Incident Reporting Templates

CHAPTER 5

Chapter Contents

- Incident Reporting Templates
  - Study Different templates of Incident reporting
- Security Operations Center (SOC)
  - Reporting templates, Incident vs Event reporting
  - Escalation matrix and policies
- Documentation Best Practices
  - Developing Incident Documentation
  - Chain of Custody
  - Evidence Preservation
  - Case Management Systems

Examples of Templates

- CERT India Incident report
- RBI: Template for reporting Cyber Incidents
- SANS Incident Handling Form
- RFC 7970

SANS Incident Handling Form

- **General Information**
  - Date/Time Detected
  - Date/Time Reported
  - Reported By (Name, Dept)
  - Incident Handler/Investigator
- **Incident Description**
  - **Short Summary of the Incident**
    - A concise overview (what happened, how it was detected)
  - **Category of Incident**
    - (e.g., Unauthorized Access, Malware, DoS, Policy Violation)

SANS Incident Handling Form

- **System(s) Affected**
  - Hostname(s)
  - IP Address(es)
  - Operating System
  - Location (Physical or Logical)
  - Function of System (e.g., Web Server, Email Gateway)

SANS Incident Handling Form

- **Impact Assessment**
  - Confidentiality Breach (Y/N, details)
  - Integrity Breach (Y/N, details)
  - Availability Breach (Y/N, details)
  - Data at Risk (e.g., PII, financial data)
- **Timeline of Events**
  - A **chronological list** of events with **timestamps**
    - When the event started
    - When it was detected
    - Actions taken (containment, recovery, etc.)

SANS Incident Handling Form

- **Indicators of Compromise (IOCs)**
  - IP addresses
  - URLs or domains
  - File hashes
  - Unusual processes or behaviour
- **Incident Response Actions**
  - Detection Actions
  - Containment Steps Taken
  - Eradication/Removal Steps
  - Recovery Steps (system restoration, password resets)

SANS Incident Handling Form

- **Lessons Learned / Post-Incident Actions**
  - What went well
  - What needs improvement
  - Recommendations (patches, policy changes, awareness training)
- **Attachments/References**
  - Screenshots
  - Log files (summarized or attached separately)
  - Email headers
  - Any forensic analysis documents

SANS Incident Handling Form

RFC 7970

RFC 7970

The Incident Object Description Exchange Format (IODEF) defines a data representation for security incident reports and indicators commonly exchanged by operational security teams for mitigation and watch and warning.

- Incident Overview
- Incident Details
- Actions Taken
- Resolution & Recovery
- Reporting & Notifications
- Supporting Documentation

Incident Overview

- **Incident ID:** [Unique Identifier, UUID preferred as per RFC 7970]
- **Date & Time of Detection:** [YYYY-MM-DD HH:MM:SS UTC, use ISO 8601 format]
- **Reporter Information:**
  - Name: [Full Name]
  - Contact: [Email, Phone]
  - Organization: [Name]
- **Incident Status:** [New, Ongoing, Resolved, Closed]
- **Incident Severity:** [Low, Medium, High, Critical]
- **Incident Classification:** [Malware, Phishing, DDoS, Data Breach, Unauthorized Access, etc.]
- **Related Activity IDs:** [If part of a broader campaign or series of incidents]

Incident Details

- **Summary:** [Brief high-level overview of the incident]
- **Description:** [Detailed narrative, including timeline, discovery method, and organizational impact]
- **Discovery Method:** [Automated Detection, Manual Review, External Notification, etc.]
- **Detection Points:** [Network, Endpoint, Application, Cloud, etc.]
- **Affected Systems/Entities:**
  - Hostnames/Ips
  - User Accounts
  - Applications or Services
  - External Parties (if applicable)

Incident Details

- **Impact Assessment:** [Describe confidentiality, integrity, availability, regulatory impact]
- **Attack Vector:** [Email, Web, USB, Remote Access, Insider, etc.]
- **Indicators of Compromise (IoCs):**
  - IP Addresses
  - Domain Names
  - URLs
  - File Names
  - Hashes (MD5, SHA1, SHA256)
  - Registry Keys
  - Process Names
  - Other Artifacts (per RFC 8727, support JSON structured lists where possible)

Actions Taken

- **Initial Response Date/Time:** [Timestamp in ISO 8601]
- **Containment Measures:** [Network isolation, user account suspension, etc.]
- **Eradication Steps:** [Malware removal, system wipe, patching, etc.]
- **Mitigation Strategies:** [Configuration updates, WAF rules, etc.]
- **Forensic Evidence Collection:** [Tools used, logs retained, hash values, etc.]
- **Preservation for Legal/Compliance:** [Yes/No, retention location and format]

Resolution & Recovery

- **Resolution Date/Time:** [ISO 8601 timestamp]
- **Recovery Actions:** [Systems restored, services validated, user access re-enabled]
- **Post-Incident Review Conducted:** [Yes/No, Date]
- **Root Cause Analysis:** [Identify underlying vulnerabilities or failures]
- **Lessons Learned:** [Summary of operational improvements identified]
- **Recommendations & Preventive Measures:** [Security training, policy updates, tech improvements]

Reporting & Notifications

- **Internal Stakeholders Notified:** [Security, Legal, Management, etc.]
- **External Reporting Requirements:** [Regulators, CERTs, Customers, etc.]
- **Public Disclosure Required:** [Yes/No, Summary of disclosure made]
- **Compliance Considerations:** [E.g., GDPR, HIPAA, PCI-DSS — list impacted regulations and actions taken]

Supporting Documentation

- **Attachments:** [Incident logs, screenshots, packet captures, forensic images — reference filenames or paths]
- **Structured Data References:** [IODEF-JSON (RFC 8727) objects or links to structured reports]
- **Related Incidents:** [Cross-reference by ID]
- **Ticket References:** [Helpdesk, SIEM, or case management system IDs]

RFC 7970

WRITING A REPORT

Writing a Report

- **How to write a useful cybersecurity incident report**
- https://www.techtarget.com/searchsecurity/tip/How-to-write-a-useful-cybersecurity-incident-report
- By **Paul Kirvan**

Questions to be answered

Questions to answer in report	Details to include
What actually happened?	Provide a clear description of the event, e.g., a ransomware attack.
When did the event happen (time of day, date)?	Provide the exact date and time the attack was detected.
Who was involved in responding to the event?	List the SOC team members who were directly involved in responding to the attack, identifying the malware and quarantining it, and neutralizing it.
What was the initial response?	Describe how the malware was identified and triaged to prevent it from causing further damage.
What was the initial assessment?	Provide an initial description of the event, based on data from the above systems and other security monitoring systems.

Questions to be answered

What technology assets were impacted?	List the technology assets, e.g., servers, storage, end-user devices, network devices and network services, affected.
What happened to the impacted assets?	Describe what happened to the affected assets, e.g., corrupted data, damaged systems and assets locked by ransomware.
How was the organization affected?	Describe how the organization's ability to perform its operations was impacted, e.g., data corruption, systems locked with a ransom note; and inability to handle customer inquiries or manufacture products.
Why did the attack happen?	Information from security systems post-event might shed light on how and where system vulnerabilities were exploited.
What steps were used to address and mitigate the attack?	Describe how the attack was confined, quarantined, sandboxed and analyzed by security tools so that an appropriate mitigation could be identified and launched.

Questions to be answered

What were the results of the actions taken?	Describe if the primary mitigation steps worked successfully, and if they did not, what alternate steps had to be taken and the results.
How was the organization able to bounce back and return to normal?	Describe how quickly the company was able to adapt to the event and return to normal operations, and if not, what alternate recovery measures were put into effect.
How could the event have been prevented?	Using data from the security systems and breach and attack simulation and/or penetration tests, provide an analysis of how the event could have been anticipated and prevented.
What can be done to prevent future occurrences?	Using data from the above resources, define steps that can reduce the likelihood of future occurrences. Risk, threat and vulnerability assessments are also advisable.
What other lessons were learned from the experience?	Describe any additional circumstances that might have helped identify the risks earlier, establish stronger prevention measures, update security platforms and increase employee awareness of the risks.

Writing a Report

SECURITY OPERATIONS CENTER (SOC)

Security Operations Center (SOC)

- Centralized unit that monitors and responds to security issues
- Type of SOC
  - In-House
  - MSSP (managed security service provider)
  - Hybrid
- SOC Functions
  - Real-time monitoring, log analysis, threat detection, incident response

Security Operations Center (SOC)

- SOC Hierarchy
  - Tier 1 (Alert triage), Tier 2 (Investigation), Tier 3 (Threat hunting), IR Team, SOC Manager
- Tools Used
  - SIEMs (Splunk, QRadar), EDR, IDS/IPS, Ticketing Systems

Security Analysts: The Frontline Defenders

- Security Analysts play a crucial role in a Security Operations Center (SOC), protecting networks and systems from cyber threats.
- Their key responsibilities include:
  - **Monitoring & Alert Handling:** Using tools like SIEM systems, they track security alerts, filter false positives, and focus on high-risk events.
  - **Incident Analysis:** They investigate security incidents, verify threats, and escalate cases when necessary.
  - **Collaboration:** Working alongside incident response teams and other departments, they help mitigate and resolve security threats efficiently.

Incident Responders: The Rapid Response Team

- Incident Responders play a vital role in handling security incidents and minimizing their impact.
- Their key responsibilities include:
  - **Incident Management:** Conducting forensic analysis, managing incidents in real time, and ensuring clear communication during major breaches.
  - **Threat Mitigation:** Acting swiftly to contain security threats and limit damage.
  - **Reporting & Improvement:** Documenting findings and applying lessons learned to strengthen future incident response strategies.

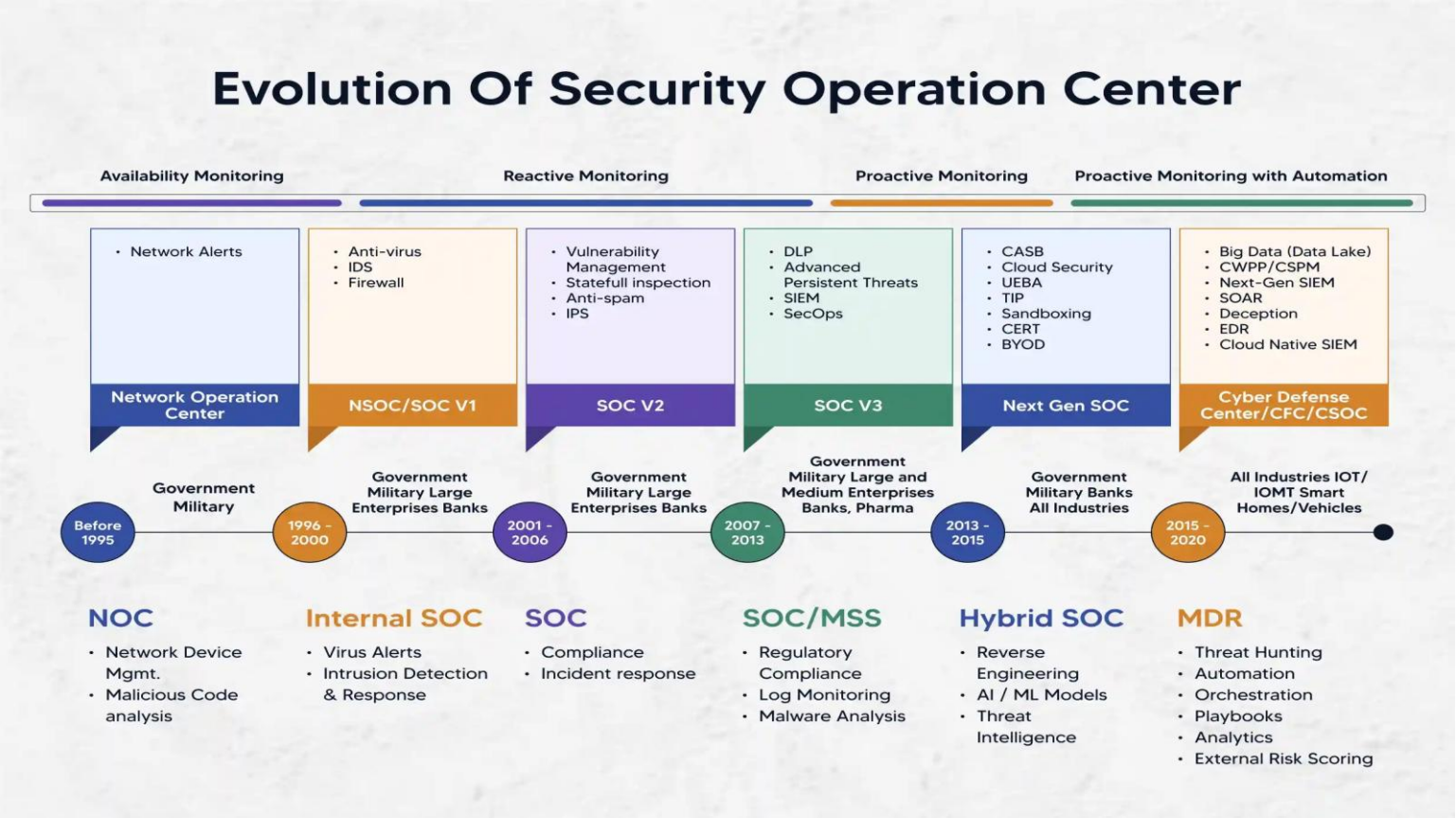
Threat Hunters: Proactive Cyber Defenders

- Threat Hunters play a crucial role in detecting hidden cyber threats before they become security incidents.
- Their key responsibilities include:
  - **Advanced Threat Detection:** Utilizing specialized tools to proactively identify risks lurking within the network.
  - **Vulnerability Assessments:** Conducting or overseeing assessments and penetration tests to uncover security weaknesses.
  - **Security Optimization:** Recommending improvements to monitoring tools, enhancing overall cybersecurity defenses.

SOC Manager: The Strategic Leader

- The SOC Manager oversees operations, ensuring security strategies align with organizational goals.
- Their key responsibilities include:
  - **Strategic Planning:** Leading coordination efforts and aligning the team with security objectives.
  - **Team Management:** Overseeing hiring, training, and personnel development to maintain a strong SOC team.
  - **Incident Response Coordination:** Ensuring swift, compliant incident handling and response.
  - **Performance Reporting:** Communicating SOC activities and insights to senior management.

Evolution of SOC



Incident vs. Event Reporting

Term	Definition	Everyday Analogy
Security Event	Any observable change in a system or environment that might affect security	A smoke detector goes off
Security Incident	A confirmed event or series of events that poses an actual threat to confidentiality, integrity, or availability (CIA)	A confirmed fire in the building

Incident vs. Event Reporting

Scenario	Is it an Event or Incident?	Why?
A user enters the wrong password three times	**Event**	Could be a mistake or normal behavior
50 failed login attempts from a foreign IP in 2 mins	**Escalated Event**	Suspicious pattern, may become an incident
A phishing link was clicked and malware was downloaded	**Incident**	System was compromised; action required
Server logs indicate a misconfiguration	**Event**	No damage yet, but worth flagging

Classification Criteria

Criteria	Questions to Ask	Example
Severity	How critical is the system affected?	Web server vs. internal printer
Source	Where is the event coming from?	Known IP vs. suspicious IP
Repetition	Is it a one-time alert or repeated?	One scan vs. repeated probes
Impact	Has the incident already caused damage?	File deleted, ransom note shown
System Sensitivity	Is the affected system mission-critical?	Finance server vs. student printer
Confidence Level	How confident are we that it's real?	IDS alert + threat intel match

Why Incident Reports Matter

- Incident reports document the who/what/when/where/how of a cybersecurity breach or threat.
- They are used for:
  - Post-incident analysis (lessons learned)
  - Compliance and legal records
  - Communication with management, legal, auditors
  - Informing future security strategy

Standard Incident Report Template

Section	Purpose	Example
Header	Basic identification info	Date: 22-Apr-2025, ID: IR#2025-004, Reported by: Aarnav
Summary	High-level “elevator pitch” of what happened	“Phishing email led to credential compromise of a faculty account.”
Timeline	Time-stamped sequence of key events	10:22 AM – Email received 10:25 AM – Link clicked 10:30 AM – Alert triggered
Affected Systems	Scope of compromise	System: mail.university.edu User: prof.john@xyz.edu IP: 192.168.2.45
Root Cause	Technical or procedural weakness	Weak email filtering + user clicked malicious link
Impact	Quantify damage	Compromised credentials Accessed grading system No sensitive data loss
Response Actions	What was done to contain and recover	Disabled account Reset password Ran antivirus scan Reviewed logs
Recommendations	Preventive next steps	Conduct phishing awareness training Update spam filter rules Enable MFA

Event vs Incident Reporting Formats

Event Report	Incident Report
Short and automated	Manual + detailed
Includes date, time, IP, user, device	Includes root cause, impact, responce, recommandations
Used for trend analysis	Used for legal, compliance, lessons learned
Can be part of normal ops	Must trigger response and post-mortem

Escalation Matrix

- A **structured table or diagram** that defines:
  - **Who** needs to be notified (person/team/department)
  - **When** they should be notified (based on severity)
  - **What** actions they should take

Sample Escalation Matrix

Severity	Who is Notified	Response Time (SLA)	Example Scenario
Low	Tier 1 Analyst	30 mins	3 failed logins from local IP
Medium	Tier 2 + SOC Lead	15 mins	Phishing email reported by multiple users
High	IR Team + SOC Manager	5 mins	Malware detected on sensitive endpoint
Critical	CISO, Legal, PR Team	Immediate	Ransomware in production; data breach confirmed

Escalation Policy

- A **written set of rules** that explains:
  - When escalation is **required**
  - How escalation is **performed** (email, phone, ticket system)
  - Who must be **informed**, including **external regulators** (e.g., under GDPR)
- Policies ensure:
  - Timely response
  - Avoidance of blame games
  - **Legal and regulatory** compliance

SLA – Service Level Agreements

Severity	Acknowledge	Investigate	Resolve
Low	30 mins	4 hours	24 hours
Medium	15 mins	1 hour	8 hours
High	5 mins	30 mins	4 hours
Critical	Immediate	15 mins	1 hour

Phishing Email in a University Setting

Step	Escalation Policy Trigger	Action Taken
1	Tier 1 analyst receives the user complaint	Confirms it's a phishing attempt
2	Tier 1 checks if similar emails were reported	Finds 3 additional reports
3	Escalation policy says “>3 users affected = MEDIUM”	Escalates to Tier 2 analyst + SOC Lead
4	Tier 2 isolates the email in quarantine system	Alerts email admin to block sender
5	SOC Lead informs IT Director (per matrix)	Awareness notification sent to all users

SLA Applied:
Acknowledge: Within 15 minutes
Initial Containment: Within 1 hour
Resolution/Communication: Within 6 hours

Malware in a Banking Network

Step	Escalation Policy Trigger	Action Taken
1	Tier 1 receives malware alert	Confirms via EDR it is active malware
2	Escalation policy: “Malware on sensitive system = HIGH”	Immediate escalation to IR Team and SOC Manager
3	IR Team isolates the server and investigates logs	CISO and Legal team informed
4	Internal communication issued to leadership	Backup server activated; containment completed

SLA Applied:
Acknowledge: 5 minutes
Investigate: 30 minutes
Resolution: 2–4 hours (based on containment plan)

Ransomware in Healthcare System

Step	Escalation Policy Trigger	Action Taken
1	Tier 1 notices ransomware alert on SIEM	Simultaneous alerts = CRITICAL
2	Escalation matrix: “Critical = CISO, Legal, PR, Executive Mgmt”	All stakeholders informed immediately
3	IR Team activates incident response playbook	Network segmented, backups initiated
4	External legal + PR consulted for breach disclosure	Coordination with health regulatory body initiated
5	Full internal and public incident report generated post-resolution	Lessons learned fed back into SOC playbooks

SLA Applied:
Acknowledge: Immediate
Mitigation: Start within 15 minutes
Public Communication: Within 1 hour

Why Documentation Matters in Cybersecurity

Purpose	Description
Audit Trail	Enables forensic investigations and compliance reviews
Knowledge Sharing	Helps new team members ramp up quickly
Accountability	Documents who did what, when, and why
Repeatability	Enables standardized responses to common incidents
Regulatory Compliance	Meets requirements from frameworks like ISO 27001, HIPAA, PCI-DSS

Documentation Best Practices

- Keep it Timely
  - Document events and incidents **as they occur**.
  - Use **timestamps** (e.g., ISO 8601 format: 2025-04-23T14:55:00Z)
- Be Accurate and Factual
  - Record only **observed facts**, not assumptions
  - Avoid emotional or vague language.
  - Good: “Firewall logs show port scanning from IP 192.0.2.44.”
  - Bad: “Looks like a hacker tried something.”

Documentation Best Practices

- Use Standardized Formats
  - Adopt **incident report templates**, SOPs, and log formats.
  - Keep terminology consistent (e.g., “Incident ID,” “Impact,” “Root Cause”).
- Structure Content Clearly
  - **Header**: Date, time, reported by, incident ID
  - **Summary**: One-paragraph overview
  - **Timeline**: Step-by-step sequence
  - Impact Assessment
  - Actions Taken
  - Root Cause
  - Recommendations

Documentation Best Practices

- Ensure Confidentiality
  - Use role-based access control (RBAC) on sensitive reports.
  - Mask PII or sensitive details when sharing externally
- Version Control
  - Use document management tools or version numbers (v1.2, v2.0) to track edits.
  - Keep a changelog of updates.
- Log Everything Relevant
  - What systems were involved?
  - Who responded and when?
  - What decisions were made?

Security Operations Center (SOC)

DEVELOPING INCIDENT DOCUMENTATION

Types of Incident Documentation

Type	Purpose
Incident Report	Describes what happened, when, and how it was handled.
Incident Timeline	Tracks actions and decisions over time.
Lessons Learned Report	Post-incident analysis for process improvement.
Investigation Log	Running log used during an ongoing incident.
Executive Summary	High-level view for non-technical stakeholders.

Things to Include

Section	What to Include
Header	Incident ID, Report Date, Reported By, Incident Date/Time
Summary	One-paragraph overview of what happened
Timeline	Timestamped sequence of key actions and discoveries
Affected Assets	IPs, hostnames, usernames, systems, apps
Detection Method	SIEM alert, user report, firewall log, etc.
Root Cause Analysis	What caused the incident and why
Impact Assessment	Operational, financial, legal, reputational
Response Actions	Containment, eradication, recovery steps
Recommendations	What to improve to prevent recurrence
Attachments	Screenshots, log snippets, ticket references

Writing Guidelines

- **Be Clear**: Use simple, straightforward language.
- **Be Objective**: Document facts, not opinions.
- **Be Complete**: Don’t leave out steps, even if minor.
- **Be Structured**: Use bullets, tables, and headings.
- **Be Time-Sensitive**: Record actions as close to real-time as possible.

Developing Incident Documentation

CHAIN OF CUSTODY

What is Chain of Custody?

Chain of Custody is a **formal process** that documents the **seizure, custody, control, transfer, analysis, and disposition** of evidence in a way that maintains its **integrity** and **admissibility in legal proceedings**.

Reason	Explanation
Evidence Integrity	Ensures that the data or device wasn't tampered with.
Legal Admissibility	Courts require a clear trail of who accessed the evidence.
Accountability	Identifies responsible individuals at each hand-off.
Investigation Quality	Supports reliable analysis and conclusions.

Key Elements in the Chain

Element	Description
Evidence ID	Unique identifier for the item
Description	Detailed summary of the evidence
Collector Info	Who collected it, when, and how
Storage Details	Where and how it was stored (e.g., locker ID, encryption)
Transfer Log	Every hand-off with timestamps and signatures
Condition of Evidence	Status (e.g., sealed, damaged, encrypted) at each stage

Challenges in Maintaining Chain of Custody

- Volatility of Digital Evidence
  - **Issue**: Data in RAM, cache, or network traffic can be lost quickly.
  - **Mitigation**:
    - Use **live forensics** tools to capture volatile data ASAP
    - Prioritize **memory acquisition** during active investigations.
- Data Duplication & Integrity
  - **Issue**: Digital evidence is easily copied, which can cast doubt on authenticity.
  - Mitigation
    - Use **cryptographic hashes** (e.g., SHA-256) before and after copying to verify integrity.
    - Maintain **hash logs** as part of documentation.

Challenges in Maintaining Chain of Custody

- Multiple Handlers
  - **Issue**: Evidence often passes through many hands — analysts, IT staff, law enforcement — increasing risk of mismanagement
  - Mitigation
    - Strict use of **Chain of Custody forms/logs** at each hand-off
    - Assign a **primary custodian** responsible for oversight
- Storage and Transport
  - **Issue**: Improper storage (e.g., unencrypted USBs or exposed drives) or transportation may lead to data leaks or tampering
  - Mitigation
    - Store evidence in **locked, access-controlled areas**
    - Use **encrypted containers or forensic bags**.
    - Document **transport logs** with timestamps and signatures.

Challenges in Maintaining Chain of Custody

- Human Error
  - **Issue**: Incomplete logs, missing signatures, incorrect timestamps
  - Mitigation
    - Regular **training sessions** for all handlers
    - Use **digital CoC systems** with mandatory fields and alerts
- Use of Improper Tools
  - **Issue**: Non-forensic tools may alter timestamps or file structures
  - Mitigation
    - Use **verified forensic tools** (e.g., FTK Imager, EnCase).
    - Validate tools periodically for compliance

Challenges in Maintaining Chain of Custody

- Long-Term Retention
  - **Issue**: Maintaining evidence over long investigations can lead to misplaced or corrupted files.
  - Mitigation
    - Use **digital evidence management systems (DEMS)** with proper backups
    - Implement **retention policies** based on legal requirements
- Legal Challenges
  - **Issue**: Opposing parties in court may challenge CoC due to a single missed log entry or protocol deviation
  - Mitigation
    - Ensure **complete and unbroken documentation**
    - Prepare staff for **legal testimony** to defend procedures

Evidence Preservation

Evidence preservation refers to the process of **protecting, securing, and maintaining the integrity** of evidence collected during an incident to ensure it remains **unchanged and admissible in court or internal investigations**.

Reason	Description
Integrity	Prevents tampering or accidental modification.
Legal Admissibility	Ensures evidence can be used in legal or disciplinary proceedings.
Accurate Investigation	Provides a reliable basis for root cause analysis and response.

Types of Digital Evidence

Evidence Type	Examples	Volatility
Volatile	RAM, open network connections, running processes	High
Semi-Volatile	Temp files, logs in memory	Medium
Non-Volatile	Disk drives, email archives, log files	Low

Techniques for Evidence Preservation

Technique	Purpose
Imaging (Bit-by-Bit Copy)	Creates an exact replica of a drive or partition.
Write Blockers	Prevent writing to evidence drives during analysis.
Hashing (MD5/SHA-256)	Confirms evidence has not been altered.
Forensic Snapshots	Captures system state at a specific time.
Isolation (Network Quarantine)	Prevents evidence systems from further communication or tampering.

Preservation Best Practices

Best Practice	Why It Matters
Use forensic tools (e.g., FTK Imager, Autopsy)	Ensures professional, repeatable results.
Log every action taken	Supports chain of custody and traceability.
Store backups in secure, access-controlled environments	Prevents unauthorized access or data loss.
Maintain original evidence untouched	Always analyze a copy, never the original.

Tools Commonly Used

- **FTK Imager** – For disk imaging.
- **Autopsy/Sleuth Kit** – For analysis.
- **dd (Linux)** – For low-level data copying.
- **EnCase** – Enterprise-grade forensic analysis
- **Wireshark** – For capturing network traffic (volatile).

Common Mistakes to Avoid

- Booting a compromised system normally (alters logs, timestamps).
- Editing evidence directly without a copy.
- Forgetting to hash before and after copying.
- Storing evidence in unprotected shared drives.
- Not documenting every preservation step.

Case Management Systems (CMS)

- A **Case Management System** is a software platform used by security teams to
  - **Track**, **manage**, and **document** security incidents or investigations
  - Ensure incidents are addressed **systematically and efficiently**.
  - Maintain a central, auditable record for **compliance**, **reporting**, and **future reference**

Case Management Matters

Purpose	Description
Centralized Tracking	All incident details and evidence are stored in one place.
Workflow Management	Automates ticket assignment, deadlines, and escalations.
Audit Readiness	Creates logs for legal, compliance, and audit purposes.
Collaboration	Enables multiple teams (e.g., SOC, legal, IT) to coordinate.
Metrics & Reporting	Tracks trends, performance, and SLA compliance.

Core Features

Feature	Function
Case Logging	Create new cases with incident type, severity, summary.
Workflow Automation	Assigns roles, sets deadlines, triggers alerts/escalations.
Evidence Attachment	Allows uploading of logs, screenshots, file hashes, etc.
Dashboard/Analytics	Real-time insights into case status, incident trends.
Role-Based Access	Ensures that only authorized personnel can view or edit sensitive data.
Linking Related Cases	Connects recurring or related incidents for better analysis.
Knowledge Base Integration	Offers resolutions or response guidelines from past cases.

Examples of Case Management Tools

Tool	Description
TheHive	Open-source incident response platform with powerful automation.
RTIR (Request Tracker for Incident Response)	Customizable for handling security incidents.
ServiceNow Security Operations	Enterprise-grade platform that integrates with SIEMs and CMDBs.
Resilient (by IBM)	Advanced playbook and case coordination tool.
Splunk SOAR (Phantom)	Automates response workflows and integrates with incident data.