CS-094 · Incident Response

Incident Response: Identification

Detecting, validating, and scoping a security incident so the team knows what it is dealing with.

Executive Summary

Identification is the phase where a possible incident is detected, confirmed as real, and scoped so the team understands what happened, what is affected, and how serious it is. It turns raw alerts and reports into a declared incident with a severity level. Getting this phase right prevents both wasted effort on false alarms and dangerous delay on real attacks.

What It Is

Identification is the second phase of the incident response lifecycle. It is the work of noticing that something may be wrong, validating whether it is truly a security incident rather than a false positive or a routine issue, and then determining its scope and severity. Signals come from many places at once: alerts from a SIEM or EDR, reports from employees, tips from external parties, and unusual patterns in logs. In the lifecycle described by NIST SP 800-61 and SANS incident handling, identification follows preparation and feeds containment. The core question in this phase is simple to state and hard to answer under pressure: is this an incident, and if so, how bad is it and what does it touch?

Why It Matters

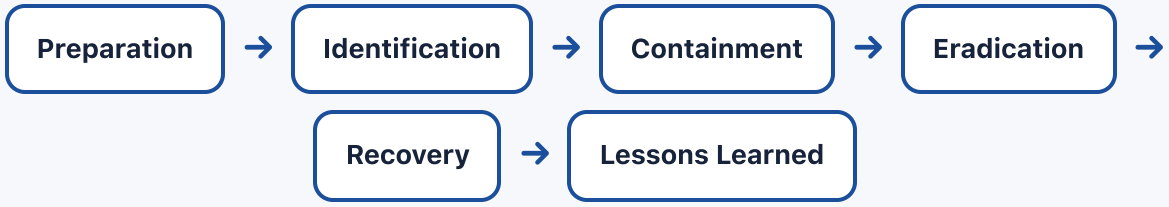
You cannot contain or fix what you have not detected and understood. Attackers often go undiscovered for a long time, and every hour of delayed identification gives them more room to steal data or spread. At the same time, security teams face floods of alerts, so a phase that cannot separate real incidents from noise leads to alert fatigue and missed attacks. Accurate scoping matters too: if the team underestimates what is affected, containment will miss compromised systems and the attacker returns. For professionals, strong detection and triage

skills are among the most sought after in security operations and digital forensics, because they are the difference between catching an intrusion early and reading about it in the news.

How It Works

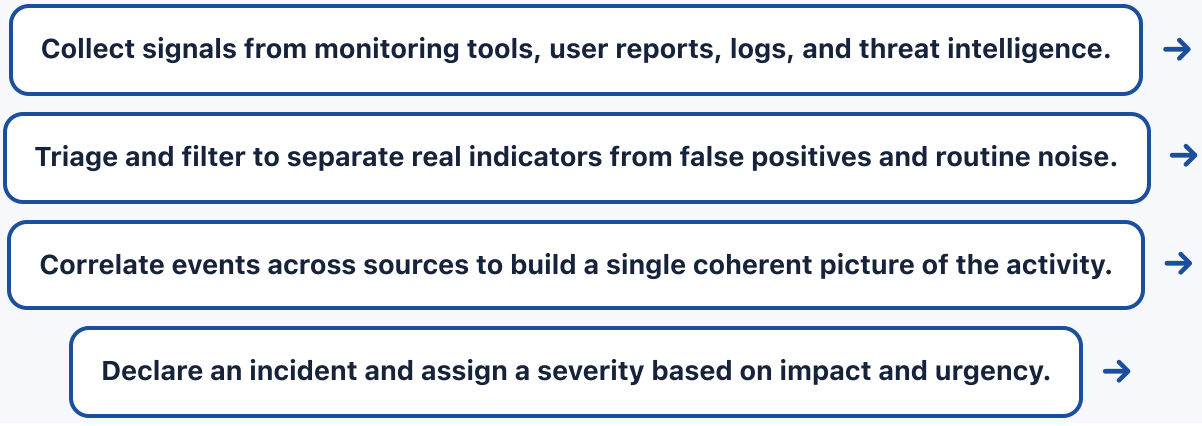
Identification begins with detection, drawing on monitoring tools, user reports, and threat intelligence. Analysts triage the incoming signals to filter out false positives and prioritize what looks real, correlating events across sources so a single alert becomes a coherent story. When the evidence supports it, the incident is formally declared and assigned a severity based on impact and urgency, which drives who is notified and how fast the team moves. The team then scopes the incident by asking which accounts, hosts, data, and services are involved and how far the activity has spread. Throughout, responders document what they find and preserve evidence carefully so it stays useful for later analysis and any legal or regulatory needs. The output of this phase is a clear, documented picture that lets the team move confidently into containment.

Architecture Diagram



Identification is the second phase: it takes readiness from preparation and produces a declared, scoped incident for containment.

Visual Workflow



Scope the incident: which accounts, hosts, data, and services are affected. →

Document findings and preserve evidence so it remains usable later.

Common Attacks

- Attacker dwell time where an intrusion goes undetected for weeks or months
- Alert fatigue that buries a real incident under a flood of low-value alerts
- Attackers deleting or altering logs to hide their activity from responders
- Living-off-the-land techniques that blend malicious action into normal admin activity
- Under-scoping the incident so compromised systems are missed and the threat persists

Common Mistakes

- Jumping to containment before confirming the incident is real and understanding its scope
- Tuning out or disabling alerts instead of tuning the rules that generate the noise
- Failing to preserve evidence, which weakens later forensics and legal options
- Treating a single alerting system as the only source of truth
- Not documenting the timeline as it unfolds, leaving gaps that are hard to reconstruct later

Best Practices

- Centralize and correlate telemetry so detection is not siloed by tool
- Define clear, repeatable triage and severity criteria before incidents happen
- Make it easy for employees to report suspicious activity and treat those reports seriously
- Use threat intelligence to recognize known indicators and attacker behaviors
- Preserve evidence with proper handling and a documented chain of custody
- Keep a running, timestamped incident timeline from the first signal onward

Quick Checklist

- [ ] Alerts triaged against defined criteria, not case by case

- [x] Incident formally declared with an assigned severity
- [x] Scope determined: affected accounts, hosts, data, and services listed
- [x] Evidence preserved with handling and chain of custody documented
- [x] Timeline started with timestamps and source of each finding
- [x] Stakeholders notified according to the severity level

Recommended Tools

SIEM
Correlates logs across sources to surface and confirm suspicious activity

EDR
Detects and shows malicious behavior on endpoints during triage and scoping

Threat intelligence feed
Provides indicators and context to recognize known attacks

Case or ticketing system
Captures the timeline, evidence, and severity decision in one record

Industry Standards

NIST SP 800-61
Computer Security Incident Handling Guide covering detection and analysis

MITRE ATT&CK
Common language for attacker techniques that aids detection and scoping

NIST Cybersecurity Framework (CSF) 2.0
The Detect function frames identification activities

Career Relevance

Identification is the daily work of SOC analysts and incident responders, and it draws heavily on the analysis skills of DFIR analysts and detection engineering by security engineers. Strong triage, correlation, and scoping ability separates effective analysts from those who drown in

alerts, and it is a frequent interview focus for security operations roles like those listed on AI-Governance-Jobs.com.

Interview Questions

- How do you decide whether an alert is a real incident or a false positive?
- Walk me through how you would scope an incident once it is confirmed.
- How would you assign severity to an incident, and why does severity matter?
- How do you handle alert fatigue without missing real attacks?
- What steps do you take to preserve evidence during identification?

Related Certifications

CompTIA CySA+ | GIAC Certified Incident Handler (GCIH) | GIAC Certified Detection Analyst (GCDA)

Further Reading

- NIST SP 800-61 Computer Security Incident Handling Guide
- CISA: Detecting and Responding to Cyber Threats
- SANS Incident Response Resources

Key Takeaways

- Identification detects, validates, and scopes a possible incident before any fix begins.
- Correlating signals from many sources beats relying on a single alert.
- Accurate scoping prevents missed compromised systems and repeat intrusions.
- Preserving evidence and keeping a timeline protects later forensics and legal needs.
- Triage and scoping skills are among the most in-demand in security operations.

FAQ

▶ **What is the difference between an event and an incident?**

▶ **How do you avoid missing real attacks in a sea of alerts?**

▶ **Why does scoping matter so much in this phase?**

Related Careers

RELATED ROLES

Incident Responder | Soc Analyst | Dfir Analyst | Security Engineer

RELATED CERTIFICATIONS

CompTIA CySA+

GIAC Certified Incident Handler (GCIH)

GIAC Certified Detection Analyst (GCDA)

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: Identification**
3. Go deeper: Incident Response: Preparation
4. Go deeper: Incident Response: Containment
5. Validate it: work toward **CompTIA CySA+**
6. Find the role: browse current openings

RELATED SHEETS

CS-093 Incident Response: Preparation
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