NIST Cybersecurity Framework Compliance Guide

Following an Executive Order to improve critical infrastructure cybersecurity, the National Institute of Standards and Technology (NIST) created the Cybersecurity Framework (CSF), which seeks to enhance security and resilience by addressing the lack of uniform cybersecurity standards. The CSF sets forth a set of best practices that help improve enterprises' cybersecurity posture and minimize organizational cybersecurity risks. Consisting of five core functions – Identify, Protect, Detect, Respond, and Recover – the CSF offers a set of standards, recommendations, and guidelines to advance enterprises' ability to identify and detect attacks, respond and prevent them, and recover, should one occur.

The CSF was developed through NIST's collaboration with leading experts in information security from around the world, as well as owners and operators of US critical infrastructure. NIST's CSF is considered the most reputable source when building a cybersecurity program, thanks to its extensive scope and broad applicability.

The absence of codified cybersecurity standards not only made it difficult for enterprises to create and implement an effective cybersecurity strategy but meant that any efforts that were undertaken could get undermined by gaps within the supply chain. Now, cybersecurity strategies can conform to the comprehensive CSF guidelines and enterprises can ensure their cybersecurity efforts are maintained by only dealing with entities that also adhere to the CSF standards.

Layer 1 Visibility and NIST CSF

Quotidian, traffic-based security solutions fail to cover Layer 1 (the Physical Layer), resulting in an inaccurate asset inventory, unaccounted-for vulnerabilities, and unidentified risks, all of which hinder further cybersecurity efforts. In turn, this lack of visibility means alignment with the CSF is limited as many of the controls cannot be met. Naturally, the enterprise suffers from weak cybersecurity and resilience capabilities, which ultimately puts it at risk.

Sepio's HAC-1 solution offers Layer 1 visibility to help enterprises fulfill many of the CSF controls, from Identify to Respond. By using Layer 1 data to accurately detect and identify all IT/OT/IoT assets on USB and network interfaces – managed, unmanaged, and hidden – HAC-1 supports and strengthens overall cybersecurity efforts by facilitating:

- Complete asset visibility
- Informed decision making
- Enhanced control
- Swifter incident detection
- Effective mitigation
- Comprehensive incident reporting

To name a few...

NIST CSF and HAC-1

FUNCTION: IDENTIFY (ID)
Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
Asset Management (ID.AM) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	***ID.AM-1*** **– Physical devices and systems within the organization are inventoried**	• HAC-1 offers complete asset visibility of all IT/OT/IoT assets on USB and network interfaces, whether managed, unmanaged or hidden – no device goes undetected. • HAC-1 generates a fingerprint of all devices through multiple Layer 1 parameters and a unique machine learning algorithm to reveal a device's true identity, not just what it claims to be, thus creating a complete and accurate asset inventory. • Assets get assigned a risk level and risk description to provide further details. • Continuous monitoring of all devices ensures the inventory is maintained in real-time, with assets tracked from time first seen until time last seen.
	ID.AM-2 **– Software platforms and applications within the organization are inventoried**	• HAC-1 event log lists all system activity regarding hardware devices, accompanied by various details including the operating system of assets and switches.
	ID.AM-5 **– Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value**	• HAC-1 enables the prioritization of hardware assets through policies, rules and tags based on a device's characteristics or risk score.

.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
Risk Assessment (ID.RA) The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	***ID.RA-1*** **– Asset vulnerabilities are identified and documented**	• HAC-1 continuously monitors all IT/OT/IoT assets on USB and network interfaces, managed, unmanaged, or hidden, to identify device and switch vulnerabilities.
	ID.RA-2 **– Cyber threat intelligence is received from information sharing forums and sources**	• HAC-1's internal threat intelligence database relies on various data sources, including external databases and internal lab research.
	ID.RA-3 **– Threats, both internal and external, are identified and documented**	• HAC-1 detects and identifies every hardware asset in the enterprise environment, both internal and external, through Layer 1 data signals, generating a digital fingerprint for every device to reveal its true identity. • HAC-1 compares a device's digital fingerprint with the system administrator's pre-defined rules and internal threat intelligence database for known-to-be-vulnerable devices to identify those which are deemed a threat, issuing an immediate alert for such instances.
	ID.RA-5 **– Threats, vulnerabilities, likelihoods, and impacts are used to determine risk**	• HAC-1 gathers Layer 1 data signals and monitors the behavior of every hardware asset. • HAC-1 compares this information against various risk indicators, including known threats and vulnerabilities, anomalies and compliance, to determine an asset's risk posture and score.

.

CONTROL	SUB-CONTROL	SUB-CONTROL
> Continued **Risk Assessment (ID.RA)**	***ID.RA-6*** **– Risk responses are identified and prioritized**	• The system administrator can define a set of rules for the system to enforce based on roles or device characteristics. • HAC-1 integrates with several IT and security orchestration products, easily automating policy enforcement and specific playbook procedures to provide a speedy response and accelerated mitigation process to block devices that breach the pre-defined rules.
Supply Chain Risk Management (ID. SC) The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	***ID.SC-2*** **– Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process**	• HAC-1 accurately identifies the vendor of every hardware device and switch using Layer 1 data. • HAC-1's real time asset validation supports the supply chain hardware risk assessment. • The system administrator can manage and prioritize supply chain hardware risks through hardware sandboxing.

FUNCTION: PROTECT (PR)

Develop and implement appropriate safeguards to ensure delivery of critical services.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
Identity Management, Authentication and Access Control (PR.AC) Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	***PR.AC-1*** **– Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes**	• HAC-1 generates a fingerprint of all devices through multiple Layer 1 parameters and a unique machine learning algorithm to reveal a device's true identity, not just what it claims to be. • Assets get assigned a risk level and risk description to provide further details. • HAC-1 verifies and continuously validates the identity of all hardware assets to maintain device integrity, issuing alerts when there are any changes to a device's risk level.
	PR.AC-2 **– Physical access to assets is managed and protected**	• HAC-1 uses Layer 1 data signals and a unique machine learning algorithm to monitor all hardware assets, ensuring no unauthorized changes were made to the hardware's Bill of Materials. • HAC-1's audit trail provides details for all user activity, including user name; user activities; user privileges; event severity; and time and date of event.
	PR.AC-3 **– Remote access is managed**	• HAC-1 collects the Layer 1 data of all remote hardware assets to generate their digital fingerprint and verify their authenticity. • HAC-1's comprehensive Zero Trust Hardware Access approach means the system administrator's pre-defined Hardware Access Control policies get applied to remote assets.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
> Continued **Identity Management, Authentication and Access Control (PR.AC)**	***PR.AC-3*** **– Remote access is managed**	• Unauthorized devices, based on the pre-set Hardware Access Control policies and HAC-1's internal threat database, get blocked through third-party integrations. • Continuous monitoring of remote assets ensures a Zero Trust Hardware Access approach in real-time.
	PR.AC-4 **– Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties**	• HAC-1's Hardware Access Control capability allows the system administrator to define granular Hardware Access Control policies for the system to enforce, supporting the principle of least privilege through Zero Trust Hardware Access. • The administrator can lock a list of approved devices based on existing and recognized devices, or on a known list of devices that were regarded as benign in other installations. • Similarly, the system administrator can define Hardware Access Control policies based on regulations, in which HAC-1 assess a device's access permissions based on its compliance with the specified regulation(s). • HAC-1 continuously monitors all hardware assets to validate that privileges are authorized, thereby ensuring the efficacy of Zero Trust Hardware Access. • HAC-1 integrates with several IT and security orchestration products, easily automating policy enforcement and specific playbook procedures to provide a speedy response and accelerated mitigation process to block devices that breach the pre-defined rules.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
> Continued **Identity Management, Authentication and Access Control (PR.AC)**	***PR.AC-5*** **– Network integrity is protected (e.g., network segregation, network segmentation)**	• HAC-1 safeguards network integrity by verifying the identity of all hardware assets through Layer 1 data signals and subsequently enforcing Hardware Access Control policies, providing enhanced security even for non-802.1X compliant devices, such as IoTs, and preventing MAC-less devices or devices with spoofed MAC addresses from bypassing network security protocols, such as segregation and segmentation. • HAC-1 identifies the BSSID of all access points to gather an accurate inventory and ensure rogue access points are not present within the enterprise.
	PR.AC-7 **– Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)**	• HAC-1's Hardware Access Control capability allows the system administrator to define Hardware Access Control policies for the system to enforce dependent on a device's risk score. • Under a Zero Trust Hardware Access approach, HAC-1 authenticates and continuously validates the identity of all hardware assets using Layer 1 parameters. Any changes to a device's risk score gets accounted for, enhancing Hardware Access Control policy enforcement.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
Data Security (PR.DS) Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	***PR.DS-5*** **– Protections against data leaks are implemented**	• HAC-1 gathers Layer 1 data signals and monitors device behavior to identify any abnormalities or suspicious activity that could indicate a possible threat to the security of enterprise data. • When a device breaches the pre-set Hardware Access Control policies or gets recognized as malicious by the internal threat intelligence database, HAC-1 initiates a mitigation process to block the device, preventing a potential data leak.
	PR.DS-8 **– Integrity checking mechanisms are used to verify hardware integrity**	• HAC-1 creates a digital fingerprint of all hardware assets – managed, unmanaged, or hidden – using Layer 1 data and a unique machine learning algorithm to verify their authenticity. • HAC-1 continuously monitors all hardware assets to verify their integrity, detecting when any changes have been made to a device's Bill of Materials.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
Information Protection Processes and Procedures (PR.IP) Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	***PR.IP-12*** **– A vulnerability management plan is developed and implemented**	• HAC-1 instantly detects vulnerable switches and hardware devices in the environment, both managed and unmanaged. • Vulnerable assets automatically trigger an alert and HAC-1 enforces the pre-defined Hardware Access Control policies
Protective Technology (PR.PT) Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	***PR.PT-1*** **– Audit/log records are determined, documented, implemented, and reviewed in accordance with policy**	• HAC-1 provides an event log for system events and an audit trail for user activity, both of which are viewable on the system administrator's online security suite. • HAC-1's event log lists all system activity regarding hardware devices, accompanied by various details, including device category and type; device source; event description; changes to device risk level; event threat severity; and time and date of event. • HAC-1's audit trail displays and provides details for all user activity, including user name; user activities; user privileges; event severity; and time and date of event. • The continuous monitoring of all hardware assets ensures the logs are maintained in real-time.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
> Continued **Protective Technology (PR.PT)**	***PR.PT-2*** **– Removable media is protected and its use restricted according to policy**	• HAC-1 detects and identifies all hardware peripherals on the USB interface using Layer 1 data signals to create a digital fingerprint. • HAC-1 restricts the use of removable media through Hardware Access Control policies which get enforced based on the device's digital fingerprint and associated risk score.
	PR.PT-4 **– Communications and control networks are protected**	• HAC-1 passively monitors device behavior and associates devices to a network port. • The system administrator can configure Hardware Access Control policies to block or quarantine a port when HAC-1 detects an unauthorized device.

FUNCTION: DETECT (DE)

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
Anomalies and Events (DE.AE) Anomalous activity is detected and the potential impact of events is understood.	***DE.AE-3*** **– Event data are collected and correlated from multiple sources and sensors**	• HAC-1 continuously and passively monitors the behavior of all hardware assets using Layer 1 data. • HAC-1's event log lists all system activity regarding hardware devices, accompanied by various details, including device category and type; device source; event description; changes to device risk level (when applicable); event severity; and time and date of event. • The solution's built-in threat intelligence database for known-to-be-vulnerable devices augments the real-time analysis by providing up-to-date threat intelligence. • HAC-1 also identifies uncommon devices as these anomalies could present a risk. • SOAR/SIEM centralized solutions are easily integrated through a dedicated API.
	DE.AE-5 **– Incident alert thresholds are established**	• HAC-1 tracks all system activity on the event log and instantly detects when a malicious device is present within the enterprise, automatically triggering an alert. • HAC-1 identifies the threat severity of system events and user activities. • The system administrator can tune the alerting threshold level according to a specified severity or device risk level so that the relevant incidents trigger an alert.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
Security Continuous Monitoring (DE.CM) The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	***DE.CM-7*** **– Monitoring for unauthorized personnel, connections, devices, and software is performed**	• Traffic-based solutions fail to identify spoofed MAC addresses, nor do they detect MAC-less and out-of-band devices that could pose a threat to the enterprise. • Rather than monitoring traffic, HAC-1 gathers Layer 1 data and polls switches to analyze activity and detect unauthorized network implants and switch vulnerabilities. • On the endpoint interface, HAC-1 gathers Layer 1 data signals and monitors device behavior to identify any unauthorized devices. • The solution's built-in threat intelligence database for known-to-be-vulnerable devices augments the real-time analysis by providing up-to-date threat intelligence.
	DE.CM-8 **– Vulnerability scans are performed**	• HAC-1 identifies switch vulnerabilities and the relevant patches (when and where applicable) through generated reports to ensure the network infrastructure is kept up to date. • HAC-1 compares devices' digital fingerprint with the internal threat intelligence database for known-to-be-vulnerable devices.
Detection Processes (DE.DP) Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	***DE.DP-4*** **– Event detection information is communicated**	• HAC-1 tracks all system activity on the event log and instantly detects when a malicious device is present within the enterprise, automatically triggering an alert. • HAC-1 performs continuous monitoring of all hardware assets to maintain device integrity and issues an alert when there are any changes to a device's risk level.

FUNCTION: RESPOND (RS)

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
Communications (RS.CO) Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	***RS.CO-2*** **– Incidents are reported consistent with established criteria**	• The system administrator can tune the alerting threshold level according to a specified severity or device risk level so that the relevant incidents trigger an alert. • Ports within a switch can be made “audit proof”, meaning alerts will not be provided.
Analysis (RS.AN) Analysis is conducted to ensure effective response and support recovery activities.	***RS.AN-3*** **– Forensics are performed**	• HAC-1’s event log and audit trail collect all system and user activity, which can be analyzed during post-incident forensics. • HAC-1 offers various types of intelligence reports for both peripheral and network interfaces using information from the event log, providing focused intel on specified areas of interest.
Mitigation (RS.MI) Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	***RS.MI-1*** **– Incidents are contained**	• When there is a breach of Hardware Access Control policies, the unauthorized device gets quarantined in an effort to contain the threat.

CATEGORY	SUB-CATEGORY	SUPPORT FROM HAC-1
> Continued **Mitigation (RS.MI)**	***RS.MI-2* – Incidents are mitigated**	• HAC-1 provides instant alerts to the system administrator when a vulnerable or unauthorized device gets detected and, through third-party integration, initiates an automated mitigation process in response. • SOAR/SIEM centralized solutions are easily integrated through a dedicated API. • When a network device breaches the system administrator's pre-set rules or gets identified as malicious by the solution's internal database, HAC-1 immediately triggers an alert and initiates an automated mitigation process carried out by the solution's northbound interface – either through its built-in Syslog Legacy/CEF interface or, for those customers who operate a NAC solution, through their REST API option. • In ARM mode, when a device on the USB interface breaches the system administrator's pre-set rules or gets identified as malicious by the solution's internal database, HAC-1 immediately triggers an alert and initiates an automated mitigation process to block the device.
	***RS.MI-3* – Newly identified vulnerabilities are mitigated or documented as accepted risks**	• HAC-1's internal threat intelligence database gets updated when new vulnerable devices get discovered through device behavior analysis, OSINT and internal lab research. • HAC-1 remains up to date and protects against the most recent hardware vulnerabilities.