SEPIO

CIS Controls Compliance Guide

Intro

The CIS Controls are a prioritized set of 18 actions that, together, establish an in-depth list of best practices to follow to improve an enterprise's cyber defenses. The abundance of cybersecurity information and resources that are currently available can overwhelm organizations and their cybersecurity departments to the point that cybersecurity efforts become ineffective. The CIS Controls aim to alleviate this challenge by prioritizing actions enterprises should take when tackling cybersecurity to ensure an extensive and effective approach.

The controls were developed by security experts who came together and pooled their knowledge on various aspects of cybersecurity, including the advancing threat landscape (covering attacks, root causes, threat actors, and more); the best defensive techniques; adoption of such techniques; and regulatory compliance. The empirical-based approach ensures that the CIS Controls are relevant, specific, and effective, covering all areas of cybersecurity, from detection and prevention to response and mitigation.

Ultimately, under the guidance of the CIS Controls, enterprises can improve their cybersecurity efforts and, in turn, reduce their attack surface and minimize cyber risks.

Layer 1 Visibility and CIS Controls

Sepio's HAC-1 solution provides Layer 1 visibility to support CIS Control compliance. Layer 1 visibility enables the complete detection and accurate identification of all hardware assets. Certain device characteristics go unaccounted for by traditional security solutions, such as NAC, EPS, IDS, or IoT Network Security, due to a lack of Layer 1 visibility; as a result, devices get wrongly identified or go undetected entirely. In the end, the enterprise is left with an inaccurate asset inventory which consequently hinders asset management efforts and the efficacy of other cybersecurity policies and practices, the effects of which increase the entity's vulnerability to cyber threats.

Layer 1, then, acts as a foundation in which the information provided (i.e. complete asset visibility) enhances subsequent cybersecurity efforts. With Layer 1 visibility, enterprises benefit from:

- ✓ Informed decision making
- ✓ Enhanced control
- ✓ Swifter incident detection
- ✓ Effective mitigation
- ✓ Comprehensive incident reporting

To name a few...

It is, however, important to note that HAC-1 is not an alternative to existing solutions, but rather a complimentary tool that meets the needs of many of the CIS Controls.

CIS Controls and HAC-1

CONTROL	SUB-CONTROL	SUB-CONTROL
Control 1: **Inventory and Control of Enterprise Asset** Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/ Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.	**1.1 – Establish and Maintain Detailed Enterprise Asset Inventory**	• 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 inventory is maintained in real-time, with assets tracked from time first seen until time last seen.
	1.2 – Address Unauthorized Assets	• When a device on the USB interface breaches the system administrator's pre-defined rules or gets recognized as malicious by the internal threat intelligence database, HAC-1 initiates a mitigation process to block the unauthorized device when in ARM mode. • On the network interface, an unauthorized device immediately triggers an alert and HAC-1 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. • The solution uses machine learning and the built-in threat intelligence database for known-to-be-vulnerable devices to discover new threats and ensure HAC-1 remains up to date.

CONTROL	SUB-CONTROL	SUB-CONTROL
> Continued **Control 1:** **Inventory and Control of Enterprise Asset**	**1.3 – Utilize an Active Discovery Tool**	• Uses network poller to determine a device’s presence and combines these signals to create a device fingerprint. • Network poller polls in a cycle of a specified frequency, determined by the system administrator based on the switch’s priority level, such as every 2 hours, to analyze activity.
	1.5 – Utilize a Passive Asset Discovery Tool	• Every connected device automatically discovered and identified by HAC-1. • HAC-1 continuously monitors devices to augment asset discovery.
Control 6: **Access Control Management** Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.	**6.1 – Establish an Access Granting Process**	• HAC-1’s Hardware Access Control capability allows the system administrator to define hardware access policies for the system to enforce dependent on roles or a device’s digital fingerprint and associated risk score. • 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. • HAC-1 verifies and continuously validates the identity of all hardware assets using Layer 1 parameters to enhance hardware access policy enforcement. • HAC-1 communicates with other access control platforms to provide a comprehensive approach to access policy enforcement.

CONTROL	SUB-CONTROL	SUB-CONTROL
> Continued **Control 6:** **Access Control Management**	**6.2 – Establish an Access Revoking Process**	• HAC-1 reveals the true identity of all devices and compares their digital fingerprint with the system administrator’s pre-defined rules to identify those which are deemed unauthorized. The real-time analysis is augmented by the solution’s internal threat intelligence database. • Through seamless third-party integration, HAC-1 automatically blocks unauthorized devices from gaining access. In doing so, HAC-1 also prevents malicious hardware assets from bypassing access controls by going undetected or spoofing legitimate devices. • HAC-1 constantly monitors devices so that any changes will be accounted for.
	6.7 – Centralize Access Control	• HAC-1 provides centralized access control for all enterprise assets. • Through specific API, HAC-1 integrates with other access control providers.
	6.8 – Define and Maintain Role-Based Access Control	• Under HAC-1’s Zero Trust Hardware Access approach, the system administrator can apply the principle of least privilege to all hardware assets by creating granular access controls based on roles or device characteristics. • HAC-1 continuously monitors all hardware assets to validate that privileges are authorized, thereby ensuring the efficacy of Zero Trust Hardware Access.

CONTROL	SUB-CONTROL	SUB-CONTROL
Control 8: **Audit Log Management** Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.	**8.1 – Establish and Maintain an Audit Log Management Process**	• HAC-1 prevents unauthorized devices from gaining access through a Zero Trust Hardware Access approach. • HAC-1 provides an event log for system events and ad audit trail for user activity, both of which are viewable on the system administrator's online security suite. • The continuous monitoring of all hardware assets ensures the logs are maintained in real-time.
	8.2 – Collect Audit Logs	• 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. • 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.
	8.3 – Ensure Adequate Audit Log Storage	• HAC-1 provides continuous monitoring and alert of storage capacity allocated for event logging.
	8.5 – Collect Detailed Audit Logs	• 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. • 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. • 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.

CONTROL	SUB-CONTROL	SUB-CONTROL
> Continued **Control 8:** **Audit Log Management**	**8.9 – Centralize Audit Logs**	• HAC-1 collects and displays all event log and audit trail information on the system administrator's online security suite.
	8.10 – Retain Audit Logs	• Event logs and audit trails are retained for a significant period, configurable to the user's storage resources, at a minimum of 90 days.
	8.11 – Conduct Audit Log Reviews	• HAC-1's event log records the threat severity of every event, triggering the server to issue alerts (dependent on the system administrator's alert threshold level) to allow for further action to be taken. • HAC-1's audit trail collects all user activity, which, upon review, can help identify anomalous or suspicious behavior, such as unusual peripheral connections or unexpected login times, that may indicate a potential threat. • The intelligence reports, generated with event log information, can offer details for a deeper analysis into specific areas of concern.
Control 10: **Malware Defenses** Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise asset.	**10.5 – Enable Anti-Exploitation Features**	• HAC-1 scans every device interface to detect, notify and prevent exploitable functionalities, such as a mass storage interface on a keyboard, that would otherwise go undetected. • HAC-1's visibility goes deeper than any other solution, identifying anomalies in device fingerprints that could indicate potential malicious activity.

CONTROL	SUB-CONTROL	SUB-CONTROL
Control 12: **Network Infrastructure Management** Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.	**12.1 – Ensure Network Infrastructure is Up-to-Date**	• 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.
	12.6 – Use of Secure Network Management and Communication Protocols	• HAC-1 is secured itself by using only HTTPS and SSH for data collection. • 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. • 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.
Control 13: **Network Monitoring and Defense** Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.	**13.1 – Centralize Security Event Alerting**	• 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. • HAC-1 performs continuous monitoring of all hardware assets to maintain device integrity, issuing alerts when there are any changes to a device's risk level.

CONTROL	SUB-CONTROL	SUB-CONTROL
> Continued **Control 13:** **Network Monitoring and Defense**	**13.2 – Deploy a Host-Based Intrusion Detection Solution**	• HAC-1 provides host-based protection by covering the endpoint interface to detect the presence of known-to-be-vulnerable or malicious peripherals that pose a potential or actual threat to the enterprise. These devices spoof their identity and impersonate legitimate HIDs by using the same VID/PID/ClassID parameters, meaning traditional host-based intrusion detection solutions do not differentiate between the legitimate and spoofed devices. • HAC-1 gathers Layer 1 data signals and monitors device behavior to identify any abnormalities or suspicious activity that could indicate a possible threat. • 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.
	13.3 Deploy a Network Intrusion Detection Solution	• 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 offers network protection by gathering Layer 1 data and polling switches to analyze activity and detect unauthorized network implants and switch vulnerabilities. • Switches polled in a polling cycle with a specified frequency dependent on their priority level; ports within a switch can be made "audit proof", meaning alerts will not be provided. • 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.

CONTROL	SUB-CONTROL	SUB-CONTROL
> Continued **Control 13:** **Network Monitoring and Defense**		• HAC-1 also lists uncommon devices as these anomalies could present a risk.
	13.5 – Manage Access Control for Remote Assets	• HAC-1 collects the Layer 1 data of all remote hardware assets to generate their digital fingerprint and verify their authenticity. • The comprehensive Zero Trust Hardware Access approach means Hardware Access Control policies get applied to remote assets. • Unauthorized devices, based on the pre-set Hardware Access Control policies and HAC-1's internal threat database, get blocked. • Continuous monitoring of remote assets ensures a Zero Trust Hardware Access approach in real-time.
	13.7 – Deploy a Host-Based Intrusion Prevention Solution	• HAC-1 provides host-based intrusion prevention by detecting the presence of known-to-be-vulnerable or malicious peripherals that pose a threat to the organization and subsequently blocking them. • These devices spoof their identity and impersonate legitimate HIDs by using the same VID/PID/ClassID parameters, meaning traditional host-based intrusion prevention solutions do not differentiate between the legitimate and spoofed devices and thus do not mitigate the threat. • In ARM mode, when a 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 to block the device.

CONTROL	SUB-CONTROL	SUB-CONTROL
> Continued **Control 13:** **Network Monitoring and Defense**	**13.8 – Deploy a Network Intrusion Prevention Solution**	• HAC-1 also lists uncommon devices as these anomalies could present a risk.
	13.11 – Tune Security Event Alerting Thresholds	• HAC-1 provides immediate alerts whenever a device breaches the pre-set policy or gets recognized as malicious. • The system administrator can tune the alerting threshold level and define whether they want the server to send system and/or audit trail events, according to a specified severity or device risk level.
Control 17: **Incident Response Management** Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.	**17.3 – Establish and Maintain an Enterprise Process for Reporting Incidents**	• 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.

CONTROL	SUB-CONTROL	SUB-CONTROL
> Continued **Control 17:** **Incident Response Management**	**17.4 – Establish and Maintain an Incident Response Process**	• 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.
	17.8 – Conduct Post-Incident Reviews	• HAC-1's event log and audit trail collect all system and user activity, which can be analyzed during post-incident forensics.
	17.9 – Establish and Maintain Security Incident Thresholds	• The system administrator can determine a sensitivity threshold that will trigger various automation processes based on a device's risk score. • The system administrator can tune the alerting threshold level and define whether they want the server to send system and/or audit trail events, according to a specified severity or device risk level.