The eight CISSP security domains

- Introduction to the eight CISSP security domains, Part 1
- Introduction to the eight CISSP security domains, Part 2
- Determine the type of attack
- Understand attackers
- Wrap-up

Introduction to the eight CISSP security domains, Part 1

As the tactics of threat actors evolve, so do the roles of security professionals. Having a solid understanding of core security concepts will support your growth in this field. One way to better understand these core concepts is by organizing them into categories, called security domains.

As of 2022, CISSP has defined eight domains to organize the work of security professionals. It's important to understand that these domains are related and that gaps in one domain can result in negative consequences to an entire organization.

It's also important to understand the domains because it may help you better understand your career goals and your role within an organization. As you learn more about the elements of each domain, the work involved in one may appeal to you more than the others. This domain may become a career path for you to explore further.

CISSP defines eight domains in total, and we'll discuss all eight between this video and the next. In this video, we're going to cover the first four: security and risk management, asset security, security architecture and engineering, and communication and network security.

Let's start with the first domain, security and risk management. Security and risk management focuses on defining security goals and objectives, risk mitigation, compliance, business continuity, and the law. For example, security analysts may need to update company policies related to private health information if a change is made to a federal compliance regulation such as the Health Insurance Portability and Accountability Act, also known as HIPAA.

The second domain is asset security. This domain focuses on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data. When working with this domain, security analysts may be tasked with making sure that old equipment is properly disposed of and destroyed, including any type of confidential information.

The third domain is security architecture and engineering. This domain focuses on optimizing data security by ensuring effective tools, systems, and processes are in place. As a security analyst, you may be tasked with configuring a firewall. A firewall is a device used to monitor and filter incoming and outgoing computer network traffic. Setting up a firewall correctly helps prevent attacks that could affect productivity.

The fourth security domain is communication and network security. This domain focuses on managing and securing physical networks and wireless communications. As a security analyst, you may be asked to analyze user behavior within your organization.

Imagine discovering that users are connecting to unsecured wireless hotspots. This could leave the organization and its employees vulnerable to attacks. To ensure communications are secure, you would create a network policy to prevent and mitigate exposure.

Maintaining an organization's security is a team effort, and there are many moving parts. As an entry-level analyst, you will continue to develop your skills by learning how to mitigate risks to keep people and data safe.

You don't need to be an expert in all domains. But, having a basic understanding of them will aid you in your journey as a security professional.

You're doing great! We have just introduced the first four security domains, and in the next video, we'll discuss four more! See you soon!

Introduction to the eight CISSP security domains, Part 2

Welcome back. In the last video, we introduced you to the first four security domains. In this video, we'll introduce you to the next four security domains: identity and access management, security assessment and testing, security operations, and software development security.

Familiarizing yourself with these domains will allow you to navigate the complex world of security. The domains outline and organize how a team of security professionals work together. Depending on the organization, analyst roles may sit at the intersection of multiple domains or focus on one specific domain. Knowing where a particular role fits within the security landscape will help you prepare for job interviews and work as part of a full security team.

Let's move into the fifth domain: identity and access management. Identity and access management focuses on keeping data secure, by ensuring users follow established policies to control and manage physical assets, like office spaces, and logical assets, such as networks and applications. Validating the identities of employees and documenting access roles are essential to maintaining the organization's physical and digital security. For example, as a security analyst, you may be tasked with setting up employees' keycard access to buildings.

The sixth domain is security assessment and testing. This domain focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities. Security analysts may conduct regular audits of user permissions, to make sure that users have the correct level of access. For example, access to payroll information is often limited to certain employees, so analysts may be asked to regularly audit permissions to ensure that no unauthorized person can view employee salaries.

The seventh domain is security operations. This domain focuses on conducting investigations and implementing preventative measures. Imagine that you, as a security analyst, receive an alert that an unknown device has been connected to your internal network. You would need to follow the organization's policies and procedures to quickly stop the potential threat.

The final, eighth domain is software development security. This domain focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services. A security analyst may work with software development teams to ensure security practices are incorporated into the software development life-cycle. If, for example, one of

your partner teams is creating a new mobile app, then you may be asked to advise on the password policies or ensure that any user data is properly secured and managed.

That ends our introduction to CISSP's eight security domains. Challenge yourself to better understand each of these domains and how they affect the overall security of an organization. While they may still be a bit unclear to you this early in the program, these domains will be discussed in greater detail in the next course. See you there!

Determine the type of attack

Previously, you learned about the eight Certified Information Systems Security Professional (CISSP) security domains. The domains can help you better understand how a security analyst's job duties can be organized into categories. Additionally, the domains can help establish an understanding of how to manage risk. In this reading, you will learn about additional methods of attack. You'll also be able to recognize the types of risk these attacks present.

Attack types

Graphic of the eight icons that represent the CISSP security domains.

Password attack

A **password attack** is an attempt to access password-secured devices, systems, networks, or data. Some forms of password attacks that you'll learn about later in the certificate program are:

- Brute force
- Rainbow table

Password attacks fall under the communication and network security domain.

Social engineering attack

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Some forms of social engineering attacks that you will continue to learn about throughout the program are:

-

Phishing

- Smishing
- Vishing
- Spear phishing
- Whaling
- Social media phishing
- Business Email Compromise (BEC)
- Watering hole attack
- USB (Universal Serial Bus) baiting

- Physical social engineering

Social engineering attacks are related to the security and risk management domain.

Physical attack

A **physical attack** is a security incident that affects not only digital but also physical environments where the incident is deployed. Some forms of physical attacks are:

- Malicious USB cable
- Malicious flash drive
- Card cloning and skimming

Physical attacks fall under the asset security domain.

Adversarial artificial intelligence

Adversarial artificial intelligence is a technique that manipulates artificial intelligence and machine learning technology to conduct attacks more efficiently.

Adversarial artificial intelligence falls under both the communication and network security and the identity and access management domains.

Supply-chain attack

A **supply-chain attack** targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed. Because every item sold undergoes a process that

involves third parties, this means that the security breach can occur at any point in the supply chain. These attacks are costly because they can affect multiple organizations and the individuals who work for them. Supply-chain attacks fall under the security and risk management, security architecture and engineering, and security operations domains.

Cryptographic attack

A **cryptographic attack** affects secure forms of communication between a sender and intended recipient. Some forms of cryptographic attacks are:

- Birthday
- Collision
- Downgrade

Cryptographic attacks fall under the communication and network security domain.

Key takeaways

The eight CISSP security domains can help an organization and its security team fortify against and prepare for a data breach. Data breaches range from simple to complex and fall under one or more domains. Note that the methods of attack discussed are only a few of many. These and other types of attacks will be discussed throughout the certificate program.

Resources for more information

To view detailed information and definitions of terms covered in this reading, visit the National Institute of Standards and Technology (NIST) glossary.

Understand attackers

Previously, you were introduced to the concept of threat actors. As a reminder, a **threat actor** is any person or group who presents a security risk. In this reading, you'll learn about different types of threat actors. You will also learn about their motivations, intentions, and how they've influenced the security industry.

Threat actor types

Advanced persistent threats

Advanced persistent threats (APTs) have significant expertise accessing an organization's network without authorization. APTs tend to research their targets (e.g., large corporations or government entities) in advance and can remain undetected for an extended period of time. Their intentions and motivations can include:

- Damaging critical infrastructure, such as the power grid and natural resources
- Gaining access to intellectual property, such as trade secrets or patents

Insider threats

Insider threats abuse their authorized access to obtain data that may harm an organization. Their intentions and motivations can include:

- Sabotage
-

Corruption

- Espionage
- Unauthorized data access or leaks

Hacktivists

Hacktivists are threat actors that are driven by a political agenda. They abuse digital technology to accomplish their goals, which may include:

- Demonstrations
- Propaganda
- Social change campaigns
- Fame

Hacker types

Six hackers on computers.

A **hacker** is any person who uses computers to gain access to computer systems, networks, or data. They can be beginner or advanced technology professionals who use their skills for a variety of reasons. There are three main categories of hackers:

- Authorized hackers are also called ethical hackers. They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are motivated to safeguard people and organizations from malicious threat actors.

- Semi-authorized hackers are considered researchers. They search for vulnerabilities but don’t take advantage of the vulnerabilities they find.

- Unauthorized hackers are also called unethical hackers. They are malicious threat actors who do not follow or respect the law. Their goal is to collect and sell confidential data for financial gain.

Note: There are multiple hacker types that fall into one or more of these three categories.

New and unskilled threat actors have various goals, including:

- To learn and enhance their hacking skills

- To seek revenge

-

To exploit security weaknesses by using existing malware, programming scripts, and other tactics

Other types of hackers are not motivated by any particular agenda other than completing the job they were contracted to do. These types of hackers can be considered unethical or ethical hackers. They have been known to work on both illegal and legal tasks for pay.

There are also hackers who consider themselves vigilantes. Their main goal is to protect the world from unethical hackers.

Key takeaways

Threat actors and hackers are technically skilled individuals. Understanding their motivations and intentions will help you be better prepared to protect your organization and the people it serves from malicious attacks carried out by some of these individuals and groups.

Resources for more information

To learn more about how security teams work to keep organizations and people safe, explore the Hacking Google series of videos.

Wrap-up

This concludes our brief introduction to some of the most influential security attacks throughout history and CISSP's eight security domains. Let's review what we've discussed.

First, we covered viruses, including the Brain virus and the Morris worm, and discussed how these early forms of malware shaped the security industry. We also discussed how many attacks today are variants of these early examples. Understanding previous attacks is critical for security professionals who are working to protect organizations and people from possible future variants.

We also discussed social engineering and threat actor motives by learning about the LoveLetter attack and the Equifax data breach. These incidents showed the widespread impacts and associated costs of more recent security breaches in the digital age.

Finally, we introduced CISSP's eight security domains and how they can be used to categorize different areas of focus within the security profession.

I hope you're feeling confident about your foundational security knowledge! Learning the history of security can allow you to better understand the current industry. CISSP's eight security domains provide a way to organize the work of security professionals.

Remember, every security professional is essential. Your unique point of view, professional background, and knowledge are valuable. So, the diversity you bring to the field will further improve the security industry as you work to keep organizations and people safe.