Cyber Suraksha

Purple Team Exercise

Situational Awareness Report

(SITREP)

Version 1.0

Date:

Time:

Incident ID:

1. Incident Overview

Description:

Severity Level:

Low

Impact:

Minimal

Affected Systems:

2. Incident Details

Detection Method:

Security Information and Event Management (SIEM)

Initial Detection Time:

Attack Vector:

Phishing

Attackers:

External

3. Response Actions Taken

Containment:

Eradication:

Recovery:

Lessons Learned:

4. Technical Analysis

Evidence:

Indicators of Compromise (IOCs):

Tactics, Techniques, and Procedures (TTPs):

Mitigation Recommendations:

---

5. Communication

Internal Notification:

External Notification:

Updates:

---

6. Additional Notes

---

7. Submission

Prepared By:

8. POC (Screenshots)
