Your security, our priority: Cybersecurity program

siemens-healthineers.com/support-documentation/cybersecurity

SIEMENS Healthineers

Content

Overview

Siemens Healthineers introduction

At Siemens Healthineers, we pioneer breakthroughs in healthcare. For everyone. Everywhere. Sustainably. As a leader in medical technology, our goal is to advance a world in which breakthroughs in healthcare create new possibilities while minimizing our impact on the planet. By consistently bringing innovations to the market, we enable healthcare professionals to innovate personalized care, achieve operational excellence, and transform the overall system of care. Our portfolio, spanning in vitro and in vivo diagnostics to image-guided therapy and cancer care, is crucial for clinical decision-making and treatment pathways. With the unique combination of our strengths in patient twinning1, precision therapy, as well as digital, data, and artificial intelligence (AI), we are well positioned to take on the greatest challenges in healthcare. We will continue to build on these strengths to help overcome the world's most threatening diseases, enable efficient operations, and expand access to care. We are a team of more than 73,000 Healthineers in over 70 countries passionately pushing the boundaries of what is possible in healthcare to help improve the lives of people around the world.

Our commitment to Cybersecurity

Our top-down approach to Cybersecurity ensures that a culture of Cybersecurity is embraced throughout the entire company. The Managing Board of Siemens Healthineers has designated Cybersecurity as a dedicated Governance Area with a centralized Corporate organization responsible for defining and driving Cybersecurity governance and strategy. In addition, we embed Cybersecurity resources within our businesses, geographical regions and the IT function. Leveraging our certified Cybersecurity Management System (CYSMS) we standardize processes and continuously strengthen security in our products, solutions, and supporting infrastructure.

Our Cybersecurity mission is to mitigate risk by continually improving our cyber resilience and supporting the protection of our customers through people, processes, and technology.

Shared responsibility

Siemens Healthineers (as a manufacturer of medical devices) and customers (healthcare providers) have a shared responsibility to protect medical solutions in clinical environments.

We are committed to integrating security throughout the life cycle of our products and services, starting with secure design and development practices. This is underlined by the commitment to provide relevant Cybersecurity information at the point of purchase, assisting with product and solution deployment within the customer's environment, and offering ongoing post-sale support including security patches, updates, and information, allowing customers to make informed, security-aware decisions.

Meanwhile, our customers are responsible for managing, monitoring and maintaining the environments where Siemens Healthineers products operate, as well as integrating the security features of these products into their overall Cybersecurity strategy.

Corporate control environment

Board structure

As a German stock corporation with a registered office in Munich, Siemens Healthineers is subject to German corporate law. Consequently, the Company has a two-tier management and oversight structure consisting of a **↗ Managing Board and a Supervisory Board (two-tier board structure).**

Elisabeth Staudinger, MA, is the Member of the Siemens Healthineers Managing Board responsible for Cybersecurity.

Governance, risk and internal control

The Corporate Governance Office maintains the Governance Framework which supports the Managing Board to fulfill their duty of care. The Corporate Governance Office manages all corporate regulations, as well as the Business Conduct Guidelines which are our cornerstone when it comes to complying with the law and business ethics in our daily work.

Risk management at Siemens Healthineers is based on a comprehensive, interactive and management-oriented Enterprise Risk Management (ERM) approach that is integrated into the organization and that addresses both risks and opportunities.

The Siemens Healthineers Risk & Internal Control (RIC) Organization promotes an integrated Risk and Internal Control (RIC) System, supporting the Siemens Healthineers Management Team in managing the identified risks effectively and provides reasonable assurance that the Organization's assets are safeguarded, financial reporting is reliable, and laws and regulations are complied with.

Audit

Siemens Healthineers Internal Audit conducts independent, risk-based, and objective audits covering operational, financial, IT, Cybersecurity, and regulatory compliance areas. These audits help verify the effectiveness of controls, processes, and governance mechanisms throughout the organization.

Cybersecurity organization at Siemens Healthineers

Corporate Cybersecurity and our Cybersecurity Management System (CYSMS)

Corporate Cybersecurity manages our Cybersecurity program via our global Cybersecurity Management System (CYSMS). We take a holistic approach to managing both the security of our organization and its assets , as well as the secure product life cycle of our products and services.

Our CYSMS is certified according to ISO/IEC 27001:2022 covering Governance and Assurance from the central Cybersecurity Organization. Additionally, our company extended its certification with ISO/IEC 27701:2019, Privacy Information Management System (PIMS). This outlines a framework for the management of data privacy throughout our organization and supports compliance with General Data Protection Regulation (GDPR), Health Information Portability and Accountability Act (HIPAA) and other related privacy legislation.

Furthermore, certain products, services and geographical locations have additional Cybersecurity certifications based on local regulatory and market needs.

Roles and responsibilities

The Corporate Cybersecurity organization is responsible for Cybersecurity topics throughout the organization. Led by our Corporate Cybersecurity Officer, Carlos Arglebe, the Cybersecurity team has been established to govern, coordinate, implement, and improve the Cybersecurity posture of the company.

Additional roles are defined throughout the organization. For example, there is a Cybersecurity Operations organization within IT, and there are local Cybersecurity Officers, responsible for the implementation of Cybersecurity, within their respective organizational units.

Data Privacy roles and responsibilities are established similar to the Cybersecurity structure, under the leadership of the Group Data Privacy Officer.

Policy management

Cybersecurity policies are established and maintained at Siemens Healthineers via a top-level Cybersecurity Directive, including supporting instructions (policies), procedures, baselines, and guidelines. There is also coordination with other governance areas such as Quality and Procurement to embed these Cybersecurity requirements into the respective quality management systems across the organization.

Compliance

Siemens Healthineers actively monitors and assesses emerging international standards and regulatory requirements. These are continuously integrated into our Cybersecurity policies and control frameworks to ensure ongoing compliance and meet the evolving needs and expectations of our customers.

Siemens Healthineers is also an active contributor in the development of standards and best practices.

Risk management

Cybersecurity risks are managed as part of our Cybersecurity Management System aligned with the Corporate ERM which are established on multiple levels with roles assigned with specific responsibilities for managing and owning risk entries.

- At the portfolio level, a threat and risk analysis is conducted for each product and solution in accordance with the secure development life cycle procedures. This analysis identifies the risks that potentially impact the product or product component. Identified risks are either mitigated, accepted or addressed through compensating controls before the product is released.
- At the organizational unit level, Cybersecurity risks are reported on a quarterly basis. This is supplemented by an ad-hoc escalation process for promptly addressing critical issues. All risks and opportunities are prioritized in terms of impact and feasibility, using both quantitative and qualitative criteria. Cybersecurity risks that exceed defined thresholds are escalated and tracked through the Corporate ERM process.

Cybersecurity assurance

The Corporate Cybersecurity team has defined metrics and key performance indicators (KPIs) to effectively monitor Cybersecurity performance and foster continuous improvement. Additionally, Corporate Cybersecurity performs assurance activities to evaluate the design and effectiveness of Cybersecurity implementation throughout the organization.

These efforts are complemented by independent audits carried out by the Siemens Healthineers Audit team, which includes Cybersecurity as a regular component of their audit program.

Awareness & training

The Cybersecurity Awareness & Training program at Siemens Healthineers empowers employees to familiarize themselves with the principles of information classification, safeguard sensitive data, recognize cyber threats, and promptly report potential incidents. The program includes formal training completed during onboarding and repeated annually, covering key topics such as data classification, incident response, phishing, password management, and social engineering, with a particular focus on healthcare-specific risks.

An additional component of the program is a role-based training initiative tailored to individuals with designated Cybersecurity responsibilities. This provides the foundational knowledge required to fulfill their roles effectively.

Beyond training, ongoing awareness campaigns and targeted communications help foster a strong Cybersecurity culture throughout the organization. Topics such as Clean Desk Policy, secure handling of paper documents, encrypted data transfer, and phishing prevention are emphasized to mitigate human-related risks.

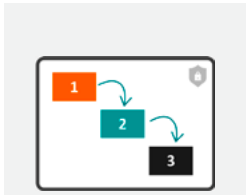
Managers are accountable for ensuring the completion of mandatory training sessions, with compliance monitored by Corporate Cybersecurity.

Third Party Management (Supplier Cybersecurity)

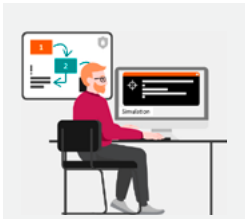
Siemens Healthineers has established policies and procedures to manage Cybersecurity risks related to suppliers and other third parties. The process includes initial risk exposure classification based on the criticality of the supplier and the sensitivity of data they interact with. This risk classification is used to define:

- Level of due diligence assessment required,
- Contract terms and legal contract reviews needed,
- Frequency of periodic assessments to ensure suppliers continue to meet Cybersecurity requirements.
- Third party reports and certifications of suppliers are subject to review during these assessments, with all identified risks managed by the business owner and monitored by the appropriate Cybersecurity team.

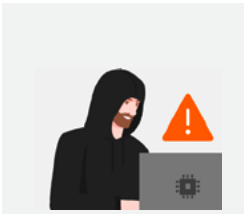
Efficiently execute and maintain your recovery plan to ensure business continuity after disruptions



Develop and maintain your Business Continuity Plan (BCP)



Test and update your plans



Continuous improvement based on lessons learned

Confirm resource availability

Streamlined incident communication: both internal and external

Incident management

An Incident Management Process is established to ensure a timely, effective, and consistent approach to handling Cybersecurity incidents throughout all Siemens Healthineers organizational units and companies, which covers, at a minimum:

- Security incidents related to Siemens Healthineers infrastructure including endpoints, offices and the Corporate network
- Security incidents related to a product or solution in a cloud environment
- Unauthorized access or disclosure of personal data including protected health information
- Security incidents at a third party supplier impacting Siemens Healthineers

Our **↗ Cybersecurity Incident Response Team (CSIRT)** leads and coordinates the response to IT and OT Cybersecurity incidents within the company, ensuring their prompt resolution by conducting the necessary investigation activities and coordinating the implementation of containment measures.

Customer Incidents that have a Cybersecurity component are managed in our customer service processes and case handling systems and our Product Security Incident Response Team (PSIRT) provides support when needed.

Business continuity & disaster recovery

We established business continuity policies and procedures to ensure ongoing information security and ICT readiness. These measures help maintain availability and redundancy of information processing facilities, and protect network systems, data, and their physical environments from relevant threats.

Siemens Healthineers provides a standardized framework including templates, training and support around each stage in the process including:

- Business Impact Analysis (BIA): Focused on identifying and evaluating the potential impacts of disruptions on business operations, specific assets or systems.
- Recovery Strategies: This phase focuses on developing strategies to recover and continue business operations after a disruption, whether it be a system level disruption or a component level failure.
- Business Continuity Plans (BCP) & Response: This phase involves creating detailed business continuity and IT disaster recovery plans and response strategies to manage and mitigate the effects of different types or combinations of disruptions.
- Testing, Verification & Exercises: We have a coordinated BCP/DR strategy over key areas of the organization.

Supporting technical and organizational measures

Operational processes are in place throughout all the core Cybersecurity domains as follows.

Human resources security

Siemens Healthineers Human Resource Security policies and procedures ensure Cybersecurity and privacy are addressed in Human Resource processes. These measures include:

- As part of the hiring process, Business Managers decide together with HR whether to carry out different types of reliability screening checks of the new employee, depending on their future role and subject to local regulations. These may include identity checks, employment and education verification and background screening/criminal history.
- An established and documented onboarding process that educates the employee on the regulations that apply to their role, which includes Cybersecurity topics. This process is monitored and managed by the country manager of a new employee.
- Assigned training modules, depending on the role and responsibilities of the employee, are managed, monitored and maintained using a corporate learning management system. The completion of the assigned modules is mandatory and traceable. As a baseline, Cybersecurity awareness, data privacy and business conduct guideline training modules are assigned to all employees.

Where there is a case of potential misconduct, employees are subject to a disciplinary review process with potential consequences depending on the nature of the misconduct.

In the case of an employee termination or change of employment, policies and procedures are in place to ensure that all previously issued physical and electronic assets are returned to the organization and that all access and access authorizations are also withdrawn from those leaving the organization within 24 hours.

Identity and access management

All identified and inventoried IT assets, including IT systems and applications, have a defined classification that dictates the level of criticality of the System or applications which then defines the required levels of authentication and authorization for Access Management. A formal process for assigning, maintaining, and revoking access rights to IT systems and applications is in place. In general, access is granted only to individuals who need it to perform their tasks.

Data classification & handling

Siemens Healthineers has an established data classification framework to assist in classifying and defining the protection measures required for each data classification level according to its business value and potential risk impact. Data protection technologies are implemented to help securely handle data.

Physical and environmental security

Furthermore, we have established physical and environmental security policies and procedures to prevent unauthorized access, damage, or disruption to its information, assets, and processing facilities. These measures are intended to minimize the risk of loss, theft, or operational interruptions.

Security contact personnel are defined for all Siemens Healthineers sites. They are responsible for the physical and organizational measures to secure personnel and properties. The measures are regularly reviewed by the on-site security organization and business departments.

Cryptographic protections

Our company provides policies, procedures, and guidelines for the use of cryptography and key management to secure and protect sensitive information from unauthorized access, ensuring confidentiality, integrity, and authenticity.

Asset management

The organization has established policies and procedures to identify and protect its assets throughout their life cycle. These include defining appropriate safeguards and responsibilities to prevent unauthorized disclosure, modification, removal, or destruction of information.

Workstations, laptops, and mobile devices that access company resources or are issued to employees are centrally inventoried and managed by the IT function.

A formal process ensures that all issued physical and electronic assets are returned when individuals terminate or change their relationship with the organization.

Applications and supporting infrastructure are managed through a centralized asset management process. All assets are recorded and/or tagged and include details about deployment, ownership, and classification.


Interesting ...

Endpoint security

All endpoint devices have a range of protection technologies installed depending on their function and the classification of the data they process to enable Siemens Healthineers to effectively protect data managed within our organization. This includes the deployment of Endpoint Detection and Response (EDR) solutions and technologies to limit privileged access.

Cloud security

Siemens Healthineers has established policies, procedures, and guidelines to support secure operations in the cloud. This includes standardized security baselines for cloud-hosted systems, structured processes to manage third-party cloud service providers, and centralized monitoring capabilities through our IT Cybersecurity Operations team. These measures enable proactive oversight and protection of assets across various cloud platforms.

Mobile device management

All mobile devices that access company information are required to be enrolled in the Corporate Mobile Device Management solution and comply with a minimum set of Cybersecurity requirements. This enforces device level controls such as minimum authentication requirements, and the implementation of security updates.

Network security

Siemens Healthineers has a Zero Trust architecture strategy that operates on the premise that no one is trusted by default. Instead, it requires verification of every identity trying to access corporate digital resources, whether they are in the office or are accessing them from a remote location, and has different levels of security dependent on the asset or information being hosted and accessed.

Operational & embedded technology

To secure operational technology (OT) in manufacturing environments, the organization has defined specific policies and procedures. These include segregation of functional processes and equipment, as well as restricted access controls to protect critical systems.

OT-specific services have been developed to address the unique requirements of these environments. These include endpoint protection for IoT devices, factory-focused vulnerability management, and anomaly detection capabilities for OT networks.

Configuration management

Established industry hardening standards and/or vendor guidance for used products, software, and hardware components are applied to ensure security.

Backup processes

Dependent on the functionality, classification and security requirements of a system or asset, a range or backup strategies are available to ensure availability and integrity or our backups. These backups include data and configuration settings, are defined, documented, and validated within the operational environment. The intervals and type of backups are defined based on the acceptable amount of data loss during adverse situations considering a business and operational perspective.

Continuous monitoring and response

The Security Operations Center has continuous monitoring processes in place across our corporate infrastructure covering Cloud Security, Network Security and Endpoint security. Through this combination of people, processes, and technology Siemens Healthineers can detect and respond to suspicious or anomalous activities or unauthorized changes in an efficient streamlined process.

Vulnerability and patch management

Policies and procedures are in place to support vulnerability scanning of corporate infrastructure and public-facing environments. This helps identify potential risks and enables effective mitigation as part of the vulnerability management program. Enterprise processes and tools ensure regular patching and follow-up on vulnerabilities found in IT and OT assets.

Penetration testing

Siemens Healthineers penetration testing team regularly tests enterprise assets, including applications, IT infrastructure, manufacturing and R&D environments, as well as Customer Service solutions. This covers both internal assets and those accessible from the Internet. The selection of assets for testing is based on various factors, such as their exposure and the sensitivity of the data they store, process, or generate[1].

[1] *See Penetration Testing White Paper for additional information*

Protecting the Siemens Healthineers portfolio

Digital Services

Protecting our customers' services and data is a top priority, which is why we apply a holistic approach that spans from solution design through to day-to-day operations. Our cloud-based solutions are hosted on certified infrastructures such as Microsoft Azure and Amazon Web Services (AWS).

Several of our services are certified to ISO/IEC 27001:2022, the globally recognized standard for information security management. In addition, we pursue regional and country-specific attestations to demonstrate compliance with local requirements and customer expectations.

We remain committed to continuously strengthening our safeguards and adopting both international and regional standards as they evolve.

Cybersecurity throughout the life cycle

Cybersecurity is a critical quality requirement and is directly linked to patient safety. It plays a key role in protecting the confidentiality, integrity, and availability of products and services. Cybersecurity considerations are integrated throughout the entire product life cycle, including the initial concept and development phases, deployment, operational use, and final decommissioning. This applies whether the solution is implemented within a customer's infrastructure or provided as a service.

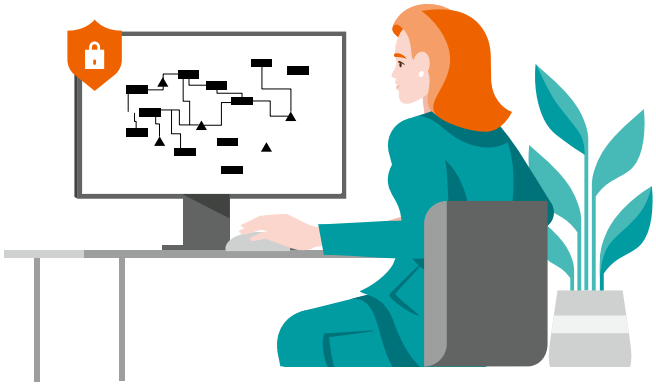
Relevant policies and procedures to support a secure product life cycle management process are integrated within the quality management systems (QMS) of the organizational units responsible for product development and maintenance, as well as those responsible for sales and service.

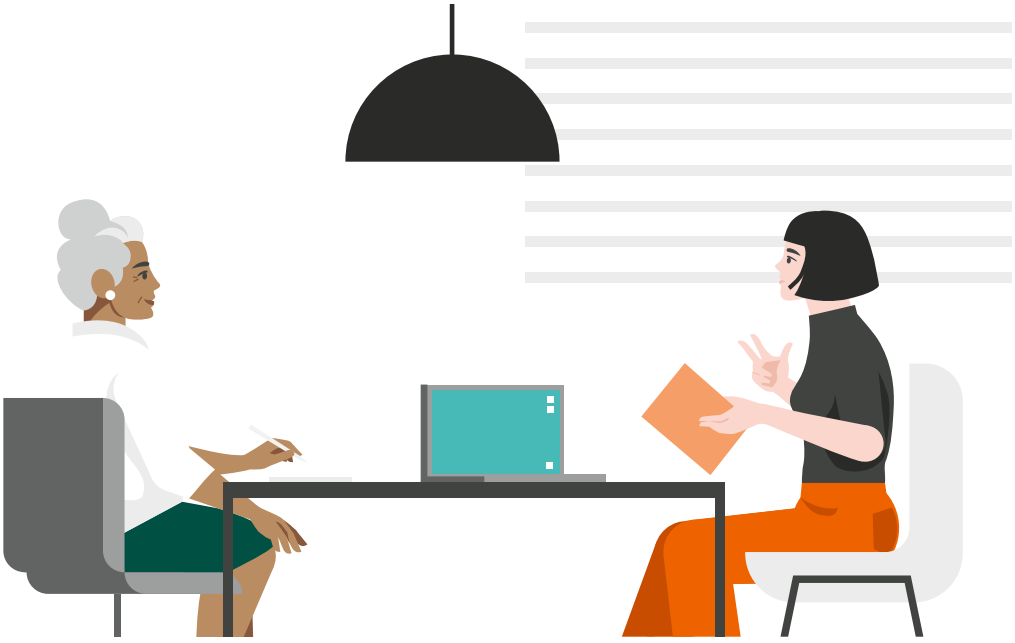
Security by design

Cybersecurity Officers are responsible for the implementation of Cybersecurity in each organization. They are supported by Cybersecurity Experts during the supported lifetime of the product/service. Siemens Healthineers leverages a global program to train and grow a pool of Cybersecurity professionals to meet the high demand in competence.

Cybersecurity requirements

Corporate Cybersecurity defines and maintains a repository of Cybersecurity requirements for products and services that are appropriate for meeting the legislative and regulatory requirements in the Healthcare industry and regional markets that we serve. These Cybersecurity requirements are evaluated during the product development life cycle to determine their applicability and traced to either implementation or to a compensating control.





Threat and risk analysis

In addition to the general cybersecurity requirements being integrated into a product's specification, a product specific Threat and Risk Analysis (TRA) is conducted to identify threats arising from the product's intended clinical use, its design, and its intended operating environment. Identified mitigations are then incorporated into the product or service requirements.

System hardening

Systems are hardened to an appropriate secure configuration based on regulatory requirements, relevant standards, and customer needs. For example, systems that are intended to be sold to United States Department of Defense are hardened to the U.S Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). Hardening is also applied to cloud-based offerings.

Security testing

Security testing ensures that the protection goals and security quality gates are effectively met. It involves a combination of various security testing activities, which may include Software Composition Analysis (SCA), Static Application Security Testing (SAST), Vulnerability Scanning, Dynamic Application Security Testing (DAST), Compliance Testing, Fuzz Testing, Penetration Testingy[2], Bug Bounty.

[2] *See Penetration Testing White Paper for additional information*

Deployment, operations, monitoring and service

Siemens Healthineers provides various service operational models that include Cybersecurity tasks and functions that assist in the management and upkeep of our products and services:

Deployment

During the deployment of products into customer environments, we provide support for installation verification and configure device features according to your requirements, such as:

- Integrity checks to verify installation packages
- User management setup for assigning roles to your staff
- Individualized credentials
- Activation of encryption to protect against machine theft
- Secured connection to peer systems, e.g. DICOM archive[3]

Shared responsibility

The US FDA defined medical device security as a shared responsibility amongst all involved parties, mainly between manufacturers and health care delivery organizations. While Siemens Healthineers works on providing Cybersecurity in products and services, the following complementing controls need to be provided by the operating organization as they are outside of the device:

- Protecting the device from unauthorized physical access (→ physical controls)
- Minimize visibility and attack surface (→ network controls)
- Security awareness and procedures in the workforce (→ organizational controls)
- Keeping the device software in a supported state by means of timely updates and upgrades

Vulnerability management

During the product and service support period, Siemens Healthineers will continuously monitor emerging vulnerabilities that affect third party components incorporated into the package, this in order to assess their impact on its security posture. This process takes into consideration the FDA[4] post-market guidance[5] and industry best practices.

For customers, the Security Profiles feature included in teamplay Fleet provides a transparent overview about device specific vulnerabilities and associated risks and required activities[6].

Coordinated disclosure of vulnerabilities

Collaboration with third parties like external researchers for coordinated vulnerability disclosure is well established practice in the Cybersecurity community. Siemens Healthineers maintains a process for **↗ coordinated vulnerability disclosure.**

Security patches, updates and upgrades

We regularly provide validated Cybersecurity updates. Patch delivery takes place through various mechanisms, including via Smart Remote Services (SRS) or Cybersecurity Profiles in teamplay Fleet (→ Anytime Software Update).

[3] *based on the specific configuration of the product*
[4] *Food and Drug Administration of the United States (FDA)*
[5] ***↗ Post-market Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff (fda.gov)***
[6] *See* ***↗ Vulnerability Management White Paper*** *for additional information*

Remote support

Siemens Healthineers provides remote support services through secure and validated infrastructures, providing our customers with:

- Assurance that the remote service identifies the full functionality of our products and does not impact the operational functionality of these products during remote connection
- Assurance that the Siemens Healthineers resource connecting into our product in their environment is a valid and authorized Siemens Healthineers employee, as registered in our Access Management system and confirmed through multi-factor authentication.
- Providing our customers with confidence that we implement industry-standard Cybersecurity checks, including robust encryption and effective measures to reduce the risk of man-in-the-middle attacks.
- Faster response times and improved uptimes to enable better patient care

Cybersecurity information transparency for customers

Siemens Healthineers products are either installed on site or connected to a customer facility. To assist our customers in assessing the risks associated with connecting our products to their infrastructure, Siemens Healthineers provides the following Cybersecurity information regarding the configuration of our products and our remote support services:

- Security Whitepaper describing the Cybersecurity features and checks included in the product or service, which also contains:
  - Product Network Integration Diagram
  - Port and Protocols used by the product or service
  - MDS^2 (Manufacturer Disclosure Statement for Medical Device Security)
  - SBOM (Software Bill of Materials)
- General Cybersecurity guidance, such as
  - Secure environment configuration recommendations
  - General product Administration Guides (where available)

teamplay Fleet

teamplay Fleet[7] is the self-service portal for fleet management that helps our customers manage their equipment from Siemens Healthineers.

teamplay Fleet offers a wide range of functionalities, helping customers to manage Cybersecurity holistically:

- Dashboard, fleet, and equipment-specific view
- Maintenance handling, including service tickets, end-of-support, and system updates
- Cybersecurity information:
  - Security Whitepaper
  - Vulnerability Assessments and mitigations
  - Options & Upgrades
  - Software Bill of Materials (SBOM)
  - Software Status (Software Version and Operating System)
- Configurable publication alerts and custom email notifications
- Connection to document library and downloadable reports

[7] myVarian is the teamplay Fleet equivalent customer portal for Varian products and services.

Siemens Healthineers Headquarters
Siemens Healthineers AG
Siemensstr. 3
91301 Forchheim, Germany
Phone: +49 9191 18-0
siemens-healthineers.com

Published by Siemens Healthineers AG · QR700028899 v1.0 · 1025 online only ·