The CIA triad: Confidentiality, integrity, and availability

- Explore the CIA triad
- Use the CIA triad to protect organizations

Explore the CIA triad

Great to see you again! While working as an entry-level security analyst, your main responsibility is to help protect your organization's sensitive assets and data from threat actors. The CIA triad is a core security model that will help you do that.

In this video, we'll explore the CIA triad and discuss the importance of each component for keeping an organization safe from threats, risks, and vulnerabilities. Let's get started!

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

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

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

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

Now that we've defined the CIA triad and its components, let's explore how you might use the CIA triad to protect an organization. If you work for an organization that has large amounts of private data like a bank, the principle of confidentiality is essential because the bank must keep people's personal and financial information safe.

The principle of integrity is also a priority. For example, if a person's spending habits or purchasing locations change dramatically, the bank will likely disable access to the account until they can verify that the account owner, not a threat actor, is actually the one making purchases.

The availability principle is also critical. Banks put a lot of effort into making sure that people can access their account information easily on the web. And to make sure that information is protected from threat actors, banks use a validation process to help minimize damage if they suspect that customer accounts have been compromised.

As an analyst, you'll regularly use each component of the triad to help protect your organization and the people it serves. And having the CIA triad constantly in mind, will help you keep sensitive

data and assets safe from a variety of threats, risks, and vulnerabilities including the social engineering attacks, malware, and data theft we discussed earlier.

Coming up, we'll explore specific frameworks and principles that will also help you protect your organization from threats, risks, and vulnerabilities. See you soon!

Use the CIA triad to protect organizations

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. It can be used to prevent access to data, such as messages on an organization's internal chat platform.

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.