INTERNSHIP REPORT

Deployment Security Operation Center (SOC) And Analysis

SUBMITTED BY

Sudipto Singha Dipto
ID: 181-35-2304
Department of Software Engineering
Daffodil International University

SUPERVISED BY

Mr. Khalid Been Badruzzaman Biplob
Senior Lecturer
Department of Software Engineering
Daffodil International University

This Report Presented in Partial Fulfilment of the Requirements for the Degree of Bachelor of Science in Software Engineering (BSc in SWE)

©Daffodil International University

APPROVAL

APPROVAL

This thesis titled on **"Deployment Security Operatin Center(SOC) and analysis"**, submitted by **Student Name: Sudipto Singha Dipto (ID: 181-35-2304)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. S M Hasan Mahmud
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

Tapushe Rabaya Toma
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Khalid Been Badruzzaman Biplob
Lecturer (Senior Scale)
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Dr. Md. Sazzadur Rahman
Professor
Institute of Information Technology
Jahangirnagar University

©Daffodil International University

DECLARATION

DECLARATION

I hereby declare that I have taken this internship under the supervision of Mr. Khalid Been Badruzzaman Biplob, Senior Lecturer, Department of Software Engineering, Daffodil International University. I also declare that neither this project nor any part of this has been submitted elsewhere for award of any degree.

15.09.2025

.....

Sudipto Singha Dipto
ID: 181-35-2304
Batch: 25th
Department of Software Engineering,
Faculty of Science and Information Technology,
Daffodil International University.

Certified by:

.....

Mr. Khalid Been Badruzzaman Biplob
Senior Lecturer
Department of Software Engineering,
Faculty of Science and Information Technology,
Daffodil International University.

©Daffodil International University

ACKNOWLEDGEMENT

First and foremost, I'd like to thank Almighty Creator for his generosity in allowing me to complete my internship report on time. I would like to offer my heartfelt appreciation to the Faculty of Science and Information Technology to maintain the internship credit in the graduation academic program and provide me with an opportunity for industrial work and the area of expertise.

I'd like to thank my supervisor, Mr. Khalid Been Badruzzaman Biplob, Senior Lecturer, Department of Software Engineering. I am profoundly grateful and obliged to him for his expert, sincere, and beneficial advice, guidance and motivation to me.

I would really like to offer my heartfelt gratitude to Dr. Imran Mahmud, Professor and Head of Software Engineering Department for his relentless encouragement. I'd like to thank everyone who supported me with my internship by making valuable suggestions. I am really glad and proud to offer my gratitude and sincere admiration to our respected faculty of the Department of Software Engineering for providing this opportunity.

I must grant with due respect the endless support and patience of my family members for finishing this internship.

©Daffodil International University

Table Of Content

 ©Daffodil International University

Chapter 1
Introduction

1.1 Background

Internships provide an essential bridge between academic learning and professional practice. They offer students the chance to apply theoretical knowledge from their undergraduate studies in a real-world context. Working alongside experienced professionals gives students invaluable firsthand insight, motivating them to hone their skills and define their future career aspirations. As a final year student of Software Engineering at Daffodil International University, I chose an internship to gain real-world experience. I worked at BRACNet Limited in the Cyber Security Department, focusing on Security Operation Center (SOC) deployment and analyst activities. This internship gave me the chance to work with FortiSIEM and handle real-time security incidents. I learned how organizations monitor, detect, and respond to different types of threats using SIEM technologies.

1.2 Motivation

Today, cybersecurity is one of the most important fields in IT. Every day, many companies face attacks like malware, phishing, or unauthorized access. To protect digital systems, Security Operation Centers are essential. I chose this topic because I am passionate about defending systems from threats, and I wanted to learn how SOCs work in real life.

1.3 Objectives

Here is a summary of the main objectives of the internship in SOC (Security Operation Center) in cyber security:

- To understand how a Security Operation Center (SOC) works.
- To learn incident monitoring and analysis using FortiSIEM.
- To improve practical knowledge about real-time incident detection and response.
- To identify and differentiate between true/false positive and negative alerts.
- To experience working in a real corporate security environment.

By adhering to these goals, I have been able to identify and address my areas for improvement. This focused effort has resulted in a significant increase in my overall productivity and effectiveness.

1.4 Scope

The scope of my internship included working in the Security Operation Center (SOC)

©Daffodil International University

at BRACNet Limited, where I gained hands-on experience with the real-time monitoring of security events, detection of abnormal behavior, and analyzing security incidents. I used FortiSIEM, a Security Information and Event Management (SIEM) platform, to monitor logs collected from various devices like firewalls, switches, and endpoint systems.

I was involved in identifying, classifying, and prioritizing security alerts, and I learned how to analyze different types of incidents such as brute force attacks, port scans, failed logins, malware behaviors, etc. My responsibilities also included understanding and differentiating between true positives, false positives, true negatives, and false negatives, which helped me improve my judgment and analytical skills as a Security Analyst.

Furthermore, I experienced how a professional SOC team coordinates, shares threat intelligence, and follows proper procedures for incident response and documentation. This internship gave me a strong foundation in the practical side of cybersecurity operations and allowed me to connect my academic knowledge with real-world practices.

©Daffodil International University

CHAPTER 2

COMPANY OVERVIEW

2.1 About Company

BRACNet Limited is one of the oldest and most respected internet and IT solution providers in Bangladesh. Founded in 1996 as a joint venture ISP, the company has now evolved into a trusted provider of secure internet, enterprise solutions, and managed services. BRACNet is known for offering services to government, corporate, NGO, and educational institutions across the country.
As part of its technology growth, BRACNet also established a dedicated Cyber Security team and Security Operation Center (SOC) to monitor and defend against digital threats. The company uses enterprise-grade tools and experienced personnel to ensure the protection of its clients' digital infrastructure.

2.1.1 Company Vision

The vision of BRACNet Limited is to become a pioneer in driving digital transformation in Bangladesh by delivering reliable, innovative, and secure ICT solutions tailored to the needs of both local and international clients. The company aims to set new standards in the fields of internet services, enterprise IT, and cybersecurity, focusing on quality, trust, and technological advancement.

BRACNet envisions a future where every organization in Bangladesh, from startups to large enterprises and government bodies, can rely on cutting-edge digital infrastructure and robust security frameworks. The company strives to contribute to national development through technological empowerment, especially by supporting education, connectivity in rural areas, and secure internet for all.

2.1.2 Company Mission

The mission of BRACNet is to provide world-class ICT solutions that help businesses and institutions become more efficient, secure, and future-ready. The company focuses on delivering:

- Enterprise-grade internet and cloud infrastructure
- Highly secure and scalable managed services
- 24/7 cyber threat detection and response through a dedicated SOC
- Affordable and accessible connectivity in underserved regions

BRACNet is committed to customer satisfaction, innovation, and reliability, supported by a team of skilled professionals and engineers. The company continuously invests in modern technologies, international partnerships, and talent development to maintain its leadership position in the ICT and cybersecurity landscape of Bangladesh.

©Daffodil International University

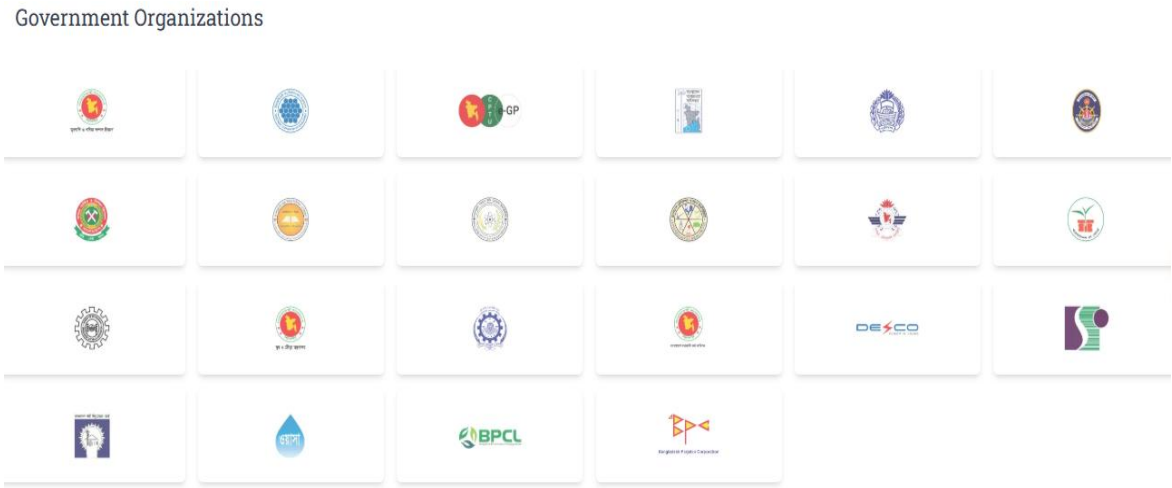
2.1.3 Services Offered by Company

BRACNet provides a variety of services, including:

- Secure Internet Connectivity
- Data Center and Cloud Solutions
- Network and Infrastructure Setup
- Cybersecurity Solutions and Services
- Managed Security Services
- SOC (Security Operation Center) as a Service
- FortiSIEM-based Security Monitoring
- VPN and Remote Access Solutions
- Hosted Servers and Virtualization
- Email and Web Hosting Services

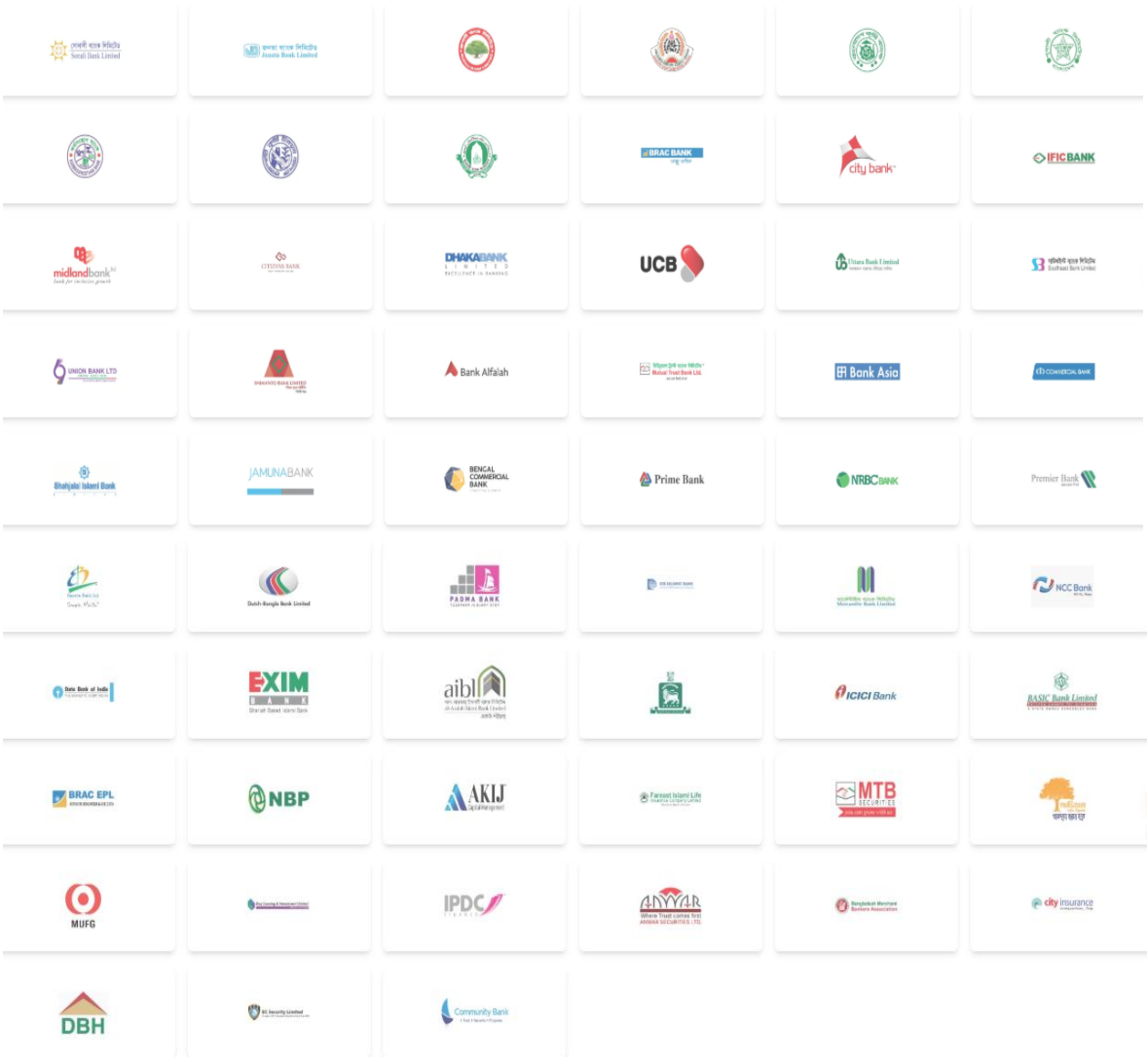
2.1.4 Clients and Coverage

BRACNet serves government offices, private companies, NGOs, educational institutions, and banks across all major divisions of Bangladesh. With a nationwide presence, BRACNet continues to grow as a trusted ICT partner.



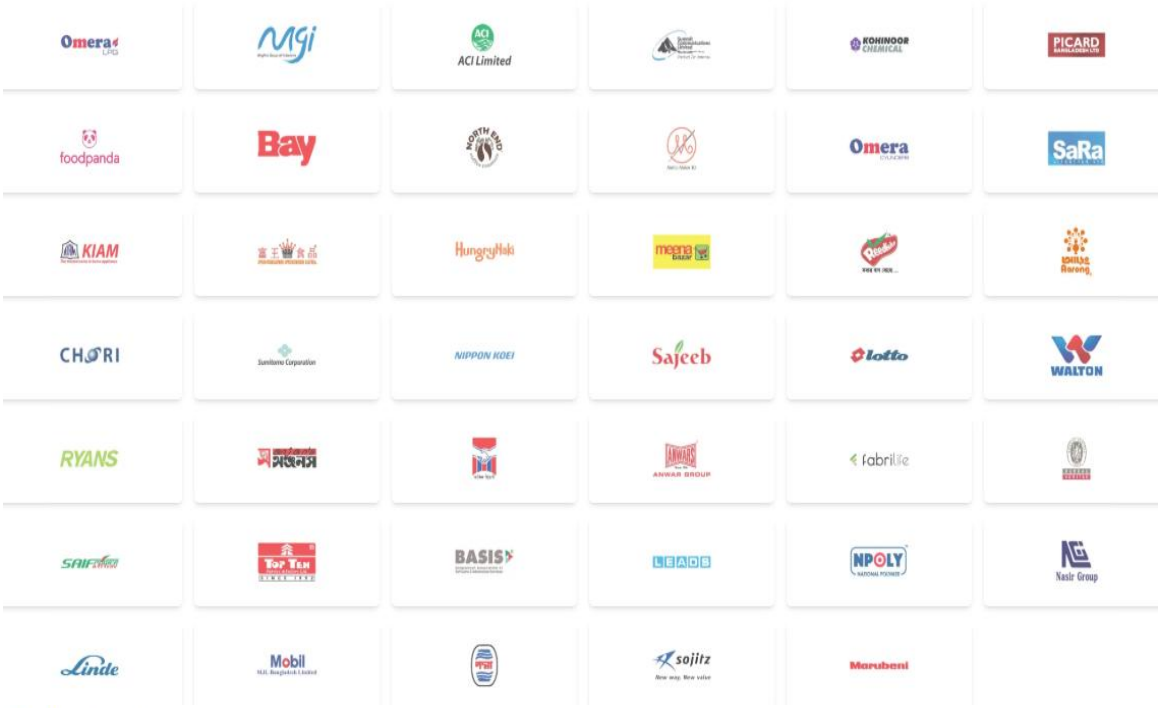
©Daffodil International University

Bank & Financial Institutes

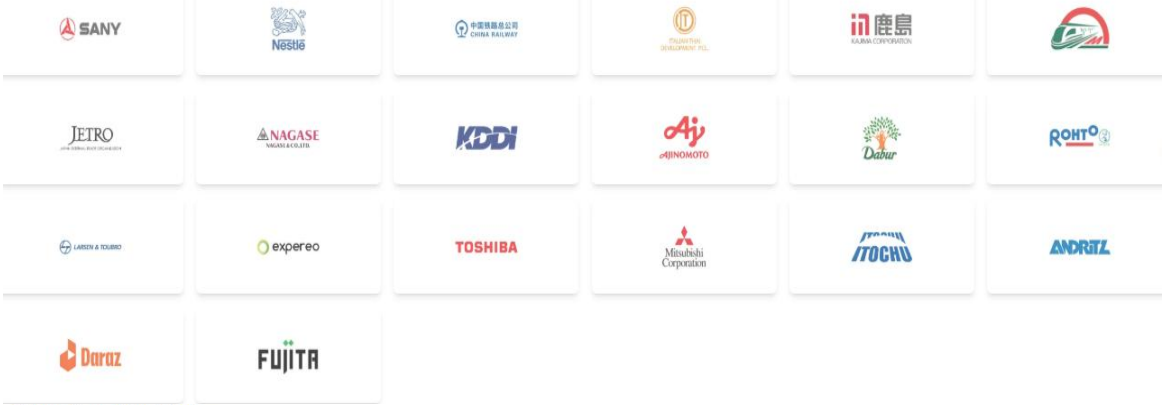


©Daffodil International University

Corporate Organization/Enterprise



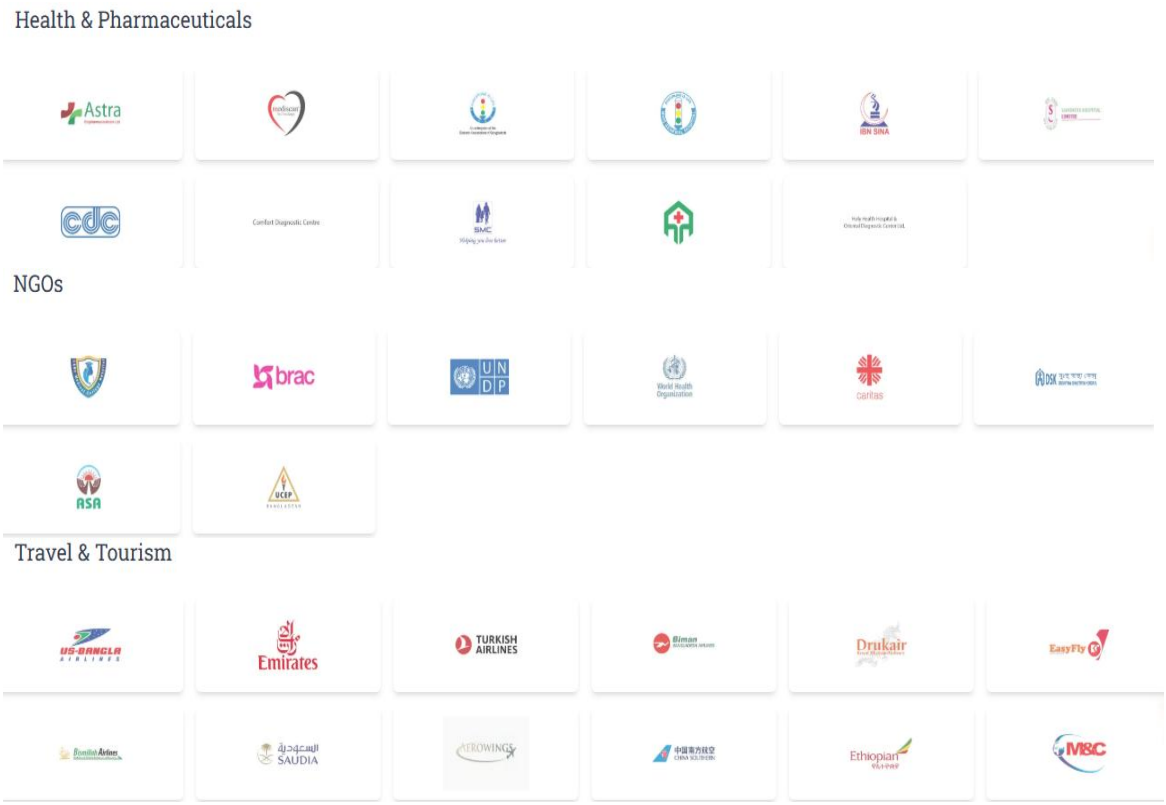
Multinational Companies



Educational Institutes

RMGs

©Daffodil International University



2.1.5 Company Location

Headquarter Office: Navana Yusuf Infinity (Level-7), 16 Mohakhali C/ A, Dhaka - 1212
Chattagram Office: Azadi Tower (Level-7), Momin Road, Chattagram- 4000
Sylhet Office: Sylhet City Center (Level-9), Zindabazar, Sylhet- 3100
Khulna Office: 129 Sir Iqbal Road (Arafat Goli), Khulna Sadar, Khulna- 9100
Rajshahi Office: Abdus Sobhan Tower 139/2, Darikharbona, Greater Road, Boalia Rajshahi
Rangpur Office: Polli Pran, Holding No # 89, Road # 01 South Gupto Para, AT Lahari Road, Rangpur-5400
Kushtia Office: Safiron Tower 2nd Floor, 50 Chand Mohammad Road, 6 Street Junction, Kushtia 7000

Phone: 16577
Email: support@bracmail.net
Official Website: www.bracnet.net

©Daffodil International University

CHAPTER 3
COMPANY CULTURE AND CARRYING OUT

3.1 Department Overview

I was placed in the Cyber Security Department at BRACNet Limited, specifically in the Security Operation Center (SOC) team. This team is responsible for continuous monitoring of security events, detecting abnormal behaviors, and responding to potential threats in real time.

The SOC operates 24/7 with a team of security analysts, engineers, and supervisors. The department uses various security tools, among which FortiSIEM is the core platform for monitoring and analysis. All incoming logs from devices like firewalls, switches, routers, and endpoints are collected and analyzed through FortiSIEM to identify and manage threats effectively.

3.2 Working Team

The SOC team at BRACNet was well-organized. My supervisor, Zahid Hossain Sajid, guided me during the internship period. The team was divided into shifts to ensure 24/7 monitoring.

Typical roles in the SOC team include:

- Level 1 Analyst (L1): Monitors alerts and creates incidents.
- Level 2 Analyst (L2): Investigates incidents in depth and suggests mitigation steps.
- Level 3 Analyst (L3): Handles advanced attacks and threat hunting.
- SOC Manager: Oversees operations and coordinates with clients.

As an intern, I worked under the supervision of L1 and L2 analysts, learning how to classify and handle various types of alerts and incidents.

3.3 Working Environments

The working environment at BRACNet was professional yet supportive. I was treated as a part of the team from day one. The office was well-equipped with modern workstations, dual monitors, secure internet, and comfortable seating. There was a friendly atmosphere among colleagues, and everyone was willing to help me whenever I had questions. We used tools like email, FortiSIEM dashboard, internal ticketing systems, and Microsoft Teams for communication and coordination.

Regular team meetings were held every week to discuss:

- Alert trends
- Significant incidents handled

©Daffodil International University

- SOC improvements
- Assignments and training updates

3.4 Internship Life Cycle

My internship followed a structured process, designed to help me gradually learn SOC operations. Here's a breakdown of the lifecycle:

1. Onboarding (August 2023)

I was introduced to the SOC team, briefed on company policies, given login access, and provided documentation to read. I observed how the FortiSIEM dashboard works and how security events are handled.

2. Shadowing Analysts (September – October 2023)

I sat beside experienced analysts, watched them handle real alerts, and learned how to triage events, open incidents, and follow workflows.

3. Assigned Tasks (November 2023 – March 2024)

I started receiving simple alerts to investigate under supervision. I worked on identifying true positives, false positives, true negatives, and false negatives. I learned how to gather event context, check raw logs, validate IPs/domains, and document findings.

4. Independent Work (April – June 2024)

I handled assigned incidents on my own and submitted reports to my supervisor. I was allowed to participate in threat analysis meetings and help write internal documentation for certain playbooks.

5. Report Preparation and Final Wrap-Up (July 2024)

In the final month, I focused on organizing my findings, preparing this report, and gathering feedback from my supervisor for future improvement.

3.5 First Day At Office

On my first day, I was both excited and nervous. After reporting to the HR desk and completing initial formalities, I was welcomed by my supervisor and introduced to the SOC team. Everyone was friendly and made me feel comfortable. I was given my workstation, security briefing, and initial reading materials on FortiSIEM and SOC concepts. I spent the rest of the day observing how security events were flowing into FortiSIEM and how analysts handled them.

©Daffodil International University

CHAPTER 4

Working Method

4.1 SOC Deployment Methodology at BRACNet

At BRACNet Limited, the Security Operation Center (SOC) is built using a structured and layered approach. The goal is to ensure complete visibility into the organization's IT infrastructure and provide real-time threat detection and response capabilities.

The deployment methodology followed these core steps:

1. Requirement Gathering
   - Identify critical assets to be monitored
   - Determine log sources (e.g., firewalls, switches, servers, endpoints)
   - Define use cases (e.g., failed login attempts, port scanning, suspicious IP activity)

2. Design and Architecture
   - Design SOC architecture using FortiSIEM as the core SIEM tool
   - Plan for log collection agents, network collectors, and central dashboard

3. Integration and Data Collection
   - Configure devices to forward logs via Syslog, WMI, or API
   - Integrate data sources into FortiSIEM using available collectors/parsers
   - Ensure log normalization and categorization

4. Use Case Development
   - Create correlation rules and dashboards to detect suspicious activity
   - Examples: brute force login attempts, malware communication, unauthorized access

5. Incident Response and Workflow Design
   - Set up a structured incident response process: alert → investigation → report → mitigation
   - Assign incident severity (Low, Medium, High, Critical) based on risk

6. Monitoring and Optimization
   - Monitor in real time
   - Tune false positives
   - Improve detection accuracy

4.2 How FortiSIEM Works in BRACNet SOC

FortiSIEM acts as the central brain of the SOC. It collects logs from different devices,

 ©Daffodil International University

normalizes them, and runs correlation rules to identify threats.

FortiSIEM Process Flow:

1. **Data Collection:** Logs are collected from devices like:
    - FortiGate Firewall
    - Windows Servers
    - Endpoint Security Tools
    - Email Gateways
    - VPN Systems

2. **Log Parsing & Normalization:** Raw logs are converted into structured formats to identify fields like IP address, username, event type.

3. **Correlation & Alerting:**
    - Rules run continuously to detect suspicious activity.
    - Example: 5 failed logins followed by a successful one within 1 minute = brute force attempt.

4. **Alert Generation:**
    - Once a rule is triggered, FortiSIEM creates an incident ticket.
    - Analysts are notified to take action.

5. **Incident Response Workflow:**
    - Check logs and asset details
    - Correlate with known threat intel
    - Classify alert as True Positive, False Positive, etc.
    - Document findings and suggest mitigation

4.3 Common Use Cases I Worked On

During my internship, I observed and helped handle use cases like:

- Brute Force Login Attempts on SSH, RDP, or Web Portals
- Failed Logins from Unknown IPs
- Port Scanning Detected from External IPs
- Access from Blacklisted Countries
- Malicious Executable Detected by Endpoint AV
- Unauthorized Admin Account Creation

Each of these was documented, investigated, and either closed as false positive or escalated for mitigation.

4.4 Understanding True/False Positives and Negatives

Type	Explanation
True Positive	Alert is real and matches a valid threat. Action required.
False Positive	The alert looks suspicious but is actually harmless.
True Negative	No alert generated, and no threat existed. Normal behavior.
False Negative	A real threat happened, but the system failed to detect it.

We focused on reducing false positives and tuning the rules to make FortiSIEM more accurate and effective.

©Daffodil International University

CHAPTER 5

Reporting and Responsibility on Internship

5.1 My Roles and Responsibilities at BRACNet Limited

During my internship at BRACNet, I worked as a Security Analyst Intern under the Security Operation Center (SOC) team. My main responsibility was to monitor, analyze, and investigate security alerts generated by FortiSIEM.

I started by observing senior analysts and gradually moved to handling incidents independently under supervision. My key responsibilities included:

Monitoring Security Events

- Regularly observed the FortiSIEM dashboard for real-time security alerts
- Checked alert categories, such as unauthorized access, malware activity, and abnormal traffic
- Used severity levels (Low, Medium, High, Critical) to prioritize incidents

Incident Handling and Analysis

- Opened and followed incident tickets based on FortiSIEM alerts
- Investigated the source of the alert using event logs, IP addresses, and system information
- Identified whether alerts were true positive, false positive, or benign activity
- Documented incident details, impact, and response actions

Log Analysis

- Reviewed logs from various devices (e.g., FortiGate Firewall, VPN gateways, Windows servers)
- Used FortiSIEM's search and filter options to correlate events across time and assets
- Cross-verified with Windows Event Viewer or raw Syslog when required

Threat Intelligence Validation

- Validated suspicious IPs/domains using:
    - AbuseIPDB
    - VirusTotal
    - WHOIS lookup
    - Shodan.io
- Checked if the behavior matched any known attack patterns or MITRE ATT&CK tactics

Incident Documentation & Reporting

- Prepared incident summary reports including:
    - Alert name
    - Affected system
    - Time of occurrence
    - Source & destination IPs
    - Root cause analysis
    - Action taken (blocked, ignored, escalated)

 ©Daffodil International University

- Maintained documentation for weekly and monthly reporting

Knowledge Sharing

- Participated in weekly team meetings to:
  - Present incident analysis
  - Share insights or mistakes
  - Learn about new attack trends and rule updates
- Maintained a personal learning log of tools, alerts, and issues I faced

5.2 Sample Alert Investigation Process

Here is an example of how I handled a real FortiSIEM alert:

Step	Action Taken
Alert Triggered	Multiple failed RDP login attempts to a Windows Server
Checked Log Details	Found over 20 failed attempts within 1 minute from an unknown IP
IP Lookup	Searched IP in AbuseIPDB — found listed as suspicious
Identified as	True Positive (Brute force attempt)
Action Taken	Informed supervisor, recommended blocking IP at firewall, created report entry

5.3 Severity Classification and Reporting Format

We used severity scoring based on the CVSS (Common Vulnerability Scoring System) and internal policies.

Severity Level	Description	Response Time
Low	No impact, informational	Monitor only
Medium	Minor suspicious behavior	24 hours
High	Real threat, limited scope	Within 6 hours
Critical	Real threat, system/data at risk	Immediate

Each incident report followed this format:

- Incident ID
- Date & Time
- Detected by (e.g., Rule ID, FortiSIEM correlation rule)
- Asset Involved
- Type of Alert
- Severity
- Analysis Summary
- Action Taken
- Status (Open/Closed/Escalated)

5.4 Summary of Tasks Performed

Task	Frequency
Alert Monitoring via FortiSIEM	Daily
Log Investigation	Daily
Threat Intelligence Lookup	Daily
Incident Report Writing	Daily/Weekly
Team Meeting Participation	Weekly
Feedback Sessions with Supervisor	Weekly
Rule Tuning Suggestions (beginner level)	Occasionally

In the next section, I'll describe what I learned, how I overcame challenges, and the impact this internship had on my technical and personal growth.

©Daffodil International University

CHAPTER 6

Knowledge Gained, Challenges, and Achievements

6.1 Technical Knowledge Gained

During my internship, I gained real-world experience in cyber defense operations through active participation in the SOC. Key learnings include:

SOC Fundamentals

- Understanding the structure, components, and functions of a modern Security Operation Center
- Roles of analysts (L1, L2), incident flow, escalation policies

FortiSIEM Operations

- How to monitor, filter, and investigate events using FortiSIEM
- Creating and editing custom views, filters, and correlation rules
- Understanding dashboards and incident lifecycles

Log Analysis Techniques

- Extracting meaningful patterns from firewall, endpoint, and system logs
- Identifying lateral movement, account misuse, malware activities

Incident Response Procedures

- Step-by-step approach: detection → validation → containment → reporting
- Classifying events by severity and urgency
- Coordinating response activities under supervision

Threat Intelligence

- Using external tools like VirusTotal, AbuseIPDB, and WHOIS to assess risks
- Validating IPs, domains, file hashes against open-source intel sources

6.2 Soft Skills Development

- Professional Communication: Writing clear and concise reports; presenting analysis in meetings
- Teamwork: Collaborating with senior analysts and taking constructive feedback
- Problem Solving: Applying logic to understand alerts, reduce false positives
- Time Management: Handling multiple alerts, maintaining shift discipline

6.3 Overcoming Challenges

Challenge	Solution/Experience
Interpreting raw log data	Learned how to use log parsers and read event details inside FortiSIEM
High number of false positives	Studied rule tuning techniques, consulted seniors for optimized filters
Lack of confidence in report writing	Practiced regularly, used report templates, and took mentor feedback
Keeping up with shift-based schedules	Adjusted my daily routine and maintained a task list to stay consistent

6.4 Sample Incident Report Template

Below is a simplified version of the format used in the SOC for internal documentation:

BRACNet SOC – Incident Report Template

Field	Details
Incident ID	SOC-2024-017
Date & Time	2024-04-15 03:45 PM
Reported By	FortiSIEM Correlation Rule ID: 1037
Assigned Analyst	Sudipto Singha Dipto
Source IP	185.212.44.77
Destination IP	10.1.2.15
Affected System	Internal Windows Server
Alert Type	RDP Brute Force Attempt
Severity	High
Description	Multiple failed RDP login attempts from unknown IP within 2 minutes
Threat Intel Status	IP listed as malicious on AbuseIPDB (Score: 90/100)

©Daffodil International University

Actions Taken	Alert validated, IP blocked via FortiGate Firewall, ticket updated
Incident Status	Closed
Analyst Remarks	True positive. Recommended future lockout policy and geo-blocking policy
Reviewed By	Zahid Hossain Sajid

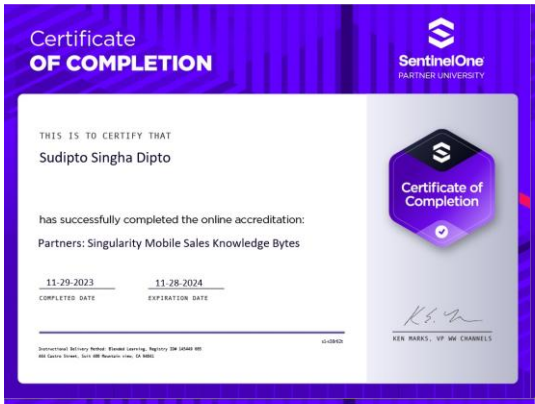
This structure ensured clarity, consistency, and traceability of every incident, which is critical in SOC operations.

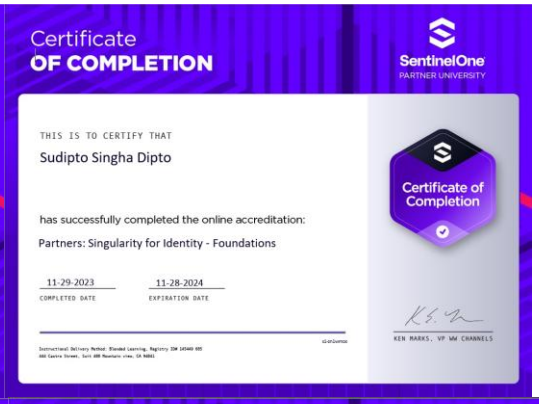
6.5 Achievements

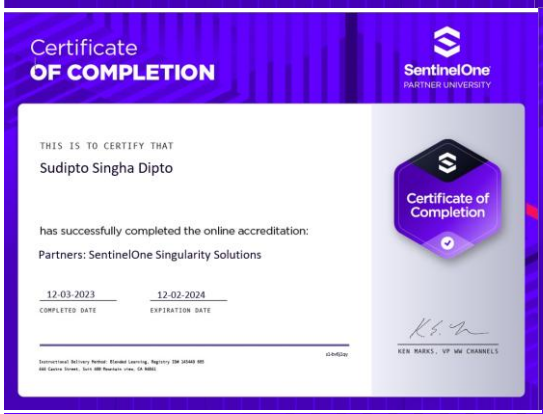
- Successfully handled 30+ real incidents
- Reduced false positive rate by identifying tuning opportunities
- Earned appreciation from my supervisor for detailed reporting
- Prepared educational materials for junior interns
- Learned to work independently in a professional SOC environment

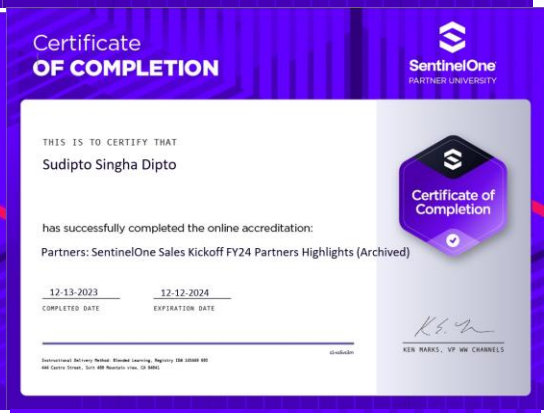
During my internship period, my organizations offered me to join tanning to enrich my skill. They supervised me on what I should learn and made necessary arrangements for gaining knowledge. They offer me to join partner tanning program for in-depth knowledge about solutions and technology.

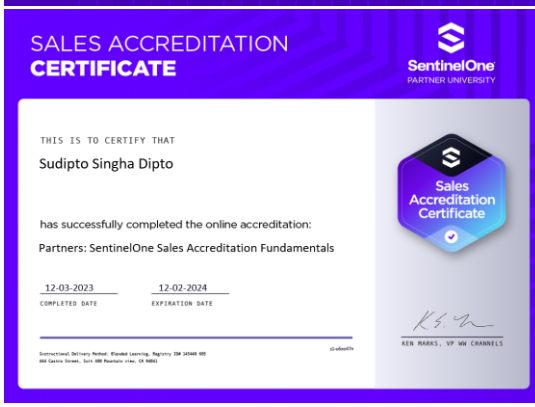
©Daffodil International University

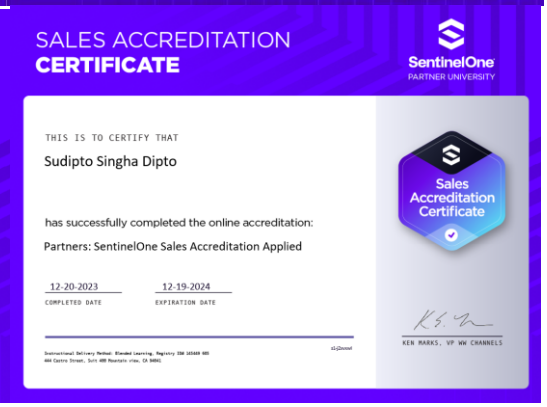




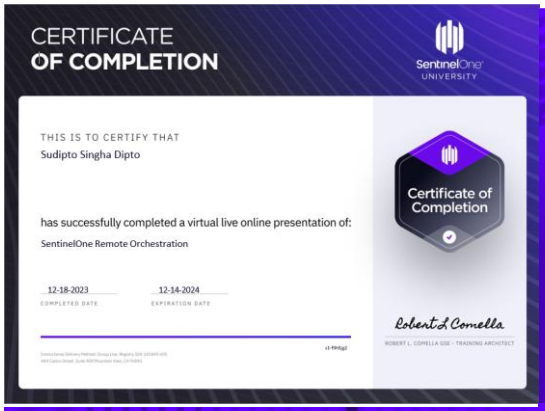


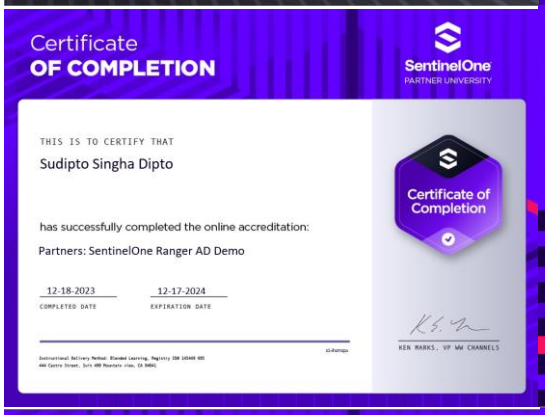


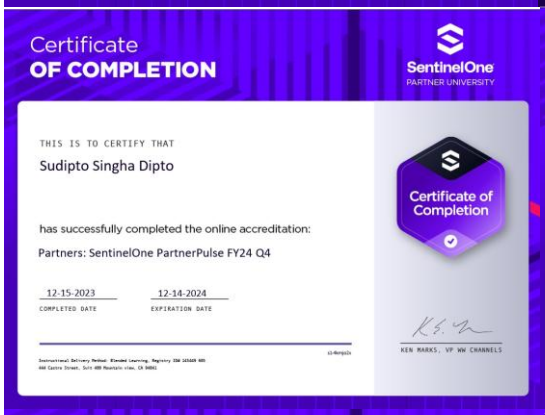


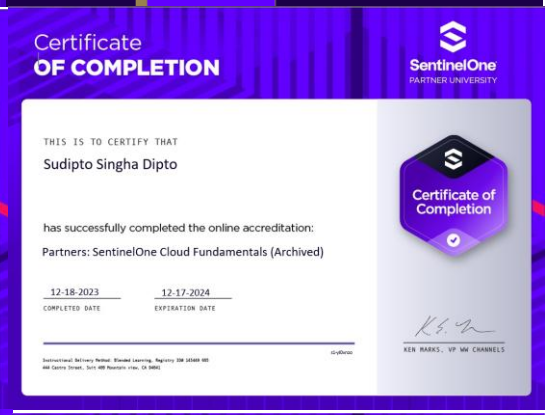


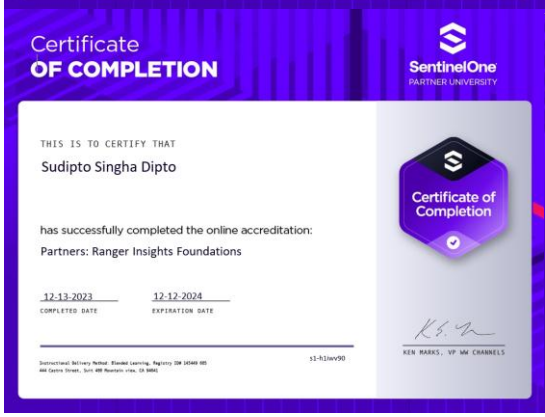
©Daffodil International University

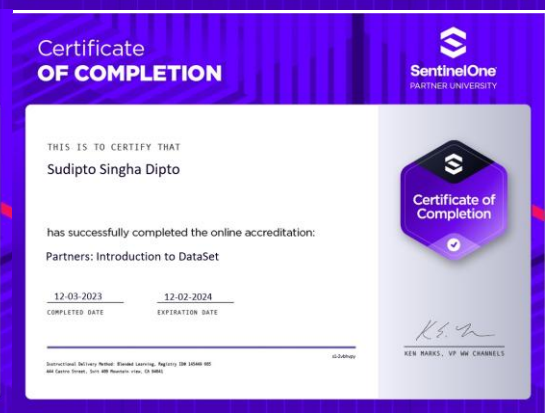




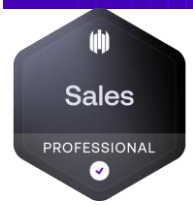








©Daffodil International University



 ©Daffodil International University

CHAPTER 7

Conclusion and Recommendations

7.1 Conclusion

Completing my internship at BRACNet Limited as part of my final semester has been one of the most valuable and transformative experiences of my academic life. I had the unique opportunity to work in a Security Operation Center (SOC), where I learned how real-world cyber threats are identified, investigated, and mitigated using FortiSIEM and other tools.

The practical experience of monitoring security events, analyzing logs, validating threats, and responding to incidents has deepened my understanding of cybersecurity beyond textbooks. I became more confident in handling complex alerts, writing reports, and contributing to a professional SOC team.

Moreover, I learned not only technical skills but also how to work under pressure, communicate effectively in a team, and adapt to a structured work environment. This internship has helped me build a solid foundation for a career in cybersecurity and information security analysis.

7.2 Recommendations for Future Interns

To help future students get the best out of their internships, I would like to share a few recommendations:

- **Be Curious:** Ask questions. Even if you are new, your willingness to learn will impress your mentors.
- **Document Everything:** Maintain notes of tasks, errors, solutions, and commands/tools. This will help in reporting and revision.
- **Focus on Understanding Alerts:** Don’t just close tickets. Understand why an alert happened and how it was classified.
- **Stay Updated:** Read about the latest threats and vulnerabilities. Cybersecurity is always evolving.
- **Be Professional:** Arrive on time, follow team protocols, and communicate clearly with your team.

©Daffodil International University

7.3 Suggestions to Daffodil International University

- Encourage Industry-Based Internships: Real-world internships in technical roles like SOC, VAPT, DevSecOps, etc., should be promoted more.

- Offer Pre-Internship Workshops: Before the internship starts, a workshop or seminar on how to behave and work in a corporate SOC environment can be helpful.

- Enhance Lab Facilities: More hands-on labs on SIEM, firewalls, and incident response can help students be better prepared.

- Promote Certifications: Students should be encouraged to take entry-level cybersecurity certifications (like CompTIA Security+, Fortinet NSE, etc.) before starting internships.

7.4 Soft Skills Development

Often referred to as core skills or transferable skills, soft skills are valuable across all industries. This internship marked my first step into the professional world, and it played a major role in shaping my personality.

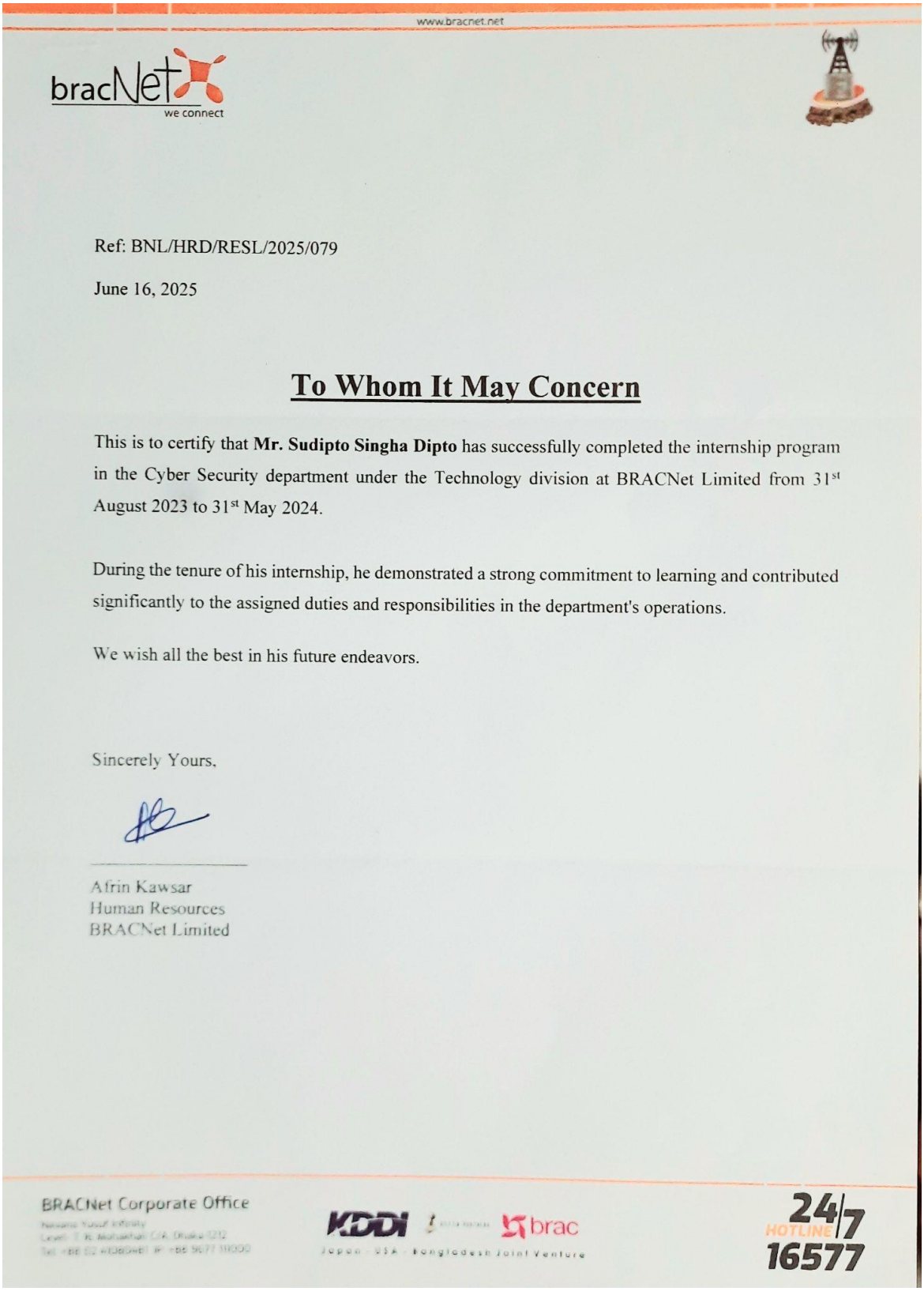
I have developed a strong sense of responsibility, improved my communication and adaptability, and learned to approach challenges with a creative and flexible mindset. These soft skills are just as important as technical knowledge and will support me throughout my career.

7.5 Personal Achievements

Life changes us—and for me, this internship became a turning point. I discovered my ability to learn quickly and work efficiently in a technical and team-based environment. Working with computers and security tools introduced me to new technologies and collaborative methods that helped me understand how large networks and organizations operate.

One of the biggest realizations I had was about the importance of time management. Being in a structured work environment made me value time more than ever, and I now see how critical it is to stay organized and focused to achieve success.

INTERNSHIP EXPERIENCED LETTER



www.bracnet.net

bracNet
we connect

Ref: BNL/HRD/RESL/2025/079

June 16, 2025

To Whom It May Concern

This is to certify that **Mr. Sudipto Singha Dipto** has successfully completed the internship program in the Cyber Security department under the Technology division at BRACNet Limited from 31st August 2023 to 31st May 2024.

During the tenure of his internship, he demonstrated a strong commitment to learning and contributed significantly to the assigned duties and responsibilities in the department's operations.

We wish all the best in his future endeavors.

Sincerely Yours,

Afrin Kawsar
Human Resources
BRACNet Limited

BRACNet Corporate Office

KDDI brac
Japan - USA - Bangladesh Joint Venture

24/7 HOTLINE 16577

©Daffodil International University

Plagiarism Report

181-35-2304

ORIGINALITY REPORT

9%	9%	1%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	6%
2	www.bracnet.net Internet Source	1%
3	fastercapital.com Internet Source	1%
4	www.theseus.fi Internet Source	<1%
5	Submitted to Karachi Institute of Economics & Technology, Karachi Student Paper	<1%
6	www.valuemarketresearch.com Internet Source	<1%
7	123dok.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

©Daffodil International University