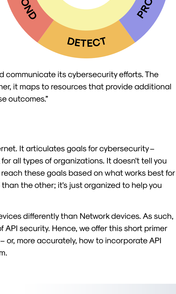
The NIST Cybersecurity Framework 2.0 and API Security

How and why CISOs should leverage the new NIST CSF to include and improve API Security

What

The Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST) is undergoing a major update. It is a widely used framework, helping organizations understand and manage their cybersecurity risks.

The NIST CSF was released as version 1.0 in 2014, updated to version 1.1 in 2018. The draft of CSF version 2.0 is open for comment until Nov-2023, and is expected to be released in early 2024.



"The NIST Cybersecurity Framework 2.0 provides guidance to industry, government agencies, and other organizations to reduce cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The Framework does not prescribe how outcomes should be achieved. Rather, it maps to resources that provide additional guidance on practices and controls that could be used to achieve those outcomes."

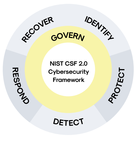
Why

The NIST CSF 2.0 is like a guidebook for keeping things safe on the internet. It articulates goals for cybersecurity – arranged by Function, Category, and Subcategory – which should work for all types of organizations. It doesn't tell you exactly what to do; rather, it's up to each organization to decide how to reach these goals based on what works best for them. And the order of these goals doesn't mean one is more important than the other; it's just organized to help you keep things safe online.

It does not get into specific technologies or how you should treat IOT devices differently than Network devices. As such, it might be a little difficult to understand how it may apply to the world of API security. Hence, we offer this short primer on how you might map the new guidelines to your API security program – or, more accurately, how to incorporate API security into your overall security posture and risk management program.

Govern (GV)

Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy.



Categories. Organizational Context (GV.OC); Risk Management Strategy (GV.RM); Cybersecurity Supply Chain Risk Management (GV.SC); Roles, Responsibilities, and Authorities (GV.RR); Policies, Processes, and Procedures (GV.PO); and Oversight (GV.OV).

Description. The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management strategy. GOVERN directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy.

Applying to APIsec. The key here is to integrate your API management and security into your overall security posture, avoiding silos that could introduce gaps or unintentionally allow APIs to slip off the governance radar. This means including your APIs in your cybersecurity risk management decision making, in your risk tolerance calculations and prioritization, and in your supply chain risk management process – especially any open-source APIs used for development, internal operations or partners.

How. Some capabilities you need to foster include being able to:

- Ensure APIs match specifications
- Detect changes in APIs
- Identify software in use

Identify (ID)

Help determine the current cybersecurity risk to the organization.

Categories. Asset Management (ID.AM); Risk Assessment (ID.RA); and Improvement (ID.IM).

Description. Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvements needed for the organization's policies, processes, procedures, and practices supporting cybersecurity risk management to inform efforts under all six Functions.

Applying to APIsec. The key here is to ensure you have full visibility across your entire API portfolio which may otherwise inhibit your ability to fully secure them. This means knowing all public, partner, and private APIs being used across your organization, understanding their importance within your larger risk strategy, and including APIs in your risk assessment process, especially externally-accessible private and partner APIs which are key to your internal operations.

How. Some capabilities you need to foster include being able to:

- Inventory all APIs and endpoints
- Classify endpoints
- Assess risk for endpoints
- Find vulnerabilities
- Detect changes to endpoints

Protect (PR)

Use safeguards to prevent or reduce cybersecurity risk.

Categories. Identity Management, Authentication, and Access Control (PR.AA); Awareness and Training (PR.AT); Data Security (PR.DS); Platform Security (PR.PS); and Technology Infrastructure Resilience (PR.IR).

Description. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events. Outcomes covered by this Function include awareness and training; data security; identity management, authentication, and access control; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

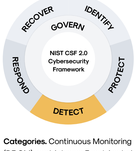
Applying to APIsec. The key here is to implement proactive and runtime API protections which reduce overall risk of APIs being the path of least resistance for cyber attacks. There are a lot of components to this, such as implementing robust AuthN and AuthZ practices, incorporating API security best practices into your SDLC, and ensuring that API endpoints handling sensitive data flows are enumerated, monitored and protected.

How. Some capabilities you need to foster include being able to:

- Identify out-of-date components in APIs
- Record session data for APIs
- Identify unauthorized/unmanaged APIs
- Block attacks against APIs

Detect (DE)

Find and analyze possible cybersecurity attacks and compromises.



Categories. Continuous Monitoring (DE.CM); and Adverse Event Analysis (DE.AE).

Description. DETECT enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring.

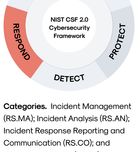
Applying to APIsec. The key here is to ensure you have visibility into your API vulnerabilities and understand threats against them, since over 80% of web traffic now flows through APIs and that many if not most development environments involve extensive use of APIs (e.g., GitHub). This should include monitoring all API endpoints regardless of protocol or underlying infrastructure, applying virtual patches, leveraging real-world attack data in your SDLC processes, and providing the same level of support to understand and mitigate API incidents as has historically been afforded to traditional infrastructure and compiled code.

How. Some capabilities you need to foster include being able to:

- Detect attacks against APIs
- Detect incidents in progress
- Deliver incident data to SIEMs

Respond (RS)

Take action regarding a detected cybersecurity incident.



Categories. Incident Management (RS.MA); Incident Analysis (RS.AN); Incident Response Reporting and Communication (RS.CO); and Incident Mitigation (RS.MI).

Description. RESPOND supports the ability to contain the impact of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

Applying to APIsec. The key here is the ability to respond at machine-speed to attacks against APIs and to ensure that any incidents are handled with the same processes and procedures as the rest of your digital domain. For instance, the same continuous monitoring approach used to automatically detect security threats, performance issues or compliance problems in IT systems and networks should be extended to APIs to ensure rapid response to similar issues in your API portfolio.

How. Some capabilities you need to foster include being able to:

- Identify attacked vulnerabilities
- Capture details about attacks
- Notify stakeholders of incidents
- Block attacks and malicious behavior

Recover (RC)

Restore assets and operations that were impacted by a cybersecurity incident.

Categories. Incident Recovery Plan Execution (RC.RP); and Incident Recovery Communication (RC.CO).

Description. RECOVER supports timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts.

Applying to APIsec. The key here is developing recovery plans which consider API-specific needs, especially regarding 3rd party or open-source tools used in your development infrastructure. This includes developing, implementing, testing, and then automating your API-specific recovery plans, and integrating your API-specific outputs into your existing security and reporting stack will ensure timely and coordinated communication internally and, if necessary, externally.

How. Some capabilities you need to foster include being able to:

- Capture details of API-related breaches
- Include API-based services in your recovery plan
- Integrate API incident reporting into existing structure

About Wallarm

The Wallarm integrated App and API Security platform provides robust protection for APIs, web applications, microservices, and serverless workloads running in cloud-native environments. Wallarm is the preferred choice of hundreds of Security and DevOps teams for comprehensive discovery of web apps and API endpoints, protection against emerging threats throughout their API portfolio, and automated incident response to enhance risk management. Our platform supports modern tech stacks, offering dozens of deployment options in cloud and Kubernetes-based environments, and also provides a full cloud solution.

(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107
www.wallarm.com