Cyber Suraksha

Purple Team Exercise

Incident Response Report

(IRREP)

Version 1.0

Date: 1/5/2024

Time: 5:19:15 pm

1. Incident Overview

Description: p

Severity Level: Low

Impact: Minimal

Affected Systems: p

---

2. Incident Details

Detection Method: Intrusion Detection System

Initial Detection Time: 2024-05-24T17:18

Attack Vector: Phishing

Attackers: External

---

3. Response Actions Taken

Containment: p

Eradication: p

Recovery: p

Lessons Learned: pp

---

4. Technical Analysis

Evidence: p

Indicators of Compromise (IOCs): p

Tactics, Techniques, and Procedures (TTPs): p

Mitigation Recommendations: pp

---

5. Communication

Internal Notification: p

External Notification: p

Updates: p

---

6. Follow-Up Action

Incident Review: 2024-05-25T17:19

Documentation: done

Training: p

---

7. Additional Notes

---

8. Submission

Prepared By:

9. POC (Screenshots)
