Incident Response Report

Project: CVE-2024-49138 Exploitation
Platform: LetsDefend (Online SOC Simulation)
Analyst: Sejal Sonar
Date: (Today's Date)

1. Executive Summary

Brief explanation of alert and findings.

2. Alert Information

- Alert Name
- Severity
- Log Source

3. Investigation Details

Explain what you checked:

- Host details
- Process logs
- File path
- Parent process

4. Technical Analysis

Explain why it is suspicious.

5. Verdict

True Positive

6. Remediation

- Isolate system
- Remove file
- Reset credentials