Google Career Certificates

Cybersecurity

Course Readings:
Course 2

Table of Contents

Google

Course 2- module 1

Hello, and welcome to Play It Safe: Manage Security Risks, the second course in the Google Cybersecurity Certificate. You're on an exciting journey!

By the end of this course, you will develop a greater understanding of the eight Certified Information Systems Security Professional (CISSP) security domains, as well as specific security frameworks and controls. You'll also be introduced to how to use security tools and audits to help protect assets and data. These are key concepts in the cybersecurity field, and understanding them will help you keep organizations, and the people they serve, safe from threats, risks, and vulnerabilities.

Certificate program progress

The Google Cybersecurity Certificate program has eight courses. **Play It Safe: Manage Security Risks** is the second course.
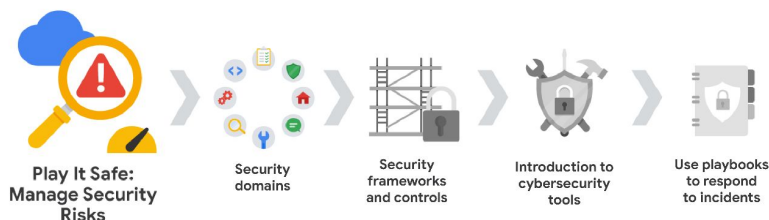

Foundations of Cybersecurity | Play It Safe: Manage Security Risks | Connect and Protect: Networks and Network Security | Tools of the Trade: Linux and SQL | Assets, Threats, and Vulnerabilities | Sound the Alarm: Detection and Response | Automate Cybersecurity Tasks with Python | Put It to Work: Prepare for Cybersecurity Jobs

1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.
2. **Play It Safe: Manage Security Risks** — *(current course)* Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools.
3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks.
4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.
6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks.
8. **Put It to Work: Prepare for Cybersecurity Jobs** — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

Google

Course 2 content

Each course of this certificate program is broken into weeks. You can complete courses at your own pace, but the weekly breakdowns are designed to help you finish the entire Google Cybersecurity Certificate in about six months.
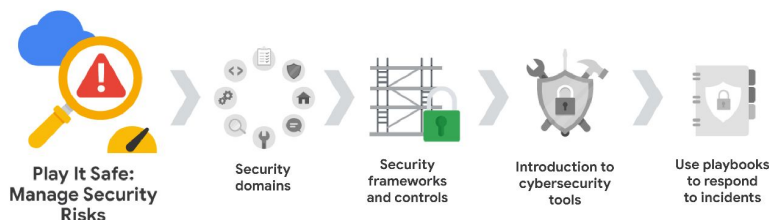
What's to come? Here's a quick overview of the skills you'll learn in each week of this course.

Week 1: Security Domains

Play It Safe: Manage Security Risks · Security domains · Security frameworks and controls · Introduction to cybersecurity tools · Use playbooks to respond to incidents
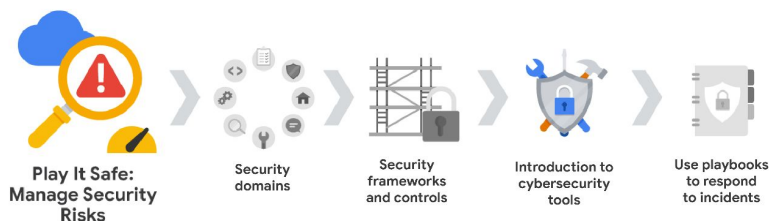
You will gain understanding of the CISSP's eight security domains. Then, you'll learn about primary threats, risks, and vulnerabilities to business operations. In addition, you'll explore the National Institute of Standards and Technology's (NIST) Risk Management Framework and the steps of risk management.

Week 2: Security frameworks and controls

Play It Safe: Manage Security Risks · Security domains · Security frameworks and controls · Introduction to cybersecurity tools · Use playbooks to respond to incidents

You will focus on security frameworks and controls, along with the core components of the confidentiality, integrity, and availability (CIA) triad. You'll learn about Open Web Application Security Project (OWASP) security principles and security audits.

Week 3: Introduction to cybersecurity tools

Play It Safe: Manage Security Risks · Security domains · Security frameworks and controls · Introduction to cybersecurity tools · Use playbooks to respond to incidents

You will explore industry leading security information and event management (SIEM) tools that are used by security professionals to protect business operations. You'll learn how entry-level security analysts use SIEM dashboards as part of their every day work.

Google

Week 4: Use playbooks to respond to incidents
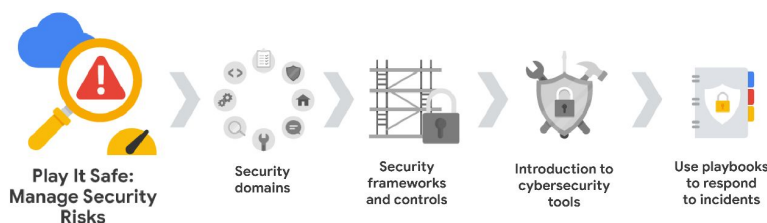
You'll learn about the purposes and common uses of playbooks. You'll also explore how cybersecurity professionals use playbooks to respond to identified threats, risks, and vulnerabilities.

What to expect

Each course offers many types of learning opportunities:

- **Videos** led by Google instructors teach new concepts, introduce the use of relevant tools, offer career support, and provide inspirational personal stories.
- **Readings** build on the topics discussed in the videos, introduce related concepts, share useful resources, and describe case studies.
- **Discussion prompts** explore course topics for better understanding and allow you to chat and exchange ideas with other learners in the discussion forums.
- **Self-review activities** and **labs** give you hands-on practice in applying the skills you are learning and allow you to assess your own work by comparing it to a completed example.
- **Interactive plug-ins** encourage you to practice specific tasks and help you integrate knowledge you have gained in the course.
- **In-video quizzes** help you check your comprehension as you progress through each video.
- **Practice quizzes** allow you to check your understanding of key concepts and provide valuable feedback.
- **Graded quizzes** demonstrate your understanding of the main concepts of a course. You must score 80% or higher on each graded quiz to obtain a certificate, and you can take a graded quiz multiple times to achieve a passing score.

Tips for success

- It is strongly recommended that you go through the items in each lesson in the order they appear because new information and concepts build on previous knowledge.
- Participate in all learning opportunities to gain as much knowledge and experience as possible.
- If something is confusing, don't hesitate to replay a video, review a reading, or repeat a self-review activity.
- Use the additional resources that are referenced in this course. They are designed to support your learning. You can find all of these resources in the **Resources** tab.
- When you encounter useful links in this course, bookmark them so you can refer to the information later for study or review.
- Understand and follow the Coursera Code of Conduct to ensure that the learning community remains a welcoming, friendly, and supportive place for all members.

Helpful resources and tips

As a learner, you can choose to complete one or multiple courses in this program. However, to obtain the Google Cybersecurity Certificate, you must complete all the courses. This reading describes what is required to obtain a certificate and best practices for you to have a good learning experience on Coursera.

Course completion to obtain a certificate

To submit graded assignments and be eligible to receive a Google Cybersecurity Certificate, you must:

- Pay the course certificate fee or apply and be approved for a Coursera scholarship.
- Pass all graded quizzes in the eight courses with a score of at least 80%. Each graded quiz in a course is part of a cumulative grade for that course.

Healthy habits for course completion

Here is a list of best practices that will help you complete the courses in the program in a timely manner:
- **Plan your time:** Setting regular study times and following them each week can help you make learning a part of your routine. Use a calendar or timetable to create a schedule, and list what you plan to do each day in order to set achievable goals. Find a space that allows you to focus when you watch the videos, review the readings, and complete the activities.
- **Work at your own pace:** Everyone learns differently, so this program has been designed to let you work at your own pace. Although your personalized deadlines start when you enroll, feel free to move through the program at the speed that works best for you. There is no penalty for late assignments; to earn your certificate, all you have to do is complete all of the work. You can extend your deadlines at any time by going to **Overview** in the navigation panel and selecting **Switch Sessions**. If you have already missed previous deadlines, select **Reset my deadlines** instead.
- **Be curious:** If you find an idea that gets you excited, act on it! Ask questions, search for more details online, explore the links that interest you, and take notes on your discoveries. The steps you take to support your learning along the way will advance your knowledge, create more opportunities in this high-growth field, and help you qualify for jobs.
- **Take notes:** Notes will help you remember important information in the future, especially as you're preparing to enter a new job field. In addition, taking notes is an effective way to make connections between topics and gain a better understanding of those topics.
- **Review exemplars:** Exemplars are completed assignments that fully meet an activity's criteria. Many activities in this program have exemplars for you to validate your work or check for errors. Although there are often many ways to complete an assignment, exemplars offer guidance and inspiration about how to complete the activity.
- **Chat (responsibly) with other learners:** If you have a question, chances are, you're not alone. Use the discussion forums to ask for help from other learners taking this program. You can also visit Coursera's Global Online Community. Other important things to know while learning with others can be found in the Coursera Honor Code and Code of Conduct.
- **Update your profile:** Consider updating your profile on Coursera with your photo, career goals, and more. When other learners find you in the discussion forums, they can click on your name to access your profile and get to know you better.

Google

Documents, spreadsheets, presentations, and labs for course activities

To complete certain activities in the program, you will need to use digital documents, spreadsheets, presentations, and/or labs. Security professionals use these software tools to collaborate within their teams and organizations. If you need more information about using a particular tool, refer to these resources:

- Microsoft Word: Help and learning: Microsoft Support page for Word
- Google Docs: Help Center page for Google Docs
- Microsoft Excel: Help and learning: Microsoft Support page for Excel
- Google Sheets: Help Center page for Google Sheets
- Microsoft PowerPoint: Help and learning: Microsoft Support page for PowerPoint
- How to use Google Slides: Help Center page for Google Slides
- Common problems with labs: Troubleshooting help for Qwiklabs activities

Weekly, course, and certificate glossaries

This program covers a lot of terms and concepts, some of which you may already know and some of which may be unfamiliar to you. To review terms and help you prepare for graded quizzes, refer to the following glossaries:

- **Weekly glossaries**: At the end of each week's content, you can review a glossary of terms from that week. Each week's glossary builds upon the terms from the previous weeks in that course. The weekly glossaries are not downloadable; however, all of the terms and definitions are included in the course and certificate glossaries, which are downloadable.
- **Course glossaries**: At the end of each course, you can access and download a glossary that covers all of the terms in that course.
- **Certificate glossary**: The certificate glossary includes all of the terms in the entire certificate program and is a helpful resource that you can reference throughout the program or at any time in the future.

You can access and download the certificate glossaries and save them on your computer. You can always find the course and certificate glossaries through the course's Resources section. To access the **Cybersecurity Certificate glossary**, click the link below and select *Use Template*.

- Cybersecurity Certificate glossary OR
- If you don't have a Google account, you can download the glossary directly from the attachment here.

Course feedback

Providing feedback on videos, readings, and other materials is easy. With the resource open in your browser, you can find the thumbs-up and thumbs-down symbols.

- Click **thumbs-up** for materials you find helpful.
- Click **thumbs-down** for materials that you do not find helpful.

If you want to flag a specific issue with an item, click the flag icon, select a category, and enter an explanation in the text box. This feedback goes back to the course development team and isn't visible to other learners. All feedback received helps to create even better certificate programs in the future.

For technical help, visit the Learner Help Center.

Google

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.
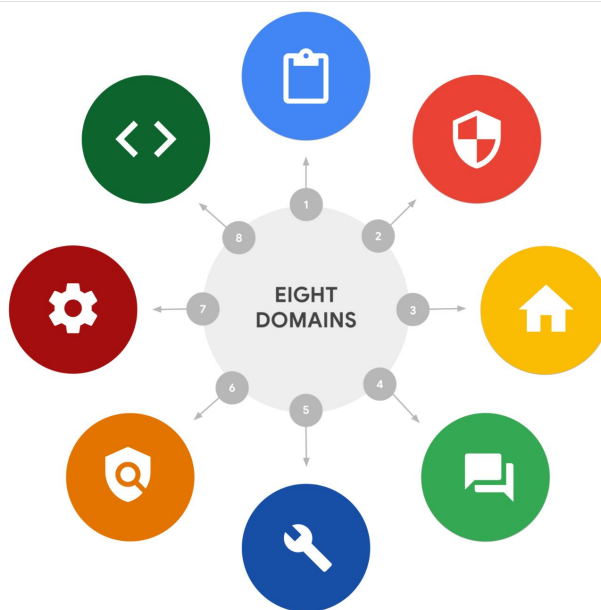
Domain one: Security and risk management

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.

Key takeaways

In this reading, you learned more about the focus areas of the eight CISSP security domains. In addition, you learned about InfoSec and the principle of least privilege. Being familiar with these security domains and related concepts will help you gain insight into the field of cybersecurity.

Google

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.

.

Google

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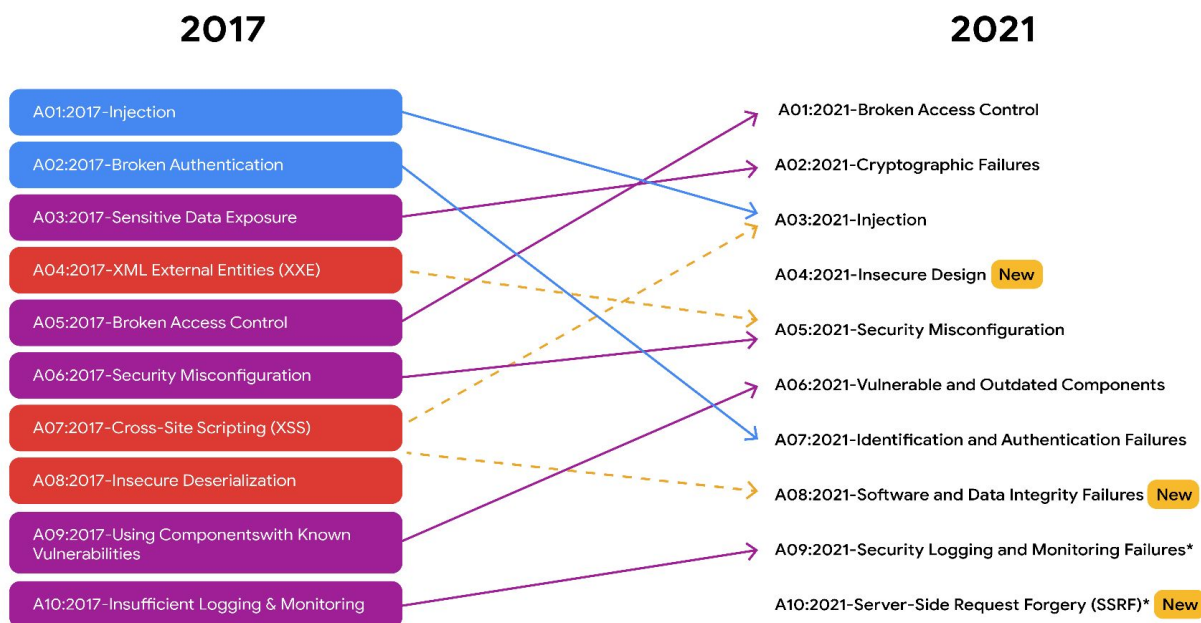
There are different factors that can affect the likelihood of a risk to an organization's assets, including:

- **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.

Google

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.

2017   2021

A01:2017-Injection   A01:2021-Broken Access Control

A02:2017-Broken Authentication   A02:2021-Cryptographic Failures

A03:2017-Sensitive Data Exposure   A03:2021-Injection

A04:2017-XML External Entities (XXE) A04:2021-Insecure Design [New]

A05:2017-Broken Access Control   A05:2021-Security Misconfiguration

A06:2017-Security Misconfiguration   A06:2021-Vulnerable and Outdated Components

A07:2017-Cross-Site Scripting (XSS)   A07:2021-Identification and Authentication Failures

A08:2017-Insecure Deserialization   A08:2021-Software and Data Integrity Failures [New]

A09:2017-Using Componentswith Known Vulnerabilities   A09:2021-Security Logging and Monitoring Failures*

A10:2017-Insufficient Logging & Monitoring   A10:2021-Server-Side Request Forgery (SSRF)* [New]

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.

Key takeaways

In this reading, you learned about some risk management strategies and frameworks that can be used to develop organization-wide policies and processes to mitigate threats, risks, and vulnerabilities. You also learned about some of today's most common threats, risks, and vulnerabilities to business operations. Understanding these concepts can better prepare you to not only protect against, but also mitigate, the types of security-related issues that can harm organizations and people alike.

Resources for more information

To learn more, click the linked terms in this reading. Also, consider exploring the following sites:
- OWASP Top Ten
- NIST RMF

Google

Course 2 - 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

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.

Key takeaways

Cybersecurity frameworks and controls are used together to establish an organization's security posture. They also support an organization's ability to meet security goals and comply with laws and regulations. Although these frameworks and controls are typically voluntary, organizations are strongly encouraged to implement and use them to help ensure the safety of critical assets.

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.

Key takeaways

The CIA triad is essential for establishing an organization's security posture. Knowing what it is and how it's applied can help you better understand how security teams work to protect organizations and the people they serve.

Google

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.

Key takeaways

Cybersecurity professionals are constantly applying security principles to safeguard organizations and the people they serve. As an entry-level security analyst, you can use these security principles to promote safe development practices that reduce risks to companies and users alike.

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.

Google

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

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.

Key takeaways

In this reading you learned more about security audits, including what they are; why they're conducted; and the role of frameworks, controls, and compliance in audits.

Although there is much more to learn about security audits, this introduction is meant to support your ability to complete an audit of your own for a self-reflection portfolio activity later in this course.

Resources for more information

Resources that you can explore to further develop your understanding of audits in the cybersecurity space are:

- [Assessment and Auditing Resources](#)
- [IT Disaster Recovery Plan](#)

Google

Course 2 - module 3

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.

Key takeaways

SIEM tools play a major role in monitoring an organization's data. As an entry-level security analyst, you might monitor SIEM dashboards as part of your daily tasks. Regularly researching new developments in SIEM technology will help you grow and adapt to the changes in the cybersecurity field. Cloud computing, SIEM-application integration, and automation are only some of the advancements security professionals can expect in the future evolution of SIEM tools.

Google

More about cybersecurity tools

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.

Key takeaways

Open-source tools are widely used in the cybersecurity profession. Throughout the certificate program, you will have multiple opportunities to learn about and explore both open-source and proprietary tools in more depth.

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.

Key takeaways

What is most important to know is that playbooks, also sometimes referred to as runbooks, provide detailed actions for security teams to take in the event of an incident. Knowing exactly who needs to do what and when can help reduce the impact of an incident and reduce the risk of damage to an organization's critical assets.

Google

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.

28

Google

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.

Key takeaways

SIEM tools provide dashboards that help security professionals organize and focus their security efforts. This is important because it allows analysts to reduce risk by identifying, analyzing, and remediating the highest priority items in a timely manner. Later in the program, you'll have an opportunity to practice using various SIEM tool features and commands for search queries.

Google

More about playbooks

Previously, you learned that playbooks are tools used by cybersecurity professionals to identify and respond to security issues. In this reading, you'll learn more about playbooks and their purpose in the field of cybersecurity.

Playbook overview

A **playbook** is a manual that provides details about any operational action. Essentially, a playbook provides a predefined and up-to-date list of steps to perform when responding to an incident.
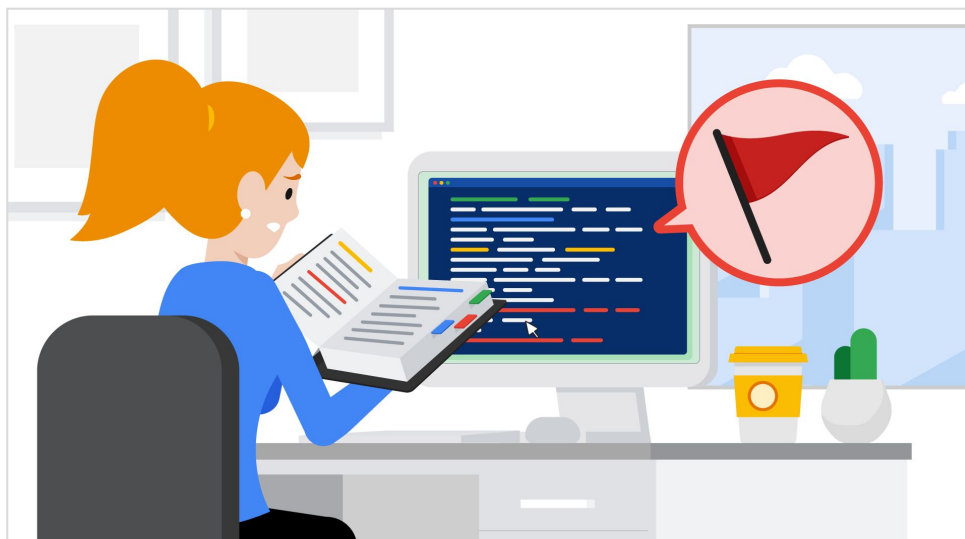
Playbooks are accompanied by a strategy. The strategy outlines expectations of team members who are assigned a task, and some playbooks also list the individuals responsible. The outlined expectations are accompanied by a plan. The plan dictates how the specific task outlined in the playbook must be completed.

Playbooks should be treated as living documents, which means that they are frequently updated by security team members to address industry changes and new threats. Playbooks are generally managed as a collaborative effort, since security team members have different levels of expertise.

Updates are often made if:
- A failure is identified, such as an oversight in the outlined policies and procedures, or in the playbook itself.
- There is a change in industry standards, such as changes in laws or regulatory compliance.
- The cybersecurity landscape changes due to evolving threat actor tactics and techniques.

Google

Types of playbooks

Playbooks sometimes cover specific incidents and vulnerabilities. These might include ransomware, vishing, business email compromise (BEC), and other attacks previously discussed. Incident and vulnerability response playbooks are very common, but they are not the only types of playbooks organizations develop.

Each organization has a different set of playbook tools, methodologies, protocols, and procedures that they adhere to, and different individuals are involved at each step of the response process, depending on the country they are in. For example, incident notification requirements from government-imposed laws and regulations, along with compliance standards, affect the content in the playbooks. These requirements are subject to change based on where the incident originated and the type of data affected.

Incident and vulnerability response playbooks

Incident and vulnerability response playbooks are commonly used by entry-level cybersecurity professionals. They are developed based on the goals outlined in an organization's business continuity plan. A business continuity plan is an established path forward allowing a business to recover and continue to operate as normal, despite a disruption like a security breach.

These two types of playbooks are similar in that they both contain predefined and up-to-date lists of steps to perform when responding to an incident. Following these steps is necessary to ensure that you, as a security professional, are adhering to legal and organizational standards and protocols. These playbooks also help minimize errors and ensure that important actions are performed within a specific timeframe.

When an incident, threat, or vulnerability occurs or is identified, the level of risk to the organization depends on the potential damage to its assets. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. For this reason, a sense of urgency is essential. Following the steps outlined in playbooks is also important if any forensic task is being carried out. Mishandling data can easily compromise forensic data, rendering it unusable.

Common steps included in incident and vulnerability playbooks include:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery from an incident

Additional steps include performing post-incident activities, and a coordination of efforts throughout the investigation and incident and vulnerability response stages.

Key takeaways

It is essential to refine processes and procedures outlined in a playbook. With every documented incident, cybersecurity teams need to consider what was learned from the incident and what improvements should be made to handle incidents more effectively in the future. Playbooks create structure and ensure compliance with the law.

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

Google

Get started on the next course

Congratulations on completing Course 2 of the Google Cybersecurity Certificate: **Play It Safe: Manage Security Risks**! In this part of the program, you learned about the focus of the eight Certified Information Systems Security Professional (CISSP) security domains. You also learned more about threats, risks, and vulnerabilities, as well as common security controls and frameworks. Additionally, you explored how to use the National Institute of Standards and Technology Risk Management Framework (NIST RMF), security information and event management (SIEM) technology, and playbooks to identify and help prevent security issues that can harm organizations and the people they serve.

The Google Cybersecurity Certificate has eight courses:

Foundations of Cybersecurity · Play It Safe: Manage Security Risks · Connect and Protect: Networks and Network Security · Tools of the Trade: Linux and SQL · Assets, Threats, and Vulnerabilities · Sound the Alarm: Detection and Response · Automate Cybersecurity Tasks with Python · Put It to Work: Prepare for Cybersecurity Jobs

1. **Foundations of Cybersecurity** — Explore the cybersecurity profession, including significant events that led to the development of the cybersecurity field and its continued importance to organizational operations. Learn about entry-level cybersecurity roles and responsibilities.
2. **Play It Safe: Manage Security Risks** — Identify how cybersecurity professionals use frameworks and controls to protect business operations, and explore common cybersecurity tools. *(This is the course you just completed. Well done!)*
3. **Connect and Protect: Networks and Network Security** — Gain an understanding of network-level vulnerabilities and how to secure networks.
4. **Tools of the Trade: Linux and SQL** — Explore foundational computing skills, including communicating with the Linux operating system through the command line and querying databases with SQL.
5. **Assets, Threats, and Vulnerabilities** — Learn about the importance of security controls and developing a threat actor mindset to protect and defend an organization's assets from various threats, risks, and vulnerabilities.
6. **Sound the Alarm: Detection and Response** — Understand the incident response lifecycle and practice using tools to detect and respond to cybersecurity incidents.
7. **Automate Cybersecurity Tasks with Python** — Explore the Python programming language and write code to automate cybersecurity tasks.
8. **Put It to Work: Prepare for Cybersecurity Jobs** — Learn about incident classification, escalation, and ways to communicate with stakeholders. This course closes out the program with tips on how to engage with the cybersecurity community and prepare for your job search.

Now that you have completed this course, you're ready to move on to the next course: **Connect and Protect: Networks and Network Security**.

Keep up the great work!