HACKER COMBAT
COMMUNITY

NIST Cybersecurity Framework: Overview

PREPARED BY

HACKER COMBAT LLC

www.hackercombat.com

Introduction

The National Institute of Standards and Framework for Cyber Security Framework (CSF) was released in February 2014 in response to the residential Executive Order 13636, which recommended a standard security framework for critical infrastructure.

The NIST CSF is recognized by many as a resource to enhance the security and management operations of public and private organizations.Although the NIST CSF is an excellent guideline, for changing organizational security and risk management from a reactive to a proactive approach can be a difficult part to research and implement.

If you are unable to adopt the NIST Cyber Framework, a brief overview and summary of this framework can help you speed up your transformation security.

Here is a brief summary of the NIST Cybersecurity Framework and detailed information:

The NIST CSF consists of four main areas. This includes features, categories, subcategories, and references.

The terminology used for the NIST CSF is briefly explained below.

Functions

The NIST CSF is divided into five main functions. The functions are arranged simultaneously to represent the lifecycle of security.

Every feature is very important for a security situation that works well and for successful cyber risk management. The definitions for each function are as follows:

List of Functions

1. **Identify:** Developing an understanding of the organization to manage the risks of cybersecurity in the system, assets, data, and functions.

2. **Protect:** Develop and implement appropriate safeguards to ensure the delivery of critical infrastructure services.

3. **Detect:** Develop and implement appropriate activities to identify the occurrence of security events.

4. **Respond:** Develop and implement appropriate activities for detecting security events.

5. **Recover:** Develop and implement appropriate resilience activities and restore capacity or services disrupted due to security events.

Categories and subcategories

With every feature stored in the image above, there are twenty-one categories and over a hundred subcategories.

Tiers

The NIST CSF Tiers represent how well an organization views cybersecurity risk and the processes in place to mitigate risks. This helps provide organizations a benchmark on how their current operations.

- **Tier 1 – Partial:** Organizational cybersecurity risk is not formalized and managed in an ad hoc and sometimes reactive manner. There is also a limited awareness of cybersecurity risk management.
- **Tier 2 – Risk-Informed:** There may not be an organizational-wide policy for security risk management. Management handles cybersecurity risk management based on risks as they happen.
- **Tier 3 – Repeatable:** A formal organizational risk management process is followed by a defined security policy.
- **Tier 4 – Adaptable:** An organization at this stage will adapt its cybersecurity policies based on lessons learned and analytics-driven to provide insights and best practices. The organization is constantly learning from the security events that do occur in the organization and will share that information with a larger network.

The NIST Cyber Framework provides a common language and systematic methodology for managing cybersecurity risk.

The Core includes activities to be incorporated in a cybersecurity program that can be tailored to meet any organization’s needs.

The Framework is designed to complement, not replace, an organization's cybersecurity program and risk management processes.