Incident Response Template (AI-Aware IR Framework)

1. Incident Overview

Incident ID:
Date/Time Detected:
Detected By (Tool/System):
Incident Type (Initial Classification):
Severity (Initial):
Status:

Summary (1–2 paragraphs):
Provide a concise description of the incident, including what triggered detection and why it matters.

---

2. Initial Context and Signals

Primary Alert(s):

- Source (SIEM, EDR, identity, cloud, etc.)
- Alert description
- Timestamp

Correlated Signals:

- Identity anomalies
- Endpoint activity
- Network behavior
- Cloud/API activity
- Threat intelligence matches

Initial Narrative:
Describe how these signals connect. This is critical and directly reflects your “alerts → context” philosophy.

---

3. Incident Classification

Incident Type (Refined):

- Credential compromise
- Phishing
- Malware
- Insider activity
- Data exfiltration
- Other

Confidence Level:

Low/Medium/High

Rationale:
Explain why this classification and confidence level were assigned.

---

4. Decision Framework (Core Section)

Dimension	Assessment	Notes
Confidence Level	Low/Medium/High	
Potential Impact	Low/Medium/High	
Speed of Progression	Slow/Moderate/Fast	
Reversibility of Action	Easy/Moderate/Difficult	

Recommended Action Based on Assessment:

- Monitor
- Investigate further
- Contain immediately
- Escalate

---

5. Investigation and Analysis

Scope of Investigation:

- Affected users
- Affected systems
- Affected data

Attack Path Reconstruction:

- Initial access
- Lateral movement
- Privilege escalation
- Data access/exfiltration

Timeline of Events:

Time Event Source

Key Findings:

- What is confirmed
- What is suspected
- What remains unknown

---

6. Containment Actions

Containment Strategy:

- Immediate
- Phased
- Monitored

Actions Taken:

- Endpoint isolation
- Account disablement
- Token/session revocation
- Network blocking

- Other

Automation vs. Human Decision:

- Automated actions taken
- Analyst-approved actions
- Escalated decisions

Business Impact Considerations:
Document any operational impact.

---

7. Eradication Activities

Root Cause Identified:

Yes/No

Persistence Mechanisms Identified:

Yes/No

Actions Taken:

- Malware/artifact removal
- Credential reset
- Patch applied
- Configuration corrected
- Access controls updated

Validation Steps:

- Systems verified clean
- No remaining persistence
- Monitoring in place

---

8. Recovery and Restoration

Systems Restored:

List of systems

Recovery Actions:

- Data restoration
- System rebuild
- Access re-enabled

Validation:

- Systems functioning normally
- No abnormal activity detected

Monitoring Period:
Define how long heightened monitoring will continue.

---

9. AI and Automation Considerations

AI Involvement in Detection or Response:

Yes/No

If Yes:

What role did AI play? (detection, prioritization, response recommendation)

Observations:

- Was AI accurate?
- Were there false positives/negatives?
- Any signs of adversarial manipulation?

Adjustments Required:

- Model tuning
- Threshold changes
- Additional validation steps

---

10. Communication and Escalation

Internal Stakeholders Notified:

- SOC
- IT
- Leadership
- Legal/Compliance

External Notifications (If Applicable):

- Customers
- Regulators
- Partners

Communication Summary:
Document key messages and timelines.

---

11. Lessons Learned

What Worked Well:

- Detection
- Response
- Coordination

What Did Not Work:

- Delays
- Missed signals
- Process gaps

Decision-Making Review:

- Were decisions timely?
- Were actions appropriate to risk?
- Any over- or under-reaction?

---

12. Improvements and Actions

Detection Improvements:

New rules or models

Playbook Updates:

Steps added/removed

Automation Changes:

Expanded or reduced automation

Visibility Gaps Addressed:

New logging or telemetry

Ownership and Timeline:
| Action | Owner | Due Date |

---

13. Metrics and Performance

Time to Detect:
Time to Contain:
Time to Eradicate:
Time to Recover:

Accuracy Assessment:

- False positives
- Missed signals

---

14. Final Incident Summary

Provide a clear, executive-level summary:

- What happened
- What was impacted
- How it was resolved
- What was improved