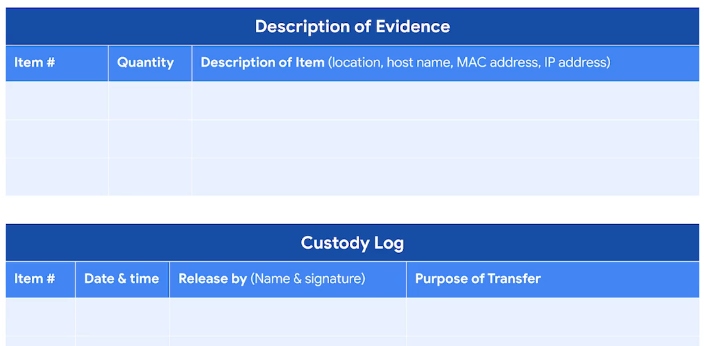
### **Documentation in Security – Key Notes**

* **Purpose of Documentation**:
  + Helps security teams respond effectively to incidents.
  + Supports scalability beyond small teams.
* **Why Document Detection Rules**:
  + Clarifies what an alert means.
  + Indicates severity levels.
  + Identifies potential false positives.
  + Guides analysts on how to confirm alerts.
* **Transparency Through Documentation**:
  + Records events for reference.
  + Enables access to relevant information.
  + Useful for:
    - Security insurance claims
    - Regulatory investigations
    - Legal proceedings
* **Standardization Benefits**:
  + Establishes consistent guidelines and workflows.
  + Example: security policies, processes, and procedures.
  + Maintains quality and consistency in work.
* **Improves Clarity**:
  + Defines roles and responsibilities clearly.
  + Provides detailed task instructions.
  + Example: playbooks reduce confusion during incident response.
* **Need for Regular Updates**:
  + Security threats and regulations constantly evolve.
  + Documentation must be reviewed and updated regularly.
* **Value of Personal Documentation**:
  + Helps recall facts and identify missed steps.
  + Supports organizational knowledge sharing.
  + Enhances individual and team efficiency.
* **Balancing Act**:
  + Documentation is a key responsibility alongside other security tasks.
  + Investing time in documentation benefits the whole organization.

### **Chain of Custody – Key Notes**

* **Purpose of Chain of Custody**:
  + Ensures transparency in tracking evidence throughout an incident’s lifecycle.
  + Critical for legal proceedings and maintaining evidence integrity.
* **Definition**:
  + A process of documenting possession and control of evidence during incident response.
  + Starts immediately after evidence is collected.
* **Example – Digital Forensic Analysis**:
  + Aisha identifies a compromised hard drive.
  + She write-protects it to prevent data changes.
  + Calculates and records a cryptographic hash of the disk image.
  + Transfers the evidence to Colin (forensics), then to Nav (analyst), and finally to Arman (manager).
  + Each transfer is logged in the chain of custody form.
* **Cryptographic Hash**:
  + Ensures data integrity—any tampering can be detected by comparing with the original hash.
* **Key Elements in a Chain of Custody Form**:
  + **Evidence description**: location, hostname, MAC/IP address.
  + **Custody log**: names of handlers, timestamps of transfer, purpose of transfer.  
      
    
* **Broken Chain of Custody**:
  + Occurs when entries are missing or logged incorrectly.
  + Can jeopardize the admissibility of evidence in legal cases.
* **Legal Importance**:
  + Validates the integrity, reliability, and accuracy of the evidence.
  + Helps ensure evidence can be used to hold malicious actors accountable.
* **No Standard Template**:
  + Forms vary but typically include common core elements.
* **Impact of Inconsistencies**:
  + Major breaks can disqualify evidence in court.
  + Proper documentation maintains the chain and supports legal actions.

# Best practices for effective documentation

**Documentation** is any form of recorded content that is used for a specific purpose, and it is essential in the field of security. Security teams use documentation to support investigations, complete tasks, and communicate findings. This reading explores the benefits of documentation and provides you with a list of common practices to help you create effective documentation in your security career.

## Documentation benefits

You’ve already learned about many types of security documentation, including playbooks, final reports, and more. As you’ve also learned, effective documentation has three benefits:

1. Transparency
2. Standardization
3. Clarity

### **Transparency**

In security, transparency is critical for demonstrating compliance with regulations and internal processes, meeting insurance requirements, and for legal proceedings. **Chain of custody** is the process of documenting evidence possession and control during an incident lifecycle. Chain of custody is an example of how documentation produces transparency and an audit trail.

### **Standardization**

Standardization through repeatable processes and procedures supports continuous improvement efforts, helps with knowledge transfer, and facilitates the onboarding of new team members. **Standards** are references that inform how to set policies.

You have learned how NIST provides various security frameworks that are used to improve security measures. Likewise, organizations set up their own standards to meet their business needs. An example of documentation that establishes standardization is an **incident response plan**, which is a document that outlines the procedures to take in each step of incident response. Incident response plans standardize an organization’s response process by outlining procedures in advance of an incident. By documenting an organization’s incident response plan, you create a standard that people follow, maintaining consistency with repeatable processes and procedures.

### **Clarity**

Ideally, all documentation provides clarity to its audience. Clear documentation helps people quickly access the information they need so they can take necessary action. Security analysts are required to document the reasoning behind any action they take so that it’s clear to their team why an alert was escalated or closed.

## Best practices

As a security professional, you’ll need to apply documentation best practices in your career. Here are some general guidelines to remember:

### **Know your audience**

Before you start creating documentation, consider your audience and their needs. For instance, an incident summary written for a security operations center (SOC) manager will be written differently than one that's drafted for a chief executive officer (CEO). The SOC manager can understand technical security language but a CEO might not. Tailor your document to meet your audience’s needs.

### **Be concise**

You might be tasked with creating long documentation, such as a report. But when documentation is too long, people can be discouraged from using it. To ensure that your documentation is useful, establish the purpose immediately. This helps people quickly identify the objective of the document. For example, executive summaries outline the major facts of an incident at the beginning of a final report. This summary should be brief so that it can be easily skimmed to identify the key findings.

### **Update regularly**

In security, new vulnerabilities are discovered and exploited constantly. Documentation must be regularly reviewed and updated to keep up with the evolving threat landscape. For example, after an incident has been resolved, a comprehensive review of the incident can identify gaps in processes and procedures that require changes and updates. By regularly updating documentation, security teams stay well informed and incident response plans stay updated.

## Key takeaways

Effective documentation produces benefits for everyone in an organization. Knowing how to create documentation is an essential skill to have as a security analyst. As you continue in your journey to become a security professional, be sure to consider these practices for creating effective documentation.

### **Playbooks in Incident Response – Key Notes**

* **What Are Playbooks?**
  + Operational manuals for security analysts.
  + Provide clear, step-by-step instructions during incident response.
  + Comparable to travel itineraries—help organize and guide actions.
* **Purpose of Playbooks**:
  + Offer structure during unpredictable incidents.
  + Reduce guesswork and uncertainty.
  + Enable fast, confident decision-making.
* **Key Components**:
  + May include checklists to ensure all steps are completed.
  + Outline specific responses to incidents like:
    - Ransomware
    - Data breaches
    - Malware
    - DDoS attacks
* **Example – DDoS Detection Playbook**:
  + Identify indicators of compromise (e.g., unknown traffic).
  + Collect logs.
  + Analyze evidence.
  + Often presented using flowcharts for clarity.
* **Types of Playbooks**:
  + **Non-Automated**:
    - All steps carried out manually by an analyst.
    - Example: manual DDoS response flowchart.
  + **Automated**:
    - Tasks like evidence collection or severity classification are performed by tools.
    - Reduces incident resolution time.
    - Can be implemented using SOAR or SIEM tools.
  + **Semi-Automated**:
    - Combines automation with human actions.
    - Automates repetitive or error-prone tasks.
    - Lets analysts focus on more critical decision-making.
* **Maintaining Playbooks**:
  + Must be updated regularly to remain effective against evolving threats.
  + Best time to revise is during the post-incident activity phase.
* **Why They Matter**:
  + Essential for swift and effective incident response.
  + Help security teams stay organized and perform under pressure.