

Common cybersecurity terminology

As you've learned, cybersecurity (also known as security) is the practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation. In this reading, you'll be introduced to some key terms used in the cybersecurity profession. Then, you'll be provided with a resource that's useful for staying informed about changes to cybersecurity terminology.

Key cybersecurity terms and concepts

There are many terms and concepts that are important for security professionals to know. Being familiar with them can help you better identify the threats that can harm organizations and people alike. A security analyst or cybersecurity analyst focuses on monitoring networks for breaches. They also help develop strategies to secure an organization and research information technology (IT) security trends to remain alert and informed about potential threats. Additionally, an analyst works to prevent incidents. In order for analysts to effectively do these types of tasks, they need to develop knowledge of the following key concepts.

Compliance is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.

Security controls are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture.

Security posture is an organization's ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization.

A threat actor, or malicious attacker, is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data.

An **internal threat** can be a current or former employee, an external vendor, or a trusted partner who poses a security risk. At times, an internal threat is accidental. For example, an employee who accidentally clicks on a malicious email link would be considered an accidental threat. Other times, the internal threat actor *intentionally* engages in risky activities, such as unauthorized data access.

Network security is the practice of keeping an organization's network infrastructure secure from unauthorized access. This includes data, services, systems, and devices that are stored in an organization's network.

Cloud security is the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized users. The cloud is a network made up of a collection of servers or computers that store resources and data in remote physical locations known as data centers that can be accessed via the internet. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud.

Programming is a process that can be used to create a specific set of instructions for a computer to execute tasks. These tasks can include:

- Automation of repetitive tasks (e.g., searching a list of malicious domains)
- Reviewing web traffic
- Alerting suspicious activity

Key takeaways

Understanding key technical terms and concepts used in the security field will help prepare you for your role as a security analyst. Knowing these terms can help you identify common threats, risks, and vulnerabilities. To explore a variety of cybersecurity

terms, visit the [National Institute of Standards and Technology glossary](#). Or use your browser to search for high-quality, reliable cybersecurity glossaries from research institutes or governmental authorities. Glossaries are available in multiple languages.