SOC response workpack

Turn an alert into an incident decision, evidence and a recovery test.

Printable workpaper. The detailed guide and all scenario branches are in the Markdown file.

Enterprise SOC and incident teams. Do not upload real keys, session tokens or personal logs; evidence remains in the organization’s authorized repository.

Process and expected evidence

1. Enrich the alert

Alert ID and scoped initial record

2. Establish decision and scope

Incident decision and timeline

3. Contain

Authorized action and execution result

4. Test persistence and recovery

Persistence review and retest

5. Translate learning into actions

Action, owner and verification plan

Work record

Scope / date:
Business / technical owner:
Decision and rationale:
Evidence reference / retest:

Example and closure

Fictional example; not evidence of actual work.

Time / zone: 10:15 UTC

Source: Synthetic identity log

Finding: Old session active

Hypothesis: Token may persist

Decision: Revoke and test

Authority: Incident lead

Action: Fictional IR-014

Verification: Old session access rejected

Closure checklist

[ ] Time zones consistent.

[ ] Findings and hypotheses separated.

[ ] Action authority and evidence trail recorded.

[ ] Recovery and learning actions tracked.

Official sources

NIST SP 800-61 Rev. 3 — Final, April 2025

https://csrc.nist.gov/pubs/sp/800/61/r3/final

NIST Cybersecurity Framework 2.0

https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final