NIST frameworks

Welcome back. Before we get started, let's quickly review the purpose of frameworks. Organizations use frameworks as a starting point to develop plans that mitigate risks, threats, and vulnerabilities to sensitive data and assets. Fortunately, there are organizations worldwide that create frameworks security professionals can use to develop those plans.

In this video, we'll discuss two of the National Institute of Standards and Technology, or NIST's frameworks that can support ongoing security efforts for all types of organizations, including for profit and nonprofit businesses, as well as government agencies. While NIST is a US based organization, the guidance it provides can help analysts all over the world understand how to implement essential cybersecurity practices. One NIST framework that we'll discuss throughout the program is the NIST Cybersecurity Framework, or CSF.

The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. This framework is widely respected and essential for maintaining security regardless of the organization you work for. The CSF consists of five important core functions, identify, protect, detect, respond, and recover, which we'll discuss in detail in a future video. For now, we'll focus on how the CSF benefits organizations and how it can be used to protect against threats, risks, and vulnerabilities by providing a workplace example.

Imagine that one morning you receive a high-risk notification that a workstation has been compromised. You identify the workstation, and discover that there's an unknown device plugged into it. You block the unknown device remotely to stop any potential threat and protect the organization. Then you remove the infected workstation to prevent the spread of the damage and use tools to detect any additional threat actor behavior and identify the unknown device. You respond by investigating the incident to determine who used the unknown device, how the threat occurred, what was affected, and where the attack originated.

In this case, you discover that an employee was charging their infected phone using a USB port on their work laptop. Finally, you do your best to recover any files or data that were affected and correct any damage the threat caused to the workstation itself.

As demonstrated by the previous example, the core functions of the NIST CSF provide specific guidance and direction for security professionals. This framework is used to develop plans to handle an incident appropriately and quickly to lower risk, protect an organization against a threat, and mitigate any potential vulnerabilities. The NIST CSF also expands into the protection of the United States federal government with NIST special publication, or SP 800-53. It provides a unified framework for protecting the security of information systems within the federal government, including the systems provided by private companies for federal government use.

The security controls provided by this framework are used to maintain the CIA triad for those systems used by the government. Isn't it amazing how all of these frameworks and controls work

together. We've discussed some really important security topics in this video that will be very useful for you as you continue your security journey. Because they're core elements of the security profession, the NIST CSF is a useful framework that most security professionals are familiar with, and having an understanding of the NIST, SP 800-53 is crucial if you have an interest in working for the US federal government. Coming up, we'll continue to explore the five NIST CSF functions and how organizations use them to protect assets and data.

Revision #1
Created 5 June 2023 23:59:01 by naruzkurai
Updated 5 June 2023 23:59:28 by naruzkurai