CORVASEC

Cybersecurity Incident Response Checklist

A practical incident-response checklist for preparation, detection, triage, containment, eradication, recovery, evidence handling, and lessons learned.

DOCUMENT CENTER

Compiled September 2026

This checklist supports incident-response organization; it does not replace organizational policy, legal advice, forensic procedures, safety requirements, or contractual/regulatory obligations.

Use this guide as a practical reference. Verify commands, targets, permissions, paths, versions, and organizational policy before making changes. Examples with placeholders must be adapted to the environment.

Contents

#	Section	Entries
1	Preparation and readiness	6
2	Detection and initial triage	8
3	Containment	6
4	Eradication and remediation	6
5	Recovery	5
6	Post-incident improvement	6
7	Evidence handling quick checklist	9

Total reference entries: 46

1. Preparation and readiness

Check	Action	Evidence / Output
1	Confirm incident roles, contacts, escalation paths, legal/privacy requirements, and decision authority.	Current IR plan and contact roster
2	Verify time synchronization and logging coverage for critical systems.	NTP status, log-source inventory
3	Confirm backups, recovery procedures, isolation methods, and known-good administrative access.	Recovery runbooks, break-glass accounts
4	Maintain clean tools and approved evidence storage.	Tool hashes, evidence repository
5	Define severity criteria and incident categories.	Severity matrix
6	Document normal business services and critical asset owners.	Asset/service inventory

2. Detection and initial triage

Check	Action	Questions
1	Record the alert/report exactly as received.	Who/what generated it? When? What asset/user?
2	Assign an incident identifier and start a timeline.	What is known vs assumed?
3	Validate whether the activity is real, duplicate, expected, or false positive.	Can it be reproduced/correlated?
4	Identify affected accounts, hosts, applications, data, and network segments.	What is the initial scope?
5	Preserve volatile evidence when justified before rebooting or reimaging.	What evidence would be lost?
6	Capture key log sources and relevant timestamps.	Security, EDR, firewall, DNS, proxy, identity, cloud, application?
7	Assess business impact and safety/mission impact.	Is service interruption occurring?
8	Set an initial severity and escalation level.	Does this require leadership/legal/privacy notification?

3. Containment

Check	Action	Considerations
1	Choose short-term containment that limits damage while preserving evidence.	Host isolation, account disable/reset, rule block, token/session revocation.
2	Avoid destroying evidence unless immediate harm requires it.	Coordinate with forensic/legal requirements.
3	Document every containment action and exact time.	Who approved and executed the action?
4	Check for alternate access paths and related assets.	Other sessions, accounts, hosts, cloud tokens, persistence.
5	Protect backups and management infrastructure.	Prevent incident spread to recovery systems.
6	Communicate service-impacting changes to owners.	Maintain operational awareness.

4. Eradication and remediation

Check	Action	Validation
1	Identify root cause and persistence mechanisms.	Evidence supports the identified entry/persistence path.
2	Remove malicious artifacts, unauthorized accounts, tasks, services, rules, and tokens.	Compare against known-good state.
3	Patch exploited vulnerabilities and remediate misconfiguration.	Version/configuration verified.
4	Rotate exposed credentials and secrets at the correct scope.	Old secrets revoked; dependencies updated.
5	Harden affected systems and reduce unnecessary exposure.	Configuration review completed.
6	Scan/corroborate related systems for the same indicators.	No remaining matching indicators or behavior.

5. Recovery

Check	Action	Success criteria
1	Restore from known-good state or rebuild when appropriate.	Integrity and business function validated.
2	Reconnect systems in a controlled sequence.	Monitoring active before exposure is restored.
3	Monitor for recurrence using high-value indicators and behavior.	No reappearance across defined observation window.
4	Confirm users, services, authentication, backups, and logging are healthy.	Operational owner signs off.
5	Close temporary containment rules only after risk is addressed.	Change documented and approved.

6. Post-incident improvement

Check	Action	Deliverable
1	Finalize timeline, scope, impact, root cause, and response actions.	Incident report
2	Document what worked and what slowed the response.	Lessons learned
3	Create corrective actions with owners and due dates.	Remediation tracker
4	Update detections, playbooks, asset data, and hardening guidance.	Improved controls
5	Retain evidence according to policy and legal requirements.	Evidence disposition record
6	Measure time to detect, contain, recover, and lessons implemented.	Metrics and trend report

7. Evidence handling quick checklist

Item	Record
`Evidence ID`	Unique identifier
`Source`	Host/account/system/location
`Collector`	Person/tool
`Date/time`	Include timezone
`Hash`	SHA-256 where applicable
`Method`	Acquisition/export procedure
`Storage`	Protected evidence location
`Transfers`	Chain-of-custody entries
`Notes`	Known limitations or transformations

Authoritative references

Use vendor and standards documentation for exact syntax, current behavior, version-specific details, licensing, and policy requirements.

NIST SP 800-61 Rev. 3

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

NIST Cybersecurity Framework 2.0

https://www.nist.gov/cyberframework