

Post-Incident Review Template

A comprehensive framework for analyzing security incidents and strengthening your defenses

CYBERSECURITY NON-PROFIT



Incident Summary

Basic Information

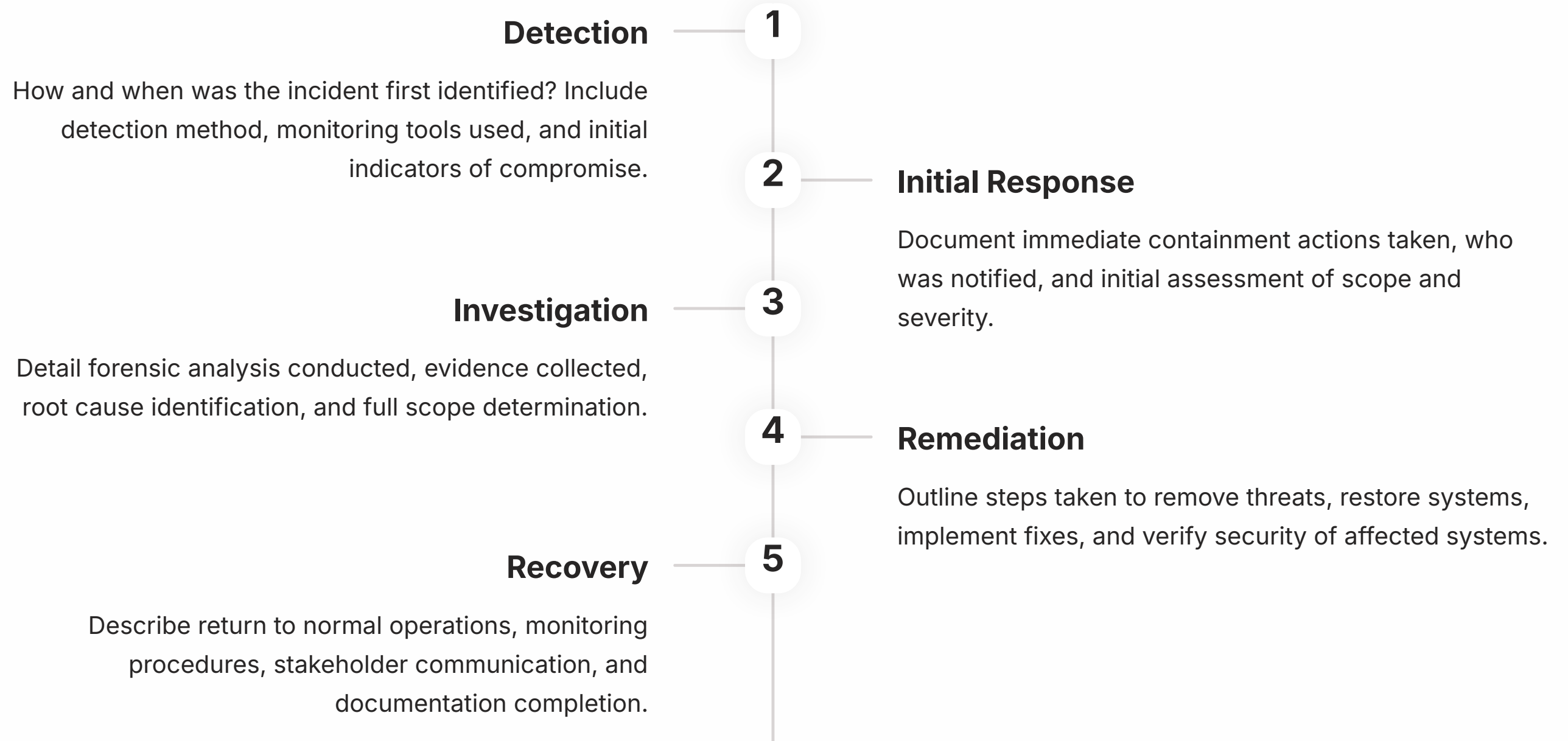
- Incident ID and classification
- Date and time of discovery
- Systems and data affected
- Severity level assessment

Impact Assessment

- Business operations disruption
- Data compromised or at risk
- Financial impact estimation
- Stakeholders affected

 Document the who, what, when, where, and why of the incident to establish a clear foundation for analysis.

Timeline and Response Actions





SECTION 3

Analysis: Strengths and Gaps

What Worked Well

List effective processes, tools, and team responses. Include successful detection methods, communication protocols that functioned smoothly, and containment strategies that limited damage.

Areas for Improvement

Identify gaps in detection capabilities, response procedures that need refinement, communication breakdowns, resource limitations, and documentation gaps that hindered the response.

Root Cause Analysis

Examine underlying factors that allowed the incident to occur. Consider technical vulnerabilities, process failures, human factors, and organizational issues that contributed.

Action Items and Recommendations

1

Immediate Actions
Critical fixes required within 24-48 hours. Address vulnerabilities exploited during the incident, update access controls, and implement emergency patches.

2

Short-Term (1-4 weeks)
Update incident response procedures, enhance monitoring capabilities, conduct targeted security training, and strengthen authentication measures.

3

Long-Term (1-6 months)
Implement comprehensive security improvements, update disaster recovery plans, invest in new security tools, and conduct regular tabletop exercises.

Assigned Ownership

Designate responsible parties for each action item with clear accountability and deadlines.

Success Metrics

Define measurable outcomes to track implementation progress and effectiveness of improvements.

About Cybersecurity Non-Profit

Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.



Business & Non-Profit Security



Family Cybersecurity



Kids Safety



Senior Digital Safety



Women's Security



Parents & Educators



Everything we offer is completely free. Visit csnp.org to learn more or explore csnp.org/resources for templates, guides, and training materials.

Visit CSNP

Free Resources