Cyber Incident Response Training Report

Date: 2025-12-26 16:02:12.215542

Scenario Summary

The analyst sees an alert from the endpoint security tool indicating "Suspicious Encryption Activity" on FINANCE-PC-23. The alert details show that the process `svchost.exe` is performing unusual encryption operations, with a high volume of file modifications in the user's Documents folder. Windows Event Logs reveal multiple `4663` (file access) events for sensitive files like `Q3_Financial_Report.xlsx`. A user report from the finance team mentions their workstation is running slowly, and files are inaccessible. The SIEM shows no recent outbound connections from FINANCE-PC-23, but the endpoint agent flags `svchost.exe` as having an unrecognized parent process. Next steps: isolate the host, check for ransomware indicators, and review recent logins.

Action Timeline

1. The analyst sees an alert from the endpoint security tool indicating "Suspicious Encryption Activity" on FINANCE-PC-23. The alert details show that the process `svchost.exe` is performing unusual encryption operations, with a high volume of file modifications in the user's Documents folder. Windows Event Logs reveal multiple `4663` (file access) events for sensitive files like `Q3_Financial_Report.xlsx`. A user report from the finance team mentions their workstation is running slowly, and files are inaccessible. The SIEM shows no recent outbound connections from FINANCE-PC-23, but the endpoint agent flags `svchost.exe` as having an unrecognized parent process. Next steps: isolate the host, check for ransomware indicators, and review recent logins.

2. check_auth_logs

3. After reviewing authentication logs, the analyst observes no anomalous logins to FINANCE-PC-23, but notices a suspicious `4624` (successful login) event from a local admin account (`FIN-ADMIN-02`) at an unusual time (3:17 AM). The endpoint agent shows this account executed `svchost.exe` with elevated privileges. No lateral movement or remote logins are detected. The finance user confirms they did not initiate any admin actions. Next steps: investigate the admin account’s recent activity, check for scheduled tasks, and verify if backups are intact.

4. reset_user_password

5. After resetting the `FIN-ADMIN-02` password, the analyst observes no new suspicious logins, but the endpoint agent still reports ongoing encryption activity on FINANCE-PC-23. The process tree shows `svchost.exe` is now spawning child processes under a different user context (`SYSTEM`). File modifications continue in the Documents folder, with extensions changing to `.locked`. The finance user reports more files are now inaccessible. Next steps: isolate the host immediately, check for persistence mechanisms, and verify backup integrity before the encryption spreads.

6. isolate_host

7. After isolating FINANCE-PC-23, the analyst sees encryption activity halt in real-time logs, and no new file modifications are detected. The endpoint agent confirms the host is offline, and network traffic from the workstation ceases. The finance user reports no further file accessibility issues. The SIEM shows no signs of lateral movement or additional compromised hosts. Next steps: begin forensic analysis on the isolated host, restore affected files from backups, and prepare a user communication plan. Containment appears successful—focus shifts to recovery and investigation.

8. escalate

9. The analyst sees the incident ticket updated with Tier 2/IR team ownership, and a request for additional forensic details. The SIEM shows no new alerts related to FINANCE-PC-23, and the isolated host remains offline. A notification from the backup team confirms recent financial files are recoverable. The IR team asks for a timeline of events, process dumps, and memory captures from the endpoint. Next steps: assist with evidence collection, monitor for any residual activity, and await IR team guidance on recovery steps. The incident is stable—no further spread detected.

10. close_incident

11. The analyst sees the incident ticket marked as "Resolved" with a summary noting successful containment, no lateral movement, and file recovery from backups. The IR team's final report confirms the ransomware was limited to FINANCE-PC-23, and the root cause was likely a phishing email. The finance user's workstation is reimaged and restored to service. The SOC manager requests a lessons-learned review to reinforce email hygiene training. No further action is required—incident is closed.

Final Score

Score: 91/100

Readiness Level: Tier-2 Ready