2025

Seceon's Global Cybersecurity Framework Mapping Guide - NIST CSF 2.0

Your essential resource to map your NIST CSF 2.0 compliance program goals to your cybersecurity program, controls and Seceon's platform.

Achieving Continuous Compliance with Seceon

Seceon streamlines continuous compliance, integrating it seamlessly into daily security operations through automated workflows, real-time insights, and alignment with compliance frameworks. Our aiSIEM and aiXDR solutions empower organizations to meet regulatory requirements without overburdening IT and compliance teams.

Common Control Framework (CCF)

Seceon's Common Control Framework (CCF) is designed to support efficient compliance with multiple global standards. By consolidating security, privacy, and compliance mandates into a unified set of controls, CCF enables us to standardize compliance processes across varied services and products.

CCF Highlights

- **Unified Compliance:** CCF integrates requirements from multiple frameworks, including ISO 27001, SOC 2, HIPAA, NIST CSF 2.0, and PCI DSS, simplifying compliance management.
- **Mapped Controls:** Each control aligns with one or more regulatory standards, allowing a single control to satisfy several compliance mandates.
- **Domain Structure:** CCF organizes controls into domains that cover key areas of security and compliance.
- **Three-Tiered Control System:** CCF categorizes controls into People, Process, and Technology.
  - **People Controls:** Address training, awareness, and organizational structure.
  - **Process Controls:** Cover documented procedures, manual rule enforcement, and risk assessment.
  - **Technology Controls:** Govern data processing, IT asset management, and network security.

Leveraging CCF along with Seceon's robust tools, organizations can generate interactive compliance reports for frameworks like HIPAA, NIST CSF, and PCI-DSS, providing audit-ready documentation for diverse regulatory needs.

Key Compliance-Enhancing Features on Seceon's Platform

1.Centralized Visibility and Monitoring: Our platform collects and correlates data from diverse sources, including firewalls, intrusion detection systems, servers, and endpoints, delivering unified visibility across the network.

2.Threat Detection and Incident Response: Powered by machine learning, Seceon's advanced threat detection swiftly identifies unusual patterns or potential incidents, enabling rapid incident response.

3.Continuous Compliance Reporting: Equipped with robust reporting tools, Seceon's platform generates detailed, framework-specific reports to simplify audits.

4.Log Management and Audit Trails: Comprehensive log collection and management support Seceon's commitment to rigorous auditing standards.

5.Risk Management Support: The platform's Risk Assessment (RA) tools analyze data to pinpoint and prioritize potential threats, fostering a proactive security posture.

Visit the offical NIST CSF 2.0

https://www.nist.gov/cyberframework

NIST CSF 2.0 Compliance:

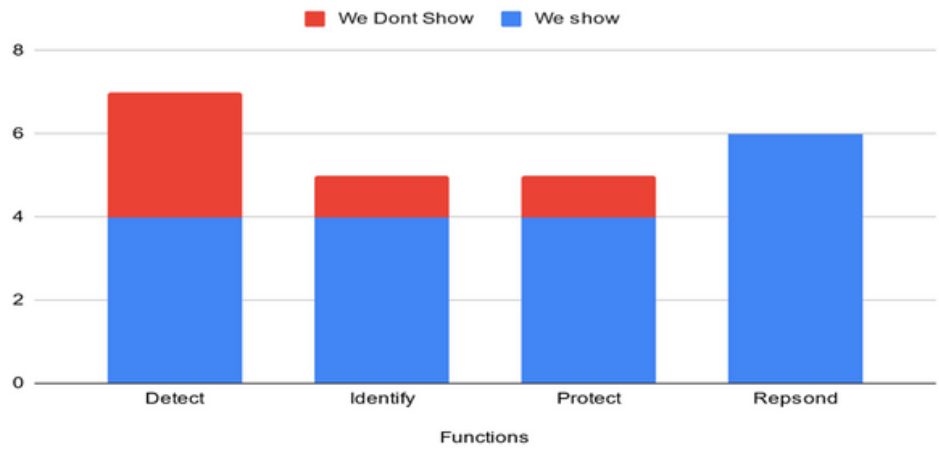
As cyber threats continue to expand in volume and complexity, the demand for a rigorous and adaptive cybersecurity framework is more critical than ever. The **NIST Cybersecurity Framework (CSF) 2.0** stands as a powerful standard, empowering organizations to strengthen defenses, respond adeptly to incidents, and recover swiftly from disruptions. The core of the NIST CSF is structured around five foundational functions: Identify, Protect, Detect, Respond, and Recover. These functions form the strategic pillars for prioritizing and organizing cybersecurity efforts within any organization. By addressing each core function, organizations can develop a comprehensive cybersecurity program tailored to their unique objectives and risk thresholds.



Seceon's approach is closely aligned with the NIST CSF's core functions, emphasizing enhanced resilience and readiness for regulatory compliance. Using our Open Threat Management (OTM) platform, we focus extensively on technology controls within the NIST CSF 2.0 framework, providing a measurable demonstration of compliance against specific technical controls. This focus includes automated threat detection, incident response, and continuous monitoring capabilities that serve as critical components of an organization's cybersecurity program.

While our reports and KPIs concentrate on technology controls, it is important to note that people, process, and governance-related controls—which often involve detailed documentation and procedural evidence—are outside the primary scope of our automated compliance reports. This distinction ensures that Seceon's OTM platform directly supports the operational and technical facets of cybersecurity, allowing organizations to focus resources effectively across their broader cybersecurity program.

NIST CSF Core Functions and Coverage:



NIST Mapping Table:

No.	Domain Title	Number of Total Controls	Number of Technical Controls	Technology Controls Mapped to Seceon	Seceon CCF Controls
1	Identify	20	8	ID.AM-03, ID.AM-07, ID.RA-01, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, ID.RA-08	N0-15, DM-02, VM-01, PS-02, VM-03, VM-22*

2	Protect	23	8	PR.AA-01,PR.AA-02, PR.AA-03,PR.AA-05, PR.DS-01,PR.DS-02, PR.PS-01,PR.PS-04	IAM-01, IAM-29, DM-13, CFM-01,SM-01
3	Detect	11	6	DE.CM-01, DE.CM-03, DE.CM-09, DE.AE-02, DE.AE-04, DE.AE-06	NO-01, SM-01, SM-18*, SM-25, SM-31, VM-03 IR-01, IR-03
4	Repsond	13	13	RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02	IR-03, IR-01, IR-02, IR-08, IR-04*

About Seceon

Seceon enables MSPs, MSSPs, and IT teams to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon augments and automates MSP, MSSP, and IT security services with an AI and ML-powered aiSIEM and aiXDR platform. It delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time with threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 680 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/



© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, aiMSSP are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.