GOOGLE CYBER SECURITY
Course 2: Play It Safe: Manage Security Risks

SKILLS: Information Systems Security, Risk Management, Security Information and Event Management (SIEM), Incident Response, Security Controls, Vulnerability Management, Auditing, Enterprise Security

Module 1

Security Domains

This module explains the focus of CISSP's eight security domains. Then, primary threats, risks, and vulnerabilities to business operations are identified and defined, along with a discussion of the threats, risks, and vulnerabilities entry-level security analysts focus on most. Additionally, NIST's Risk Management Framework (RMF) is introduced.

What you'll learn

- CISSP's eight security domains
- Security frameworks and controls
- Security audits
- Basic security tools
- Protect assets and data

Overview of the Cybersecurity Program

Purpose of the Program:
The program is designed to equip you with the **knowledge, skills, and tools** necessary to work effectively in the **world of cybersecurity** (also called **security**).

What You'll Learn:

1. **CISSP's 8 Security Domains**
   - You'll get an overview of the **eight core domains** from the **CISSP (Certified Information Systems Security Professional)** framework.
   - These domains represent the **main focus areas** in cybersecurity.
2. **Threats, Risks, and Vulnerabilities**
   - You'll dive deeper into:

   - What **threats** are (potential dangers),
   - What **risks** mean (the chances that a threat will exploit a vulnerability),
   - And what **vulnerabilities** are (weaknesses in systems or processes).
3. **Three Layers of the Web:**
   - **Surface Web** – the part of the internet we use every day.
   - **Deep Web** – data not indexed by search engines (like academic databases, private emails).
   - **Dark Web** – anonymous part of the web often associated with illegal activity.

     You'll see examples to help understand each of these.

4. **Types of Attacks:**
   - You'll be introduced to different kinds of **cyber attacks** (like phishing, malware, ransomware, etc.), which will be explained more later in the course.
5. **Risk Management with NIST RMF:**
   - You'll learn about the **NIST Risk Management Framework** – a structured approach developed by the **National Institute of Standards and Technology (NIST)**.
   - It helps **identify, assess, and manage cybersecurity risks** in organizations.

Why This Matters:

- These topics are considered **foundational** in cybersecurity.
- Gaining a strong understanding will help you:
  - **Prevent attacks**
  - **Reduce risks**
  - **Protect organizations** from daily threats

CISSP security domains:

1. Security and Risk Management

Focus Areas:

- **Defining goals & objectives**: Helps reduce risks to sensitive data like PII (Personally Identifiable Information)
- **Risk mitigation**: Having rules and processes to reduce the impact of security events (e.g., breaches)
- **Compliance**: Developing internal security policies based on laws, standards, and regulations
- **Business continuity**: Ensuring daily operations continue during disruptions using recovery plans
- **Legal and ethical behavior**: Following laws and ethical guidelines to avoid negligence, abuse, and fraud

2. Asset Security

Focus Areas:

- Protecting both **digital and physical assets**
- Ensuring proper:
  - **Storage**
  - **Maintenance**
  - **Retention**
  - **Destruction** of sensitive data (like PII or SPII – Sensitive PII)
- Tracking **who has access** to what data
- Example: Security analysts may oversee the proper destruction of hard drives to prevent data leaks

3. Security Architecture and Engineering

Focus Areas:

- Implementing secure **tools**, **systems**, and **processes** to protect data
- Promoting the idea of **shared responsibility**:
  - Everyone in the organization should actively participate in maintaining security
  - Encouraging users to report suspicious activity or concerns

4. Communication and Network Security

Focus Areas:

- Securing **physical networks**, **wireless networks**, and **cloud communications**
- Protecting remote connections, such as:
  - Insecure Bluetooth
  - Public Wi-Fi
- Example: Security teams may disable risky communication channels to reduce unsafe user behavior

5. Identity and Access Management (IAM)

Purpose:
To control **who can access what** in an organization by using **access and authorization policies**.

Key Goals:

- Ensure users only have access to what they need.
- Prevent unauthorized access.
- Reduce risk to systems and data.

Real-world example:

- If everyone uses the same admin login, you can't track individual actions. This makes it impossible to investigate who did what during a breach.

IAM Core Components:

1. **Identification** – Verifying who a user is (e.g., username, ID card, fingerprint)
2. **Authentication** – Proving identity (e.g., password, PIN)
3. **Authorization** – Granting access based on user roles
4. **Accountability** – Logging and monitoring user actions

6. Security Assessment and Testing

Purpose:
To **evaluate and improve security controls** regularly through testing, auditing, and analysis.

Key Activities:

- Conduct **security control tests**
- Perform **security audits**
- Collect and analyze **security data**

These actions help detect risks and vulnerabilities and improve the organization's defense mechanisms.

Example:
Introducing **multi-factor authentication (MFA)** after a test shows that password-only access is weak.

7. Security Operations

Purpose:
To **detect, respond to, and investigate security incidents** while also preventing future ones.

Key Steps:

1. **Incident response** – Act quickly during an active attack to reduce damage
2. **Forensic investigation** – Collect digital/physical evidence to understand the breach
3. **Post-incident improvement** – Analyze the incident to strengthen future defenses

8. Software Development Security

Purpose:
To integrate **security into every phase of the software development lifecycle (SDLC)**.

Key Practices:

- Use **secure coding guidelines**
- Perform **security reviews** during design, development, testing, and deployment
- Conduct **penetration testing** before releasing the software

Example:

- Do a secure design review early
- Review code for vulnerabilities during development
- Test for security flaws before launching the product

Conclusion:

Understanding all **eight domains** helps you see how organizations build and maintain strong security. These domains also highlight the essential work of cybersecurity teams in defending assets, systems, and data.

Let me know when you're ready to go over threats, risks, vulnerabilities, ransomware, and the layers of the web.

What Are Assets?

- An **asset** is anything valuable to an organization (digital or physical).
- Examples: Computers, office spaces, customer PII (Personally Identifiable Information), patents, and intellectual property.

1. Threats

- A **threat** is anything that can **negatively impact assets**.
- Example: **Social engineering attacks**
  - Specifically, **phishing**: Tricking users (via fake emails or links) into giving up sensitive data like usernames or banking info.

2. Risks

- A **risk** is the **potential for a threat to exploit a vulnerability** and impact an asset's:
  - **Confidentiality** (privacy)
  - **Integrity** (accuracy)
  - **Availability** (accessibility)
- Think of **risk** as the **likelihood** of something bad happening.
- **Example of a risk**: No backup plan for recovering important data in case of a breach or accident.

Risk Levels:

- **Low risk**: Public data (e.g., website content) – no serious impact if exposed.
- **Medium risk**: Sensitive internal data (e.g., unreleased earnings reports) – may hurt reputation or finances.
- **High risk**: Protected data (e.g., SPII, PII, intellectual property) – serious legal, financial, and operational consequences if compromised.

3. Vulnerabilities

- A **vulnerability** is a **weakness** that a **threat can exploit**.
- **Examples:**
  - Outdated firewalls or software
  - Weak passwords
  - Unprotected sensitive data
  - Even people (e.g., unaware employees) can be vulnerabilities
- Important note:
  Both a vulnerability and a threat must exist for a risk to occur.

Role of Entry-Level Analysts

- Educate staff to identify threats (e.g., phishing awareness)
- Use security tools (e.g., access cards to restrict building entry)
- Encourage reporting of suspicious activity
- Monitor and document access to critical assets
- Help the organization **reduce risk** by **managing vulnerabilities**

Ransomware

- **Ransomware** is a type of **malware** used by threat actors to **encrypt an organization's data**.
- Once encrypted:
  - Systems are frozen
  - Devices become unusable
  - Confidential data is locked
- The attacker demands a **ransom payment** in exchange for a **decryption key** (used to unlock the data).
- These events, including negotiations or leaked data, often happen via the **dark web** due to its secrecy.

Three Layers of the Web

1. **Surface Web**
   - Publicly accessible and searchable via standard web browsers
   - Examples: Social media, online shopping, news sites
2. **Deep Web**
   - Not indexed by search engines; requires authorization
   - Example: Company intranet (for internal use only)
3. **Dark Web**
   - Only accessible through special tools like **Tor**
   - Known for anonymous activity; often used for illegal actions like selling stolen data

Three Key Impacts of Threats, Risks, and Vulnerabilities

1. **Financial Impact**
   - High costs from:
     - Production/service interruption
     - Fixing systems
     - Fines due to **non-compliance**
   - Example: After a ransomware attack, restoring operations and paying penalties can be very expensive
2. **Identity Theft**

   - Storing sensitive information like **PII** (Personally Identifiable Information) introduces risk
   - Leaked PII can be sold on the dark web
   - Affects employees, customers, and vendors
3. **Reputational Damage**
   - Loss of customer trust and loyalty
   - Bad publicity and negative media coverage
   - Can lead to long-term harm, customer loss, and even legal penalties

NIST Risk Management Framework (RMF)

What is the NIST RMF?

- Developed by the **National Institute of Standards and Technology (NIST)**.
- A structured **7-step process** to help organizations **manage risks, threats, and vulnerabilities**.
- While entry-level analysts may not perform all steps, understanding the full process is valuable and can help you stand out during job applications.

The 7 Steps of the NIST Risk Management Framework (RMF)

1. Prepare

- **Goal:** Get ready to manage risks **before** any breach happens.
- **Tasks for analysts:** Monitor for risks, identify helpful controls, and gather information.
- **Example:** Watching for suspicious activity or known vulnerabilities.

2. Categorize

- **Goal:** Understand what's at risk and how it could impact **confidentiality, integrity, and availability (CIA)**.
- **Tasks for analysts:** Follow processes to reduce risks to critical assets, like customer data.
- **Example:** Categorizing data as low, medium, or high risk.

3. Select

- **Goal:** Choose and document security controls.
- **Tasks for analysts:** Help update security documentation like **playbooks** or **guidelines**.
- **Example:** Recording which controls are used to protect employee login data.

---

4. Implement

- **Goal:** Put the selected security controls and privacy plans into action.
- **Tasks for analysts:** Apply security changes to fix observed issues.
- **Example:** Updating password policies if users often request password resets.

5. Assess

- **Goal:** Check if controls are working correctly.
- **Tasks for analysts:** Evaluate how effective tools, procedures, and systems are.
- **Example:** Spotting weaknesses in current defenses and suggesting changes.

6. Authorize

- **Goal:** Accept accountability for risks that remain.
- **Tasks for analysts:** Create reports, write action plans, and help define project goals.
- **Example:** Documenting risk reports to present to management.

7. Monitor

- **Goal:** Continually track system performance and risk levels.
- **Tasks for analysts:** Daily monitoring, identifying any deviation from security goals.
- **Example:** If current systems aren't keeping risk low, flag it for updates.

Key Reminder:

Even if you don't set up these processes yourself, your job will involve **ensuring they're functioning correctly** to reduce risk for your organization and its customers.

Let me know if you'd like a simplified visual of the 7 steps or help memorizing them.

Recap: Foundations of Cybersecurity

1. **CISSP's Eight Security Domains**
    - Covered the broad areas that define information security (e.g., risk management, security architecture, asset security).
2. **Threats, Risks, and Vulnerabilities**
    - Explored how these concepts impact organizations.
    - Included a focus on **ransomware** and its implications.
    - Introduced the **three layers of the web**:
        - Surface web
        - Deep web
        - Dark web
3. **NIST Risk Management Framework (RMF)**
    - Learned the **7 steps** for managing risk in a structured and repeatable way.

Glossary terms from module 1

Assess: The fifth step of the NIST RMF that means to determine if established controls are implemented correctly

Authorize: The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that may exist in an organization

Business continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

Categorize: The second step of the NIST RMF that is used to develop risk management processes and tasks

External threat: Anything outside the organization that has the potential to harm organizational assets

Implement: The fourth step of the NIST RMF that means to implement security and privacy plans for an organization

Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk

Monitor: The seventh step of the NIST RMF that means be aware of how systems are operating

Prepare: The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs

Ransomware: A malicious attack where threat actors encrypt an organization’s data and demand payment to restore access

Risk: Anything that can impact the confidentiality, integrity, or availability of an asset

Risk mitigation: The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

Security posture: An organization’s ability to manage its defense of critical assets and data and react to change

Select: The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization

Shared responsibility: The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Vulnerability: A weakness that can be exploited by a threat

Module 2

Security Frameworks and Controls

Security Analyst's Role:

- Not just about protecting organizations — it's also about **protecting people**.
- **Breaches** can damage:
  - Customers' and employees' **financial stability**
  - Their **reputation**
- Your daily work helps ensure the **safety of both people and organizations**.

What's Coming Up in This Section:

- You'll explore:
  - **Security frameworks**
  - **Security controls**
  - **Design principles**
- Learn how they are used in **security audits** to protect systems and data.

Example from Google:

- At Google, keeping **customer information confidential** is a top priority.
- The **NIST Cybersecurity Framework** helps ensure:
  - Protection of tools and data
  - Compliance through **security controls**

What Are Security Frameworks?

- **Security frameworks** are **guidelines** organizations use to create **policies and procedures** that help:
  - **Mitigate threats, risks, and vulnerabilities**
  - Protect **data, privacy**, and **people**
- They are used as **starting points** for developing customized security strategies.

Types of Protection Covered

- Frameworks address both:
  - **Virtual threats** (e.g., ransomware, phishing)
  - **Physical threats** (e.g., unauthorized building access)
    - Example: Requiring **key cards** or **badges** to enter offices

Purpose of Frameworks

- Help **prevent, detect, and respond** to security breaches.
- Especially useful against **social engineering attacks** that target human behavior (like phishing).

Why People Matter Most

- **Human error** is the biggest security threat.
- Frameworks include guidance to:
  - **Increase employee awareness**
  - **Train staff** to recognize red flags and suspicious behavior
  - **Report issues** quickly and effectively

Your Role as an Analyst

- Understand and help implement the **security plans** based on frameworks.
- Contribute to keeping the **organization, employees, and customers** safe from attacks and breaches.

What Are Security Controls?

- **Security controls** are **safeguards** or measures designed to reduce **specific security risks**.
- Without proper controls, organizations face **financial loss** and **reputation damage** due to risks like:
  - **Trespassing**
  - **Fake employee accounts**
  - **Unauthorized access to benefits or resources**

Three Common Types of Security Controls

1. Encryption

- Converts **plaintext** into unreadable **ciphertext**.
- Ensures **confidentiality** of sensitive data (e.g., Social Security numbers, customer accounts).
- Data must be **decrypted** back into readable form to be useful.

2. Authentication

- Verifies **who someone is** before granting access.
- Example: Logging in with a **username and password**.
- **Multi-Factor Authentication (MFA)** adds another layer:
  - Requires an additional proof like a **code**, **fingerprint**, **voice**, or **face scan**.

3. Authorization

- Determines **what someone is allowed to access** after authentication.
- Ensures only approved users access specific **resources or data**.
- Example: A government analyst having access to **deep web** internal data that others can't see.

Note on Biometrics & Social Engineering

- **Biometrics** (like fingerprint, eye scan) are used for authentication.
- **Vishing** (voice phishing) is a social engineering attack that can **mimic someone's voice** to bypass biometric verification.

Relationship between frameworks and controls

What Are Frameworks?

- **Security frameworks** are **guidelines** to help organizations **plan** for managing **risks, threats, and vulnerabilities**.
- They help with **compliance** (e.g., HIPAA in healthcare).
- Example: NIST RMF, NIST CSF, ISO/IEC 27001, and Cyber Threat Framework (CTF).

What Are Controls?

- **Security controls** are **actions or tools** used to reduce specific risks.
- They are used **alongside frameworks** to achieve security goals.
- Example: Using **multi-factor authentication (MFA)** to protect medical records.

Types of Controls

Type	Description	Examples
Physical	Protect physical spaces	Locks, security guards, CCTV, access cards
Technical	Protect systems & data	Firewalls, MFA, antivirus
Administrative	Define roles, rules, and processes	Authorization, separation of duties, asset classification

---

Examples of Frameworks

- **CTF (Cyber Threat Framework)**: Developed by U.S. intelligence to create a **common language** for sharing info about cyber threats.
- **ISO/IEC 27001**: Global framework for managing **information security** (financial data, IP, employee info). It provides a **list of controls**, but they're optional.

Key Takeaways

- **Frameworks = plans**
- **Controls = tools/actions**
- Together, they:
  - Help meet **compliance** laws (like HIPAA)
  - Reduce **risks and threats**
  - Strengthen an organization's **security posture**

CIA Triad – Core Security Model

It stands for:

1. **Confidentiality**

   → Only **authorized users** can access data.

   → Data is shared on a **need-to-know** basis.

   Example: A bank protects customers' financial info from unauthorized access.

2. **Integrity**

   → Data must be **correct, authentic, and reliable**.

   → Any change should be **intentional and authorized**.

   Example: Bank blocks suspicious activity to ensure account data isn't tampered with.

3. **Availability**

   → Data must be **accessible** to authorized users **when needed**.

   → Systems and apps must run reliably.

   Example: Bank ensures customers can always access their accounts online.

Why it Matters

As a **security analyst**, you'll apply the CIA triad daily to:

- Set security policies
- Reduce risk from **malware**, **social engineering**, and **data breaches**
- Protect both **organizations** and the **people they serve**

CIA Triad in the Workplace

1. Confidentiality

- **Goal:** Ensure only **authorized users** can access sensitive data.
- **How analysts apply it:**
  - Use the **principle of least privilege** (give users access only to what they need).
  - Example: An HR employee can access employee records, but not company financials.
- **Tools/Methods:**
  - Access controls
  - Encryption
  - User authentication

2. Integrity

- **Goal:** Keep data **correct**, **authentic**, and **trustworthy**.
- **How analysts apply it:**
  - Use **cryptographic techniques** to prevent unauthorized changes.
  - Example: Chat messages are **encrypted** so they can't be altered in transit.
- **Tools/Methods:**
  - Encryption
  - Hashing (to detect tampering)
  - Checksums

3. Availability

- **Goal:** Ensure **authorized users** can access data **when needed**.
- **How analysts apply it:**
  - Maintain system uptime and fast recovery from disruptions.
  - Example: Remote employees get secure access to internal networks.
- **Tools/Methods:**
  - Firewalls
  - Redundant systems
  - Backups and disaster recovery plans

Key Point

The **CIA triad** supports a strong **security posture**, meaning the organization:

- Can defend its critical assets
- Can respond effectively to changes and threats
- Keeps employees, customers, and data protected

NIST frameworks

Purpose of Frameworks

- Frameworks help organizations **create plans** to reduce **risks, threats, and vulnerabilities** to sensitive **data** and **assets**.
- Used by all types of organizations — **for-profit**, **non-profit**, and **government**.

NIST Cybersecurity Framework (CSF)

- **Voluntary** and **globally respected**.
- Provides **standards**, **guidelines**, and **best practices** to manage cybersecurity risk.
- Applies to **any industry**, not just government.

Five Core Functions of CSF:

1. **Identify** – Know your assets, risks, and who has access.
2. **Protect** – Implement safeguards (like access controls).
3. **Detect** – Identify if a threat or breach has occurred.
4. **Respond** – Take steps to investigate and contain.
5. **Recover** – Restore systems and data, learn from the incident.

Example (From Video):

- You detect a **high-risk** alert on a workstation.
- An **unknown device** is plugged in — you **block it**, **analyze the threat**, and find it's an **infected phone**.
- You then take steps to **recover files**, fix the system, and learn how it happened.

NIST SP 800-53

- A special publication of NIST used for **federal government systems**.
- Provides **security controls** to ensure **confidentiality**, **integrity**, and **availability** (CIA triad).
- Applies to **government systems** and also **private companies** working with the government.

Key Takeaway

- **CSF** helps handle incidents quickly and efficiently.
- **SP 800-53** helps protect **U.S. federal systems**.
- Together, they ensure security plans are in place to **prevent**, **respond to**, and **recover from** attacks.

Five core functions of the NIST Cybersecurity Framework (CSF)

NIST CSF – 5 Core Functions

These five functions help organizations **manage cyber risks**, **respond to incidents**, and **recover from damage**:

1. Identify

- Understand what needs protection: **people, systems, assets, and data**.
- Example: You monitor your internal network to **spot weaknesses** or **suspicious activity**.

2. Protect

- Use **policies**, **training**, **tools**, and **procedures** to defend against threats.
- Example: Improve old security policies based on **lessons learned from past attacks**.

3. Detect

- **Find** cybersecurity events quickly using **monitoring tools**.
- Example: Check if a new tool **correctly flags threats** and **alerts the team**.

4. Respond

- **Take action** when an incident happens — contain and analyze it.
- Example: Help document what happened and **suggest improvements** to avoid future attacks.

5. Recover

- **Restore systems and data** after a security incident.
- Example: Help your team **bring services back online**, including restoring **legal or financial files**.

Key Takeaway

From **planning** to **response and recovery**, all five functions work together to:

- Reduce risks,
- Improve security processes,
- And help the organization **bounce back quickly** after an attack.

OWASP Security Principles

OWASP Security Principles

1. **Minimize the Attack Surface Area**
    - Reduce the number of ways attackers can break in.
    - Example: Disable unused features, block phishing emails, and use strong password policies.
2. **Principle of Least Privilege**
    - Give users **only the access they need** — nothing more.
    - Example: You can view logs but **not change permissions**, so if your account is hacked, damage is limited.
3. **Defense in Depth**
    - Use **multiple layers of protection**.
    - Example: Combine MFA, firewalls, intrusion detection, and permissions to block attackers at many points.
4. **Separation of Duties**
    - **No one person should control everything** — this prevents abuse or fraud.
    - Example: One person writes paychecks; another signs them.
5. **Keep Security Simple**
    - **Don't overcomplicate** controls — complexity leads to mistakes and poor collaboration.
    - Example: Use clear, manageable policies everyone understands.
6. **Fix Security Issues Correctly**
    - Identify the **real cause** of a problem and fix it completely.
    - Example: Weak Wi-Fi password? Fix it by enforcing **strong password rules** and test after fixing.

Why This Matters

Understanding and applying these principles:

- **Reduces risk**
- **Prevents breaches**
- **Makes you a smarter and more effective security analyst**

OWASP Security Principles Summary

Previously Covered Principles:

1. **Minimize Attack Surface Area**
   Reduce the number of potential vulnerabilities that threat actors can exploit.
   Example: Disable unnecessary features or services.
2. **Principle of Least Privilege**
   Users should only have the minimum access necessary to perform their job.
   Example: A user can view logs but cannot modify configurations.
3. **Defense in Depth**
   Use multiple layers of security controls to protect assets.
   Example: Combine firewalls, antivirus software, and multi-factor authentication.
4. **Separation of Duties**
   Distribute critical tasks among multiple individuals to prevent abuse of power.
   Example: One person prepares payroll, another approves it.
5. **Keep Security Simple**
   Avoid overly complex security solutions that are difficult to manage.
   Example: Use standardized access rules instead of custom code.
6. **Fix Security Issues Correctly**
   Address the root cause of a security issue and verify the fix works.
   Example: Patch a vulnerability rather than just restarting the system.

Newly Introduced Principles:

7. **Establish Secure Defaults**
   The most secure settings should be the default configurations.
   Example: New user accounts start with limited permissions.
8. **Fail Securely**
   When a system fails, it should do so in a secure manner.
   Example: If a firewall fails, it blocks all traffic rather than allowing it.
9. **Don't Trust Services**
   External services or third-party vendors should not be assumed secure. Always verify their data and behavior.
   Example: Validate data from a vendor before sharing it with customers.
10. **Avoid Security by Obscurity**
    Security should not rely solely on secrecy of implementation or hidden details.
    Example: Use proper access controls rather than relying on hidden URLs.

Plan a Security Audit

How Everything Works Together: Security Audits

What is a Security Audit?

A **security audit** is a detailed review of an organization's **security controls**, **policies**, and **procedures** to ensure they meet established expectations, like industry frameworks and legal regulations.

Types of Security Audits:

- **External Audits** – Performed by third parties (e.g., regulatory bodies).
- **Internal Audits** – Conducted by internal security teams and stakeholders.

Purpose of Internal Security Audits

- Improve **security posture**
- Identify **risks and vulnerabilities**
- Verify **compliance** with regulations
- Recommend fixes for weaknesses before external audits occur

Five Key Elements of an Internal Security Audit

1. Establish Scope and Goals

- **Scope**: Defines what will be audited (people, assets, systems, policies, etc.)
- **Goals**: Security objectives like improving controls or meeting compliance standards

Example:

- **Scope** includes: reviewing user permissions, identifying current controls, analyzing policies
- **Goals** include: applying NIST CSF functions, improving compliance, and strengthening system security

2. Conduct Risk Assessment

- Identify **threats**, **risks**, and **vulnerabilities**
- Helps determine which **controls**, **frameworks**, and **regulations** to focus on

Example:

- Audit reveals lack of asset management, insecure storage devices, and weak access controls

3. Controls Assessment

- Evaluate the **effectiveness of current controls**
- Identify gaps (e.g., outdated antivirus, no MFA)

4. Compliance Assessment

- Ensure policies align with legal and industry frameworks (e.g., HIPAA, NIST, ISO/IEC 27001)

5. Report Findings to Stakeholders

- Share results clearly
- Suggest improvements
- Help guide future security investments

How Everything Connects

Concept	Role in Audit
Frameworks	Guide what to assess (e.g., NIST CSF)
Controls	Are reviewed and tested
Security Principles	Are used to evaluate and recommend changes
Compliance Regulations	Are checked for violations or risks

Final Elements of an Internal Security Audit

You've already learned about:

- **Scope and Goals**
- **Risk Assessment**

Now, you'll complete:

1. **Controls Assessment**
2. **Compliance Assessment**
3. **Communication of Results**

1. Controls Assessment

You review existing controls and check if they're effective at protecting assets.

Types of controls:

Type	Description	Examples
Administrative	Human-related controls via policies & procedures	Password policies, access control policies
Technical	Software or hardware-based controls	Firewalls, IDS/IPS, encryption
Physical	Controls that block physical access to assets	CCTV cameras, locks, access cards

2. Compliance Assessment

You check if the organization is following required **laws and standards**.

Examples:

- If working in the EU → Must comply with **GDPR**
- If accepting credit card payments → Must comply with **PCI DSS**

3. Communication of Results

Once the audit is complete, results are shared with stakeholders.

A typical report includes:

- A summary of **scope and goals**
- A list of **existing risks and vulnerabilities**
- **Compliance gaps**, if any
- **Recommendations** for improvement
- **Urgency levels** for addressing risks

Example:

After a password audit, the team found many weak passwords. The compliance team then enforced stronger password policies.

Key Takeaway:

Security audits help find weaknesses in controls, verify legal compliance, and improve an organization's ability to defend its critical assets. As a new analyst, your role in reviewing, classifying, and reporting findings is crucial.

Security Audits Overview

A **security audit** is a **review of an organization's security controls, policies, and procedures** against internal and external expectations. These reviews help evaluate whether an organization is meeting both its own security policies (internal criteria) and compliance requirements like laws and regulations (external criteria).

Purpose of Security Audits

- To **assess controls** to reduce specific risks.
- To **ensure ongoing security monitoring** is in place (e.g., SIEM dashboards).
- To **identify threats, risks, and vulnerabilities**.
- To **implement remediation** if issues are discovered.
- To **improve the organization's security posture**.

Goals vs. Objectives of an Audit

- **Goal:** Ensure the organization's IT practices meet industry and organizational standards.
- **Objective:** Identify weaknesses, suggest improvements, and develop plans to fix gaps and reduce risk.
- **Importance:** Avoid government penalties and fines for non-compliance.
- **Audit frequency:** Depends on laws and federal or local compliance regulations.

Factors That Influence Audit Types

- Industry type
- Size of the organization
- Applicable government regulations
- Geographic location
- Voluntary business decision to adopt specific compliance standards

Role of Frameworks and Controls in Audits

- **Frameworks like NIST CSF and ISO 27000** help organizations prepare for audits and align with regulatory requirements.
- **Controls** work with frameworks to reduce risk and support compliance.
- **Three categories of controls** reviewed during an audit:
    - Administrative (Managerial)
    - Technical
    - Physical

Control Categories and Types

Administrative Controls

Control	Type	Purpose
Least Privilege	Preventative	Reduce risk of insider threats and account compromise
Disaster Recovery Plans	Corrective	Ensure business continuity
Password Policies	Preventative	Prevent brute-force/dictionary attacks
Access Control Policies	Preventative	Protect confidentiality and integrity
Account Management	Preventative	Manage account lifecycle, reduce attack surface
Separation of Duties	Preventative	Prevent abuse of privilege by single users

Technical Controls

Control	Type	Purpose
Firewall	Preventative	Block malicious traffic
IDS/IPS	Detective	Detect/prevent suspicious activity
Encryption	Deterrent	Maintain confidentiality of data
Backups	Corrective	Restore systems/data after incidents
Password Management	Preventative	Reduce password fatigue
Antivirus	Corrective	Detect and remove known threats
Manual Monitoring	Preventative	Identify/manage outdated system threats

Physical Controls

Control	Type	Purpose
Time-Controlled Safe	Deterrent	Reduce risk from physical threats
Adequate Lighting	Deterrent	Reduce hiding spots for attackers
CCTV	Preventative/Detective	Deter and investigate incidents
Locking Cabinets	Preventative	Protect network gear from unauthorized access
Alarm Service Signage	Deterrent	Deter intrusions by signaling monitoring
Locks	Deterrent/Preventative	Control physical access
Fire Alarms/Sprinklers	Detective/Preventative	Protect physical assets from fire damage

---

Control Types

1. **Preventative** – Prevent incidents (e.g., firewalls, password policies)
2. **Detective** – Identify if incidents occur (e.g., IDS, CCTV)
3. **Corrective** – Recover from incidents (e.g., backups, AV)
4. **Deterrent** – Discourage attacks (e.g., signage, encryption)

Audit Checklist

1. **Identify the Audit Scope**
    - Define the assets to be reviewed (e.g., firewalls, PII, physical security).
    - State how the audit supports the organization's security goals.
    - Set audit frequency.
    - Review policies and procedures for effectiveness and enforcement.
2. **Complete a Risk Assessment**

   - Analyze risks related to budgets, controls, internal processes, and regulations.
3. **Conduct the Audit**
   - Evaluate controls, practices, and implementation for the listed assets.
4. **Create a Mitigation Plan**
   - Suggest actions to lower risks and avoid compliance issues or security incidents.
5. **Communicate Results to Stakeholders**
   - Report:
     - Scope and goals
     - Risks and their urgency
     - Compliance needs
     - Recommendations for improving security posture

Key Takeaways

- A **security audit** is essential to assess how well an organization protects its data and assets.
- It involves planning, assessing, identifying controls, and recommending improvements.
- **Frameworks, controls, and compliance regulations** all work together during the audit process.
- Entry-level analysts often assist in these audits by reviewing scopes, assessing controls, and helping develop mitigation strategies.

Recap: Strengthening Security Foundations

1. **Security Frameworks**
   - Defined what they are and how they guide organizations in protecting data.
   - Emphasized the **importance of using structured approaches** like frameworks for building a strong security posture.
2. **Security Controls**
   - Explored **administrative**, **technical**, and **physical** controls.
   - Discussed how controls reduce risks, mitigate threats, and respond to vulnerabilities.
3. **CIA Triad**
   - **Confidentiality**: Protect data from unauthorized access.
   - **Integrity**: Ensure data is trustworthy and unaltered.
   - **Availability**: Ensure data/systems are accessible when needed.
4. **NIST Frameworks**
   - **NIST CSF (Cybersecurity Framework)**: A guide to reduce risk.
   - **NIST SP 800-53**: A catalog of security and privacy controls.
5. **OWASP Secure Design Principles**
   - Introduced key OWASP principles like **least privilege**, **defense in depth**, and **minimizing the attack surface**.
6. **Security Audits**
   - Focused on internal audits.
   - Explained how audits identify gaps and ensure compliance with both internal policies and external regulations.

Glossary terms from module 2

Asset: An item perceived as having value to an organization

Attack vectors: The pathways attackers use to penetrate security defenses

Authentication: The process of verifying who someone is

Authorization: The concept of granting access to specific resources in a system

Availability: The idea that data is accessible to those who are authorized to access it

Biometrics: The unique physical characteristics that can be used to verify a person's identity

Confidentiality: The idea that only authorized users can access specific assets or data

Confidentiality, integrity, availability (CIA) triad: A model that helps inform how organizations consider risk when setting up systems and security policies

Detect: A NIST core function related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections

Encryption: The process of converting data from a readable format to an encoded format

Govern: A NIST core function related to ensuring an organization establishes, oversees, and improves its cybersecurity strategy, policies, roles, and risk management processes to align with business goals and regulations

Identify: A NIST core function related to management of cybersecurity risk and its effect on an organization's people and assets

Integrity: The idea that the data is correct, authentic, and reliable

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

National Institute of Standards and Technology (NIST) Special Publication (S.P.) 800-53: A unified framework for protecting the security of information systems within the U.S. federal government

Open Web Application Security Project/Open Worldwide Application Security Project (OWASP): A non-profit organization focused on improving software security

Protect: A NIST core function used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats

Recover: A NIST core function related to returning affected systems back to normal operation

Respond: A NIST core function related to making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process

Risk: Anything that can impact the confidentiality, integrity, or availability of an asset

Security audit: A review of an organization's security controls, policies, and procedures against a set of expectations

Security controls: Safeguards designed to reduce specific security risks

Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy

Security posture: An organization’s ability to manage its defense of critical assets and data and react to change

Threat: Any circumstance or event that can negatively impact assets

---

Module 3

Introduction to Cybersecurity Tools

Security Tools Overview

Security professionals use various **tools** to:

- Collect **security data**
- **Detect and analyze** threats
- **Automate** security tasks

These tools support a **strong security posture** for organizations.

What's Next in This Section

You'll learn about:

1. **Different types of logs** – what they track and how they're used.
2. **SIEM (Security Information and Event Management)** dashboards – how they help analyze and manage logs.
3. **Common SIEM tools** used in the cybersecurity industry.

SIEM DASHBOARDS

Logs and SIEM tools

Log Sources in Cybersecurity

As a **security analyst**, you'll regularly review different types of **logs** to detect threats and vulnerabilities. Three common log types include:

1. **Firewall Logs**
    - Track incoming/outgoing connections
    - Show attempts from external sources or internal outbound traffic
2. **Network Logs**
    - Record all device entries/exits on the network
    - Log connections between devices and services
3. **Server Logs**
    - Log events related to services (web, email, file sharing)
    - Track login attempts, username/password entries

SIEM (Security Information and Event Management) Tools

- **Purpose**: Collect, store, and analyze log data
- **Functions**:
  - Real-time monitoring
  - Alert generation
  - Centralized log storage
  - Automated event analysis
- **Benefits**:
  - Saves time by reducing manual log reviews
  - Increases visibility into potential threats
- **Important Note**: SIEM tools **must be tailored** to an organization's specific environment and updated regularly to remain effective against evolving threats.

SIEM Dashboards: What They Are and How They're Used

SIEM dashboards display cybersecurity data in a visual, easy-to-understand format—just like weather apps show temperature and forecasts with charts and graphs.

Why SIEM Dashboards Matter

- **Visual Clarity**: Dashboards use **charts, graphs, and tables** to show trends, patterns, and alerts.
- **Fast Decision-Making**: Analysts can act quickly on threats based on visual summaries.
- **Customization**: Dashboards can be tailored to show data relevant to different roles (e.g., login attempts, traffic volume, failure rates).

Real-Life Use Case

- A security analyst gets an alert for suspicious login activity.
- They open the **SIEM dashboard** and notice:
  - **500 login attempts** for one account in 5 minutes
  - Attempts are from **unusual locations and times**
- This helps the analyst **identify and confirm** the incident quickly.

Metrics Tracked in Dashboards

Dashboards can show various **metrics** like:

- **Response time**
- **Availability**
- **Failure rate**
- **Network traffic volume**

These help teams monitor **system performance** and **cybersecurity threats** in real time.

The Future of SIEM Tools

What Are SIEM Tools? (Current Use)

- **SIEM (Security Information and Event Management)** tools collect and analyze **log data** to monitor critical activities in real time.
- They help identify threats, risks, and vulnerabilities through **dashboard visualizations**.
- Analysts still **manually review and respond** to alerts and events using these tools.

How SIEM Tools Are Evolving

1. Cloud Functionality

- **Cloud-Hosted SIEM**:
  - Managed and maintained by vendors.
  - Accessed via the internet.
  - Ideal for organizations that **don't want to manage their own infrastructure**.
- **Cloud-Native SIEM**:
  - Built specifically for the cloud.
  - Takes advantage of **cloud benefits** like:
    - **Scalability**
    - **Flexibility**
    - **High availability**

2. Responding to New Threats

- With more **IoT (Internet of Things)** devices, the **attack surface grows**, increasing risks.
- **Threats are becoming more diverse and data-heavy**, needing smarter tools.

3. Use of AI and Machine Learning

- **AI/ML** will enhance:
  - **Detection of threats**
  - **Log analysis**
  - **Data visualization**
  - **Event correlation**
- Tools will become **smarter and faster** at identifying unusual or malicious patterns.

4. Automation and SOAR

- **SOAR (Security Orchestration, Automation, and Response)** helps:

  - **Automate common security tasks**
  - **Speed up response times**
  - **Reduce manual workload** for analysts
- This allows analysts to **focus on complex threats** that can't be automated.

5. Integration of Cybersecurity Platforms

- Future platforms are expected to **communicate and work together**, improving efficiency.
- Full **interconnectivity between tools and devices** is still under development.

Key Takeaways

- **SIEM tools are essential** for monitoring and securing organizational data.
- As an entry-level analyst, you may work with SIEM dashboards daily.
- Stay updated on **emerging trends** like:
  - Cloud-native tools
  - AI/ML integration
  - Automation with SOAR
  - Cross-platform communication

Explore SIEM Tools

Common SIEM Tools

Types of SIEM Tools

1. **Self-hosted SIEM tools**
   - Installed and maintained on the organization’s own infrastructure.
   - Managed by the organization's IT team.
   - Suitable when **physical control over data** is required.
2. **Cloud-hosted SIEM tools**
   - Managed by third-party providers.
   - Accessed via the internet.
   - Suitable for organizations that don’t want to build or maintain internal infrastructure.
3. **Hybrid SIEM tools**
   - Combination of self-hosted and cloud-hosted.
   - Offers both **control** and **scalability**.

Common SIEM Tools

1. **Splunk Enterprise**
   - Self-hosted.
   - Real-time alerts, log retention, and search capabilities.
2. **Splunk Cloud**
   - Cloud-hosted version of Splunk.
   - Ideal for hybrid or fully cloud environments.
3. **Google Chronicle**
   - Cloud-native (designed specifically for the cloud).
   - Offers **log monitoring**, **data analysis**, and **data collection**.
   - Benefits from cloud features like **scalability** and **flexibility**.

Why SIEM Tools Matter

- Help detect and respond to evolving cyber threats.
- Improve security visibility.
- Support defense strategies for **confidentiality**, **integrity**, and **availability** (CIA triad).

More about cybersecurity tools

Open-Source Tools

- **Free** and **community-built**, promoting **collaboration** and **security**.
- **Customizable**: Users can modify the source code to suit their specific needs.
- Commonly used in the industry and often come with training material.
- Developers and users can **identify and fix issues quickly**.
- **Myth**: Open-source tools are unsafe — in reality, community oversight often makes them more secure.

Examples:

1. **Linux**
   - Open-source **operating system**.
   - Uses a **command-line interface (CLI)**.
   - Popular in cybersecurity for flexibility and control.
2. **Suricata**
   - Open-source **network analysis and threat detection** tool.
   - Developed by the **Open Information Security Foundation (OISF)**.
   - Inspects network traffic, logs data, detects threats.
   - Can be integrated with SIEM and other tools.

Proprietary Tools

- Owned and maintained by companies.
- Often require **payment** for usage, training, or updates.
- Only the owner can access or update the source code.
- Users have **limited customization options**.

Examples:

- **Splunk**
- **Google SecOps (Chronicle)**

Common Misconception

- **False belief**: Open-source tools are less effective.
- **Reality**: They're often more secure due to open access, faster updates, and broader community involvement.

Key Takeaways

- Both **open-source and proprietary** tools are essential in cybersecurity.
- Open-source tools are **highly trusted** and widely used.
- You'll get hands-on experience with both types throughout your cybersecurity training.

Use SIEM tools to protect organizations

SIEM Tools and Dashboards Overview

Security Information and Event Management (SIEM) tools help security professionals collect, monitor, analyze, and visualize log data to detect threats, risks, and vulnerabilities. Two major SIEM tools covered are:

- **Splunk** (Enterprise and Cloud)
- **Google Chronicle** (Cloud-native)

Splunk Dashboards

Splunk offers dashboards that help security teams manage infrastructure and gain full visibility over operations.

1. Security Posture Dashboard

- **Purpose**: For Security Operations Centers (SOCs)
- **Displays**: Last 24 hours of notable events and trends
- **Use**: Monitor real-time events like suspicious IP activity

2. Executive Summary Dashboard

- **Purpose**: For high-level organizational insights
- **Use**: Summarizes incidents and trends over time for stakeholders

3. Incident Review Dashboard

- **Purpose**: Spot patterns during or before incidents
- **Use**: Shows higher-risk items needing immediate analyst attention

4. Risk Analysis Dashboard

- **Purpose**: Analyze risk per object (user, IP, system)
- **Use**: Prioritize mitigation efforts based on behavioral anomalies (e.g., logins at odd hours)

Chronicle Dashboards

Chronicle focuses on cloud-native log retention and analysis with multiple customizable dashboards.

1. Enterprise Insights Dashboard

- **Purpose**: Identify recent alerts and IOCs (Indicators of Compromise)
- **Use**: Shows severity and confidence scores of threats

2. Data Ingestion and Health Dashboard

- **Purpose**: Track log sources and data processing success
- **Use**: Ensure proper ingestion and identify issues

3. IOC Matches Dashboard

- **Purpose**: Highlight top threats and trends
- **Use**: Track domain names, IPs, and devices to focus on high-priority threats

4. Main Dashboard

- **Purpose**: Display a summary of data ingestion, alerts, and events
- **Use**: Track security event trends (e.g., failed login spikes)

5. Rule Detections Dashboard

- **Purpose**: Track which detection rules generate alerts
- **Use**: Manage recurring incidents (e.g., malicious email attachment detection)

6. User Sign-In Overview Dashboard

- **Purpose**: Monitor user sign-in behavior
- **Use**: Spot suspicious activity (e.g., sign-ins from two locations at once)

Key Takeaways

- SIEM dashboards help organize and prioritize security work.
- They allow analysts to **focus on the highest risk areas**, reduce response time, and improve an organization's security posture.
- Later in the program, you'll practice using these tools and commands for real-world scenarios.

Recap: SIEM Tools and Logs

1. **Importance of Logs in Cybersecurity**
    - Logs are records of events in systems and networks.
    - Common log types:
        - **Firewall logs** – track inbound/outbound connections.
        - **Network logs** – record device and service connections.
        - **Server logs** – show login events, password requests, etc.
2. **SIEM Dashboards**
    - Visual tools that help security teams:
        - Monitor real-time activity.
        - Detect suspicious patterns.
        - Quickly assess security posture using charts, graphs, and tables.
    - Examples: **User Sign-In Overview**, **Risk Analysis**, **Incident Review**.
3. **Common SIEM Tools**
    - **Splunk**:
        - *Enterprise*: self-hosted, real-time analysis of log data.
        - *Cloud*: hosted by Splunk, for hybrid/cloud environments.
    - **Chronicle** (by Google):
        - Cloud-native tool designed for fast, scalable log analysis and threat detection.

Glossary terms from module 3

Chronicle: A cloud-native tool designed to retain, analyze, and search data

Incident response: An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

Log: A record of events that occur within an organization's systems

Metrics: Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application

Operating system (OS): The interface between computer hardware and the user

Playbook: A manual that provides details about any operational action

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that use automation to respond to security events

SIEM tools: A software platform that collects, analyzes, and correlates security data from various sources across your IT infrastructure that helps identify and respond to security threats in real-time, investigate security incidents, and comply with security regulations

Splunk Cloud: A cloud-hosted tool used to collect, search, and monitor log data

Splunk Enterprise: A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time

Module 4

Use playbooks to Respond to incidents

Phases of Incident Response Playbooks

Here's a quick summary of what you'll be diving into next:

Playbooks in Cybersecurity

- **What are Playbooks?**
  They're step-by-step guides used by security teams to respond **consistently and effectively** to threats, risks, or vulnerabilities detected by tools like SIEM.
- **Why are Playbooks Important?**
  They ensure **standardized, repeatable responses** so that every analyst—regardless of experience—knows exactly what to do when an incident occurs.

Six Phases of Incident Response

You'll also learn about the **NIST Incident Response Lifecycle**, which includes:

1. **Preparation** – Set up tools, policies, and training.
2. **Detection and Analysis** – Identify and assess potential threats.
3. **Containment** – Limit the scope of the incident.
4. **Eradication** – Remove the root cause (e.g., malware).
5. **Recovery** – Restore systems and confirm they're working.
6. **Lessons Learned** – Review what happened and improve the process.

What is a Playbook in Cybersecurity?

- A **playbook** is like a **step-by-step instruction manual** that tells the security team what to do when a security problem happens (like a cyberattack).
- It helps people respond **quickly, correctly, and in the same way every time**, no matter who is handling the situation.

Why Playbooks Matter

- Zack admits he doesn't know how to handle every situation on his own.
- Playbooks give him **confidence** by showing exactly **what to do** during an incident.
- When Zack handled his **first vulnerability report**, he was nervous—but the **remediation steps** in the playbook guided him.

What is an Incident Response Playbook?

It has **6 phases** that guide a team from the start of a problem to the end:

1. **Preparation**
   → Get ready before anything bad happens.
   Example: Make a plan, assign roles, train staff.
2. **Detection and Analysis**
   → Look for signs of trouble using tools like SIEM and figure out what's going on.
   Example: An alert from a SIEM tool says there's suspicious login activity.
3. **Containment**
   → Stop the problem from spreading.
   Example: Disconnect the affected computer or system.
4. **Eradication and Recovery**
   → Remove the threat completely and bring systems back to normal.
   Example: Delete malware, fix weaknesses, restore backups.
5. **Post-Incident Activity**
   → Learn from the incident.
   Example: Write a report, discuss what went wrong, and improve for next time.
6. **Coordination**
   → Keep everyone informed and make sure communication follows the rules.
   Example: Report the breach to leadership and share info with legal/compliance teams if required.

🛠 SIEM + Playbooks = Powerful Team

- SIEM tools **detect and alert** about threats.
- Playbooks help the team **know exactly what to do** when an alert is received.

Playbook?

- A **playbook** is a **manual or guide** used by cybersecurity teams.
- It gives a **step-by-step list** of what to do when a **security problem** (like a cyberattack) happens.
- It includes:
  - **Who** should do what
  - **How** the task should be done
  - And the **strategy** for responding to incidents

Living Document

- A playbook is **regularly updated** based on:
  - **New threats**
  - **Changes in laws or compliance**
  - **Mistakes found** in the past response

Types of Playbooks

1. **Incident Response Playbooks**
   Used when an attack (like ransomware, phishing, etc.) happens.
2. **Vulnerability Response Playbooks**
   Used when a weakness is found in a system that needs fixing before it's exploited.
3. **Other Playbooks**
   May be **team-specific** or **product-specific**, depending on the organization's needs.

Different Laws = Different Playbooks

- Playbooks vary by **country** or **region**, because:
  - Different **laws** and **data regulations** apply
  - Reporting rules may **change based on location** or **data type**

Why Are They Important?

- **Ensure legal and organizational compliance**
- **Help respond fast and correctly**
- **Avoid errors** during high-stress incidents
- **Protect forensic data** (important for investigating attacks)
- **Reduce risks** and damages

Common Steps in Playbooks

These usually follow the **Incident Response Lifecycle**:

1. **Preparation**
2. **Detection**
3. **Analysis**
4. **Containment**
5. **Eradication**
6. **Recovery**
7. **Post-incident activity**
8. **Coordination**

Key Takeaways

- Playbooks bring **structure**, help with **faster response**, and ensure **no important step is missed**.
- After each incident, **improvements** should be made based on what was learned.
- Following a playbook is **critical**—especially during forensic investigations—because **one**
- **wrong step can destroy evidence**.

Phases of Incident Response Playbooks
Explore Incident Response

Use a playbook to respond to threats risks or vulnerabilities

SIEM Tools + Playbooks: Working Together

- **SIEM tools** generate alerts based on unusual or suspicious activity detected in logs.
- **Playbooks** guide security professionals through standardized response procedures after receiving those alerts.

How Playbooks Help During Incidents (e.g., Malware Attack)

1. **Assess the Alert**
    - Confirm if the SIEM alert is valid.
    - Investigate why it was triggered (e.g., by checking log data and metrics).
2. **Contain the Threat**
    - Take action to stop the spread.
    - Example: Disconnect the infected machine from the network.
3. **Eradicate and Recover**
    - Remove all traces of the threat.
    - Restore systems and data from clean backups.
4. **Post-Incident Activity & Coordination**
    - Document what happened.
    - Report to stakeholders or authorities (e.g., FBI).
    - Improve procedures based on lessons learned.

Playbooks Are Living Documents

- Constantly **updated** to reflect:
    - New attack methods
    - Past incident lessons
    - Regulatory changes

For Entry-Level Analysts

- Playbooks are **essential tools** you'll likely use daily.
- They help ensure **consistency, accuracy, and compliance** in your incident response actions.

Playbooks, SIEM Tools, and SOAR Tools

What are Playbooks?

- Step-by-step **guides** for security teams to respond to incidents.
- Ensure **consistent, correct actions**—no matter who is handling the case.
- Can include **flowcharts, tables**, and role-specific instructions.
- Used during incidents like **ransomware attacks** and **unusual user behavior**.

Playbooks + SIEM Tools

- **SIEM tools** monitor logs and detect threats.
- When a SIEM tool **flags an issue** (e.g., odd user activity), a playbook guides analysts on:
  - What to do
  - When to do it
  - Who should handle it

Playbooks + SOAR Tools

- **SOAR** = Security Orchestration, Automation, and Response.
- SOAR automates tasks that SIEM or MDR (Managed Detection & Response) tools identify.
- Example: If someone enters the wrong password many times,
  - **SOAR blocks the account automatically**
  - Then, the analyst uses the **playbook** to take next steps (like investigate, report, restore access)

Key Takeaway

Playbooks (also called **runbooks**) are **essential tools** that tell security teams exactly **what to do, when, and by whom** during security incidents — helping reduce risk and damage.

RECAP

1. **Purpose of Playbooks**:
   - They guide security analysts through **step-by-step responses** to incidents.
   - Ensure **consistent and efficient** handling of security threats, regardless of who is on shift.
2. **6 Phases of Incident Response Playbook**:
   - **Preparation**
   - **Detection and Analysis**
   - **Containment**

- **Eradication and Recovery**
- **Post-Incident Activity**
- **Coordination**

3. **Playbooks in Action**:
   - Used alongside **SIEM** and **SOAR** tools.
   - Help analysts make **informed decisions**, reduce errors, and limit **organizational damage**.
4. **Communication Matters**:
   - Following the playbook isn't just technical—it includes communicating clearly with the team to ensure coordinated response.

Why It Matters

Understanding and using playbooks effectively can be the difference between **containing a threat quickly** and letting it **escalate into a major incident**. As an entry-level analyst, playbooks empower you to handle situations with **confidence and consistency**.

Glossary terms from module 4

Incident response: An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

Playbook: A manual that provides details about any operational action

Course wrap-up

Key Topics Covered:

1. **CISSP's 8 Security Domains**
   Gained foundational insight into the structure of security responsibilities.
2. **Threats, Risks, and Vulnerabilities**
   Understood how they impact business operations and how to address them.
3. **Security Frameworks & Controls**
   - CIA Triad (Confidentiality, Integrity, Availability)
   - NIST CSF and SP 800-53
   - Secure design principles
   - How frameworks support audits and compliance.
4. **Security Tools – SIEM**
   Learned about tools like **Splunk** and **Chronicle**, and their dashboards to monitor security posture.
5. **Incident Response Playbooks**
   Understood how structured response guides help manage and mitigate incidents effectively (including phases like detection, containment, recovery, and coordination).