CS-096 · Incident Response

Incident Response: Eradication

Removing the threat and closing the door it came through so the attacker cannot return.

Executive Summary

Eradication is the phase where the team fully removes the threat from the environment and closes the weakness that let it in. It goes beyond stopping the spread to eliminating malware, backdoors, and attacker access, and to fixing the root cause. If eradication is incomplete, the attacker comes back and the whole cycle starts again.

What It Is

Eradication is the fourth phase of the incident response lifecycle. Where containment stops an incident from spreading, eradication removes it entirely: deleting malware, closing backdoors, revoking stolen or added credentials, and eliminating any persistence the attacker set up so they cannot quietly return. It also addresses the root cause, the underlying weakness such as an unpatched vulnerability or a misconfiguration that allowed the compromise. In the lifecycle described by NIST SP 800-61 and SANS incident handling, eradication follows containment and precedes recovery. In practice eradication and recovery are closely linked, because removing the threat and restoring clean systems often happen together, but the distinction matters: eradication is about getting rid of the threat, recovery is about safely returning to normal.

Why It Matters

Incomplete eradication is one of the most common reasons an organization gets hit again by the same attacker. Modern intruders plant multiple footholds precisely so that removing one does not lock them out, and they often lie low after initial containment. If the team cleans the obvious malware but misses a hidden backdoor or leaves the original vulnerability open, the attacker simply walks back in, sometimes with more caution the second time. Eradication is also where

root-cause thinking pays off, because fixing only the symptom guarantees a repeat. For professionals, thorough eradication reflects deep technical skill and discipline, and the ability to confirm a threat is truly gone is a defining strength of experienced DFIR analysts and incident responders.

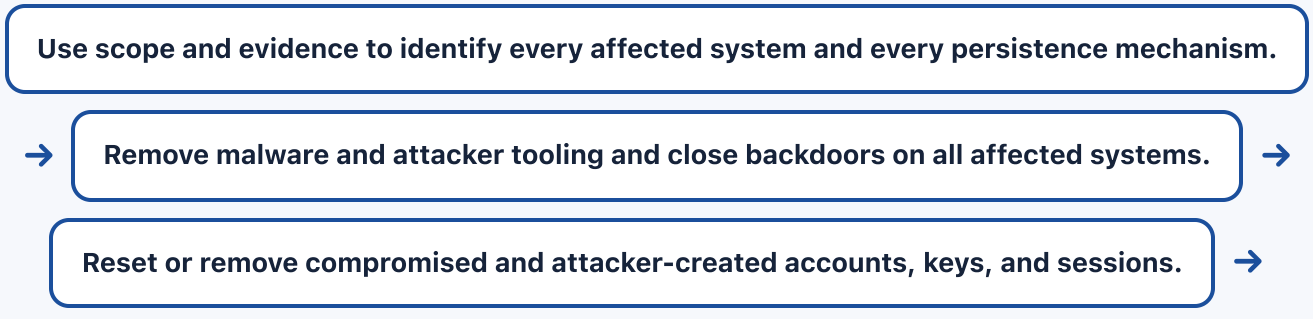
How It Works

Eradication builds directly on the scope and evidence gathered earlier, because you cannot remove what you have not found. The team identifies every affected system and every mechanism of persistence, then removes malware and attacker tooling, closes backdoors, and resets or removes compromised and attacker-created accounts and keys. For heavily compromised systems, rebuilding from a known-good image is often safer than trying to clean in place, because it removes the uncertainty of a hidden implant. Crucially, the team fixes the root cause by patching the exploited vulnerability, correcting the misconfiguration, or removing the exposed service, so the same door does not stay open. Before declaring eradication complete, responders verify that the threat is actually gone through scanning, hunting for remaining indicators, and monitoring for signs of return. All of this is documented, because it feeds recovery and the lessons-learned review.

Architecture Diagram

Eradication is the fourth phase: it removes the threat contained earlier and fixes the root cause before recovery.

Visual Workflow



Rebuild heavily compromised systems from a known-good image where appropriate. →

Fix the root cause by patching, reconfiguring, or removing the exposed weakness. →

Verify eradication through scanning, threat hunting, and monitoring before moving to recovery.

Common Attacks

- Hidden backdoors or implants that survive removal of the obvious malware
- Multiple footholds planted so removing one does not lock the attacker out
- Attacker-created accounts, keys, or scheduled tasks that provide quiet re-entry
- Leaving the exploited vulnerability unpatched so the same door stays open
- Reinfection when a system is restored from a backup that already contained the threat

Common Mistakes

- Removing symptoms without finding and fixing the root cause
- Cleaning only the systems seen first and missing others in the true scope
- Trusting an in-place cleanup on a deeply compromised host instead of rebuilding
- Declaring eradication complete without verifying the threat is actually gone
- Forgetting to rotate credentials and secrets the attacker may have stolen

Best Practices

- Drive eradication from a confirmed scope so no affected system is left behind
- Rebuild deeply compromised systems from known-good images rather than cleaning in place
- Fix the root cause, not just the visible symptom of the compromise
- Rotate credentials, keys, and secrets that the attacker could have accessed
- Verify removal with scanning, threat hunting, and heightened monitoring
- Coordinate closely with recovery so clean systems are not reinfected on restore

Quick Checklist

- [x] Full scope confirmed and every affected system identified
- [x] Malware, tooling, and backdoors removed across all affected systems
- [x] Compromised and attacker-created accounts and keys reset or removed
- [x] Root cause fixed through patching or reconfiguration
- [x] Credentials and secrets rotated where exposure is possible
- [x] Removal verified by scanning, hunting, and monitoring before recovery

Recommended Tools

EDR
Removes malicious processes and files and confirms endpoints are clean

Vulnerability scanner
Confirms the exploited weakness is fixed and finds related exposures

Forensic and threat-hunting tools
Locate hidden persistence and confirm the threat is fully removed

Identity and access management
Rotates and removes compromised and attacker-created accounts and keys

Industry Standards

NIST SP 800-61
Computer Security Incident Handling Guide covering eradication and root-cause fixing

NIST SP 800-40
Guidance on patch management, central to closing the exploited weakness

NIST Cybersecurity Framework (CSF) 2.0
The Respond function frames threat removal activities

Career Relevance

Eradication is deep technical work for DFIR analysts, incident responders, and security engineers, who must find and remove persistence, fix root causes, and prove the threat is gone. SOC analysts support with scanning and verification. The discipline to confirm complete removal, rather than assuming it, is a defining strength that senior security employers listed on AI-Governance-Jobs.com look for.

Interview Questions

- How do you make sure you have removed every foothold an attacker planted?
- When would you rebuild a system from a known-good image instead of cleaning it in place?
- Why is fixing the root cause essential, and how do you identify it?
- How do you verify that a threat has actually been eradicated?
- Why must credentials and secrets be rotated during eradication?

Related Certifications

GIAC Certified Forensic Analyst (GCFA) | GIAC Certified Incident Handler (GCIH) | CompTIA CySA+

Further Reading

- NIST SP 800-61 Computer Security Incident Handling Guide
- CISA: Incident Response Guidance
- SANS Incident Response Resources

Key Takeaways

- Eradication removes the threat entirely and fixes the weakness that let it in.
- Incomplete eradication is a leading reason attackers return after an incident.
- Rebuilding from known-good images is often safer than cleaning a deeply compromised host.
- Fixing the root cause and rotating exposed secrets prevents an immediate repeat.

- Verifying removal, not assuming it, is a defining strength of experienced responders.

FAQ

Related Careers

RELATED ROLES

Incident Responder | Soc Analyst | Dfir Analyst | Security Engineer

RELATED CERTIFICATIONS

GIAC Certified Forensic Analyst (GCFA) | GIAC Certified Incident Handler (GCIH) | CompTIA CySA+

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Incident Response: Eradication**
3. Go deeper: Incident Response: Preparation
4. Go deeper: Incident Response: Identification
5. Validate it: work toward **GIAC Certified Forensic Analyst (GCFA)**

6. Find the role: browse current openings

RELATED SHEETS

- CS-093 Incident Response: Preparation
- CS-094 Incident Response: Identification
- CS-095 Incident Response: Containment
- CS-097 Incident Response: Recovery
- CS-098 Incident Response: Lessons Learned
- CS-099 Digital Evidence
- CS-086 SIEM
- CS-001 Cybersecurity