them.

- MeghOps Firewall (WAF) - We have a Web Application Firewall (WAF) that acts as the entry point to many web-based attacks such as SQL injection, cross-site scripting (XSS), cross site request forgery (CSRF), and other gaps. It is highly safe and it ensures security of the vital applications and sensitive data.

- Dedicated Log Analyzer - A log analysis tool that improves the level of security by continually reviewing system logs in order to identify anomalies, possible threats, and suspicious activities. It enables rapid identification and reaction to threats and mitigating the chances of cyber attacks.

- Server Health Monitoring - This solution will also guarantee the constant scrutiny of the health of the servers to notice an early alert of anomalies or a

performance problem. By identifying potential failures before they develop to major ones, businesses can be in a position to evade serious interruptiveness and the smooth running of businesses.

Services

- Vulnerability Assessment and Penetration Testing (VAPT) - Our VAPT services assist companies in establishing and determining security vulnerabilities within their online infrastructures. Through an extensive vulnerability scan and penetration testing, we make sure that systems are strengthened against possible cyber threats.

- Cloud Migration and Security Tests - The process of cloud transition may be expensive and dangerous in the absence of security measures. The security analysis and migration of our cloud services would guarantee a smooth migration process with strong security measures to safeguard the assets of business operations.

- Cloud Compliance Auditing and Security Consulting - We offer endto-end audits and specialized advice to aid organizations to obtain regulatory conformity and enhance the position of their cloud security. Our team makes sure that businesses do not fail to comply with industry-specific security standards and reduce compliance risks.

- Security Training and Awareness - Among the major causes of cyber incidence is human error. Our security awareness training and sensitization of employees on cybersecurity threats and best practices and regulatory obligations mitigate the risk of breaches by educating them on the importance of cybersecurity.

- Security Response and Incident Monitoring - To counteract the threats in time, our round-the-clock security monitoring services monitor the flow of traffic on the network, logging of activities in the system, and user actions. Our rapid response team also handles the risks swiftly in case of an incident to minimize the damage and restore security.

- Managed Security Services - Our security services are 24/7 managed and have got advanced threat detection and quick responsive services. By using the latest technology, we are able to offer 24-hour protection to businesses and enable them to work on their growth as we can take care of their cybersecurity requirements.

In Meghops, our mission is to provide high quality cybersecurity services capable of safeguarding businesses against threats of change. Our innovative security products or our professionally led services enable organizations in the digital age to operate safely and without fear.

3.1.4 Partners Clients

We are proud that at MeghOps, we are working with the most successful organizations in the industry and startups to achieve cybersecurity excellence. Our partners and clients belong to various industries and comprise technology and finance, agriculture, and e-commerce, which speaks of our willingness to provide particular security solutions to various business needs.
enumitem

Strategic Partners

We are also happy to be in globally acclaimed start-up programs which have earned us a chance to be exposed to latest technology, resources, and expertise. The very presence of such alliances gives us the opportunity to constantly develop our cybersecurity solutions and keep pace with the emerging threats. We have strategic partners who include:

- Google for Startups - Helping start ups and innovations to grow and implement Google technology and guidance.
- Microsoft for Startups - Aims at supporting our security product based on cloud, AI, and security solutions.
- AWS Startup Programs - For customers of AWS based cloud security solutions.

Valued Clients & Collaborations

We collaborate with a wide variety of businesses, and they have the tools and support to enable them to secure their digital assets. Our highly valued customers and partners are:

- DIVC - A reliable investment and venture capital partner.
- GitHub – Buying code protection and secure software development.
- iFarmer - Data-driven Agricultural Ecosystem: Enhancing the security of Agricultural technology.
- aamarPay - Increasing the security of the processing of online payment and financial transactions.
- SkilledIn Green - Though it is a relatively new company, it focuses on offering cybersecurity services to support sustainable skill development systems.
- Ostad - Protecting data and system security in online education services.

Chapter 4

4.1 My Contributions

In my internship experience in MeghOps Ltd., I did take part in the smooth running of the Tech Operations department. I was able to deliver on the support side of the back-end, the technical documentation, and the improvement of communication within the team. Key contributions include:

- The records of inventory should be maintained and updated to enable effective monitoring of the purchases and resources.
- Designing and establishing technical documentation to facilitate operation.
- Helping in troubleshooting and fixing system-related problems.
- Assisting in implementation and setup of software solutions.
- Helping in vulnerability tests and penetration testing.
- Working with a team in order to optimize processes and improve productivity

4.2 Methodology

The approach used during the internship involved observation, working experience, documenting and problem-solving altogether that would solve the assigned tasks.

- **Observation:** It is a certain understanding of the operating principles at MeghOps through shadowing of seniors in the working team.
- **Practical Work:** The participation in troubleshooting of the on-site system, the software installation, inventory, and documentation.
- **Documentation:** To maintain continuity of knowledge processes and findings have to be documented.

- **Teamwork:** The team will work hand in hand with the Tech Operations team to provide feedback and streamline processes and resolve problems

4.2.1 Primary Sources

- First-hand work experience and activities performed during the internship at MeghOps Ltd.
- MeghOps gave internal reports, documents and technical records.
- Supervisor and peer advice and feedback.
- Live formative operation data and logs of the MeghOps systems.

4.2.2 Secondary Sources

- Policies of the company, manuals of operation and technical documentation.
- Cybersecurity practices On-line materials and technical literature.
- Vulnerability assessment and penetration testing research papers, articles, and case studies.
- The related textbooks and scholarly sources in the fields of computer science and cybersecurity.

4.3 Findings Analysis

- Process Efficiency: Tech Operations processes at MeghOps are well-organized but could use documents and orderly inventories.
- Documentation Gaps: Absence of standardization of documentation around some technical processes was a source of difficulty in the continuity of the workflow.
- Team Communication: The communication within the department was very effective and this helped increase the efficiency of problem solving.
- Security Practices: Active vulnerability testing and penetration testing enhanced the security of the system and recognized primary areas of possible

improvement.

- Technical Skills Development: Practical experience on operational and cybersecurity activities helped in achieving high levels of skills development and knowledge application to the field.

4.4 Recommendations

- Standardize documentation guidelines on all the basic operational processes in order to provide consistency and to facilitate knowledge transfer.
- Adopt a centralized inventory control system to simplify the process of tracking resources.
- Enhance the team knowledge-sharing through frequent regular programmes.
- Implement vulnerability scanning using automated tools to enhance performance and precision.
- Implement a feedback mechanism of the operational processes in order to foster continuous improvement.

Chapter 5

5.1 Technical Aspects of the Internship

5.1.1 Technical Tools Technologies Used

My internship experience in MeghOps Ltd. I was also able to witness the application of some of the tools in cybersecurity and operations, which are critical when it comes to making the systems supportable and secure. I was able to access internal systems because the arm of the company has stringent security policies, but I tracked the application of these technologies by the Tech Operation team in the day-today operations. To monitor the network and vulnerability, Nmap [8] and OWASP ZAP [9] were utilized in order to determine the number of open ports, available vulnerabilities and web application vulnerabilities. Burp Suite [6] was also used by the team to scan and test the web application traffic in order to find weak points such as SQL injection and cross-site scripting (XSS). To monitor the health of the servers and track their performance, Zabbix [10] was employed to monitor the server health and resources used so that the abnormalities can be detected before they become problems. Moreover, the workflow and documentation were conducted via the use of Google Workspace [7], which guarantees a well-structured tracking of tasks and the productive work of a team. The fact that these tools were used in real time operations provided me with a good understanding of how cybersecurity experts ensure that their systems are reliable, perform security testing, and act in advance to avert any possible threat in a live enterprise setting.

Network & Vulnerability Assessment Tools

- Nmap - Network topology, service, and port scanner.

- OWASP ZAP - Web application vulnerability scanner assists in detecting such problems as insecure configuration or ineffective authentication.

Web Application Security Testing Tools

- Burp Suite - Full suite of software to test the security of web applications, identify vulnerabilities, including SQL injection and cross-site scripting (XSS), and view web traffic.

System Monitoring & Performance Tools

- Zabbix - Server and network monitoring application on the enterprise level, which monitors performance indicators, publicity, and irregularities.

Documentation & Collaboration Tools

- Google Workspace - productivity (Docs, sheets, drive, Gmail, etc.) to collaborate with your team and share documents.

The fact that these tools were used in real time operations provided me with a good understanding of how cybersecurity experts ensure that their systems are reliable, perform security testing, and act in advance to avert any possible threat in a live enterprise setting.

Figure 5.1: Technical Tools and Technologies Used

5.1.2 Security Workflow Overview

Our internship in Meghops Ltd., Another aspect that I paid keen attention to is how the Tech Operation team used a methodical approach in provision of security in the various client systems. This would have started with the identification of vulnerabilities, the tools, which include the automated scanning tools like the Nmap or OWASP ZAP would have been utilized in order to identify the security vulnerabilities, old configurations, or open services. The second move that the team did after

identifying potential risk was the analysis whereby they ranked the vulnerabilities based on their severity and the extent of them affecting the infrastructure of the client. Having conducted the analysis, the remediation process might have involved the use of patches or adjustment of settings or the modification of firewall settings to increase the security of the system. Verification and testing was the next phase and in it, it was re-assessed that the modified systems worked to prevent the problems but without causing any operational inconveniences. Lastly, every observation and action was recorded, and a security report was created to be reviewed by the internal and communicated to the client. This process, as observed, made me realize how it is possible to have a continuous security cycle; identify, assess, mitigate, and validate threats through a professional cybersecurity team in order to maintain system integrity and reliability.

5.1.3 Cybersecurity Best Practices Learned

As an intern in the Tech Operation group, I witnessed some of the main cybersecurity practices observed by the group that helped me grasp how organizations can have a good security posture. Among the most notable practices that I learnt are based on industry standards such as the NIST Cybersecurity Framework [3] and technical guidelines for information security testing [1]. These frameworks provide comprehensive approaches to vulnerability assessment, penetration testing, and security controls implementation. Additionally, through resources like EC-Council's Cybersecurity Exchange [2], I gained insights into current threat landscapes and defensive strategies.

- Vulnerability Assessment on a regular basis: A periodical scan is done to establish vulnerabilities in systems and fix them before they can be turned to an advantage.

- Patch Management: Software and operating systems should be updated to avoid security attacks due to old components.

- Access Control and Privilege Management: Authorization of access to the system according to the role and need which guarantees that only the authorized individuals can access sensitive information.

- Network Segmentation: Is the division of networks into smaller portions to reduce the effects of any possible attack and enhance the efficiency of monitoring.

- Firewalls and Intrusion Detection Systems (IDS): It involves the use of security levels that monitor traffic and/or block various activities that are suspicious.

- Secure Configuration: It is important to make sure that servers, applications and cloud environments are configured to standardized security settings to minimize vulnerabilities.

- Data Backup and Recovery Planning: It is intended to be done on a schedule and regular basis to ensure continuity of the business as a result of data backup and disaster recovery plans.

- Monitoring System Logs: Monitoring System logs and application logs to monitor suspicious or unauthorized access.

- Training and Awareness of employees: Employee training on the lifelong learning to minimize the possibility of human error and general training on cybersecurity.

- Documentation and Incident Reporting: To ensure that the transparency and speedy response is enhanced, it is necessary to include proper technical records and report about any of the incidents as early as possible.

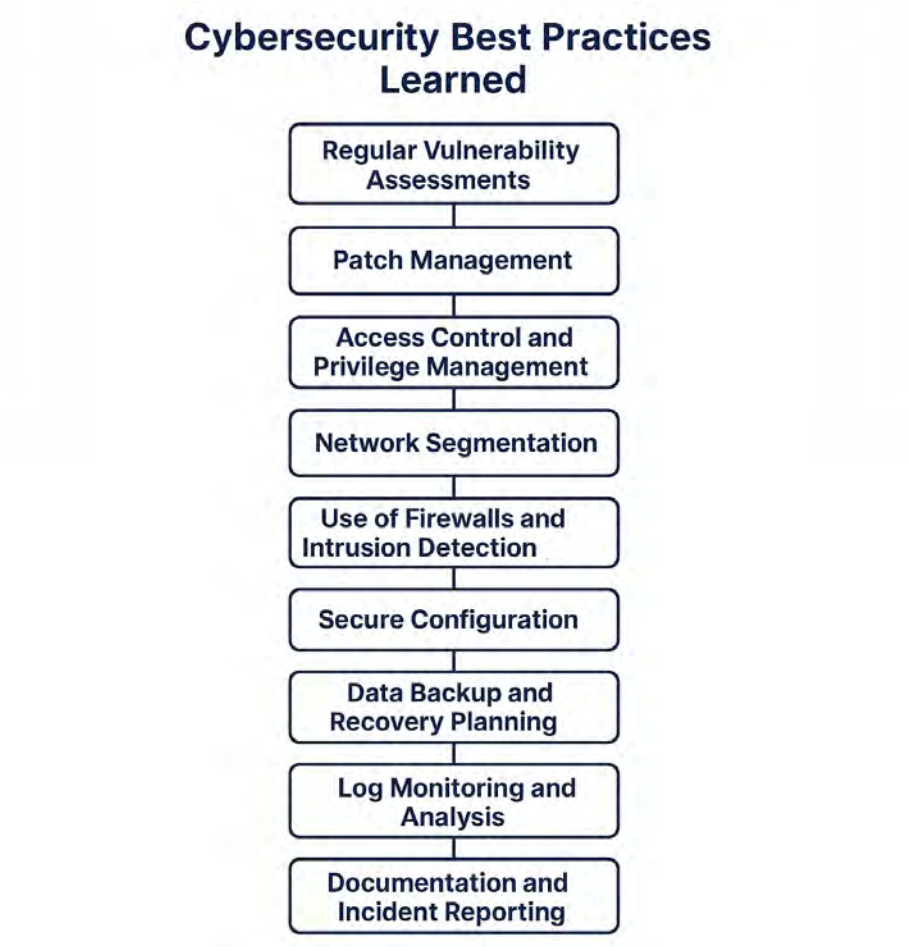

Figure 5.2: Cybersecurity Best Practices

5.1.4 Quantitative Data

Megahops Ltd. internship experience. I was in a position to observe how Tech Operation team can make the working process to be tolerable and structured and could

evaluate the performance. The management was also managing approximately 20-25 active client system on weekly basis across various issues that the management was addressing over the server uptime and fire wall status and real time log activity. The other thing that I observed was that over the time, the team was characterized by a very well documented team, the team had over 15 workflow documents that were developed within the team to standardize the repetitive functions. I also observed that technical or vulnerability report preparation of 8-10 per annum was prepared and short report taken in connection with system evaluation and discovery on behalf of the clients. The consistency of templates and procedures to be employed lowered the overall turnaround time of activities by approximately 15-20 percent because documentation was done on a daily basis and process optimization was realized. Through an analysis of these measures I concluded that data-based monitoring can help in improving coordination, improving timely reporting, and improving cybersecurity activities within a workplace.

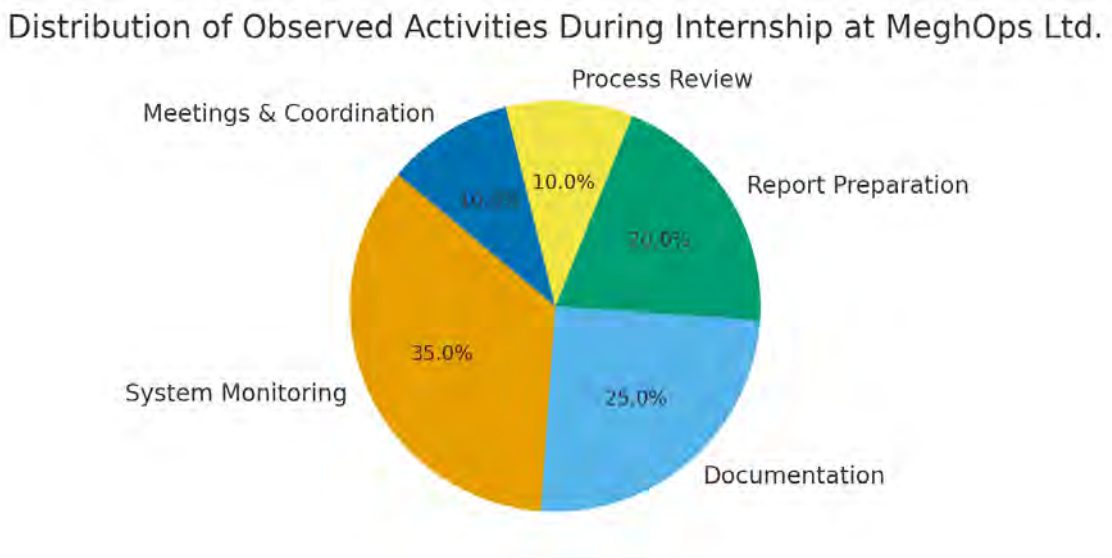

Figure 5.3: Quantitative Data Analysis

Chapter 6

6.1 Growth

6.1.1 Professional Growth

The professional growth provided through the internship experience was exceptional and enhanced my level of knowledge regarding the dynamics of the workplace environment and made my career more stable. I have also been able to adjust to a formal working environment and how to meet deadlines and how to interact with my supervisors and other workers. The exposure to the real world projects helped me to complete the assignments independently and boost my self-confidence in working to deliver quality work. This internship helped me to adopt a professional attitude that would guide me in my career proceedings later in the future.

6.1.2 Technical Growth

I had my internship comprised a lot of technical learning. I had the opportunity to have practical experience on the tools, platforms, and procedures that were relevant to the work that I did at the Technical Operations department. I have developed the knowhow on problem solving as regards troubleshooting, system monitoring, vulnerability scanning, and software packaging. Another areas I was able to develop knowledge in were in cybersecurity practices, network management, and operational efficiency tools. This kind of technical experience has made me more resourceful when it comes to solving problems and has prepared me to handle even more complex issues in the profession.

6.1.3 Interpersonal Growth

This internship was very helpful in developing me personally. The experience of working in a team with the co-working people who had a very rich pool of professional experiences also helped me learn the communication skills and teambuilding traits. I also had the opportunity of learning the qualities of a good listener, a positive feeder, and adaptability in a work setting. I was also able to learn my conflict handling skills, team work management, and favorable work relationship with the team workers. Such social competence will be helpful in the workplace.

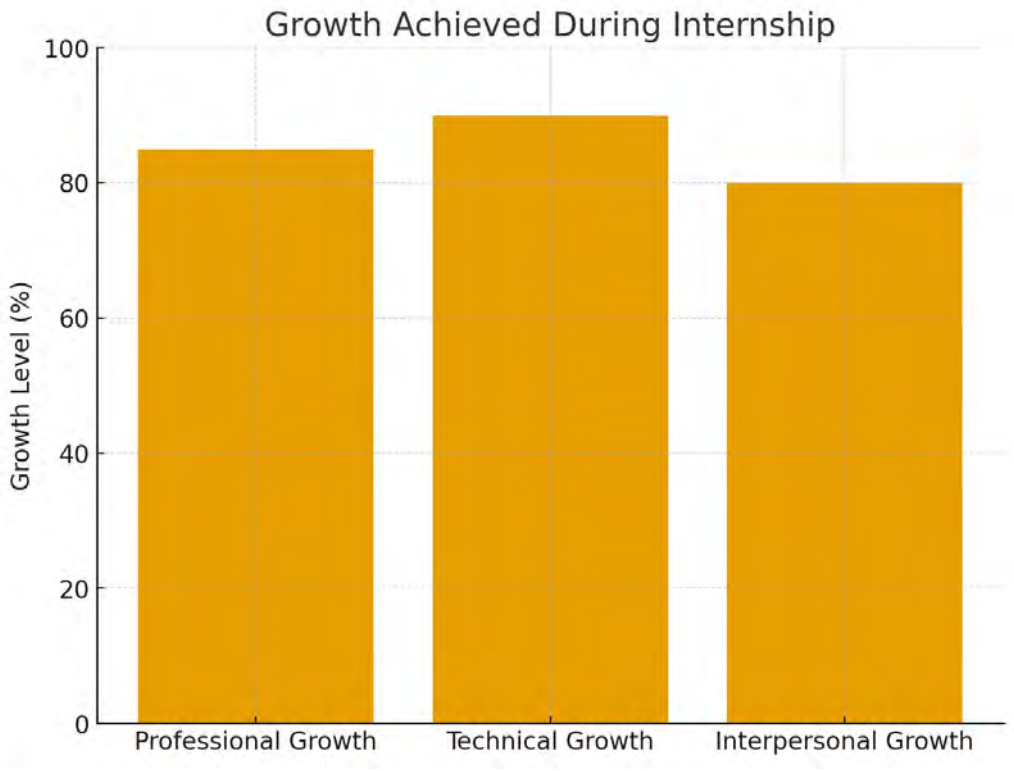

Figure 6.1: Technical Tools and Technologies Used

Chapter 7

7.1 Conclusion

The learning process in MeghOps Ltd. internship has made me a better person and transformed me and helped to bridge the gap between my theoretical studies and the practical knowledge of the industry. As an active participant of the Tech Operations Department, I managed to gain some experience in the field of back-end support, system troubleshooting, documentation, and cybersecurity practices such as vulnerability testing and penetration testing. In addition to adding to my technical competencies, this experience enabled me to develop my problem-solving, teamwork, and communication skills.

The internship helped me to gain understanding of the importance of protocols, good administration and continuous improvement in the practice of perfection in operations. It also highlighted the critical element of documentation and collaboration as one of the methods of ensuring that work flows are smooth. The acquired experience and practices will assist me in becoming a better person in my work and be prepared to confront the issues of the technological and cybersecurity-related industry in the future.

In addition, the internship has served as a milestone in my life of studying and career development. Not only did it expand my knowledge on how theoretical contents will be utilized in practical technical application in the real world, but it also provided me with the much needed professional skills like flexibility, analysis prowess and group effectiveness.

My involvement with the senior staff in the Tech Operations Department enabled me to observe the manner in which cybersecurity, system management, and operational strategies are interdependent in ensuring that there is resilience of the organization and reliability of services. The exposure and mentorship that I received have motivated me to continuously develop technical knowledge and learn about the latest technological and cybersecurity advances.

This is one of the things that have cemented my ambition to pursue a computer science and cybersecurity career and this has made me choose lifelong learning and innovation. The experience, knowledge, expertise provided in this internship will become an excellent beginning in my further activity and will contribute to making a significant contribution to the vibrant world of the Internet.

Bibliography

[1] K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, "Technical guide to information security testing and assessment," National Institute of Standards and Technology, Tech. Rep., 2008. DOI: 10.6028/nist.sp.800-115.

[2] "Cybersecurity exchange," EC-Council. [Online]. Available: https://www.eccouncil.org/cybersecurity-exchange/.

[3] "Cybersecurity framework," NIST. [Online]. Available: https://www.nist.gov/cyberframework.

[4] "Axiler — innovating cyber horizons," Accessed: Jun. 14, 2025. [Online]. Available: https://meghops.io/.

[5] "Axiler — the autopilot of cyber defence. "[Online]. Available: https://www.axiler.com/.

[6] "Burp - web application security, testing, & scanning," PortSwigger. [Online]. Available: https://portswigger.net/burp.

[7] "Google workspace: Secure online productivity & collaboration tools," Google. [Online]. Available: https://workspace.google.com/.

[8] "Nmap: The network mapper - free security scanner. "[Online]. Available: https://nmap.org/.

[9] "Vulnerability scanning tools," OWASP Foundation. [Online]. Available: https://owasp.org/www-community/Vulnerability_Scanning_Tools.

[10] "Zabbix: The enterprise-class open source observability solution. "[Online]. Available: https://www.zabbix.com/.