Demonstrating NIST CSF 2.0 Compliance with Cyber Intelligence

Posted on March 22, 2024

Cybersecurity is a top priority for most organizations, with 96% of CEOs saying it is critical for success. However, most CEOs worry their organizations cannot fully defend against cyber attacks.

To help organizations achieve their cybersecurity goals, the National Institute of Standards and Technology (NIST) updated the widely adopted Cybersecurity Framework (CSF) in February 2024. NIST CSF 2.0 has an expanded scope, making it applicable to all organizations across sectors and types.

What Is NIST CSF?

NIST CSF is a set of cybersecurity guidelines and best practices that help organizations minimize cyber risks. It is only mandatory for all federal agencies and government suppliers. However, even though the framework is voluntary for private sector companies, research shows that about 74% of organizations that adhere to a security framework use NIST CSF.

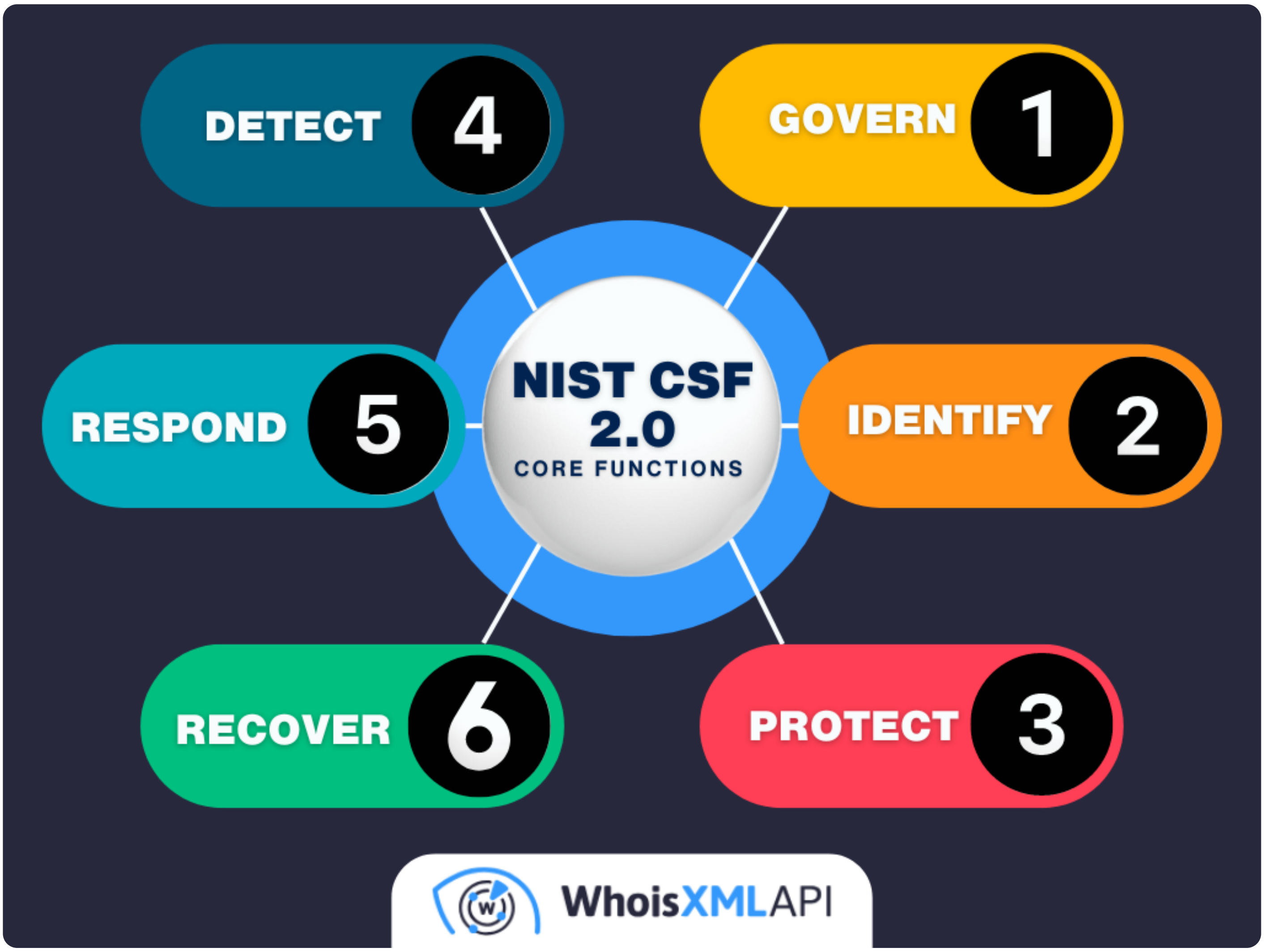
The flexibility NIST CSF offers could be the reason for its widespread adoption. The framework doesn’t dictate specific tools or technologies. Instead, it offers a library of best practices. Organizations can choose the practices that best suit their risk profile and industry needs.

The recent release of CSF version 2.0 makes the framework more flexible and useful for all organizations, regardless of industry and size. Along with the new version, NIST updated the framework’s core guidance and developed several resources, such as CSF 2.0 profile templates for organizations and communities.

NIST CSF 2.0 is also scalable. Small businesses can leverage the framework’s core principles to establish a basic security foundation, while larger organizations can build upon it to create a more sophisticated security program.

What Are the Core Functions of NIST CSF 2.0?

NIST CSF 2.0 outlines six core functions crucial for effective cybersecurity—Govern, Identify, Protect, Detect, Respond, and Recover. These functions provide a road map for organizations to build a comprehensive security strategy.



- **Govern:** This function is new in NIST CSF 2.0. It emphasizes the importance of establishing a clear cybersecurity governance structure. It includes defining roles and responsibilities, developing a cybersecurity risk management strategy, and creating policies that guide security practices across the organization.

- **Identify:** Through this core function, organizations can understand their current cyber risks. It involves asset inventory, vulnerability and threat detection, and staying informed about potential cyber threats.

- **Protect:** Here, the focus lies on implementing safeguards to prevent cyber attacks and mitigate their impact. This function includes securing systems and data, implementing access controls, monitoring networks and devices, and training employees.

- **Detect:** Early detection of security incidents is crucial. This function involves deploying security measures to continuously monitor your systems and identify any suspicious activity that may indicate an attack.

- **Respond:** This function refers to actions to take in the event of a cybersecurity incident. It involves incident response planning, containing the incident to prevent further damage, eradicating the threat, and reporting the incident.

- **Recover:** Organizations must be able to restore normal operations after a cyber attack. Its core function focuses on developing and maintaining a recovery plan that ensures business continuity. It includes procedures for restoring critical systems and data after an incident.

How Does NIST CSF 2.0 Work?

Aside from the six core functions, a significant part of CSF 2.0 are the organizational profiles. The Organizational Profile Template comes in a spreadsheet that organizations can fill out to determine their current and target cybersecurity profiles. The template has around 128 categories and subcategories under each core function, each with a detailed outcome description.

The Detect core function, for instance, has two categories—Continuous Monitoring (DE.CM) and Adverse Event Analysis (DE.AE). DE.CM has five subcategories, while DE.AE has six. Each subcategory is associated with outcomes that drill down to the specific core function category. For example, the CSF outcome description for subcategory DE.AE-02 is “Potentially adverse events are analyzed to better understand associated activities.” Outcomes like this help organizations think deeply about every aspect of their cybersecurity posture.

In filling out the template, organizations can include or exclude categories and subcategories as they see fit. They can then evaluate their current and target cybersecurity practices for achieving each subcategory’s outcomes, particularly in terms of these aspects:

- Priority
- Status
- Policies, processes, and procedures
- Internal practices
- Roles and responsibilities
- Informative references

After completing the profile, organizations can analyze the gap between their current and target cybersecurity posture and create an action plan to move closer to the target. Once the action plan is implemented, they can revisit and update their profile to check if their strategies are effective.

How Can WhoisXML API Intelligence Help with NIST CSF 2.0 Implementation?

When going through the CSF Organizational Profile Template, organizations may realize the need for a comprehensive intelligence source stack that includes domain, IP, and DNS data. This cyber intelligence can aid organizations with the framework’s Identify (ID), Protect (PR), Detect (DE), and Respond (RE) functions. Below are some examples of categories where WhoisXML API intelligence can fit.

- **Asset Management (ID.AM):** This category in the Identify function requires organizations to identify, inventory, prioritize, and manage all their critical assets. These assets include company-registered domain names, website metadata, SSL certificates, DNS records, and other assets WhoisXML API provides visibility to.

- **Risk Assessment (ID.RA):** One of the goals of CSF is to help organizations understand the cybersecurity risks they face. To achieve this objective, they need to identify vulnerabilities and any other weakness that can lead to cyber threats. WhoisXML API's threat intelligence feeds can help with that, particularly in satisfying ID.RA-02 (Cyber threat intelligence is received from information-sharing forums and sources). In addition, domain, IP, and DNS data points can reveal infrastructure misconfigurations that organizations may overlook.

- **Identity Management, Authentication, and Access Control (PR.AA):** NIST describes this category's outcome as organizations limiting and managing access to assets to authorized users, services, and hardware. WhoisXML API's IP intelligence can help with that, particularly in blocking connections coming from devices located outside the organization's service area or those whose IP addresses violate regulatory stipulations. Threat intelligence sources also enable organizations to block malicious domains, URLs, IP addresses, CIDR numbers, and hashes.

- **Continuous Monitoring (DE.CM):** In the context of CSF's Detect function, continuous monitoring refers to tracking assets to discover anomalies, IoCs, and other adverse events. This process involves scanning networks and third-party services for malicious indicators, which can be made more effective when WhoisXML API's threat intelligence data is integrated into network monitoring tools.

- **Adverse Event Analysis (DE.AE) and Incident Analysis (RS.AN):** Once potentially malicious resources and events are detected, NIST CSF 2.0 further requires organizations to analyze them under DE.AE. The same is true when cybersecurity incidents are detected (RS.AN). These outcomes are within organizations' grasp by gleaning ownership, resolution, configuration, and association context into identified malicious indicators, notably using passive DNS data.

Conclusion

NIST CSF compliance is not just about ticking boxes. It’s about safeguarding customers and your business and fostering a culture of ethical and responsible operations. You need a reliable stack of cyber intelligence sources to fully analyze your compliance and determine how robust your cybersecurity posture is.

***Contact us now* to learn more about the WhoisXML API cyber intelligence sources that can help you satisfy NIST CSF 2.0 functions and categories.**