**Cybersecurity Incident Response Simulation Report**

**Task:** Develop a structured response plan for handling cybersecurity incidents effectively.

Duration: July- September

**Intern:** Ammad Aziz

**Organization:** Internee.pk

**1. Objective**

The primary goal of this task was to create a structured and safe environment to simulate a ransomware incident. The simulation allows staff to practice **threat detection, mitigation, and recovery** without impacting production data.

**2. Scope**

This simulation was carried out on an **isolated lab setup** (C:/lab\_test\_data/) to ensure:

* No production systems or real data were affected.
* The ransomware behavior was **emulated in a reversible and controlled way**.
* The incident response workflow was tested end-to-end.

**3. Incident Response Plan**

**3.1 Threat Detection**

* Suspicious encryption activity was simulated on **staged copies** of files.
* A **manifest.json** file was generated containing metadata (SHA-256 checksums, file sizes, encryption salts, and nonces).
* A **mock ransom note** was created in the staging folder to simulate attacker communication.

**3.2 Mitigation**

* The original files in TARGET\_DIR remained **untouched and safe**.
* The encryption targeted only staged copies in STAGING\_DIR, minimizing real-world risks.
* AES-256-GCM encryption with passphrase-derived keys ensured confidentiality.
* A strict **safety mechanism** enforced operation only within paths containing "lab\_test\_data".

**3.3 Recovery**

* The decryption function successfully restored files from the encrypted staging area back into RESTORE\_DIR.
* Recovery required the same **passphrase** used during simulation, emulating a real-world scenario where key management is critical.
* Logs provided detailed feedback on restored and failed files.

**4. Simulation Execution Steps**

**Step 1: Simulation (Attack Phase)**

* Files copied from TARGET\_DIR → encrypted in STAGING\_DIR.
* Ransom note dropped in STAGING\_DIR.
* Manifest created documenting the simulation metadata.

**Command:**

python ransomware\_simulation.py simulate

**Step 2: Status Check (Incident Monitoring)**

* Staff can verify simulation details (time, source, file count).

**Command:**

python ransomware\_simulation.py status

**Step 3: Recovery (Decryption Phase)**

* Files decrypted back into RESTORE\_DIR using the original passphrase.

**Command:**

python ransomware\_simulation.py decrypt

**5. Training & Awareness**

To strengthen preparedness, **Internee.pk staff** were trained on:

* Recognizing **indicators of ransomware attacks** (unexpected file encryption, ransom notes, sudden access denial).
* Following **incident response procedures** (isolate affected systems, preserve evidence, notify security team).
* Executing **recovery protocols** (using backup data or decryption routines).
* Importance of **secure passphrase/key management** to prevent data loss.

**6. Outcomes**

✅ Safe ransomware simulation successfully executed.  
✅ Incident response workflow tested end-to-end (detection → mitigation → recovery).  
✅ Staff trained on recognizing, responding, and recovering from ransomware scenarios.  
✅ No production systems/data were harmed during the exercise.

**7. Recommendations**

* Implement **regular ransomware simulation drills** to enhance staff readiness.
* Maintain **secure backups** and test recovery procedures frequently.
* Deploy **EDR (Endpoint Detection & Response) solutions** for real-time monitoring.
* Establish a **communication protocol** for reporting and escalating incidents.

**8. Conclusion**

This task provided Internee.pk with a **safe, reversible ransomware simulation** to practice and refine its cybersecurity incident response plan. The exercise ensured that staff are better equipped to handle real-world ransomware threats through effective detection, mitigation, and recovery strategies.