WHITEPAPER

Operationalizing the NIST Cybersecurity Framework (CSF) 2.0 with Tanium

Introduction to NIST CSF 2.0

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 is an industry-standard approach to managing cybersecurity risks, emphasizing continuous improvement and alignment with business objectives. NIST CSF 2.0 introduces the Govern function, reflecting the increasing importance of governance and policy oversight in today's interconnected environment. Together with the existing functions — Identify, Protect, Detect, Respond, Recover — this update underscores the importance of aligning cybersecurity efforts with broader business objectives, regulatory requirements, and enterprise risk management practices. NIST CSF 2.0 offers a roadmap for building resilient and efficient cybersecurity programs. By addressing the full spectrum of cybersecurity activities — from risk identification and mitigation to recovery and continuous improvement — the framework helps organizations protect their critical assets, maintain stakeholder trust, and achieve regulatory compliance.

First introduced in 2014, the NIST Cybersecurity Framework has become a cornerstone for organizations seeking to enhance their cybersecurity posture. The 2024 NIST CSF 2.0 update reflects the growing complexity of the digital environment and the need for robust governance with key updates of:

- The addition of the Govern function, focusing on integrating cybersecurity governance into enterprise risk management and improving alignment with strategic objectives.
- Enhanced guidance within the existing core functions to support scalability and adaptability for diverse use cases.
- A continued emphasis on flexibility, making the framework suitable for small businesses, multinational corporations, and critical infrastructure providers alike.

Organizations can leverage Tanium to achieve robust security, operational efficiency, and compliance with regulatory standards. Tanium Autonomous Endpoint Management (AEM) strengthens cybersecurity resilience while aligning security initiatives with business objectives and stakeholder expectations.

Framework overview: Functions and Tanium capabilities

The six core functions of NIST CSF 2.0 form the foundation for a comprehensive approach to cybersecurity. Each function builds on the others to create a comprehensive, iterative process for risk management, incident response, and resilience.

Below is a summary of how Tanium can help organizations achieve prescribed controls in each c function.

NIST CSF 2.0 Function	NIST CSF 2.0 Function Objective	Example Tanium Support
Govern	Integrate cybersecurity governance into broader enterprise risk management standards to enforce and monitor compliance and ensure consistent application of security policies.	Tanium provides comprehensive visibility and control over endpoint security, supporting robust governance and policy enforcement. Its capabilities allow organizations to align cybersecurity practices with business objectives and regulatory requirements, ensuring a cohesive and strategic approach to security.
Identify	Get comprehensive insights into devices and vulnerabilities to develop a thorough understanding of assets, risks, and vulnerabilities through continuous, automated discovery and inventory.	Tanium's real-time data collection and asset discovery tools help organizations maintain an up-to-date inventory of assets, manage vulnerabilities, and understand their cybersecurity risks.
Protect	Implement safeguards to manage the organization's cybersecurity risks, reduce the attack surface, and minimize the impact of incidents.	Through automated patch management, configuration management, and compliance enforcement, Tanium helps safeguard systems against threats, reducing the attack surface and enhancing endpoint protection.
Detect	Develop and implement timely processes for identifying and analyzing cybersecurity events.	Tanium's detection capabilities enable continuous monitoring and swift identification of suspicious activities and anomalies across endpoints, ensuring early detection of potential security incidents.
Respond	Take action to contain and mitigate the effects of cybersecurity incidents.	Tanium facilitates rapid incident response through its real-time data and remediation capabilities, allowing organizations to contain and mitigate threats swiftly and efficiently.
Recover	Restore assets, services, and operations impacted by cybersecurity events to ensure operational resilience and minimal downtime.	Tanium supports the recovery process by ensuring data integrity and providing tools to restore affected systems, helping organizations resume normal operations quickly after an incident.

Tanium's automation imperative for NIST CSF 2.0

As cyber threats escalate and digital ecosystems grow more complex, automation has become crucial for effective cybersecurity strategies. The NIST CSF 2.0 acknowledges this shift, recognizing automation as essential for efficient and responsive security operations. By reducing manual workloads, streamlining operations, and enhancing real-time responsiveness with automation, organizations can achieve the speed and efficiency necessary to address modern threats.

Tanium Autonomous Endpoint Management (AEM) unlocks value across a comprehensive suite of endpoint solutions, including asset discovery and inventory, vulnerability management, endpoint management, incident response, and digital employee experience. AEM leverages AI/ML capabilities built into the platform to drive faster, better decision making and significant business outcomes for customers.

Tanium AEM boosts operational efficiency by automating routine tasks, allowing resources to focus on growth initiatives without compromising security, performance, or availability. Its reliable and scalable automation enhances security posture and accelerates risk mitigation by proactively managing vulnerabilities and incidents. With real-time data and analysis of changes on global cloud-managed endpoints, Tanium AEM makes recommendations and automates changes safely and reliably, ensuring operational health, reducing business risk, and enhancing endpoint security.

Business benefits of adopting NIST CSF 2.0

Here are some examples where Tanium supports NIST CSF 2.0 and delivers tangible benefits across risk management, compliance, and operational efficiency.

- **Proactive risk management:** Reducing vulnerabilities through structured action plans minimizes risk exposure.
- **Improved compliance:** Aligning with global standards simplifies audits, reduces regulatory penalties, and ensures stakeholder confidence.
- **Operational efficiency:** Automation and streamlined processes reduce manual security tasks and improve outcomes.
- **Cost savings:** Enhanced security lowers incident-related expenses, including legal and reputational costs.

Conclusion

NIST CSF 2.0 represents a framework for building resilience and alignment in cybersecurity. Tanium can help support organizations operationalize the framework to achieve robust security and compliance in an ever-evolving threat landscape.

For more information

Please **contact us** or connect with your Tanium account team to learn more.

Additional Resources

NIST Cybersecurity Resource Center

TANIUM

The Power of Certainty.™

Visit us at www.tanium.com and follow us on LinkedIn and X.