Incident Response Playbook

INCIDENT RESPONSE PLAYBOOK (NIST/SANS)

1. Preparation

- Ensure logging coverage (Sentinel, Defender, AD)

- IR communication plan established

- SOC runbooks available

- Backup & recovery validated

2. Identification

- Intake alert (SIEM/EDR)

- Validate severity & impact

- Gather initial evidence: logs, processes, network activity

- Classify incident type (BEC, Malware, Ransomware, Credential Theft)

3. Containment

- Short-term: isolate host, disable user, block IP

- Long-term: MFA enforcement, password resets, revoke tokens

- Preserve volatile data

4. Eradication

- Remove malware/persistence

- Patch vulnerabilities exploited

- Clean registry & scheduled tasks

- Terminate malicious sessions

5. Recovery

- Restore systems from backups

- Reconnect devices after clean verification
- Monitor for re-entry attempts

6. Lessons Learned

- Produce IR report
- Update detection rules
- Improve security controls