Cyber Suraksha

Purple Team Exercise

Incident Response Report

(IRREP)

Version 1.0

Date: 1/5/2024

Time: 5:45:39 pm

1. Incident Overview

Description: j

Severity Level: Low

Impact: Minimal

Affected Systems: j

---

2. Incident Details

Detection Method: Endpoint Detection and Respons

Initial Detection Time: 2024-05-28T17:45

Attack Vector: Phishing

Attackers: External

---

3. Response Actions Taken

Containment: h

Eradication: h

Recovery: h

Lessons Learned: hh

---

4. Technical Analysis

Evidence: h

Indicators of Compromise (IOCs): h

Tactics, Techniques, and Procedures (TTPs): h

Mitigation Recommendations: hh

---

5. Communication

Internal Notification: h

External Notification: h

Updates: h

---

6. Follow-Up Action

Incident Review: 2024-05-22T17:45

Documentation: done

Training: h

---

7. Additional Notes

hh

---

8. Submission

Prepared By: h

9. POC (Screenshots)
