The **SANS Incident Response (IR) template** is structured based on the **SANS Incident Handling Process**, which consists of six key phases:

1. **Preparation**
2. **Identification**
3. **Containment**
4. **Eradication**
5. **Recovery**
6. **Lessons Learned**

Below is a structured **Incident Response Report Template** following SANS guidelines:

Incident Response Report

1. Incident Summary

- **Incident Name:** [Provide a short name for the incident]
- **Date & Time of Incident Detection:** [YYYY-MM-DD HH:MM]
- **Incident Detection Source:** [SIEM, IDS/IPS, SOC Analyst, User Report, etc.]
- **Incident Severity:** [Low | Medium | High | Critical]
- **Brief Description:** [Summarize what happened, e.g., malware infection, phishing attack, DDoS, etc.]

2. Preparation

- **Incident Response Team Members & Roles:**
    - Incident Handler: [Name]
    - Forensic Analyst: [Name]
    - SOC Analyst: [Name]
    - Management Liaison: [Name]
- **Security Controls in Place:**
    - Firewalls
    - Endpoint Protection
    - SIEM
    - IDS/IPS
- **Previous Similar Incidents:** [Yes/No – If Yes, describe past incidents]

3. Identification

- **How was the incident detected?** [Alert from SIEM, anomaly in logs, user report, etc.]
- **Timestamp of First Malicious Activity:** [YYYY-MM-DD HH:MM]
- **Affected Systems & Users:**
    - System Name: [Hostname/IP]
    - User Accounts: [Compromised user accounts]
- **Indicators of Compromise (IOCs):**
    - Malicious File Hashes: [MD5/SHA256]
    - Suspicious Domains: [example.com]
    - IP Addresses: [Attacker IPs]
    - Malware Signatures: [If identified]
- **Log Sources Analyzed:** [Firewall, Syslog, Windows Event Logs, etc.]

4. Containment

- **Immediate Actions Taken:**
    - Isolated infected machines? [Yes/No]
    - Blocked malicious domains/IPs? [Yes/No]
    - Disabled compromised user accounts? [Yes/No]
    - Other actions? [Describe]
- **Short-Term Containment Strategy:** [Example: Disconnect affected hosts, block access to suspicious services]
- **Long-Term Containment Strategy:** [Example: Apply firewall rules, enforce stricter authentication policies]

5. Eradication

- **Root Cause Analysis (RCA) Findings:**
    - Attack Vector: [Phishing, Exploit, RDP brute force, etc.]
    - Vulnerabilities Exploited: [Outdated software, misconfigured system, etc.]
- **Steps Taken to Remove Threats:**
    - Malware removed? [Yes/No – If Yes, describe how]
    - Systems patched? [Yes/No]
    - User credentials reset? [Yes/No]

- Other mitigation steps? [Describe]

6. Recovery

- **Restoration Process:**
  - Systems restored from backup? [Yes/No]
  - Backups verified? [Yes/No]
  - Network services resumed? [Yes/No]
- **Monitoring Strategy:**
  - Increased SIEM logging? [Yes/No]
  - Endpoint behavior monitoring? [Yes/No]
  - Additional security controls implemented? [Yes/No]
- **Estimated Downtime:** [HH:MM]
- **Business Impact Analysis:** [What operations were affected?]

7. Lessons Learned

- **Summary of Key Findings:**
  - What went well?
  - What could be improved?
- **Security Enhancements Suggested:**
  - Implement stronger endpoint security? [Yes/No]
  - Conduct security awareness training? [Yes/No]
  - Improve incident detection and response time? [Yes/No]
  - Other improvements? [Describe]
- **Future Prevention Measures:**
  - Policy updates
  - Security tool enhancements
  - Additional monitoring

8. Incident Closure & Reporting

- **Incident Status:** [Resolved | Under Investigation | Escalated]
- **Final Report Submission Date:** [YYYY-MM-DD]

- **Reviewed By:** [Security Team, IT Management]
- **Next Steps:** [Follow-up actions or scheduled reviews]

Additional Notes:

- Attach supporting logs, screenshots, or forensic analysis reports.
- If regulatory reporting is required (e.g., GDPR, HIPAA), document compliance steps.