Phishing Incident Response – Case 2025-05-22

Purpose

Provide step-by-step guidance for responding to phishing emails like the one reported by Astor Mydz.

Scope

Applicable for Finance Department emails and any alerts triggered in the SIEM.

Steps

1. **Initial Report**
   - User reports suspicious email.
   - Log the report in SOC system.
2. **Investigation**
   - Verify sender and links.
   - Check SIEM for related alerts.
3. **Containment**
   - Block domain `malicious-domain.com`.
   - Reset passwords for affected users.
4. **Eradication**
   - Remove email from inboxes.
   - Scan endpoints for malware.
5. **Recovery**
   - Confirm no unauthorized transactions occurred.
   - Validate account integrity.
6. **Notification**
   - Inform affected users and department heads.
   - Share phishing awareness tips.
7. **Post-Incident**
   - Document IoCs: domain, IP, file hash.
   - Update SOC records and threat intel feeds.