

Introduction to Incident Response

Introduction to Incident Response

Prepared as a quick-reference guide for students, new analysts, or anyone needing a concise overview.

1. What Is Incident Response (IR)?

Aspect	Description
Definition	A coordinated set of actions taken to detect, analyze, contain, eradicate, and recover from a security event or breach.
Goal	Minimize impact on business operations, protect data integrity, and restore normal service as quickly as possible.
Scope	Can cover anything from malware infections and phishing attacks to insider threats and ransomware.

2. Core Phases of the Incident Response Lifecycle

Phase	Primary Activities	Key Deliverables
1. Preparation	- Develop IR policies & playbooks - Build and train the response team - Deploy detection tools (SIEM, IDS/IPS, EDR) - Establish communication & escalation paths - Monitor alerts and logs	- IR plan - Asset inventory - Contact lists (internal, legal, PR, law enforcement)
2. Identification	- Correlate events to spot anomalies - Verify whether an event is a true incident	- Incident ticket - Initial classification (e.g., malware, data breach)
3. Containment	- Short-term: isolate affected systems (network segmentation, account lockout) - Long-term: apply temporary controls to prevent spread while preserving evidence	- Containment checklist - Evidence preservation log
4. Eradication	- Remove malicious artifacts (malware, backdoors) - Patch vulnerable software - Reset compromised credentials	- Cleanup report - Updated system baselines

Introduction to Incident Response

Phase	Primary Activities	Key Deliverables
5. Recovery	• Restore systems from clean backups • Validate functionality and security • Monitor for re?infection • Conduct a post?mortem (often called a “debrief”)	• Recovery validation checklist • Post?recovery monitoring plan
6. Lessons Learned	• Identify gaps in detection, containment, or processes • Update policies, playbooks, and training	• After?action report (AAR) • Revised IR documentation

3. Incident Response Team (IRT) Roles

Role	Responsibilities
Incident Response Manager	Oversees the whole process, coordinates with leadership, ensures timelines are met.
Security Analyst / SOC Engineer	Detects alerts, performs triage, gathers forensic data.
Forensic Investigator	Acquires and analyzes evidence (disk images, memory dumps, network traffic).
Malware Analyst	Disassembles suspicious code, determines behavior, creates detection signatures.
IT Operations / System Admin	Executes containment, eradication, and recovery tasks on affected assets.
Legal / Compliance Officer	Advises on regulatory obligations, evidence handling, and potential notification requirements.
Communications / PR	Prepares internal/external statements, handles media inquiries.
Management / Executive Sponsor	Provides resources, approves budget, makes high?level decisions (e.g., public disclosure).

4. Key Concepts & Terminology

Term	Meaning
------	---------

Introduction to Incident Response

Indicator of Compromise (IOC)

Artefacts that suggest a breach (e.g., malicious IP, hash, domain).

Tactics, Techniques, and Procedures (TTPs)

Attackers'