**FUTURE\_CS\_02**

\*Internship Track:\* Cyber Security

\*Task 2:\* Security Alert Monitoring & Incident Response

**Objective**

Monitor simulated security alerts using Splunk, identify suspicious activities, classify incidents, and draft an incident response report.

**Tools Used**

- Splunk (Free Trial)

- Sample SOC log files

**Findings**

- Multiple failed login attempts from IP 203.0.113.77 and 198.51.100.42 (possible brute-force).

- Suspicious activities by user accounts: alice, bob, charlie, david, and eve.

- Malware detection alerts triggered on endpoints.

- Repeated unauthorized access attempts from unusual IPs.

---

**Incident Classification**

- Brute Force Attack Attempts→ Repeated failed login attempts.

- Malware Infection→ Critical malware detection logs.

- Suspicious Account Activity→ Abnormal user log behavior.

**Recommendations**

- Block malicious IPs immediately.

- Enforce Multi-Factor Authentication (MFA).

- Reset and monitor flagged user accounts.

- Apply latest system patches and run antivirus scans.

- Strengthen Splunk monitoring rules.

- Conduct employee cybersecurity awareness training.

**Repository Contents**

- Incident\_Response\_Report\_Task2.pdf → Full incident response report (formal PDF).

- README.md → Documentation of Task 2 (this file).

- Screenshots/ → Splunk alert screenshots (to be uploaded).

**Status**

✔ Task 2 Completed: Security Alert Monitoring & Incident Response.