ALIGNMENT WITH THE CIS CRITICAL SECURITY CONTROLS

How the Armis Platform can help

The Critical Security Controls published by the Center for Internet Security (the "CIS Controls") are considered the de facto cyberdefense guidelines by virtually every security professional. These guidelines map to popular compliance frameworks, including the NIST Cybersecurity Framework, NIST 800-53, and ISO 27000. They help organizations comply with regulations like PCI DSS, HIPAA, NERC CIP, and FISMA. And they are endorsed by respected authorities, including the U.S. Government and the European Telecommunications Standards Institute (ETSI).

This guide explains how the Armis agentless device security platform can help your organization align with eight of the 20 CIS Controls requirements.

Control 1: Inventory and control of hardware assets

The Armis platform uses passive listening techniques to discover devices on your network and uses radio frequency analysis to discover off-network devices in your environment. This agentless discovery covers both primarily connected devices (those with an IP address) and peripherally connected devices (those connected to an attached device using protocols like Bluetooth, NRF, Zigbee, etc.). The result is a complete inventory of devices, right down to make, model, MAC address, IP address, and operating system.

Control 2: Inventory and control of software assets

The Armis platform uses passive network monitoring to discover software running on devices in your environment. This discovery includes software running on managed computers, BYOD devices, and the increasingly large number of connected "things" like video cameras, thermostats, interactive voice assistants, medical devices, industrial controls, and more.

THE ARMIS DEVICE KNOWLEDGEBASE

The Armis Device Knowledgebase is a crowd-sourced knowledgebase that tracks and continuously analyzes the characteristics and behavior of over 500 million devices daily.

The Knowledgebase stores individual known-good baselines for every device. The Armis platform uses this information to detect deviations that could indicate increased risk, security gaps, potential threats, or possible compromises.

Since the Armis Device Knowledgebase uses crowd-sourced device and threat information, the Armis platform has no learning period, enabling it to detect threats faster and with fewer false positives.

Control 3: Continuous vulnerability management

When a device is first detected, the Armis platform uses information from the Armis Device Knowledgebase to identify its known hardware and software vulnerabilities. The platform then performs continuous vulnerability assessments based on a device's activities and behavior.

Device characteristics, vulnerabilities, and behaviors contribute to the risk score the Armis platform maintains for every device. When the platform detects new hardware or software characteristics or vulnerabilities, or abnormal behavior like known attack patterns, it updates the device risk score and, depending on customer-defined risk thresholds and policies, triggers alerts and actions that mitigate and help manage risk.

Control 8: Malware defenses

Traditional anti-malware defenses can not protect IoT devices because they use signature-based detections rather than behavioral analysis. From the moment the Armis platform detects a device, the platform's cloud-based threat detection engine starts identifying abnormal behavior that could indicate unusual software (e.g., malware or ransomware) running on a device.

Control 9: Limit & control of network ports, protocols & services

The Armis platform monitors device communications passively and associates active ports, services, and protocols to the hardware assets in the asset inventory. The Armis policy engine can alert or remediate (e.g., quarantine) whenever the platform observes a device utilizing unauthorized ports, protocols, or services.

Control 11: Secure configurations for network devices like firewalls, routers, & switches

The Armis platform can detect unencrypted Wi-Fi traffic, which indicates a misconfiguration in your wireless access points.

Control 12: Boundary defense

The Armis platform continuously monitors all connections in your environment and alerts you if a device has connected across a boundary. This detection includes connections that occur within your network and off-network connections, such as a corporate computer mistakenly connected to a rogue access point. The platform detects unintended network bridges and open (unsecured) hotspots often included in modern printers.

The Armis platform's boundary defense is effective on wired, Wi-Fi, and IoT wireless protocols such as Bluetooth, NRF, Zigbee, etc. Traditional network firewalls have no visibility to these points of data leakage, which is why the platform is uniquely valuable for this Critical Security Control.

Control 15: Wireless access control

The Armis platform can provide a complete inventory of all authorized and unauthorized (rogue) wireless access points in your enterprise airspace. The platform monitors all wireless connections in your airspace and detect unintended network bridges and open (unsecured) hotspots frequently found in modern printers. As well, the platform monitors Wi-Fi (802.11) and ten other wireless protocols like Bluetooth, NRF, Zigbee, Z-Wave, etc.

ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged "smart" devices like video cameras, smart TVs, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on & off the network that connect and communicate via wired, Wi-Fi, Bluetooth, Zigbee, and many other common protocols that are invisible to legacy security systems. Armis continuously analyzes endpoint behavior to identify risks and attacks, to protect critical information and systems. Through integration with your switches and wireless LAN controllers, as well as your existing security enforcement points like Cisco and Palo Alto Networks firewalls or network access control (NAC) products, Armis can quarantine suspicious and malicious devices.

©2021 Armis, Inc. Armis is a registered trademark of Armis, Inc. All other trademarks are the property of their respective owners. All rights reserved.

20210310-1