Introduction to security frameworks and controls

Imagine you're working as a security analyst and receive multiple alerts about suspicious activity on the network. You realize that you'll need to implement additional security measures to keep these alerts from becoming serious incidents. But where do you start?

As an analyst, you'll start by identifying your organization's critical assets and risks. Then you'll implement the necessary frameworks and controls.

In this video, we'll discuss how security professionals use frameworks to continuously identify and manage risk. We'll also cover how to use security controls to manage or reduce specific risks.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. Security frameworks provide a structured approach to implementing a security lifecycle. The security lifecycle is a constantly evolving set of policies and standards that define how an organization manages risks, follows established guidelines, and meets regulatory compliance, or laws.

There are several security frameworks that may be used to manage different types of organizational and regulatory compliance risks. The purpose of security frameworks include protecting personally identifiable information, known as PII, securing financial information, identifying security weaknesses, managing organizational risks, and aligning security with business goals.

Frameworks have four core components and understanding them will allow you to better manage potential risks. The first core component is identifying and documenting security goals. For example, an organization may have a goal to align with the E.U.'s General Data Protection Regulation, also known as GDPR. GDPR is a data protection law established to grant European citizens more control over their personal data. A security analyst may be asked to identify and document areas where an organization is out of compliance with GDPR.

The second core component is setting guidelines to achieve security goals. For example, when implementing guidelines to achieve GDPR compliance, your organization may need to develop new policies for how to handle data requests from individual users.

The third core component of security frameworks is implementing strong security processes. In the case of GDPR, a security analyst working for a social media company may help design procedures to ensure the organization complies with verified user data requests. An example of this type of request is when a user attempts to update or delete their profile information.

The last core component of security frameworks is monitoring and communicating results. As an

example, you may monitor your organization's internal network and report a potential security issue affecting GDPR to your manager or regulatory compliance officer.

Now that we've introduced the four core components of security frameworks, let's tie them all together. Frameworks allow analysts to work alongside other members of the security team to document, implement, and use the policies and procedures that have been created. It's essential for an entry-level analyst to understand this process because it directly affects the work they do and how they collaborate with others. Next, we'll discuss security controls.

Security controls are safeguards designed to reduce specific security risks. For example, your company may have a guideline that requires all employees to complete a privacy training to reduce the risk of data breaches. As a security analyst, you may use a software tool to automatically assign and track which employees have completed this training.

Security frameworks and controls are vital to managing security for all types of organizations and ensuring that everyone is doing their part to maintain a low level of risk.

Understanding their purpose and how they are used allows analysts to support an organization's security goals and protect the people it serves.

In the following videos, we'll discuss some well-known frameworks and principles that analysts need to be aware of to minimize risk and protect data and users.

Revision #1
Created 2023-06-01 18:35:12 UTC by naruzkurai
Updated 2023-06-01 18:37:03 UTC by naruzkurai