



Industrial cybersecurity



**Life Science equipment
to support secure operation**

Contents

NIS2 (Network and Information Systems Directive) 3

Which sectors are affected by NIS2? 3

How to comply with NIS2? 3

How IEC 62443 standard supports NIS2 directive? 4

Directive CRA (2024/2847) & Machinery Regulation (2023/1230) 6

Comparison between the CRA (2024/2847) and the Machinery Regulation (2023/1230) 6

Siemens, Rockwell Automation, B&R ABB Group / WIS configuration 8

Getinge Main Control Board (ULTIMA washers, PACS Sterilizer) 8

ULTIMA 8

PACS 8

Annex 9

Security disclaimer

Our white paper has been compiled with great care. It contains information about the current Getinge interpretation of the new EU Machinery Regulation, the second EU Directive on Network and Information Security NIS2 and the Cyber Resilience Act. While every effort has been made to ensure the information provided is accurate, we cannot accept liability for the accuracy and entirety of the information provided, except in the case of gross negligence. In particular, it should be noted that statements do not have the legal quality of assurances or assured properties. We are grateful for any feedback on the contents.

Getinge provides washers, sterilizers, and isolators based on strongest components solutions that support the secure operation of an IACS (Industrial Automation and

Control System). To protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines, and networks. Such systems, machines, and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Getinge strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates, may increase a customer’s exposure to cyber threats.

Regulatory context

The key elements of industrial security

With the networking of companies and machinery, the risk increases that vulnerabilities in information systems are exploited and that economic losses and physical harm occur. To reduce the risks, European lawmakers have introduced new sets of rules. The three pillars, Machinery

Regulation, Cyber Resilience Act (CRA) and the directive on measures for a high common level of cybersecurity across the union (NIS 2) are key components of the European Union's strategy to enhance cybersecurity.

	NIS 2	Directive CRA	Machinery Regulation
Directed toward	Companies	Components	Machinery
Adopted on	27/12/2022	10/10/2024	29/06/2023
Binding from	18/10/2024	11/12/2027	20/01/2027
Obligations	<ul style="list-style-type: none">+ Measures for managing cyber security risks+ Compliance with technical and organizational measures+ Notification of significant security incidents	<ul style="list-style-type: none">+ Secure development lifecycle process+ EU type examination for critical products+ Notification of vulnerabilities+ Provision of security updates	<ul style="list-style-type: none">+ Protection against corruption (with focus on functional safety functions)+ Attention to malicious attempts by third parties

NIS2 (Network and Information Systems Directive)

The objectives of the NIS2 Directive are to strengthen the security of network and information systems in the European Union. The Directive aims to improve cooperation between EU member states on cybersecurity and to ensure a high level of security of network and information systems across the European Union. The Directive also imposes obligations on digital service providers and critical infrastructure operators to ensure the security of their networks and information systems.

Which sectors are affected by NIS2?

If you operate a business or organization in Europe, you may wonder whether the NIS2 Directive applies to you. The answer depends on various factors, including the sector in which you operate, your company size, and your organization's importance to society.

This simulator analyzes your situation:

<https://monespacenis2.cyber.gouv.fr/simulateur>

In the future, these companies will be obligated to implement risk management measures for cyber security.

This includes:

- + Risk analyses and security concepts for information systems, protection of the supply chain and the safety of personnel
- + Concepts for access control and the management of plants
- + Mandatory training for management
- + In the event of serious security incidents, an early warning will occur within 24 hours and within 72 hours the responsible authority will be notified

How to comply with NIS2?

- + Duty of care: organizations must conduct a risk assessment and take appropriate measures to secure their services.
- + Reporting obligation: incidents must be reported to the supervisory authority within 24 hours. A cyber incident must also be reported to the Computer Security Incident Response Team (CSIRT), which can provide assistance.
- + Supervision: an independent supervisory authority will monitor compliance with the Directive's obligations.

How IEC 62443 standard supports the NIS2 Directive?

One of the most widespread and frequently adopted standards by industrial organizations is the IEC 62443 standard. This standard includes guidelines that define the procedures for implementing electronically secured industrial automation and control systems (IACS) for different parts of a network.

The asset owner carries out a risk analysis that, once the model has been established, assigns to each zone and

conduit a target **SL***, based on a consequence analysis that describes the desired security for the respective zone or conduit.

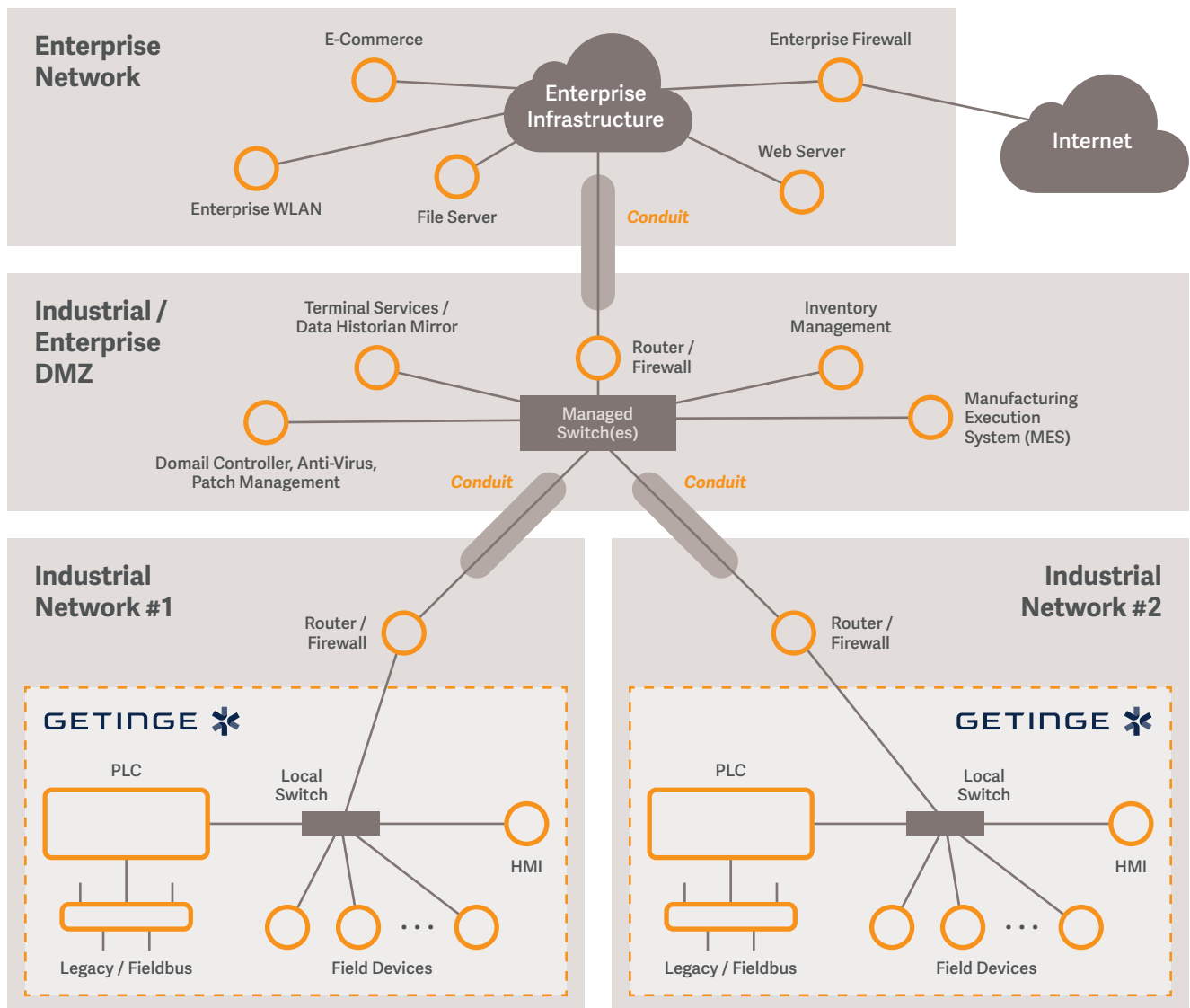
***Security Level (SL)**

The requirements for systems and components are described with Security Levels.

These are defined as follows:

Security Level 0	No special requirement or protection required.
Security Level 1	Protection against unintentional or accidental misuse.
Security Level 2	Protection against intentional misuse by simple means with few resources, general skills and low motivation
Security Level 3	Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific skills and moderate motivation
Security Level 4	Protection against intentional misuse by sophisticated means with extended resources, IACS-specific skills and high motivation

In this example, each industrial network operates relatively independently with its own PLCs, field devices and human-machine interface.



The objective is to implement a successful segmentation depending on the determined target **SL**, meaning that there is an effective reduction of the opportunities for attack as well as a system whose performance is not limited.

To ensure security, Getinge recommends implementing a network architecture in alignment with the IEC 62443-1-1 reference architecture. This reference architecture reflects the network configuration recommended for Cyber Security at the Asset Owner's site.

Directive CRA (2024/2847) & Machinery Regulation (2023/1230)

While the NIS2 Directive focuses on the security and resilience of networks and systems used by entities that provide essential or important services, the CRA focuses on the security and certification of products with digital elements placed on the market.

From 2027 the Machinery Regulation (2023/1230), which replaces the Machinery Directive, and the Cyber Resilience Act (CRA) (2024/2847) will apply to Machinery manufacturers.

Comparison between the CRA (2024/2847) and the Machinery Regulation (2023/1230)

Criterion	CRA (2024/2847)	Machinery Regulation (2023/1230)
Scope	Products with digital elements connected to a network or device. Specified exceptions.	Machines, quasi-machines and related products. Specified exceptions.
Main objective	Cybersecurity throughout the product lifecycle.	Functional safety: protection of health, safety of people and the environment.
Security requirements	No physical security requirements.	Safety requirements at the core of the regulation (Annex III).
Cybersecurity requirements	CRA core (Annex I).	Protection against malicious attacks (Annex III, sections 1.1.9 and 1.2.1).
Risk assessment	Mandatory cybersecurity risk assessment (Art. 13, Annex I).	Mandatory safety risk assessment (Annex III, section 1).
Evaluation objective	Prevent cybersecurity incidents and limit their impact.	Identify hazards that can cause injury or damage to health.

Without waiting for 2027, Getinge WIS products meet the security requirement by offering hardware and software solutions from suppliers that maintain an ISA/IEC 62443-4-1 third party-certified software development lifecycle process.

ISA/IEC 62443-4-1 is a specialized industrial automation-based security certification that requires a formal lifecycle

that is institutionalized across development teams and includes security requirements definition, secure design, secure implementation, verification, validation, defect management, patch management, vulnerability management, and product end-of-life management.

Annex: **Siemens, Rockwell Automation, B&R ABB Group, IXON Cloud** Certificate IEC 62443-4-1



The security of the components with which we build our machine is particularly important. In addition, we pay attention to the following points:

+ Reduction of the attack surface

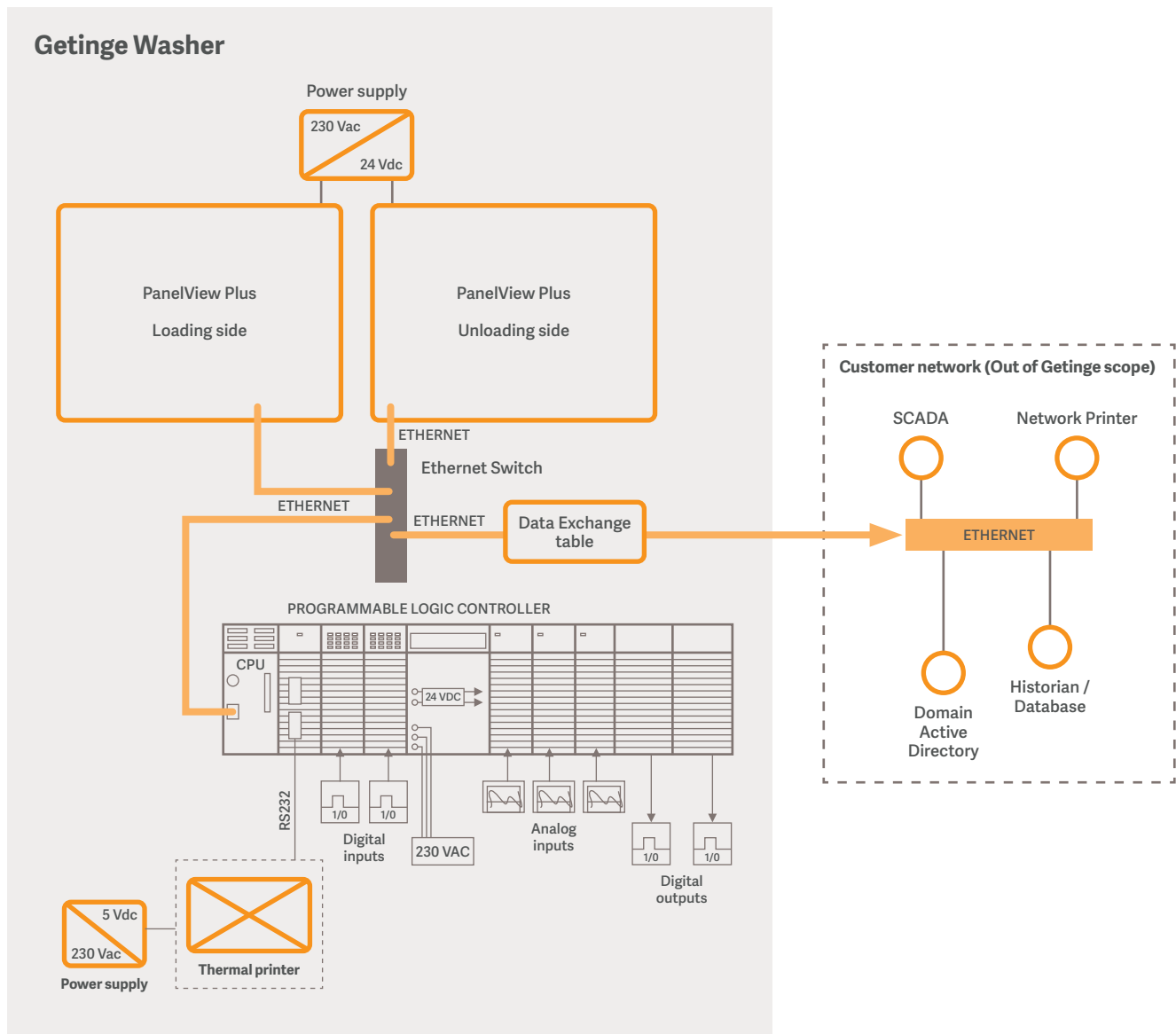
Unnecessary functionalities and interfaces are to be deactivated, or the hardware is to be made accessible only to authorized persons.

+ Patch management

The components must be kept up to date**, if possible and feasible. This applies to the firmware of the components that are used. The system operator is responsible for setting up a patch management process.

+ Backup and restore

The machine manufacturer should make a backup of all configurations of the machine when it is completed so these can be restored in case of a security incident.



** In accordance with IEC 62443-3-3 requirements for safety in systems and safety levels SR 7.8 (control system component inventory) we make available a list of installed components that includes hardware, software, and firmware versions.

Siemens, Rockwell Automation, B&R ABB Group / WIS configuration

	Siemens	Rockwell	B&R
PLC	SIMATIC S7-1500	CompactLogix / ControlLogix	Compact S X20CP0484
Switch Ethernet	Scalance	STRATIX 2000	Weidmuller - IE-SW-BL05-5TX
HMI	TP advanced	Panel View Plus	Power Panel T30 (6PPT30.XXXX)
HMI	IPC	IPC Rockwell 6300P	/
HMI	HMI MTP	/	Power Panel T30 (6PPT30.XXXX)
Engineering	TIA Portal Win CC Unified	FT view (HMI) --> FT Optix	Automation studio Mapp view
Engineering	TIA Portal Win CC advanced	Studio 5000 (PLC)	Automation studio VC4

The plant operator must keep this list up to date in case of extensions, updates, or component replacement. The machine manufacturer should provide the list of software used with their respective release versions as well as their origins. This list can also be used to check the component management of the plant operator for accuracy.

Getinge Main Control Board (ULTIMA washers, PACS Sterilizer)

ULTIMA washers (lab washers)

In accordance with Regulation 2024/2847 cybersecurity requirements for products with digital elements Annex VII, a cyber risk analysis is carried out, followed by internal pentest.

The pentests were performed locally on the Ethernet and USB ports, without network connection to Fleetview.



Penetration Testing

Scope / Internal Penetration Testing: Focuses on internal network infrastructure and the potential impact of insider threats or compromised internal systems.

Objective / Internal Penetration Testing: Establishes a security baseline and identifies vulnerabilities from an insider's perspective.

- + Denial of service
- + Identification of technologies used in HTTP responses
- + Open ports on the machine
- + HTTP verb tempering
- + Obsolete software and libraries
- + Unencrypted communications
- + Security of the SSH connection

The objectives were as follows:

- + Test the security of the elements described in the scope of the mission
- + Identify vulnerabilities
- + Present recommendations for measures to be implemented
- + Raise awareness of the actors (management, IT specialists)


Machines with PACS: CPU CARD PACS 3500



We have performed tests on the Netcom Card that enables Getinge Online for PACS, not on the PACS system itself. We are now working on an update of the Netcom software to solve some of the risks identified.

We might perform the test with direct connection to PACS (serial and I2C ports).

Certificate



No.: 968/FSP 1792.02/25

Product tested	Programmable Logic Controller	Certificate holder	Rockwell Automation, Inc. 1201 South Second Street Milwaukee, WI 53204 USA
Type designation	ControlLogix & GuardLogix 5580 Controller Families CompactLogix & Compact GuardLogix 5380 Controller Families		
Codes and standards	IEC 62443-4-1:2018 (Edition 1.0)	IEC 62443-4-2:2019 (Edition 1.0)	
Intended application	The ControlLogix & GuardLogix 5580 Controller Families and the CompactLogix & Compact GuardLogix 5380 Controller Families comply with the requirements according to IEC 62443-4-1 and Security Level Capability 1 (SL-C 1) according to IEC 62443-4-2.		
Specific requirements	The instructions of the associated User Manuals and the Reference Manual released by manufacturer must be considered, The current versions of the product are specified in the currently valid revision list, The list is released by the manufacturer in cooperation with the certification body.		

Valid until 2030-05-20

The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT CS1 V3.0:2021 in its actual version, whose results are documented in Report No. 968/FSP 1792,16/25 dated 2024-05-20. This certificate is valid only for products, which are identical with the product tested. Issued by the certification body accredited by DAkkS according to DIN EN ISO/IEC 17065. The accreditation is only valid for the scope listed in the annex to the accreditation certificate D-ZE-11052-02-00.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2025-05-20

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. (FH) Sergei Biberdorf

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1730, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com



Product Service

CERTIFICATE

No. IITS2 128627 0001 Rev. 00

Holder of Certificate: **Siemens AG**
DI FA
Gleiwitzer Straße 555
90475 Nürnberg
GERMANY

Certification Mark:



Product Type: **Industrial IT Security**

Model(s): **SIMATIC S7-1500 Controller Family**
(Applicable from Firmware Version 3.1 and later)
Software Controller
(Applicable from Firmware Version 30.1 and later)

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003C:2024 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See <http://www.tuvsud.com/ps-cert> for details.

Test report no.: 713318447-04
Valid until: 2027-10-23

Date, 2024-10-28

(Stefan Würth)

Certificate



Cyber Security Management

CS Management (TÜV Rheinland)

IEC 62443-4-1 - Security Product Development Lifecycle

CSM 134 - Centralized Group Certification

Certificate No.

968/CSM 134.01/24

**Certified Company
& Location**

B&R Industrial Automation GmbH

B&R Straße 1

5142 Eggelsberg

Austria

B&R

A member of the ABB Group

for further regional locations see appendix

Scope of Certification

IEC 62443-4-1:2018 (Edition 1.0)

Security Product Development Lifecycle Requirements

Centralized Group Certification

The certified company has successfully demonstrated during an audit process that the "B&R Secure Product Development Lifecycle" Process has been established.

Achieved Maturity Level 2: Managed.

The Certification only refers to the listed company location and their involved departments listed in the attached Certification Appendix 968/CSM 134.01/24. Latest revision of the Certificate Appendix could be found following the QR-Code above or on web page www.certipedia.com/fs-products.

This certificate does not imply approval or certification for specific security related developments of products.

Validity

This certificate is valid until 2025-02-16

Cologne, 2024-05-14

Dipl.-Ing. (FH) Wolf Rückwart

TÜV Rheinland Industrie Service GmbH

Bereich Automation

Funktionale Sicherheit

Am Grauen Stein, 51105 Köln

TÜV Rheinland
Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety & Security for Automation & Grid
Further information referring to the scope of certification, see <https://www.tuvasi.com>. The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT SDLA V2.0 2020:2020 in its actual version, whose results are documented in Report No. 968/CSM 134.01/24 dated 2024-05-03. Issued by the certification body accredited by DAkkS according to DIN EN ISO/IEC 17065. The accreditation is only valid for the scope listed in the annex to the accreditation certificate D-ZE-11052-02-00.

www.fs-products.com
www.tuv.com

 **TÜVRheinland®**
Precisely Right.



**Applied
Risk**

Cyber Security Certificate

Security Audit 2021



Tested Products: IXON Cloud, Version 1.2

Manufactured By: IXON B.V., The Netherlands

Audit Process: Modified NIST SP800-115 & OSSTMM

Concept Audit: IEC62443-4-1, IEC62443-4-2 Draft

Component Audits: Vulnerability assessment and penetration testing, analysis of communication principle

System Audit: Security assessment of end-to-end reference setup, threat assessment of 3rd party components based upon CVSS & OWASP Top 10 threat analysis

Test results: Tests passed with some recommendations. A detailed report has been issued.

Status:

Pass

Amsterdam, July 23rd, 2021

DocuSigned by:

Jalal Bouhdada

BB17A7CEE6174F1...

Jalal Bouhdada
CEO, Founder



With a firm belief that every person and community should have access to the best possible care, Getinge provides hospitals and life science institutions with products and solutions aiming to improve clinical results and optimize workflows. The offering includes products and solutions for intensive care, cardiovascular procedures, operating rooms, sterile reprocessing and life science. Getinge employs over 10,000 people worldwide and the products are sold in more than 135 countries.

Ekebergsvägen 26 · Box 69 · SE-305 05 Getinge · Sweden

www.getinge.com