socauthority.com

INCIDENT RESPONSE RUNBOOK BUNDLE

Four production-tested response playbooks for security teams and managers.

Phishing **Ransomware** **Credential Compromise** **Insider Threat**

Phase-by-Phase Steps	Communication Scripts	Evidence Checklists	Post-Incident Template

Built from 10 years of hands-on SOC operations at major Canadian financial institutions. Every step in these runbooks has been executed on real incidents using CrowdStrike, Splunk, and Microsoft Sentinel.

7. Block the sender domain and sending IP at your email gateway for all users, not just the reporter.
8. Block the malicious URL or domain at your web proxy and DNS filter.
9. If anyone opened an attachment or clicked a link: isolate the endpoint through your EDR before doing anything else. In CrowdStrike, right-click the host and select Network Isolation.
10. Quarantine the email from all mailboxes using the Defender portal Threat Explorer or your equivalent platform.
11. If credentials may have been entered: force a password reset and revoke all active sessions in Entra ID immediately.
12. Disable any inbox forwarding rules on the affected account. Attackers configure these within minutes of a successful phish.

PHASE 3 INVESTIGATE

Build the full picture before you close anything.

13. On the isolated endpoint, pull the process tree for the 30 minutes following the email open. Look for child processes spawned by your email client, browser, or Office applications.
14. Run this CrowdStrike LogScale query to find post-click activity on the affected host:

```
#event_simpleName=ProcessRollup2
ComputerName=<AFFECTED_HOST>
ParentBaseFileName IN ("WINWORD.EXE","EXCEL.EXE","OUTLOOK.EXE",
  "chrome.exe","msedge.exe","firefox.exe")
| table @timestamp ComputerName UserName ImageFileName CommandLine
ParentBaseFileName
| "sort" @timestamp desc
```

15. Check for new scheduled tasks (EventCode 4698), new services (EventCode 7045), and new registry run keys on the affected host.
16. Check Azure Sign-In logs for successful authentications from new countries or IP addresses in the 72 hours following the phishing email.
17. Check for OAuth application grants made under the affected identity in the past 30 days.
18. Document every indicator of compromise: sending IP, URLs, file hashes, C2 IPs, and MITRE techniques identified.

PHASE 4 ERADICATE AND RECOVER

Return the environment to a known good state.

19. If any payload executed on the endpoint: reimage the machine from a known clean baseline.
20. Re-enable the account only after password reset, MFA re-enrollment, and session revocation are all confirmed complete.
21. Submit IOCs to your threat intel platform and to your email gateway vendor.
22. Require the affected user to complete phishing awareness training before returning to full email access.