# Google - CyberSecurity - 2nd Chapter

## MODULE - 1

**Security Posture -** It can be defined as an organization's ability to manage its defense of critical assets and data, and react to change.

**Risk Mitigation -** the process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

**Business Continuity -** An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans.

## Security domains cybersecurity analysts need to know

As an analyst, you can explore various areas of cybersecurity that interest you. One way to explore those areas is by understanding different security domains and how they're used to organize the work of security professionals. In this reading you will learn more about CISSP's eight security domains and how they relate to the work you'll do as a security analyst.

## Domain one: Security and risk management

All organizations must develop their security posture. Security posture is an organization’s ability to manage its defense of critical assets and data and react to change. Elements of the security and risk management domain that impact an organization's security posture include:

- Security goals and objectives
- Risk mitigation processes
- Compliance
- Business continuity plans
- Legal regulations
- Professional and organizational ethics

Information security, or InfoSec, is also related to this domain and refers to a set of processes established to secure information. An organization may use playbooks and implement training as a part of their security and risk management program, based on their needs and perceived risk. There are many InfoSec design processes, such as:

- Incident response
- Vulnerability management
- Application security
- Cloud security
- Infrastructure security

As an example, a security team may need to alter how personally identifiable information (PII) is treated in order to adhere to the European Union's General Data Protection Regulation (GDPR).

## Domain two: Asset security

Asset security involves managing the cybersecurity processes of organizational assets, including the storage, maintenance, retention, and destruction of physical and virtual

data. Because the loss or theft of assets can expose an organization and increase the level of risk, keeping track of assets and the data they hold is essential. Conducting a security impact analysis, establishing a recovery plan, and managing data exposure will depend on the level of risk associated with each asset. Security analysts may need to store, maintain, and retain data by creating backups to ensure they are able to restore the environment if a security incident places the organization’s data at risk.

## Domain three: Security architecture and engineering

This domain focuses on managing data security. Ensuring effective tools, systems, and processes are in place helps protect an organization’s assets and data. Security architects and engineers create these processes.

One important aspect of this domain is the concept of shared responsibility. Shared responsibility means all individuals involved take an active role in lowering risk during the design of a security system. Additional design principles related to this domain, which are discussed later in the program, include:

- Threat modeling
- Least privilege
- Defense in depth
- Fail securely
- Separation of duties
- Keep it simple
- Zero trust
- Trust but verify

An example of managing data is the use of a security information and event management (SIEM) tool to monitor for flags related to unusual login or user activity that could indicate a threat actor is attempting to access private data.

## Domain four: Communication and network security

This domain focuses on managing and securing physical networks and wireless communications. This includes on-site, remote, and cloud communications.

Organizations with remote, hybrid, and on-site work environments must ensure data remains secure, but managing external connections to make certain that remote workers are securely accessing an organization’s networks is a challenge. Designing network security controls—such as restricted network access—can help protect users and ensure an organization’s network remains secure when employees travel or work outside of the main office.

## Domain five: Identity and access management

The identity and access management (IAM) domain focuses on keeping data secure. It does this by ensuring user identities are trusted and authenticated and that access to physical and logical assets is authorized. This helps prevent unauthorized users, while allowing authorized users to perform their tasks.

Essentially, IAM uses what is referred to as the principle of least privilege, which is the concept of granting only the minimal access and authorization required to complete a task. As an example, a cybersecurity analyst might be asked to ensure that customer service representatives can only view the private data of a customer, such as their phone number, while working to resolve the customer's issue; then remove access when the customer's issue is resolved.

## Domain six: Security assessment and testing

The security assessment and testing domain focuses on identifying and mitigating risks, threats, and vulnerabilities. Security assessments help organizations determine whether their internal systems are secure or at risk. Organizations might employ penetration testers, often referred to as “pen testers,” to find vulnerabilities that could be exploited by a threat actor.

This domain suggests that organizations conduct security control testing, as well as collect and analyze data. Additionally, it emphasizes the importance of conducting security audits to monitor for and reduce the probability of a data breach. To contribute to these types of tasks, cybersecurity professionals may be tasked with auditing user permissions to validate that users have the correct levels of access to internal systems.

## Domain seven: Security operations

The security operations domain focuses on the investigation of a potential data breach and the implementation of preventative measures after a security incident has occurred. This includes using strategies, processes, and tools such as:

- Training and awareness
- Reporting and documentation
- Intrusion detection and prevention
- SIEM tools
- Log management
- Incident management
- Playbooks
- Post-breach forensics
- Reflecting on lessons learned

The cybersecurity professionals involved in this domain work as a team to manage, prevent, and investigate threats, risks, and vulnerabilities. These individuals are trained to handle active attacks, such as large amounts of data being accessed from an organization's internal network, outside of normal working hours. Once a threat is identified, the team works diligently to keep private data and information safe from threat actors.

## Domain eight: Software development security

The software development security domain is focused on using secure programming practices and guidelines to create secure applications. Having secure applications helps deliver secure and reliable services, which helps protect organizations and their users.

Security must be incorporated into each element of the software development life cycle, from design and development to testing and release. To achieve security, the software development process must have security in mind at each step. Security cannot be an afterthought.

Performing application security tests can help ensure vulnerabilities are identified and mitigated accordingly. Having a system in place to test the programming conventions,

software executables, and security measures embedded in the software is necessary. Having quality assurance and pen tester professionals ensure the software has met security and performance standards is also an essential part of the software development process. For example, an entry-level analyst working for a pharmaceutical company might be asked to make sure encryption is properly configured for a new medical device that will store private patient data.

**RISK - A risk is anything that can impact the confidentiality, integrity, or availability of an asset. Think of a risk as the likelihood of a threat occurring, Organizations tend to rate risks at different levels: low, medium, and high, depending on possible threats and the value of an asset.**

- **Low - risk asset -** A low-risk asset is information that would not harm the organization's reputation or ongoing operations, and would not cause financial damage if compromised. This includes public information such as website content, or published research data.
- **Medium - risk asset -** A medium-risk asset might include information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations. For example, the early release of a company's quarterly earnings could impact the value of their stock.
- **High - risk asset -** A high-risk asset is any information protected by regulations or laws, which if compromised, would have a severe negative impact on an organization's finances, ongoing operations, or reputation. This could include leaked assets with SPII, PII, or intellectual property.

**Vulnerability -** A vulnerability is a weakness that can be exploited by a threat. And it's worth noting that both a vulnerability and threat must be present for there to be a risk. Examples of vulnerabilities include: an outdated firewall, software, or application; weak passwords; or unprotected confidential data. People can also be considered a vulnerability. People's actions can significantly affect an organization's internal network. Whether it's a client, external vendor, or employee, maintaining security must be a united effort.

# Manage common threats, risks, and vulnerabilities

Previously, you learned that security involves protecting organizations and people from threats, risks, and vulnerabilities. Understanding the current threat landscapes gives organizations the ability to create policies and processes designed to help prevent and mitigate these types of security issues. In this reading, you will further explore how to manage risk and some common threat actor tactics and techniques, so you are better prepared to protect organizations and the people they serve when you enter the cybersecurity field.

## Risk management

A primary goal of organizations is to protect assets. An **asset** is an item perceived as having value to an organization. Assets can be digital or physical. Examples of digital assets include the personal information of employees, clients, or vendors, such as:

- Social Security Numbers (SSNs), or unique national identification numbers assigned to individuals
- Dates of birth
- Bank account numbers
- Mailing addresses

Examples of physical assets include:

- Payment kiosks
- Servers
- Desktop computers
- Office spaces

Some common strategies used to manage risks include:

- **Acceptance**: Accepting a risk to avoid disrupting business continuity
- **Avoidance**: Creating a plan to avoid the risk altogether
- **Transference**: Transferring risk to a third party to manage

- **Mitigation**: Lessening the impact of a known risk

Additionally, organizations implement risk management processes based on widely accepted frameworks to help protect digital and physical assets from various threats, risks, and vulnerabilities. Examples of frameworks commonly used in the cybersecurity industry include the National Institute of Standards and Technology Risk Management Framework (NIST RMF) and Health Information Trust Alliance (HITRUST).

Following are some common types of threats, risks, and vulnerabilities you'll help organizations manage as a security professional.

# Today's most common threats, risks, and vulnerabilities

## Threats

A **threat** is any circumstance or event that can negatively impact assets. As an entry-level security analyst, your job is to help defend the organization's assets from inside and outside threats. Therefore, understanding common types of threats is important to an analyst's daily work. As a reminder, common threats include:

- **Insider threats:** Staff members or vendors abuse their authorized access to obtain data that may harm an organization.
- **Advanced persistent threats (APTs):** A threat actor maintains unauthorized access to a system for an extended period of time.

## Risks

A **risk** is anything that can impact the confidentiality, integrity, or availability of an asset. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. One way to think about this is that a risk is being late to work and threats are traffic, an accident, a flat tire, etc.

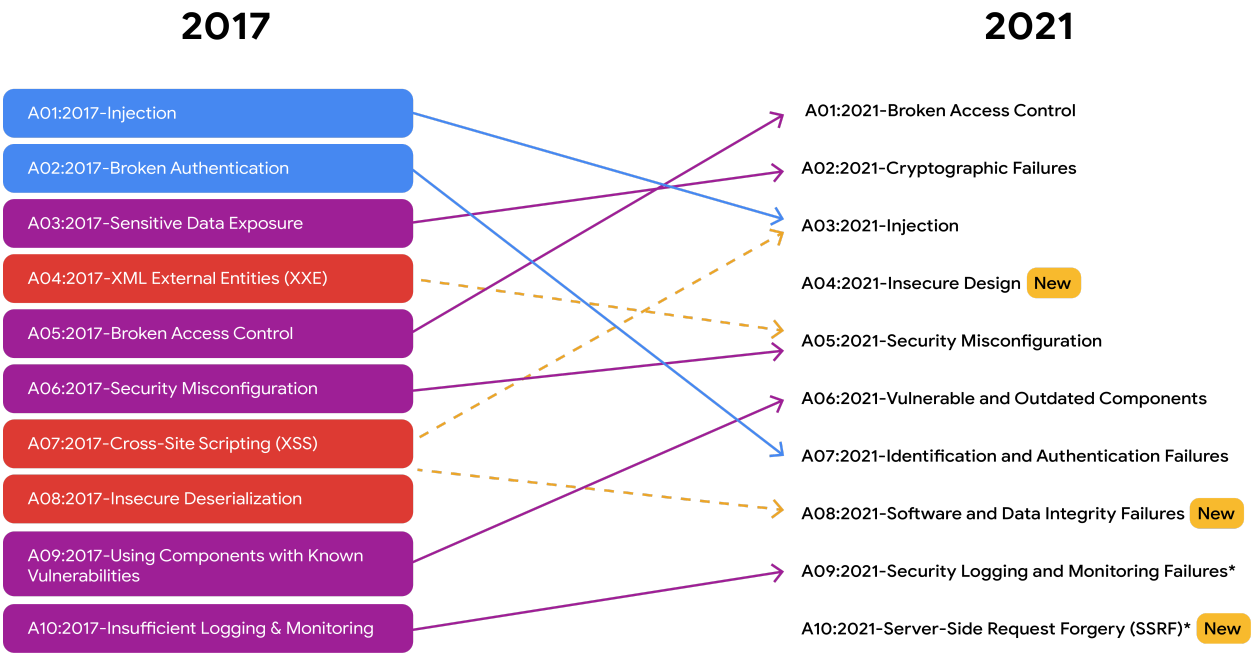
There are different factors that can affect the likelihood of a risk to an organization's assets, including:

- **External risk:** Anything outside the organization that has the potential to harm organizational assets, such as threat actors attempting to gain access to private information

- **Internal risk:** A current or former employee, vendor, or trusted partner who poses a security risk
- **Legacy systems:** Old systems that might not be accounted for or updated, but can still impact assets, such as workstations or old mainframe systems. For example, an organization might have an old vending machine that takes credit card payments or a workstation that is still connected to the legacy accounting system.
- **Multiparty risk:** Outsourcing work to third-party vendors can give them access to intellectual property, such as trade secrets, software designs, and inventions.
- **Software compliance/licensing:** Software that is not updated or in compliance, or patches that are not installed in a timely manner

There are many resources, such as the NIST, that provide lists of cybersecurity risks. Additionally, the Open Web Application Security Project (OWASP) publishes a standard awareness document about the top 10 most critical security risks to web applications, which is updated regularly.

**Note:** The OWASP's common attack types list contains three new risks for the years 2017 to 2021: insecure design, software and data integrity failures, and server-side request forgery. This update emphasizes the fact that security is a constantly evolving field. It also demonstrates the importance of staying up to date on current threat actor tactics and techniques, so you can be better prepared to manage these types of risks.



## Vulnerabilities

A **vulnerability** is a weakness that can be exploited by a threat. Therefore, organizations need to regularly inspect for vulnerabilities within their systems. Some vulnerabilities include:

- **ProxyLogon:** A pre-authenticated vulnerability that affects the Microsoft Exchange server. This means a threat actor can complete a user authentication process to deploy malicious code from a remote location.
- **ZeroLogon:** A vulnerability in Microsoft's Netlogon authentication protocol. An authentication protocol is a way to verify a person's identity. Netlogon is a service that ensures a user's identity before allowing access to a website's location.
- **Log4Shell:** Allows attackers to run Java code on someone else's computer or leak sensitive information. It does this by enabling a remote attacker to take control of devices connected to the internet and run malicious code.
- **PetitPotam:** Affects Windows New Technology Local Area Network (LAN) Manager (NTLM). It is a theft technique that allows a LAN-based attacker to initiate an authentication request.
- **Security logging and monitoring failures:** Insufficient logging and monitoring capabilities that result in attackers exploiting vulnerabilities without the organization knowing it
- **Server-side request forgery:** Allows attackers to manipulate a server-side application into accessing and updating backend resources. It can also allow threat actors to steal data.

As an entry-level security analyst, you might work in vulnerability management, which is monitoring a system to identify and mitigate vulnerabilities. Although patches and updates may exist, if they are not applied, intrusions can still occur. For this reason, constant monitoring is important. The sooner an organization identifies a vulnerability and addresses it by patching it or updating their systems, the sooner it can be mitigated, reducing the organization's exposure to the vulnerability.

To learn more about the vulnerabilities explained in this section of the reading, as well as other vulnerabilities, explore the NIST National Vulnerability Database and CISA Known Exploited Vulnerabilities Catalog.

**NIST’s Risk Management Framework -**

- **The RMF(Risk Management Framework) -**

1. **Prepare** - Prepare refers to activities that are necessary to manage security and privacy risks before a breach occurs. As an entry-level analyst, you'll likely use this step to monitor for risks and identify controls that can be used to reduce those risks.
2. **Categorize -** It is used to develop risk management processes and tasks. Security professionals then use those processes and develop tasks by thinking about how the confidentiality, integrity, and availability of systems and information can be impacted by risk. As an entry-level analyst, you'll need to be able to understand how to follow the processes established by your organization to reduce risks to critical assets, such as private customer information.
3. **Select -** Select means to choose, customize, and capture documentation of the controls that protect an organization. An example of the select step would be keeping a playbook up-to-date or helping to manage other documentation that allows you and your team to address issues more efficiently.
4. **Implement -** It means to implement security and privacy plans for the organization. Having good plans in place is essential for minimizing the impact of ongoing security risks. For example, if you notice a pattern of employees constantly needing password resets, implementing a change to password requirements may help solve this issue.
5. **Assess -** Assess means to determine if established controls are implemented correctly. An organization always wants to operate as efficiently as possible. So it's essential to take the time to analyze whether the implemented protocols, procedures, and controls that are in place are meeting organizational needs. During this step, analysts identify potential weaknesses and determine whether the organization's tools, procedures, controls, and protocols should be changed to better manage potential risks.
6. **Authorize -** Authorize means being accountable for the security and privacy risks that may exist in an organization. As an analyst, the authorization step could involve generating reports, developing plans of action, and establishing project milestones that are aligned to your organization's security goals.

7. **Monitor -** Monitor means to be aware of how systems are operating. Assessing and maintaining technical operations are tasks that analysts complete daily. Part of maintaining a low level of risk for an organization is knowing how the current systems support the organization's security goals. If the systems in place don't meet those goals, changes may be needed.

**Security Frameworks -** Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy, such as social engineering attacks and ransomware.

**Security Controls -** Security controls are safeguards designed to reduce specific security risks.

***Three Common types of Controls are -***

1) **Encryption -** Encryption is the process of converting data from a readable format to an encoded format. Typically, encryption involves converting data from plaintext to ciphertext. Ciphertext is the raw, encoded message that's unreadable to humans and computers. Ciphertext data cannot be read until it's been decrypted into its original plaintext form. Encryption is used to ensure confidentiality of sensitive data, such as customers' account information or social security numbers.

2) **Authentication -** Authentication is the process of verifying who someone or something is. A real-world example of authentication is logging into a website with your username and password. This basic form of authentication proves that you know the username and password and should be allowed to access the website. More advanced methods of authentication, such as multi-factor authentication, or MFA, challenge the user to demonstrate that they are who they claim to be by requiring both a password and an additional form of authentication, like a security code or biometrics, such as a fingerprint, voice, or face scan.

3) **Authorization -** Authorization refers to the concept of granting access to specific resources within a system. Essentially, authorization is used to verify that a person has permission to access a resource. As an example, if you're working as an entry-level security analyst for the federal government, you could have permission to access data through the deep web or other internal data that is only accessible if you're a federal employee.

# MODULE - 2

# The relationship between frameworks and controls

Previously, you learned how organizations use security frameworks and controls to protect against threats, risks, and vulnerabilities. This included discussions about the National Institute of Standards and Technology's (NIST's) Risk Management Framework (RMF) and Cybersecurity Framework (CSF), as well as the confidentiality, integrity, and availability (CIA) triad. In this reading, you will further explore security frameworks and controls and how they are used together to help mitigate organizational risk.

## Frameworks and controls

**Security frameworks** are guidelines used for building plans to help mitigate risk and threats to data and privacy. Frameworks support organizations' ability to adhere to compliance laws and regulations. For example, the healthcare industry uses frameworks to comply with the United States' Health Insurance Portability and Accountability Act (HIPAA), which requires that medical professionals keep patient information safe.

**Security controls** are safeguards designed to reduce *specific* security risks. Security controls are the measures organizations use to lower risk and threats to data and privacy. For example, a control that can be used alongside frameworks to ensure a hospital remains compliant with HIPAA is requiring that patients use multi-factor authentication (MFA) to access their medical records. Using a measure like MFA to validate someone's identity is one way to help mitigate potential risks and threats to private data.

# Specific frameworks and controls

There are many different frameworks and controls that organizations can use to remain compliant with regulations and achieve their security goals. Frameworks covered in this reading are the Cyber Threat Framework (CTF) and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001. Several common security controls, used alongside these types of frameworks, are also explained.

## Cyber Threat Framework (CTF)

According to the Office of the Director of National Intelligence, the CTF was developed by the U.S. government to provide “a common language for describing and communicating information about cyber threat activity.” By providing a common language to communicate information about threat activity, the CTF helps cybersecurity professionals analyze and share information more efficiently. This allows organizations to improve their response to the constantly evolving cybersecurity landscape and threat actors' many tactics and techniques.

## International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001

An internationally recognized and used framework is ISO/IEC 27001. The ISO 27000 family of standards enables organizations of all sectors and sizes to manage the security of assets, such as financial information, intellectual property, employee data, and information entrusted to third parties. This framework outlines requirements for an information security management system, best practices, and controls that support an organization’s ability to manage risks. Although the ISO/IEC 27001 framework does not require the use of specific controls, it does provide a collection of controls that organizations can use to improve their security posture.

## Controls

Controls are used alongside frameworks to reduce the possibility and impact of a security threat, risk, or vulnerability. Controls can be physical, technical, and administrative and are typically used to prevent, detect, or correct security issues.

Examples of physical controls:

- Gates, fences, and locks

- Security guards
- Closed-circuit television (CCTV), surveillance cameras, and motion detectors
- Access cards or badges to enter office spaces

Examples of technical controls:

- Firewalls
- MFA
- Antivirus software

Examples of administrative controls:

- Separation of duties
- Authorization
- Asset classification

**“**To learn more about controls, particularly those used to protect health-related assets from a variety of threat types, review the U.S. Department of Health and Human Services’ Physical Access Control presentation.

*The **CIA triad** is a foundational security model that helps inform how organizations consider risk when setting up systems and security policies. As a reminder, the three letters in the CIA triad stand for confidentiality, integrity, and availability. As an entry-level analyst, you'll find yourself constantly referring to these three core principles as you work to protect your organization and the people it serves.*

***Confidentiality -** Confidentiality means that only authorized users can access specific assets or data. Sensitive data should be available on a "need to know" basis, so that only the people who are authorized to handle certain assets or data have access.*

***Integrity -** Integrity means that the data is correct, authentic, and reliable. Determining the integrity of data and analyzing how it's used will help you, as a security professional, decide whether the data can or cannot be trusted.*

***Availability -** Availability means that the data is accessible to those who are authorized to access it. Inaccessible data isn't useful and can prevent people from being able to do their jobs. As a security professional, ensuring that systems, networks, and applications are functioning properly to allow for timely and reliable access, may be a part of your everyday work responsibilities.**”***

# Use the CIA triad to protect organizations

Previously, you were introduced to the confidentiality, integrity, and availability (CIA) triad and how it helps organizations consider and mitigate risk. In this reading, you will learn how cybersecurity analysts use the CIA triad in the workplace.

## The CIA triad for analysts

The **CIA triad** is a model that helps inform how organizations consider risk when setting up systems and security policies. It is made up of three elements that cybersecurity analysts and organizations work toward upholding: confidentiality, integrity, and availability. Maintaining an acceptable level of risk and ensuring systems and policies are designed with these elements in mind helps establish a successful **security posture**, which refers to an organization’s ability to manage its defense of critical assets and data and react to change.

### Confidentiality

**Confidentiality** is the idea that only authorized users can access specific assets or data. In an organization, confidentiality can be enhanced through the implementation of design principles, such as the principle of least privilege. The principle of least privilege limits users' access to only the information they need to complete work-related tasks. Limiting access is one way of maintaining the confidentiality and security of private data.

### Integrity

**Integrity** is the idea that the data is verifiably correct, authentic, and reliable. Having protocols in place to verify the authenticity of data is essential. One way to verify data integrity is through cryptography, which is used to transform data so unauthorized parties cannot read or tamper with it (NIST, 2022). Another example of how an organization might implement integrity is by enabling encryption, which is the process of converting data from a readable format to an encoded format. Encryption can be used to prevent access and ensure data, such as messages on an organization's internal chat platform, cannot be tampered with.

## Availability

**Availability** is the idea that data is accessible to those who are authorized to use it. When a system adheres to both availability and confidentiality principles, data can be used when needed. In the workplace, this could mean that the organization allows remote employees to access its internal network to perform their jobs. It’s worth noting that access to data on the internal network is still limited, depending on what type of access employees need to do their jobs. If, for example, an employee works in the organization’s accounting department, they might need access to corporate accounts but not data related to ongoing development projects.

# NIST CYBER SECURITY FRAMEWORK -

NIST CSF focuses on five core functions: ***identify, protect, detect, respond, and recover***. These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes. Basically, when it comes to security operations, NIST CSF functions are key for making sure an organization is protected against potential threats, risks, and vulnerabilities. So let's take a little time to explore how each function can be used to improve an organization's security.

**The first** core function is identify, which is related to the management of cybersecurity risk and its effect on an organization's people and assets. For example, as a security analyst, you may be asked to monitor systems and devices in your organization's internal network to identify potential security issues

**The second** core function is protect, which is the strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats. **For example**, as a security analyst, you and your team might encounter new and unfamiliar threats and attacks. For this reason, studying historical data and making improvements to policies and procedures is essential.

**The third** core function is detect, which means identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections. For example, as an analyst, you might be asked to review a new security tool's setup to make sure it's flagging low, medium, or high risk, and then alerting the security team about any potential threats or incidents.

**The fourth** function is respond, which means making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process. As an analyst, you could be working with a team to collect and organize data to document an incident and suggest improvements to processes to prevent the incident from happening again.

**The fifth** core function is recover, which is the process of returning affected systems back to normal operation. **For example**, as an entry-level security analyst, you might work with your security team to restore systems, data, and assets, such as financial or legal files, that have been affected by an incident like a breach.

## Open Web Application Security Project, or OWASP, security principles

***OWASP security principles are -***

- Minimize attack surface area
- Principle of least privilege
- Defense in depth
- Separation of duties
- Keep security simple
- Fix security issues correctly

**1)** The first OWASP principle is to **minimize the attack surface area**. An attack surface refers to all the potential vulnerabilities that a threat actor could exploit, like attack vectors, which are pathways attackers use to penetrate security defenses. Examples of common attack vectors are phishing emails and weak passwords. To minimize the attack surface and avoid incidents from these types of vectors, security teams might disable software features, restrict who can access certain assets, or establish more complex password requirements.

**2)** The **principle of least privilege** means making sure that users have the least amount of access required to perform their everyday tasks. The main reason for limiting access to organizational information and resources is to reduce the amount of damage a security breach could cause. For example, as an entry-level analyst, you may have access to log data, but may not have access to change user permissions. Therefore, if a threat actor compromises your credentials, they'll only be able to gain limited access to

digital or physical assets, which may not be enough for them to deploy their intended attack.

**3)** The next principle we'll discuss is **defense in depth**. Defense in depth means that an organization should have multiple security controls that address risks and threats in different ways. One example of a security control is multi-factor authentication, or MFA, which requires users to take an additional step beyond simply entering their username and password to gain access to an application. Other controls include firewalls, intrusion detection systems, and permission settings that can be used to create multiple points of defense, a threat actor must get through to breach an organization.

**4)** Another principle is **separation of duties**, which can be used to prevent individuals from carrying out fraudulent or illegal activities. This principle means that no one should be given so many privileges that they can misuse the system. For example, the person in a company who signs the paychecks shouldn't also be the person who prepares them.

**5) Keep security simple** is the next principle. As the name suggests, when implementing security controls, unnecessarily complicated solutions should be avoided because they can become unmanageable. The more complex the security controls are, the harder it is for people to work collaboratively.

**6)** The last principle is **to fix security issues correctly**. Technology is a great tool, but can also present challenges. When a security incident occurs, security professionals are expected to identify the root cause quickly. From there, it's important to correct any identified vulnerabilities and conduct tests to ensure that repairs are successful. **An example** of an issue is a weak password to access an organization's wifi because it could lead to a breach. To fix this type of security issue, stricter password policies could be put in place.

# More about OWASP security principles

Previously, you learned that cybersecurity analysts help keep data safe and reduce risk for an organization by using a variety of security frameworks, controls, and security principles. In this reading, you will learn about more Open Web Application Security Project, recently renamed Open Worldwide Application Security Project® (OWASP), security principles and how entry-level analysts use them.

# Security principles

In the workplace, security principles are embedded in your daily tasks. Whether you are analyzing logs, monitoring a security information and event management (SIEM) dashboard, or using a vulnerability scanner, you will use these principles in some way.

Previously, you were introduced to several OWASP security principles. These included:

- **Minimize attack surface area**: Attack surface refers to all the potential vulnerabilities a threat actor could exploit.
- **Principle of least privilege**: Users have the least amount of access required to perform their everyday tasks.
- **Defense in depth**: Organizations should have varying security controls that mitigate risks and threats.
- **Separation of duties**: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
- **Keep security simple**: Avoid unnecessarily complicated solutions. Complexity makes security difficult.
- **Fix security issues correctly**: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.

# Additional OWASP security principles

Next, you'll learn about four additional OWASP security principles that cybersecurity analysts and their teams use to keep organizational operations and people safe.

## Establish secure defaults

This principle means that the optimal security state of an application is also its default state for users; it should take extra work to make the application insecure.

## Fail securely

Fail securely means that when a control fails or stops, it should do so by defaulting to its most secure option. For example, when a firewall fails it should simply close all connections and block all new ones, rather than start accepting everything.

### Don’t trust services

Many organizations work with third-party partners. These outside partners often have different security policies than the organization does. And the organization shouldn’t explicitly trust that their partners’ systems are secure. For example, if a third-party vendor tracks reward points for airline customers, the airline should ensure that the balance is accurate before sharing that information with their customers.

### Avoid security by obscurity

The security of key systems should not rely on keeping details hidden. Consider the following example from OWASP (2016): The security of an application should not rely on keeping the source code secret. Its security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

# More about security audits

Previously, you were introduced to how to plan and complete an internal security audit. In this reading, you will learn more about security audits, including the goals and objectives of audits.

## Security audits

A **security audit** is a review of an organization's security controls, policies, and procedures against a set of expectations. Audits are independent reviews that evaluate whether an organization is meeting internal and external criteria. Internal criteria include outlined policies, procedures, and best practices. External criteria include regulatory compliance, laws, and federal regulations.

Additionally, a security audit can be used to assess an organization's established security controls. As a reminder, **security controls** are safeguards designed to reduce specific security risks.

Audits help ensure that security checks are made (i.e., daily monitoring of security information and event management dashboards), to identify threats, risks, and vulnerabilities. This helps maintain an organization’s security posture. And, if there are security issues, a remediation process must be in place.

## Goals and objectives of an audit

The goal of an audit is to ensure an organization's information technology (IT) practices are meeting industry and organizational standards. The objective is to identify and address areas of remediation and growth. Audits provide direction and clarity by identifying what the current failures are and developing a plan to correct them.

Security audits must be performed to safeguard data and avoid penalties and fines from governmental agencies. The frequency of audits is dependent on local laws and federal compliance regulations.

## Factors that affect audits

Factors that determine the types of audits an organization implements include:

- Industry type
- Organization size
- Ties to the applicable government regulations
- A business’s geographical location
- A business decision to adhere to a specific regulatory compliance

To review common compliance regulations that different organizations need to adhere to, refer to the reading about controls, frameworks, and compliance.

## The role of frameworks and controls in audits

Along with compliance, it’s important to mention the role of frameworks and controls in security audits. Frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the international standard for information security (ISO 27000) series are designed to help organizations prepare for regulatory compliance security audits. By adhering to these and other relevant frameworks, organizations can save time when conducting external and internal audits. Additionally, frameworks, when used alongside controls, can support organizations’ ability to align with regulatory compliance requirements and standards.

There are three main categories of controls to review during an audit, which are administrative and/or managerial, technical, and physical controls. To learn more about specific controls related to each category, click the following link and select “Use Template.”

Link to template: Control categories

OR

Control-categories.docx

## Audit checklist

It’s necessary to create an audit checklist before conducting an audit. A checklist is generally made up of the following areas of focus:

**Identify the scope of the audit**

- The audit should:
  - List assets that will be assessed (e.g., firewalls are configured correctly, PII is secure, physical assets are locked, etc.)
  - Note how the audit will help the organization achieve its desired goals
  - Indicate how often an audit should be performed
  - Include an evaluation of organizational policies, protocols, and procedures to make sure they are working as intended and being implemented by employees

**Complete a risk assessment**

- A risk assessment is used to evaluate identified organizational risks related to budget, controls, internal processes, and external standards (i.e., regulations).

**Conduct the audit**

- When conducting an internal audit, you will assess the security of the identified assets listed in the audit scope.

**Create a mitigation plan**

- A mitigation plan is a strategy established to lower the level of risk and potential costs, penalties, or other issues that can negatively affect the organization’s security posture.

**Communicate results to stakeholders**

- The end result of this process is providing a detailed report of findings, suggested improvements needed to lower the organization's level of risk, and compliance regulations and standards the organization needs to adhere to.

# MODULE 3

## Logs & SIEM Tools

→ **Log -** A record of events that occur within an organization’s system and networks. Security analysts access a variety of logs from different sources. Three common log sources include **firewall logs, network logs**, and **server logs.**

**Firewall log -** A firewall log is a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.

**Network log-** A network log is a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.

**Server Log -** a server log is a record of events related to services such as websites, emails, or file shares. It includes actions such as login, password, and username requests.

→**SIEM Tools -** A security information and event management, or SIEM, tool is an application that collects and analyzes log data to monitor critical activities in an organization. It provides real-time visibility, event monitoring and analysis, and automated alerts. It also stores all log data in a centralized location.

**SIEM tools can also be used to create dashboards -** You might have encountered dashboards in an app on your phone or other device. They present information about your account or location in a format that's easy to understand.

For example, weather apps display data like temperature, precipitation, wind speed, and the forecast using charts, graphs, and other visual elements. This format makes it easy to quickly identify weather patterns and trends, so you can stay prepared and plan your day accordingly.

Just like weather apps help people make quick and informed decisions based on data, SIEM dashboards help security analysts quickly and easily access their organization's security information as charts, graphs, or tables.

For example, a security analyst receives an alert about a suspicious login attempt. The analyst accesses their SIEM dashboard to gather information about this alert. Using the dashboard, the analyst discovers that there have been 500 login attempts for Ymara's account in the span of five-minutes. They also discover that the login attempts happened from geographic locations outside of Ymara's usual location and outside of her usual working hours. By using a dashboard, the security analyst was able to quickly review visual representations of the timeline of the login attempts, the location, and the exact time of the activity, then determine that the activity was suspicious.

In addition to providing a comprehensive summary of security-related data, SIEM dashboards also provide stakeholders with different metrics. Metrics are key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application.

SIEM dashboards can be customized to display specific metrics or other data that are relevant to different members in an organization. For example, a security analyst may create a dashboard that displays metrics for monitoring everyday business operations, like the volume of incoming and outgoing network traffic.

# The future of SIEM tools

Previously, you were introduced to security information and event management (SIEM) tools, along with a few examples of SIEM tools. In this reading, you will learn more about how SIEM tools are used to protect organizational operations. You will also gain insight into how and why SIEM tools are changing to help protect organizations and the people they serve from evolving threat actor tactics and techniques.

## Current SIEM solutions

A **SIEM** tool is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools offer real-time monitoring and tracking of security event logs. The data is then used to conduct a thorough analysis of any potential security threat, risk, or vulnerability identified. SIEM tools have many dashboard options. Each dashboard option helps cybersecurity team members manage and monitor organizational data. However, currently, SIEM tools require human interaction for analysis of security events.

## The future of SIEM tools

As cybersecurity continues to evolve, the need for cloud functionality has increased. SIEM tools have and continue to evolve to function in cloud-hosted and cloud-native environments. Cloud-hosted SIEM tools are operated by vendors who are responsible for maintaining and managing the infrastructure required to use the tools. Cloud-hosted tools are simply accessed through the internet and are an ideal solution for organizations that don’t want to invest in creating and maintaining their own infrastructure.

Similar to cloud-hosted SIEM tools, cloud-native SIEM tools are also fully maintained and managed by vendors and accessed through the internet. However, cloud-native tools are designed to take full advantage of cloud computing capabilities, such as availability, flexibility, and scalability.

Yet, the evolution of SIEM tools is expected to continue in order to accommodate the changing nature of technology, as well as new threat actor tactics and techniques. For example, consider the current development of interconnected devices with access to the internet, known as the Internet of Things (IoT). The more interconnected devices there are, the larger the cybersecurity attack surface and the amount of data that threat actors can exploit. The diversity of attacks and data that require special attention is expected to grow significantly. Additionally, as artificial intelligence (AI) and machine learning (ML) technology continues to progress, SIEM capabilities will be enhanced to better identify threat-related terminology, dashboard visualization, and data storage functionality.

The implementation of automation will also help security teams respond faster to possible incidents, performing many actions without waiting for a human response.

**Security orchestration, automation, and response (SOAR)** is a collection of applications, tools, and workflows that uses automation to respond to security events. Essentially, this means that handling common security-related incidents with the use of SIEM tools is expected to become a more streamlined process requiring less manual intervention. This frees up security analysts to handle more complex and uncommon incidents that, consequently, can’t be automated with a SOAR. Nevertheless, the expectation is for cybersecurity-related platforms to communicate and interact with one another. Although the technology allowing interconnected systems and devices to communicate with each other exists, it is still a work in progress.

## Different types of SIEM Tools -

- **Self - Hosted SIEM tools -** Self-hosted SIEM tools require organizations to install, operate, and maintain the tool using their own physical infrastructure, such as server capacity. These applications are then managed and maintained by the organization's IT department, rather than a third party vendor. Self-hosted SIEM tools are ideal when an organization is required to maintain physical control over confidential data.
- **Cloud - Hosted SIEM tools -** Alternatively, cloud-hosted SIEM tools are maintained and managed by the SIEM providers, making them accessible through the internet. Cloud-hosted SIEM tools are ideal for organizations that don't want to invest in creating and maintaining their own infrastructure.
- ***Hybrid -*** *An organization can choose to use a combination of both self-hosted and cloud-hosted SIEM tools, known as a hybrid solution. Organizations might choose a hybrid SIEM solution to leverage the benefits of the cloud while also maintaining physical control over confidential data.*

***Splunk Enterprise, Splunk Cloud, and Chronicle are common SIEM tools that many organizations use to help protect their data and systems.***

NOTE - **Splunk is a data analysis platform**

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

- **Splunk Cloud** - Splunk Cloud is a cloud-hosted tool used to collect, search, and monitor log data. Splunk Cloud is helpful for organizations running hybrid or cloud-only environments, where some or all of the organization's services are in the cloud.
- **Google’s - Chronicle** - Chronicle is a cloud-native tool designed to retain, analyze, and search data. Chronicle provides log monitoring, data analysis, and data collection. Like cloud-hosted tools, cloud-native tools are also fully maintained and managed by the vendor. But cloud-native tools are specifically designed to take full advantage of cloud computing capabilities such as availability, flexibility, and scalability.

Because threat actors are frequently improving their strategies to compromise the confidentiality, integrity, and availability of their targets, it's important for organizations to use a variety of security tools to help defend against attacks. The SIEM tools we just discussed are only a few examples of the tools available for security teams to use to help defend their organizations.

# Use SIEM tools to protect organizations

Previously, you were introduced to security information and event management (SIEM) tools and a few SIEM dashboards. You also learned about different threats, risks, and vulnerabilities an organization may experience. In this reading, you will learn more about SIEM dashboard data and how cybersecurity professionals use that data to identify a potential threat, risk, or vulnerability.

## Splunk

Splunk offers different SIEM tool options: Splunk® Enterprise and Splunk® Cloud. Both allow you to review an organization's data on dashboards. This helps security professionals manage an organization's internal infrastructure by collecting, searching, monitoring, and analyzing log data from multiple sources to obtain full visibility into an organization’s everyday operations.

Review the following Splunk dashboards and their purposes:

### Security posture dashboard

The security posture dashboard is designed for security operations centers (SOCs). It displays the last 24 hours of an organization’s notable security-related events and

trends and allows security professionals to determine if security infrastructure and policies are performing as designed. Security analysts can use this dashboard to monitor and investigate potential threats in real time, such as suspicious network activity originating from a specific IP address.

### Executive summary dashboard

The executive summary dashboard analyzes and monitors the overall health of the organization over time. This helps security teams improve security measures that reduce risk. Security analysts might use this dashboard to provide high-level insights to stakeholders, such as generating a summary of security incidents and trends over a specific period of time.

### Incident review dashboard

The incident review dashboard allows analysts to identify suspicious patterns that can occur in the event of an incident. It assists by highlighting higher risk items that need immediate review by an analyst. This dashboard can be very helpful because it provides a visual timeline of the events leading up to an incident.

### Risk analysis dashboard

The risk analysis dashboard helps analysts identify risk for each risk object (e.g., a specific user, a computer, or an IP address). It shows changes in risk-related activity or behavior, such as a user logging in outside of normal working hours or unusually high network traffic from a specific computer. A security analyst might use this dashboard to analyze the potential impact of vulnerabilities in critical assets, which helps analysts prioritize their risk mitigation efforts.

## Chronicle

Chronicle is a cloud-native SIEM tool from Google that retains, analyzes, and searches log data to identify potential security threats, risks, and vulnerabilities. Chronicle allows you to collect and analyze log data according to:

- A specific asset
- A domain name
- A user

- An IP address

Chronicle provides multiple dashboards that help analysts monitor an organization’s logs, create filters and alerts, and track suspicious domain names.

Review the following Chronicle dashboards and their purposes:

## Enterprise insights dashboard

The enterprise insights dashboard highlights recent alerts. It identifies suspicious domain names in logs, known as indicators of compromise (IOCs). Each result is labeled with a confidence score to indicate the likelihood of a threat. It also provides a severity level that indicates the significance of each threat to the organization. A security analyst might use this dashboard to monitor login or data access attempts related to a critical asset—like an application or system—from unusual locations or devices.

## Data ingestion and health dashboard

The data ingestion and health dashboard shows the number of event logs, log sources, and success rates of data being processed into Chronicle. A security analyst might use this dashboard to ensure that log sources are correctly configured and that logs are received without error. This helps ensure that log related issues are addressed so that the security team has access to the log data they need.

## IOC matches dashboard

The IOC matches dashboard indicates the top threats, risks, and vulnerabilities to the organization. Security professionals use this dashboard to observe domain names, IP addresses, and device IOCs over time in order to identify trends. This information is then used to direct the security team’s focus to the highest priority threats. For example, security analysts can use this dashboard to search for additional activity associated with an alert, such as a suspicious user login from an unusual geographic location.

## Main dashboard

The main dashboard displays a high-level summary of information related to the organization’s data ingestion, alerting, and event activity over time. Security professionals can use this dashboard to access a timeline of security events—such as a spike in failed login attempts— to identify threat trends across log sources, devices, IP addresses, and physical locations.

### Rule detections dashboard

The rule detections dashboard provides statistics related to incidents with the highest occurrences, severities, and detections over time. Security analysts can use this dashboard to access a list of all the alerts triggered by a specific detection rule, such as a rule designed to alert whenever a user opens a known malicious attachment from an email. Analysts then use those statistics to help manage recurring incidents and establish mitigation tactics to reduce an organization's level of risk.

### User sign in overview dashboard

The user sign in overview dashboard provides information about user access behavior across the organization. Security analysts can use this dashboard to access a list of all user sign-in events to identify unusual user activity, such as a user signing in from multiple locations at the same time. This information is then used to help mitigate threats, risks, and vulnerabilities to user accounts and the organization’s applications.

# More about cybersecurity tools

Previously, we learned about several tools that are used by cybersecurity team members to monitor for and identify potential security threats, risks, and vulnerabilities. In this reading, we’ll learn more about common open-source and proprietary cybersecurity tools that you may use as a cybersecurity professional.

## Open-source tools

Open-source tools are often free to use and can be user friendly. The objective of open-source tools is to provide users with software that is built by the public in a collaborative way, which can result in the software being more secure. Additionally, open-source tools allow for more customization by users, resulting in a variety of new services built from the same open-source software package.

Software engineers create open-source projects to improve software and make it available for anyone to use, as long as the specified license is respected. The source code for open-source projects is readily available to users, as well as the training

material that accompanies them. Having these sources readily available allows users to modify and improve project materials.

## Proprietary tools

Proprietary tools are developed and owned by a person or company, and users typically pay a fee for usage and training. The owners of proprietary tools are the only ones who can access and modify the source code. This means that users generally need to wait for updates to be made to the software, and at times they might need to pay a fee for those updates. Proprietary software generally allows users to modify a limited number of features to meet individual and organizational needs. Examples of proprietary tools include Splunk® and Chronicle SIEM tools.

### Common misconceptions

There is a common misconception that open-source tools are less effective and not as safe to use as proprietary tools. However, developers have been creating open-source materials for years that have become industry standards. Although it is true that threat actors have attempted to manipulate open-source tools, because these tools are open source it is actually harder for people with malicious intent to successfully cause harm. The wide exposure and immediate access to the source code by well-intentioned and informed users and professionals makes it less likely for issues to occur, because they can fix issues as soon as they’re identified.

## Examples of open-source tools

In security, there are many tools in use that are open-source and commonly available. Two examples are Linux and Suricata.

### Linux

Linux is an open-source operating system that is widely used. It allows you to tailor the operating system to your needs using a command-line interface. An **operating system** is the interface between computer hardware and the user. It’s used to communicate with the hardware of a computer and manage software applications.

There are multiple versions of Linux that exist to accomplish specific tasks. Linux and its command-line interface will be discussed in detail, later in the certificate program.

### Suricata

Suricata is an open-source network analysis and threat detection software.  Network analysis and threat detection software is used to inspect network traffic to identify suspicious behavior and generate network data logs. The detection software finds activity across users, computers, or Internet Protocol (IP) addresses to help uncover potential threats, risks, or vulnerabilities.

Suricata was developed by the Open Information Security Foundation (OISF). OISF is dedicated to maintaining open-source use of the Suricata project to ensure it’s free and publicly available. Suricata is widely used in the public and private sector, and it integrates with many SIEM tools and other security tools. Suricata will also be discussed in greater detail later in the program.

# MODULE 4

## Phases of an incident response playbook

**Playbook -** A playbook is a manual that provides details about any operational action. Playbooks also clarify what tools should be used in response to a security incident. In the security field, playbooks are essential.

Urgency, efficiency, and accuracy are necessary to quickly identify and mitigate a security threat to reduce potential risk. Playbooks ensure that people follow a consistent list of actions in a prescribed way, regardless of who is working on the case.

Different types of playbooks that are used are - These include playbooks for **incident response, security alerts, teams-specific**, and **product-specific** purposes.

Here, we'll focus on a playbook that's commonly used in cybersecurity, called an incident response playbook. Incident response is an organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach. An incident response playbook is a guide with six phases used to help mitigate and manage security incidents from beginning to end.

1. **Preparation -** *The first phase is preparation. Organizations must prepare to mitigate the likelihood, risk, and impact of a security incident by documenting procedures, establishing staffing plans, and educating users. Preparation sets the foundation for successful incident response. For example, organizations can create incident response plans and procedures that outline the roles and responsibilities of each security team member.*
2. **Detection & Analysis -** *The second phase is detection and analysis. The objective of this phase is to detect and analyze events using defined processes and technology. Using appropriate tools and strategies during this phase helps security analysts determine whether a breach has occurred and analyze its possible magnitude.*
3. **Containment -** *The third phase is containment. The goal of containment is to prevent further damage and reduce the immediate impact of a security incident. During this phase, security professionals take actions to contain an incident and minimize damage. Containment is a high priority for organizations because it helps prevent ongoing risks to critical assets and data.*
4. **Eradication & Recovery -** *The fourth phase in an incident response playbook is eradication and recovery. This phase involves the complete removal of an incident's artifacts so that an organization can return to normal operations. During this phase, security professionals eliminate artifacts of the incident by removing malicious code and mitigating vulnerabilities. Once they've exercised due diligence, they can begin to restore the affected environment to a secure state. This is also known as IT restoration.*
5. **Post - Incident Activity -** *The fifth phase is post-incident activity. This phase includes documenting the incident, informing organizational leadership, and applying lessons learned to ensure that an organization is better prepared to handle future incidents. Depending on the severity of the incident, organizations can conduct a full-scale incident analysis to determine the root cause of the incident and implement various updates or improvements to enhance its overall security posture.*
6. **Coordination** - *The sixth and final phase in an incident response playbook is coordination. Coordination involves reporting incidents and sharing information, throughout the incident response process, based on the organization's established standards. Coordination is important for many reasons. It ensures that organizations*

*meet compliance requirements and it allows for coordinated response and resolution.*

There are many ways security professionals may be alerted to an incident. You recently learned about SIEM tools and how they collect and analyze data. They use this data to detect threats and generate alerts, which can inform the security team of a potential incident. Then, when a security analyst receives a SIEM alert, they can use the appropriate playbook to guide the response process. SIEM tools and playbooks work together to provide a structured and efficient way of responding to potential security incidents.

## Some Resources for more information

Incident and vulnerability response playbooks are only two examples of the many playbooks that an organization uses. If you plan to work as a cybersecurity professional outside of the U.S., you may want to explore the following resources:

- United Kingdom, National Cyber Security Center (NCSC) - Incident Management
- Australian Government - Cyber Incident Response Plan
- Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) - Vulnerability Handling and related guidelines
- Government of Canada - Ransomware Playbook
- Scottish Government - Playbook Templates

# Playbooks, SIEM tools, and SOAR tools

Previously, you learned that security teams encounter threats, risks, vulnerabilities, and incidents on a regular basis and that they follow playbooks to address security-related issues. In this reading, you will learn more about playbooks, including how they are used in security information and event management (SIEM) and security orchestration, automation, and response (SOAR).

## Playbooks and SIEM tools

Playbooks are used by cybersecurity teams in the event of an incident. Playbooks help security teams respond to incidents by ensuring that a consistent list of actions are

followed in a prescribed way, regardless of who is working on the case. Playbooks can be very detailed and may include flow charts and tables to clarify what actions to take and in which order. Playbooks are also used for recovery procedures in the event of a ransomware attack. Different types of security incidents have their own playbooks that detail who should take what action and when.

Playbooks are generally used alongside SIEM tools. If, for example, unusual user behavior is flagged by a SIEM tool, a playbook provides analysts with instructions about how to address the issue.

## Playbooks and SOAR tools

Playbooks are also used with SOAR tools. SOAR tools are similar to SIEM tools in that they are used for threat monitoring. SOAR is a piece of software used to automate repetitive tasks generated by tools such as a SIEM or managed detection and response (MDR). For example, if a user attempts to log into their computer too many times with the wrong password, a SOAR would automatically block their account to stop a possible intrusion. Then, analysts would refer to a playbook to take steps to resolve the issue.