# Mock Incident Report - Phishing Attack

Mock Incident Report - Phishing Attack

Executive Summary:
On 2025-08-18, the SOC detected a phishing campaign targeting internal staff. A suspicious email contained a link to a creden

Timeline:
2025-08-18 14:00 - Alert triggered in Wazuh.
2025-08-18 14:10 - Analyst isolated affected mailbox.
2025-08-18 14:30 - IOC validated with VirusTotal.
2025-08-18 15:00 - Users notified, block applied.

Impact Analysis:
No accounts compromised. Attempted data theft mitigated before success. Minimal business disruption.

Remediation Steps:
- Blocked malicious domain.
- Reset potentially exposed credentials.
- Updated phishing awareness training.

Lessons Learned:
Improve email filtering, enhance user training, implement automated IOC blocking.