SANS Incident Response Report – Alert Management

1. Executive Summary

On 18 August 2025, a phishing email impersonating the internal HR department was sent to multiple employees. One user clicked the malicious link, triggering an attempted credential-harvesting attack. The SOC team quickly isolated the endpoint, verified no credential compromise due to MFA, and blocked the sender domain. The incident was contained with minimal impact.

2. Timeline of Events

Timestamp (IST)	Action Taken
2025-08-18 14:00:00	SOC detected phishing alert in Wazuh
2025-08-18 14:05:00	Endpoint isolated from corporate network
2025-08-18 14:10:00	Email headers collected and analyzed
2025-08-18 14:20:00	Link reputation checked via VirusTotal
2025-08-18 14:30:00	Affected user interviewed; browser logs reviewed
2025-08-18 15:00:00	Blocked malicious domain on email gateway
2025-08-18 15:20:00	Incident declared contained

3. Impact Analysis

- Affected Users: 1 employee
- Affected Asset: Employee workstation
- Data Compromise: None confirmed
- Credential Harvesting Attempt: Blocked by MFA
- Systems Impacted: No lateral movement or system compromise
- Overall Severity: Low

4. Remediation Steps

- Isolated affected workstation to prevent further communication
- Cleared browser history and removed malicious artifacts
- Forced immediate password reset for affected user
- Blocked sender domain and phishing URL at the email gateway
- Updated Wazuh detection rules for enhanced phishing detection
- Conducted refresher phishing awareness training for employees

5. Lessons Learned

- Multi-factor authentication (MFA) significantly reduced the risk of credential theft.
- Employees require ongoing training to identify realistic phishing attempts.
- Email filtering and detection rules must be improved for quicker identification.
- Early detection minimized the spread and impact of the incident.