

Supply Chain Incident Response Checklist

Act on a credible warning: coordinate the response, contain the threat, and assess potential exposure.

Incident / lead / time opened (UTC): _____

Endpoint / identity / CI owners: _____

Trusted channel / fallback / next update: _____

Record all times in Coordinated Universal Time (UTC). Run containment, investigation, and communication in parallel. For each item, record **owner**, **scope**, **time in UTC**, and **evidence reference** in the incident record. Tick only for the scope supported by evidence. Keep unknowns open; mark N/A with a reason.

1. Assign response owners and open a trusted channel

- ☐ **01 - Reach someone authorized to contain.** Establish a trusted channel, response lead, technical owners, and escalation backup. Use an independent route if normal accounts or channels are suspect. **Evidence:** owners acknowledge authority and assignments; first update time recorded.
- ☐ **02 - Record the warning and direct action.** Save the advisory or event, affected identifiers, discovery time, and earliest plausible exposure. Tell affected teams what to stop, preserve, and report. **Evidence:** warning retained, instructions acknowledged, unknown dates flagged.

2. Interrupt execution and access

03 - Contain the initial threat. Apply every scenario that fits.

- ☐ **A - Compromised dependency or developer tool.** Block compromised versions across endpoints, CI, mirrors, and caches; pause affected installs, updates, builds, and releases. **Evidence:** package/tool versions or hashes; install/update logs tied to endpoints and CI runs; matching package, proxy, or endpoint deny rules/events.
- ☐ **B - Pull request crossing a trust boundary.** For public forks or internal cross-team contributions, stop affected jobs and block privileged execution and suspect artifact/cache handoffs. **Evidence:** triggering event, approved/executed commit SHAs, job dispositions, and verified permission restrictions.
- ☐ **C - Suspected insider misuse.** Have an independent administrator restrict implicated access and protect evidence outside that authority; involve insider-response and HR/legal contacts. **Evidence:** identity-linked audit events (repository access, workflow/permission changes, new credentials); role/change approvals; revocation results for sessions, tokens, keys, and delegated grants.

Shared response - continue here for all scenarios

- ☐ **04 - Isolate affected execution environments.** Isolate suspect endpoints/runners; preserve volatile evidence before destructive cleanup without delaying containment. **Evidence:** host/runner IDs with isolation acknowledgments or network restrictions; runner job intake disabled; collection manifest naming logs, configuration, samples, collection times, and hashes.
- ☐ **05 - Revoke credibly exposed access now.** From a trusted environment, prioritize administration, publishing, signing, and production access without waiting for misuse. **Evidence:** token/key IDs mapped to identities and permissions, issuer revocation/disablement results, effective times, and unresolved failures. Isolation does not invalidate stolen credentials.
- ☐ **06 - Address surviving and newly issued access.** Inventory active sessions, refresh tokens, derived credentials, and newly added keys/apps/accounts/grants. Restrict authority to mint replacements. **Evidence:** issuance records and invalidation/removal results; each surviving credential's expiry, interim restriction, and owner.
- ☐ **07 - Verify containment persists.** Check who or what can undo package, workflow, network, or identity blocks. **Evidence:** enforced rules; control evaluations or harmless test results; admin permissions and automation configurations that could recreate access; owner and revalidation trigger.

3. Establish the Blast Radius

- ☐ **08 - Build or refresh the Blast Radius prediction.** Trace what affected identities, credentials, sessions, and delegated automation could read, change, trigger, or publish. **Evidence:** access map supported by exposure-window permission snapshots, secret bindings, role-assumption policies, and workflow permissions; record assumptions, unresolved paths, and historical configurations that cannot be reconstructed.

Handoff: affected scope / outstanding blocks / evidence owner: _____

Supply Chain Incident Response Checklist

Determine what happened, restore trusted operations, and strengthen readiness for the next incident.

Incident / lead / time updated (UTC): _____

3. Establish the Blast Radius (continued)

- ☐ **09 - Secure queryable evidence and verify coverage.** Retrieve protected endpoint, source-control, CI, identity, cloud, and registry records; record custodians. **Evidence:** each source's covered time range, retention, collection gaps/delays, preserved originals, and queries retrieving a known event. Bound conclusions to verified coverage.
- ☐ **10 - Follow activity across trust boundaries.** Trace execution and subsequent access; distinguish fetched/installed/executed and accessible/accessed/exfiltrated. **Evidence:** linked event IDs and saved queries connecting workflow runs, credential issuance, cloud activity, and newly created credentials. Record per-system conclusions and a timeline; separate verified connections from inferred links.
- ☐ **11 - Account for data and released outputs.** Quarantine suspect outputs; trace exposed data and recipients. Preserve evidence before public-data removal. **Evidence:** affected commits, package versions, image digests, build runs, deployment locations, known downloads/consumers, and quarantine/removal results. Record distribution you cannot account for; removal cannot retract copies.
- ☐ **12 - Communicate bounded conclusions.** State confirmed facts, possible exposure, unknowns, actions, and next update. Assign upstream and customer/partner communication through designated owners. **Evidence:** decision and message record, affected scope, acknowledgments, next owner/time; restrict sensitive attribution and evidence access.

4. Recover and authorize a defined scope

- ☐ **13 - Restore through a trusted path.** Rebuild from reviewed inputs and trusted build/deploy authority; preserve evidence before clearing contaminated caches/mirrors. **Evidence:** rebuilt host/runner image IDs, reviewed workflow commits, resolved dependency versions, replacement artifact digests, and connecting build/deployment records. Test independent restoration where needed; a signature alone does not establish safety.
- ☐ **14 - Reissue only necessary access.** Issue replacement credentials to trusted systems after relevant invalidation, using minimum permissions and short lifetimes where supported. **Evidence:** replacement identity/credential IDs, actual permissions, lifetimes, owners, and receiving systems. Compare with pre-incident access to avoid restoring excess privileges.
- ☐ **15 - Approve resumption per system or service.** Review containment, evidence coverage, recovered environments, and output integrity. **Evidence:** lead/service-owner approval naming systems and validation results; accepted gaps, remaining restrictions, monitoring/alert records, monitoring owner/duration, and triggers for renewed containment. A successful build does not clear the incident.
- ☐ **16 - Close with accountable follow-up.** Assign unresolved investigation, detection, access, and recovery improvements. **Evidence:** owners, deadlines, and scheduled verification exercises; retained decision/evidence record. Track warning-to-action delays and evidence gaps without inventing missing timestamps.

Readiness: build tabletop exercises from this checklist

Build exercises around your own environment. Assign follow-up actions and verify procedures through safe technical tests.

- ☐ **P1 - Test your Blast Radius prediction.** Choose a starting point from your threat model and trace direct and delegated access. **Exercise output:** an access map, assumptions to validate, and opportunities to reduce access.
- ☐ **P2 - Test your ability to investigate.** Identify the records needed to establish what happened and where visibility may be incomplete. **Exercise output:** evidence sources, access owners, usable queries, and gaps to address.
- ☐ **P3 - Test containment and recovery decisions.** Establish who can take action, what they need to act, and what would justify resuming operations. **Exercise output:** decision owners, escalation routes, containment procedures, and recovery criteria.

Recovery approval / scope / accepted gaps reference: _____

Next review / monitoring owner / follow-up reference: _____