WHITE PAPER

Armis Support for Health Industry Cybersecurity Practices (HICP) 2023 Edition

Quick Takeaways

- Align IT security with HICP 2023
- Inventory every connected device to your network
- Prioritize vulnerabilities for greatest reduction in attack surface
- Identify abnormal behavior indicative of compromise or attack
- Integrate with existing tool sets for workflows automations, network segmentations and patch management

The Healthcare Industry Cybersecurity Practices (HICP) document from Health and Human Services (HHS) has been updated for 2023 to enable healthcare organizations to prioritize resources and focus on the most pressing threats, and mitigations, to the healthcare sector.

Covering the top five threats, and the top ten cybersecurity best practices, the document is split into two technical volumes; volume one highlights best practices for small healthcare organizations and volume two highlights best practices for medium to large organizations.

In this document we will combine the best practices for all organizations into a single document.

Securing Connected Care

Connected devices are growing at an unprecedented rate in healthcare. While HICP 2023 mainly focuses on medical devices and traditional endpoints and servers, it is critical to note that an increasing footprint of IoT and OT devices are also connected to the same network, and are also a readily exploitable attack vector. An average patient may encounter parking systems, door security, security cameras, elevators, the heating and cooling of a building etc. before coming into contact with a medical device. In fact, research from Armis showed that 56% of IP cameras in healthcare environments have unpatched high or critical severity CVE's.

The Armis Centrix™ platform provides visibility into every connected asset - medical, IoT, IT and OT (building management systems, HVAC etc). Armis is the industry's most comprehensive asset visibility and security platform, enabling healthcare providers to identify and secure the devices and technologies that are the foundation of connected care innovation.

The Armis Asset Intelligence Engine tracks anonymized data from over 5 billion protected assets to identify a broad range of assets and highlight abnormal traffic or configurations that could indicate compromise. Trusted by healthcare organizations worldwide, Armis helps customers protect against unseen operational and cyber risks, increase medical device efficiencies, optimize use of resources, and safely innovate with new technologies to deliver improved patient care.

This document will help healthcare organizations meet many of the recommended steps in HICP 2023 including:

- Inventory of every connected assets
- Vulnerability assessment
- Enforcing network segmentation policies for all devices
- Security incident identification and response

For more information on Armis for healthcare please visit www.armis.com and request a demo.

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-3	Manage administrative accounts	Armis can display user access rights and leverage integrations to help facilitate review of access to applications / sensitive systems
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-4	Remove unnecessary administrative accounts	Armis can display user access rights and leverage integrations to help facilitate review of access to applications / sensitive systems
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-5	Audit your software applications	Armis is able to identify and report on configurations through integrations
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-6	Always keep your endpoints patched	Armis is able to provide a gap analysis identifying devices with out of date or vulnerable patch versions
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-7	Implement Antivirus software	Armis can identify if devices connected to the internet have antivirus or antimalware software installed or not. Armis can compare its inventory with that of a security platform and identify any misconfigured or failed installs
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-8	Remove End of Life (EOL) operating systems	Armis is able to identify and report on device operating system versions. Risk scoring incorporates EOL status
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-10	Enable endpoint encryption	Armis is able to report on endpoint encryption status including BitLocker through integrations
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-9	Enable Network Firewalls	Armis can provide a device inventory of all firewalls to supply evidence of deployment
4	2.S.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-11	Enable MFA for remote access	Armis can help identify (through integration) where user accounts are lacking MFA.
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-7	Establish a unique account for each user	Armis can display user access rights and leverage integrations to help facilitate review of access to applications / sensitive systems

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-8	Limit the use of shared or generic accounts	Armis can display user access rights and leverage integrations to help facilitate review of access to applications / sensitive systems
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-9	Tailor access to the needs of each user	Armis can display user access rights and leverage integrations to help facilitate review of access to applications / sensitive systems
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-10	Terminate user access as soon as the user leaves your organization	Armis can support this by real time reports to identify user accounts which have not been terminated or still have access after having exited the organization
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-12	Provide role-based access	Armis can display user access rights and leverage integrations to help facilitate review of access to applications / sensitive systems
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-13	Periodic review of access	Armis can display user access rights and leverage integrations to help facilitate review of access to applications / sensitive systems
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-14	Configure systems and endpoints with automatic lock and log-off	Armis can identify assets that support this via MDS2
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-16	Use multi-factor authentication	Armis can help identify (through integration) where user accounts are lacking MFA.
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-16	Implement MFA for VPN Access	Armis can help identify (through integration) where user accounts are lacking MFA.
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-18	Restrict use of elevated privi-leged accounts	Armis can help identify breaches in the usage parameters for elevated accounts such as time of use, or scope of assets.
5	3.S.A	Basic Access Management	Basic user account configuration and provisioning procedures	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-19	Disable inbound Remote Desktop Protocol (RDP	Armis can monitor for inbound connections of remote access protocols.

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
9	5.S.A	Inventory	Conduct and manage an inventory of IT Assets	ID.AM-1		Armis can identify, classify and provide a complete inventory of hardware and software assets for the organization whether they are on-prem, cloud, or remote. Armis has the ability to assign business criticality / impact and owners of each asset. Armis is able to capture the following: • Asset ID (primary key) • Host Name • Operating System • Media Access Control (MAC) Address • IP Address • User Last Logged On The following information can also be tracked and maintained • Purchase Order • Deployed To (User) • Purchase Date • Cost • Physical Location
10	5.S.B	Procurement	Keep asset inventory up to date with procurement of new devices	ID.AM-6		As new devices are added to the network Armis can automatically identify and classify those hardware and software assets. The near real-time view of the assets within the organization can be exported to CMDB and CMMS systems to ensure an up to date centralized record.
11	5.S.C	Decommissioning	Securely remove devices from the circulation	PR.IP-6, PR.DS-3		Armis is able to provide reports highlighting devices that haven't been used for a period of time to support decommissioning. Armis can also quarantine devices to remove any exposure from risk while devices await decomisisoning
12	6.S.A	Network Segmentation	Segment devices into various networks, restricting access	PR.AC-5, PR.AC-3, PR.AC-4, PR.PT-3		Armis can assist in the creation and enforcement of network segmentation policies including the identification of device types that are not meeting the established segmentation rules. ACLs can be exported enabling NAC solutions to automatically segment devices into the correct network segment as they are detected improving security

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
14	6.S.C	Intrusion Prevention	Implement and operate an IPS system to stop well known cyber attacks	PR.IP-1		Armis is able to alert on known exploits and leverage integrations to provide better coverage / visibility than traditional IPS systems alone
15	7.S.A	Vulnerability Management	Discover technical vulnerabilities (host and web) and remediate	PR.IP-12		Armis can identify assets communicating on the network. Through integrations with threat feeds Armis can automatically identify CVE's and FDA recalls associated with each asset, score the risk and degree of vulnerability, and provide guidance on which are the most urgent vulnerabilities to attend to based on settings, policies, in the wild exploitation etc.
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-9	Roles and responsibilities	Armis can aid in incident response by highlighting the highest risk or most vulnerable devices enabling response teams to assign resources
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-10	Incident Commander	Armis can provide reports and dashboards to reduce the person hours required creating and maintaining incident reports.
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-11	Executive/ Senior Leadership	Armis can provide reports and dashboards to reduce the person hours required creating and maintaining incident reports
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-12	Cybersecurity Teams - Teams comprised of people with cybersecurity expertise who understand attacks, vulnerabilities, and the methods by which threat vectors are exploited. They provide technical knowledge and detail to technical teams and execute procedures in the playbook.	Armis can aid in incident response by highlighting the highest risk or most vulnerable devices enabling response teams to assign resources

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-13	Technical Teams - Teams comprised of SMEs for the technologies that have been compromised and who are engaged in developing and implementing the response. These SMEs may be system owners, system administrators, or other individuals with specialized IT expertise. They take instruction from the cybersecurity teams as part of the playbook execution.	Armis can aid in incident response by highlighting the highest risk or most vulnerable devices enabling response teams to assign resources
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-14	Legal Teams	Armis can provide reports and dashboards to reduce the person hours required creating and maintaining incident reports
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-15	Emergency Management	Armis can provide reports and dashboards to reduce the person hours required creating and maintaining incident reports.
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-17	Privacy and Compliance Team	Armis can provide reports and dashboards to reduce the person hours required creating and maintaining incident reports.
16	8.S.A	Incident Response	Establish procedures for managing cyber attacks, especially malware and phishing	PR.IP-18	Other external teams	Armis can provide reports and dashboards to reduce the person hours required creating and maintaining incident reports.

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
18	9.S.A	Medical Device Security	Secure medical devices within your practice	PR.PT		Armis can provide guidance through IP connections and ACL's for network segmentation to help secure the medical devices. Armis can provide guidance through IP connections and ACL's for network segmentation to help secure the medical devices. Armis can also perform real time risk assessment to streamline remediation and mitigation
19	10.S.B	Cybersecurity Risk Assessment and Management		ID.RA		Armis can identify the medical devices and provide risk and vulnerabilty scores for those devices. Utilizing the MDS2 documents Armis can narrow the focus to those with PHI.
19	10.S.C:	Cyber Insurance		ID.RM, ID.GV		Demonstarting real time awareness of inventory, risk and vulnerability exposure can be a part of cyber insurance cost reduction
22, 23	1.M.B, 1.L.B	MFA for Remote Email Access	Enabling multi-factor authentication for remote email access	PR.AC-7		Armis can help identify (through integration) where user accounts are lacking MFA.
34, 35	3.M.C, 3.L.C	Authentication	Implement and monitor secure authentication for users and privileged accounts	PR.AC-7		Armis can help identify (through integration) where user accounts are lacking MFA.
36, 37	3.M.D, 3.L.C	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources	PR.AC-3, PR.AC-7		Armis can help identify (through integration) where user accounts are lacking MFA.
38, 39	4.M.A, 4.L.A	Classification of Data	Classify data by sensitivity	ID.AM-5		Armis can help identify resources with PHI
40, 41	4.M.B, 4.L.B	Data Use Procedures	Implement data use procedures based upon data classification	ID.GV-1		Armis provides custom policy/ report/dashboards to enable monitoring of compliance, anomalous behaviors, unencrypted data, PII / PHI transmission.

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
42, 43	4.M.C, 4.L.C	Data Security	Implement data protections based upon data classification	PR.DS, PR.DS-1, PR.DS-2, PR.IP-6, PR.DS-5		Armis provides custom policy/ report/dashboards to enable monitoring of compliance, anomalous behaviors, unencrypted data, PII / PHI transmission.
44, 45	4.M.D, 4.L.D	Backup Strategies	Backup important data in the case of loss of access, or loss of data	PR.IP-4		Armis provides custom policy/ report/dashboards to enable monitoring of compliance, anomalous behaviors, unencrypted data, PII / PHI transmission.
46, 47	4.M.E, 4.L.E	Data Loss Prevention (DLP)	Implement technology and processes to automate security of sensitive data	PR.DS-5		Armis provides custom policy/ report/dashboards to enable monitoring of compliance, anomalous behaviors, unencrypted data, PII / PHI transmission.
48, 49	5.M.A, 5.L.A	Inventory of Endpoints and Servers	Establish an asset management inventory database and roll out	ID.AM-1		Armis can identify, classify and provide a complete inventory of hardware and software assets for the organization whether they are on-prem, cloud, or remote. Armis has the ability to assign business criticality / impact and owners of each asset
50, 51	5.M.B, 5.L.B	Procurement	Keep asset inventory up to date with procurement of new devices	ID.AM		As new devices are added to the network Armis can automatically identify and classify those hardware and software assets. The near real-time view of the assets within the organization can be exported to CMDB and CMMS systems to ensure an up to date centralized record.
54, 55	5.M.D, 5.L.D	Decommissioning Assets	Securely remove devices from the circulation	PR.IP-6, PR.DS-3		Armis can identify operating system versions of all devices on the network and highlight EOL operating systems, vulnerabilities and risks.
58, 59	6.M.B, 6.L.B	Network Segmentation	Establish a network segmentation strategy with clearly defined zones	PR.AC-5		Armis can assist in the creation and enforcement of network segmentation policies including the identification of device types that are not meeting the established segmentation rules. ACLs can be exported enabling NAC solutions to automatically segment devices into the correct network segment as they are detected improving security

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
62, 63	6.M.D, 6.L.D	Web Proxy Protection	Protect end users browsing the web with outbound proxy technologies	PR.AC-3, PR.AC-5		Armis can detect malicious connections and then invoke network controls to help mitigate risks
66, 67	7.M.A, 7.L.A	Host/Server Based Scanning	Discover host based technical vulnerabilities	DE.CM-8		Armis utilises passive analysis of the network to identify critical or high risk vulnerabilities
68, 69	7.M.B, 7.L.B	Web Application Scanning	Discover web based technical vulnerabilities	DE.CM-8		Armis utilises passive analysis of the network to identify critical or high risk vulnerabilities
70, 71	7.M.C, 7.L.C	System Placement and Data Classification	Determine vulnerability risk based on system classification and location	ID.RA-5		Armis utilises passive analysis of the network to identify critical or high risk vulnerabilities
72, 73	7.M.D, 7.L.D	Patch Management, Configuration Management, Change Management	Routinely patch and mitigate vulnerabilities	PR.IP-1, PR.IP-3, PR.IP-12		Armis can identify critical or high risk vulnerabilities and provide the remediation of those vulnerabilities when available, or also assist in mitigating controls such as segmentation.
76, 77	8.M.B, 8.L.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks	PR.IP-9, RS.AN-1, RS.MI-1, RS.MI-2, RC		Armis can aid in incident response by highlighting the highest risk or most vulnerable devices enabling response teams to assign resources
78, 79	8.M.C, 8.L.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information	ID.RA-2		Armis partners with and contributes to a number of security threat intel feeds. Armis also receives information from vendors, government agencies and threat research organizations to support risk and vulnerability scoring
80, 81	9.M.A, 9.L.A	Medical Device Management	Set a strategy for managing the security of medical devices, utilizing existing processes	PR.MA-2		Armis can be a core part of any medical device security strategy in terms of discovery, on going monitoring, threat intelligence and executive reporting.
82, 83	9.M.B, 9.L.B	Endpoint Protections	Configure and secure medical devices based on 6 steps	PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1	AV software	Though many medical devices cannot have AV installed, Armis is able to identify versions of AV software where applicable and perform a gap analysis to identify version drift or missing AV. For devices that can't install AV Armis is able to identify devices and ensure they have the correct network segmentation applied

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
82, 83	9.M.B, 9.L.B	Endpoint Protections	Configure and secure medical devices based on 6 steps	PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1	Local firewalls	Armis is able to identify all traffic coming from and going to a medical device. This can be utilized to identify any communications with devices that should not be permitted and to identify anomolous behaviour which could indicate compromise or attack of the device
82, 83	9.M.B, 9.L.B	Endpoint Protections	Configure and secure medical devices based on 6 steps	PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1	Encryption	Armis is able to identify whether a device is encrypted and whether unencrpyted PHI is being communicated
82, 83	9.M.B, 9.L.B	Endpoint Protections	Configure and secure medical devices based on 6 steps	PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1	Application allowlist	Armis is able to identify applications running on a device through the network traffic coming from that application
82, 83	9.M.B, 9.L.B	Endpoint Protections	Configure and secure medical devices based on 6 steps	PR.MA-2, DE.CM-4, PR.AC-5, PR.DS-1, PR.AC-1, PR.IP-1	Default password changes	Armis is able to identify devices utilizing default passwords
82, 83	9.M.B, 9.L.B	Endpoint Protections	Configure and secure medical devices based on 6 steps	PR.IP-9, RS.AN-1, RS.MI-1, RS.MI-2, RC	Routine Patching	Armis is able to identify and report upon patch versions as well as highlighting vulnerabilities associated with patches in order to direct security teams to the highest risk devices
84, 85	9.M.C, 9.L.C	Identity and Access Management	Ensure authentication and remote access is managed	PR.AC, PR.AC-7, PR.AC-4		Armis can help identify (through integration) where user accounts are lacking MFA.
86, 87	9.M.D, 9.L.D	Asset Management	Inventory hardware and software of medical devices	ID.AM, ID.AM-1, PR.IP-6		Armis can identify, classify and provide a complete inventory of hardware and software assets for the organization whether they are on-prem, cloud, or remote. Armis has the ability to assign business criticality / impact and owners of each asset
88, 89	9.M.E, 9.L.E	Network Management	Segment medical devices on dedicated, highly restrictive networks	PR.AC-5		Armis is able to detect and positively identify all devices communicating in the network. Policies can ensure that medical devices are automatically segmented through integration with existing NAC tools

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
90, 91	10.M.A, 10.L.A	Policies	Establish cybersecurity policies and a default expectation of practices	ID.GV-1		Armis has a powerful policy engine that can be used to enforce cybersecurity poilicies. Integrations with security, workflow and other platforms provide automations to enforce policies through existing processes and tools.
96	2.L.B	Mobile Device Management	Leverage MDM tools to secure mobile devices	PR.AC-3		Armis can identify MDM agent software running on mobile devices and identify missed or non compliant devices
102	3.L.B	Authorization	Authorize access based on role (RBAC) or attribute (ABAC	PR.AC-6, PR.AC-4		The Armis console supports RBAC
105	4.L.A	Advanced Data Loss Prevention	Implement advanced technology and processes to automated security of data	PR.DS-5		Armis supports automation of data security through identification of indicators of attack and compromise, risk scoring and vulnerability management. Integration with many security and automation platforms enable seamless protection of information
106	4.L.B	Mapping of Data Flows	Identify and document data storage and data flows between systems	ID.AM-3, DE.AE-1		Armis provides detailed traffic flows highlighting malicious domains, known exploits and abnormal device behavior
107	5.L.A	Automated Discovery and Maintenance	Leverage automation to keep asset inventory details up to date	PR.IP-5, ID.SC-3		Armis can identify, classify and provide a complete inventory of hardware and software assets for the organization whether they are on-prem, cloud, or remote. Armis has the ability to assign business criticality / impact and owners of each asset
108	5.L.B	Integration with Network Access Control	Catch endpoints on the network that fall out of compliance or are outliers	PR.MA-1, PR.MA-2, PR.DS-3		Armis can assist in the creation and enforcement of network segmentation policies including the identification of device types that are not meeting the established segmentation rules. Armis can also support gap analysis and security hygiene analysis to identify EOL and EOS operating systems • Integrate all medical, IoT, IT and OT assets into a single platform • Quickly identify vulnerabilities for any device and guide you on prioritization and available fixes • Identify the indicators of attack and compromise to re-duce the risk of ransomware cyber attacks

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
109	6.L.A	Additional Network Segmentation	Further implement segmentation strategies for remote VPN access to data center	PR.AC-5, PR.AC-6, PR.PT-4		Armis can provide visibility into traffic and devices accessing the data center
110	6.L.B	Command and Control Monitoring of Perimeter	Monitor for malicious outbound Command and Control traffic	DE.CM-1, DE.CM-7		Armis identifies traffic targeting command and control servers
111	6.L.C	Anomalous Network Monitoring and Analytics	Monitor for anomalous network traffic based on analytics and baselines	DE.CM-1, DE.CM-7		Armis monitors more than 3billion devices through the Unified Asset Intelligence Engine. This enables Armis to identify anomolous behavior without a learning period for every device
113	6.L.E	Network Access Control (NAC)	Ensure endpoints are secure on the network through automated tools	PR.AC-5, PR.AC-6, PR.AC-4		Armis can assist in the creation and enforcement of network segmentation policies including the identification of device types that are not meeting the established segmentation rules
115	7.L.B	Remediation Planning	Implement formal mechanisms for remediating vulnerabilities and risks	PR.IP-12		Armis policies and automation integrations can be part of remediation processes
117	8.L.B	Advanced Information Sharing	Share and receive threat intelligence information from partner organizations	ID.RA-2		Armis can create executive reports that identify malicious network activity that could be shared with other organizations
118	8.L.C	Incident Response Orchestration	Automate the manual response of IR playbooks through advanced tools	PR.IP-9		Armis can aid in incident response by highlighting the highest risk or most vulnerable devices enabling response teams to assign resources. Armis can also automate responses through integration with security, ticket management and other platforms
119	8.L.D	Baseline Network Traffic	Establish digital footprints on systems and alert when they deviate	ID.AM-3, DE.AE-1		Armis monitors more than 3billion devices through the unified asset intelligence engine. This enables Armis to identify anomolous behavior without a learning period for every device

index #	SP #	SP Title	Short Description	NIST CSF XWALK	Security Controls	How Armis Helps
120	8.L.E	User Behavior Analytics	Establish baseline patterns of user access and alert when they deviate	PR.PT-1, DE.AE-1		Armis monitors more than 3 billion devices through the Unified Asset Intelligence Engine. This enables Armis to identify anomolous behavior without a learning period for every device
122	9.L.A	Vulnerability Management	Carefully identify vulnerabilities on medical devices, and remediate accordingly	ID.RA-1, PR.IP-12, ID.RA-5, RS.CO-5, DE.CM-8		Armis can identify assets communicating on the network. Through integrations with threat feeds Armis can automatically identify CVE's and FDA recalls associated with each asset, score the risk and degree of vulnerability, and provide guidance on which are the most urgent vulnerabilities to attend to based on settings, policies, in the wild exploitation etc.
123	9.L.B	Security Operations and Incident Response	Ensure IR playbooks account for patient safety implications of connected medical devices	PR.IP-9, DE.CM-8, DE.CM-1, DE.CM-7		Armis can aid in incident response by highlighting the highest risk or most vulnerable devices enabling response teams to assign resources
124	9.L.C	Procurement and Security Evaluations	Conduct security evaluations for newly purchased medical devices	ID.SC		As new devices are added to the network Armis can automatically identify and classify those hardware and software assets. The near real-time view of the assets within the organization can be exported to CMDB and CMMS systems to ensure an up to date centralized record.
125	9.L.D	Contacting the FDA	Contact the FDA for risk security issues that are unresolved	RS.AN-5		Armis reports can be utilized to provide suspicious activity information to other organizations and agencies

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial