

1. **Security and Risk Management** – Focuses on setting security goals, risk mitigation, compliance, and business continuity. Example: Updating policies to comply with HIPAA regulations.
2. **Asset Security** – Involves securing digital and physical assets, including **data storage, maintenance, and destruction**. Example: Ensuring old equipment is properly disposed of to prevent data leaks.
3. **Security Architecture and Engineering** – Optimizes data security by implementing tools and systems. Example: Configuring **firewalls** to filter network traffic and prevent cyberattacks.
4. **Communication and Network Security** – Manages and secures **physical and wireless networks**. Example: Enforcing policies to prevent employees from using **unsecured wireless hotspots** that could expose company data.
5. **Identity and Access Management** – Ensures users follow policies to protect **physical and digital assets** by managing identities and access controls. Example: Setting up **keycard access** for employees.
6. **Security Assessment and Testing** – Focuses on **security control testing, audits, and risk analysis** to detect vulnerabilities. Example: Conducting **user permission audits** to prevent unauthorized access to payroll data.
7. **Security Operations** – Involves **investigations and preventive security measures** to address threats. Example: Responding to alerts about **unknown devices** connecting to the internal network.
8. **Software Development Security** – Ensures **secure coding practices** are integrated into the **software development lifecycle**. Example: Advising developers on **password policies** and user data protection for a new mobile app.

**Different Types of Attacks:**

**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](https://www.nccoe.nist.gov/ai/adversarial-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 can fall under several domains, including but not limited to 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.

**Understanding 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**

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.