Incident Response Documentation

List of SANS Templets used for incident Response Report:

- **Executive Summary**:
  - On 11 December 2025, the SOC detected a phishing email targeting the Finance department.
    The email attempted to steal Microsoft 365 credentials using a fake login page.
    One user clicked the link but did not submit credentials. The malicious domain was blocked, and no compromise occurred.
- **Timeline of Events:**
  - Discuss this Timeline of Events with the Logical reason;

Time (IST)	Event	Source	Analyst
09:42	Alert triggered: User clicked phishing link	Wazuh/M365 logs	SOC
09:45	Analyst validated email header and URL	SOC	alex
09:50	User contacted and confirmed email receipt	Phone	Alex
09:55	Verified user did NOT enter credentials	User confirmation	Alex
10:00	Malicious domain blocked in firewall & Defender	SOC Tools	Alex
10:10	Forced password reset for safety	IAM	SOC
10:20	SIEM monitoring for follow-up activity	SIEM	SOC
12:00	Incident marked Contained	SOC	Alex

Impact Analysis:

- One user interacted with the link
- No credential submission detected
- Zero lateral movement
- No malware execution

Remediation Steps:

- Block malicious URL
- Update web filter blacklist
- Reset user password
- Conduct awareness training
- Update SIEM detection rule

Investigation Steps – Mock Phishing Incident:

Timestamp	Action Performed
2025-08-18 13:45:00	SOC alert triggered for suspicious phishing email
2025-08-18 13:50:00	Analyst reviewed email headers and identified spoofing
2025-08-18 13:55:00	Verified malicious URL via Threat Intel sources
2025-08-18 14:00:00	**Isolated endpoint** (EDR network containment)
2025-08-18 14:10:00	Contacted user to confirm interaction with email
2025-08-18 14:15:00	Checked Office 365 sign-in logs for credential misuse
2025-08-18 14:30:00	**Collected memory dump** for forensic review
2025-08-18 14:45:00	Exported browser history and network activity logs
2025-08-18 15:00:00	Quarantined phishing email across organization
2025-08-18 15:20:00	Blocked malicious domain on firewall & DNS filter
2025-08-18 15:40:00	Forced user password reset & verified MFA status
2025-08-18 16:10:00	Completed endpoint malware scan (no threats found)
2025-08-18 16:30:00	Documented IOCs and added to SIEM detection rules
2025-08-18 17:00:00	Final review completed and incident marked **Contained**
Timestamp	**Action Performed**

Phishing Response Checklist:

- Confirm email headers (SPF / DKIM / DMARC validation).
- Check link reputation in VirusTotal / URLScan / Threat Intel.
- Identify affected users (email distribution list, forwarded copies).
- Inspect sender domain and reply-to address.
- Analyze any attachments (sandbox or AV scan).
- Extract IOCs (URLs, domains, IPs, file hashes).
- Quarantine phishing email in mail gateway.
- Review Office 365 / Google Workspace login logs.
- Check unusual login attempts or risky sign-ins.
- Inspect endpoint EDR alerts.
- Block malicious domain in firewall/DNS.
- Block sender address or domain.
- Add indicators to SIEM watchlist.
- Submit report to Threat Intel team.

Post-Mortem Summary:

The phishing incident exposed gaps in email filtering and user awareness. No systems were compromised, but response time can improve. Automating URL reputation checks and strengthening user training will reduce similar incidents. Updating SIEM rules and conducting periodic phishing simulations will enhance detection and response efficiency.