Cybersecurity Job Simulation – Incident Analysis (AIG)

This report demonstrates a complete incident response workflow, from vulnerability identification to ransomware recovery, reflecting practical cybersecurity operations.

1. Scenario Overview

As part of the Cyber & Information Security Team, I worked on a simulated scenario involving a critical Log4j vulnerability and a ransomware attempt. The goal was to identify risks, notify affected teams, and support recovery without paying ransom.

2. Analysis & Actions Performed

Task 1: Reviewed CISA advisory on Log4j (CVE-2021-44228), identified Product Development Staging Environment as affected, and notified the Product Development Team.
Task 2: Analysed ransomware impact, avoided ransom payment, and used Python brute force with a password list to recover the encrypted file.

3. Key Findings

Log4j allowed remote code execution. Attackers deployed ransomware, but weak encryption enabled brute-force recovery. Attack pattern suggested low sophistication.

4. Security Issues Identified

Unpatched Log4j vulnerability, lack of proactive monitoring, delayed detection, and weak attacker encryption implementation.

5. Response & Remediation

Issued advisory, recommended patching, avoided ransom, recovered data using brute force, and suggested improved monitoring and patch management.

6. Real-World Insight

Many ransomware attacks exploit known vulnerabilities like Log4j. Timely patching and monitoring are critical to prevent such incidents.

7. What I Learned

Vulnerability management is essential. Incident response includes communication and recovery. Python can support security operations. End-to-end thinking is key in SOC roles.

Report Prepared By

Shaik Abdul Rehman
Aspiring SOC Analyst | IAM Enthusiast
Project: AIG Cybersecurity Job Simulation (Forage)
Date: October 2025

"— End of Report —"