CS-093 · Incident Response

Incident Response: Preparation

Getting ready before an incident so the team can act fast and correctly under pressure.

Executive Summary

Preparation is the first phase of the incident response lifecycle, and it is the work done before any incident occurs. It builds the plan, the team, the tools, and the practiced habits that let an organization respond quickly and calmly when an attack happens. Everything that comes later in the lifecycle depends on how well this phase was done.

What It Is

Preparation is the foundation phase of incident response. It covers writing and approving an incident response plan, naming who does what, standing up communication channels, provisioning the tools responders will need, and rehearsing the whole thing so people are not learning on the job during a real crisis. In the widely used lifecycle described in NIST SP 800-61 and taught in SANS incident handling, preparation sits ahead of identification, containment, eradication, recovery, and lessons learned. It is the only phase that is entirely proactive. A useful way to think about it is that preparation turns a chaotic emergency into a rehearsed procedure.

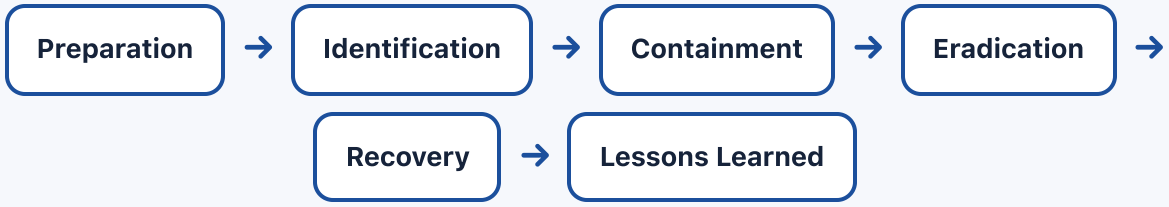
Why It Matters

When an incident hits, the clock starts and stress runs high, so there is no time to invent a process. Teams that prepared can move straight to containing damage, while unprepared teams lose critical hours deciding who is in charge, where the logs are, and who to call. That lost time often translates directly into more data stolen, more systems encrypted, and higher recovery cost. For professionals, preparation is where much of the durable career value in incident response lives, because building plans, running exercises, and improving readiness is steady work that continues between incidents, not just during them.

How It Works

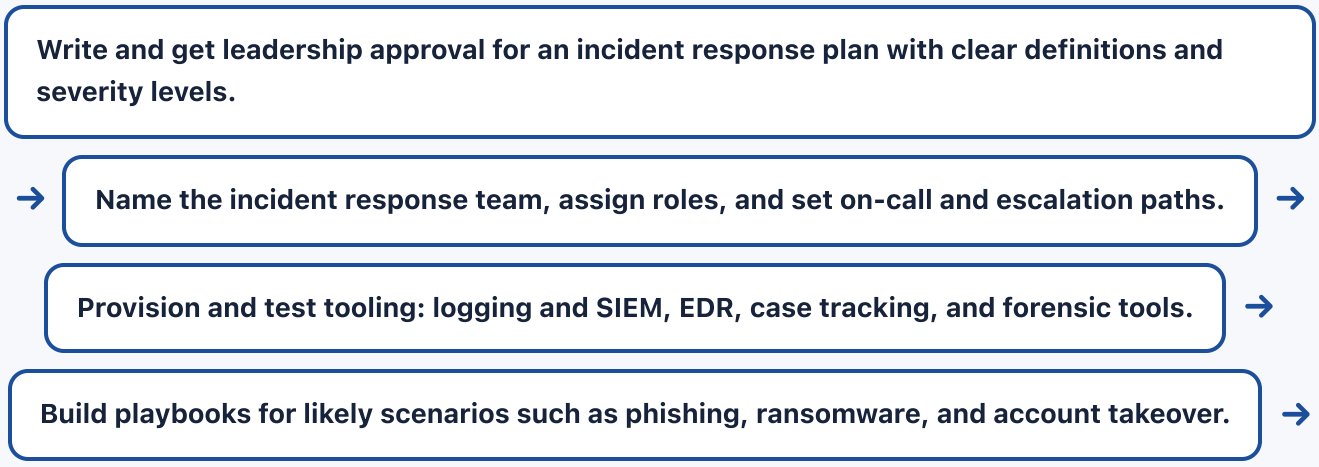
Preparation starts with a written incident response plan that defines what counts as an incident, how incidents are classified by severity, and the roles and responsibilities of everyone involved. From there the team assembles a computer security incident response team with clear on-call coverage and an escalation path to leadership, legal, and communications. Responders need ready access to tooling such as a SIEM for centralized logs, EDR on endpoints, a ticketing or case system to track the incident, and forensic and analysis tools that are installed and tested in advance. Just as important are the practiced parts: playbooks or runbooks for common scenarios, out-of-band communication so responders can talk even if normal systems are compromised, and regular tabletop and technical exercises that expose gaps while the stakes are low. Preparation is continuous, because the environment, the threats, and the team all change over time.

Architecture Diagram



Preparation is the proactive first phase that feeds the rest of the lifecycle: prepare, then identify, contain, eradicate, recover, and learn.

Visual Workflow



Establish out-of-band communication channels and contact lists for internal and external parties.

→ **Run tabletop and technical exercises regularly and fix the gaps they reveal.**

Common Attacks

- Being caught with no plan, so the first incident becomes an expensive live rehearsal
- Logging that is missing or too short, leaving no evidence to investigate later
- Contact lists and escalation paths that are out of date when an incident finally hits
- Forensic and response tools that were never installed, licensed, or tested before they are needed
- Reliance on normal email and chat that an attacker may be reading or has taken down

Common Mistakes

- Treating the plan as a document to file away rather than a procedure to rehearse
- Never running an exercise, so the first real test of the plan is a real incident
- Failing to define severity levels, so every alert is treated the same or ignored
- Leaving legal, communications, and executives out of the plan until it is too late
- Assuming backups exist and work without ever confirming it during preparation

Best Practices

- Base the plan on a recognized lifecycle such as NIST SP 800-61 or SANS incident handling
- Keep an up-to-date contact list including leadership, legal, insurers, and external responders
- Ensure centralized logging with retention long enough to investigate a real incident
- Pre-authorize common containment actions so responders do not wait for approval mid-crisis
- Run tabletop exercises at least yearly and after major changes, then track the fixes
- Store the plan and playbooks where they are reachable even if primary systems are down

Quick Checklist

- [x] Approved incident response plan with severity classifications
- [x] Named IR team with roles, on-call schedule, and escalation path
- [x] Centralized logging and SIEM with sufficient retention
- [x] EDR deployed and case tracking in place and tested
- [x] Playbooks for phishing, ransomware, and account takeover
- [x] Out-of-band communication channel established and known to the team
- [x] Tabletop or technical exercise completed in the last 12 months

Recommended Tools

SIEM
Centralizes and retains logs so responders have evidence when an incident starts

EDR
Monitors endpoints and gives responders visibility and control before and during an incident

Case or ticketing system
Tracks incident tasks, timeline, and decisions in one place

Out-of-band communication tool
Lets the team coordinate even if normal email and chat are compromised

Industry Standards

NIST SP 800-61
Computer Security Incident Handling Guide that defines the lifecycle and preparation expectations

NIST Cybersecurity Framework (CSF) 2.0
The Respond and Recover functions frame readiness activities

ISO/IEC 27035
International guidance on information security incident management planning

Career Relevance

Preparation is core work for incident responders, SOC analysts, DFIR analysts, and security engineers, and it is a frequent focus for GRC and security program managers who own the plan and the exercise schedule. Because so much of it happens between incidents, this phase is where junior analysts often build credibility and where leaders demonstrate program maturity to auditors, insurers, and executives, an audience AI-Governance-Jobs.com serves.

Interview Questions

- What belongs in an incident response plan, and how do you decide severity levels?
- How would you prepare a team so it can respond effectively at 3 a.m.?
- Why are out-of-band communications important during an incident?
- What is the value of a tabletop exercise, and how would you run one?
- How do you make sure the logging and tools you need will actually be there during an incident?

Related Certifications

GIAC Certified Incident Handler (GCIH) | CompTIA CySA+ | ISC2 CISSP (for program leadership)

Further Reading

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

Key Takeaways

- Preparation is the only fully proactive phase and it sets up every phase after it.
- A written, approved plan plus named roles and escalation paths removes confusion in a crisis.
- Logging, EDR, case tracking, and forensic tools must be ready and tested before an incident.

- Playbooks and regular exercises turn an emergency into a rehearsed procedure.
- Much of the career value in incident response lives in this between-incidents work.

FAQ

How is preparation different from the other incident response phases?

How often should we test our incident response plan?

Do small organizations really need a full IR plan?

Related Careers

RELATED ROLES

Incident Responder | Soc Analyst | Dfir Analyst | Security Engineer

RELATED CERTIFICATIONS

GIAC Certified Incident Handler (GCIH)

CompTIA CySA+

ISC2 CISSP (for program leadership)

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: Preparation**
3. Go deeper: Incident Response: Identification
4. Go deeper: Incident Response: Containment
5. Validate it: work toward **GIAC Certified Incident Handler (GCIH)**

6. Find the role: browse current openings

RELATED SHEETS

- CS-094 Incident Response: Identification
- CS-095 Incident Response: Containment
- CS-096 Incident Response: Eradication
- CS-097 Incident Response: Recovery
- CS-098 Incident Response: Lessons Learned
- CS-099 Digital Evidence
- CS-086 SIEM
- CS-001 Cybersecurity