Incident Response Report (Mock Phishing Case)

1. Executive Summary

On **18th August 2025**, a phishing email was reported by an employee in the Finance team. The email contained a suspicious link that redirected to a fake login page. Wazuh triggered an alert, and the SOC immediately began investigation. The affected endpoint was isolated, and remediation steps were completed within 2 hours. No sensitive data loss was confirmed, but one user account was at risk.

2. Timeline of Actions

Timestamp	Action Taken	Notes
2025-08-18 14:00	User reported suspicious email	Employee clicked link before reporting
2025-08-18 14:10	Wazuh alert generated	Flagged phishing domain activity
2025-08-18 14:20	Endpoint isolated	Disconnected from LAN & WiFi
2025-08-18 14:30	Memory dump collected	Saved for later forensic review
2025-08-18 14:45	Email headers analyzed	Spoofed sender domain identified
2025-08-18 15:00	User credentials reset	MFA enforced
2025-08-18 15:20	Blocked malicious IP/domain	Added to firewall + mail gateway blocklist
2025-08-18 16:00	Post-incident review started	Report being documented

3. Impact Analysis

- **Users Affected:** 1 (Finance employee)
- **Systems Affected:** 1 workstation temporarily offline
- **Data Exposure:** No confirmed data exfiltration
- **Risk Level:** Medium – user credentials potentially compromised, phishing campaign could have been broader

4. Remediation Steps Taken

1. Isolated the user’s machine from the corporate network.
2. Reset account credentials and re-enrolled MFA.
3. Blocked the phishing domain and related IPs in the firewall and mail gateway.
4. Forensic data collected (memory dump + logs) for later deep analysis.
5. Sent awareness reminder to all staff about reporting suspicious emails.

5. Phishing Response Checklist

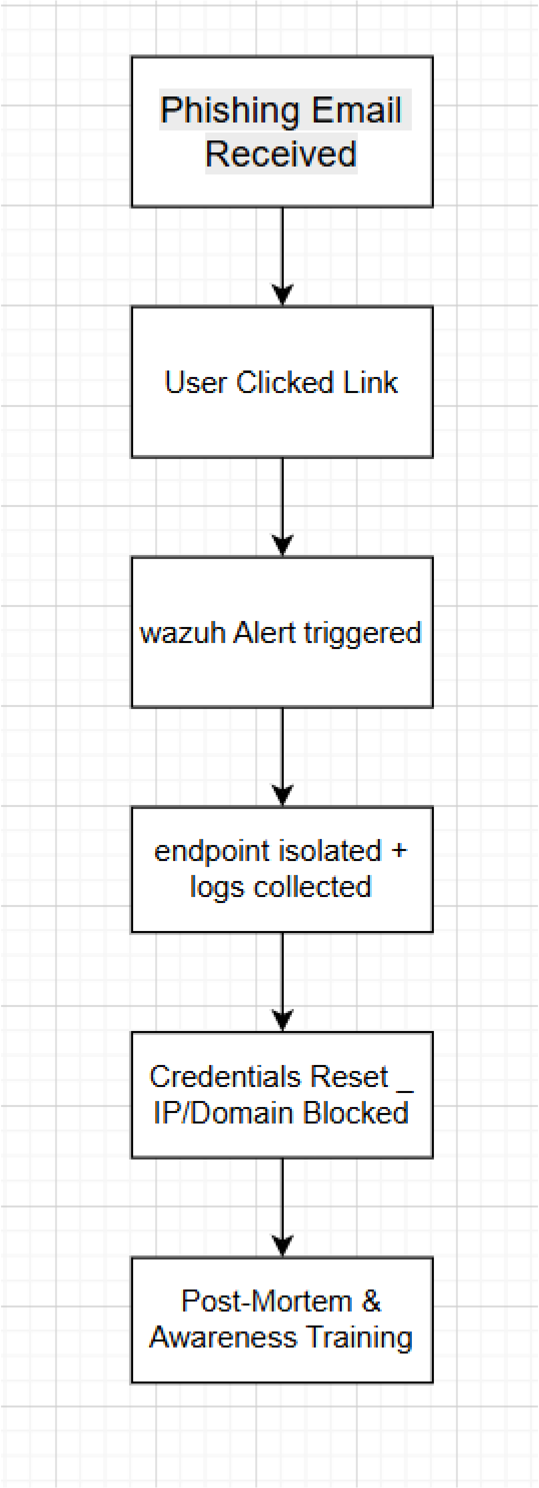
- ☐ Verified email headers (SPF/DKIM/DMARC check)
- ☐ Checked the link on VirusTotal (confirmed malicious)
- ☐ Identified and isolated the affected user’s system
- ☐ Reset credentials and enforced MFA
- ☐ Blocked malicious IP/domain on firewall and gateway
- ☐ Documented actions and findings in IR report

6. Post-Mortem (Lessons Learned)

The SOC team responded quickly, and containment was effective. Still, the user clicked the phishing link before reporting, showing a gap in awareness. Our email filtering rules also missed the spoofed sender.

Summary :

The phishing incident was handled promptly, with minimal impact. The main improvement areas are user training and email filtering. Regular phishing simulations will be conducted, and email gateway rules will be tightened. This will help reduce the likelihood of users interacting with malicious links in the future.


Phishing Email Received
User Clicked Link
wazuh Alert triggered
endpoint isolated + logs collected
Credentials Reset _ IP/Domain Blocked
Post-Mortem & Awareness Training