New EU directive, NIS2, comes into play

ABB Gebruikersdag 2023

Tobias Nitzsche, ABB

 Document ID.: Rev.:

Introduction

NIS2 directive went into force on January 16th, 2023, and member-states have until October 17th, 2024, to adopt and publish necessary measures to comply with the directive.

What does this mean for operators and suppliers?

This presentation focuses on their duties and tasks with some examples.

Today’s Board of presenters

Today’s expert

Tobias Nitzsche
Global Cyber Security Practice Lead
ABB AG
Email: tobias.nitzsche@de.abb.com

Agenda

01. Introduction
02. Summary
03. Critical Sectors
04. Risk management measures
05. Operator duties and how suppliers can support
06. Conclusion
07. Q&A

Summary

The NIS2 directive includes the following focus areas

- New obligations that apply to both member-states and companies
- A broader scope than with NIS1
- A size cap for identifying entities more than 50 persons and whose annual turnover and/or annual balance sheet total exceed EUR 10 million (medium size) but there are exclusions regardless of their size and these details you should follow up with a lawyer
- Administrative fines on essential entities for infringements of the directive
- Requiring 24 hours for early warning of a significant incident and 72 hours for incident reporting
- Obligatory cyber security risk-management measures
- Coordinated vulnerability disclosure and the creation of a European vulnerability database
- The official establishment of the EU-CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises at an operational level
- Supply chain security

Critical sectors in the EU

Bolt is introduced in NIS2 (Scope Extends)

Essential Services

Energy: electricity, oil, gas, heat**, hydrogen**

Health: providers, **labs, R&D, pharma**

Transport: air, rail, water, road

Banks and financial markets

Water and **wastewater**

Digital: IXP, DNS, TLD, **DC, CSP, CDN, TSP, MSP, MSSP**

Space

Public administration

Important Services

- **Postal and courier**
- **Waste management**
- **Chemicals**
- **Food**
- **Manufacturing: technology and engineering**
- Digital services: social, search, markets

Article 21 cyber security risk management measures

Applies to essential and important entities - “all-hazard” approach

Technical and organizational measures to manage risks

Risk analysis and information system security policies

Incident handling (prevention, detection, and response to and recovery from incidents)

Business continuity and crisis management

Supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

Security in network and information systems acquisition, development and maintenance including vulnerability handling and disclosure

Policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures

Policy on the use of cryptography and encryption

Human resources security, access control policies and asset management

Basic cyber hygiene practices and cyber security training

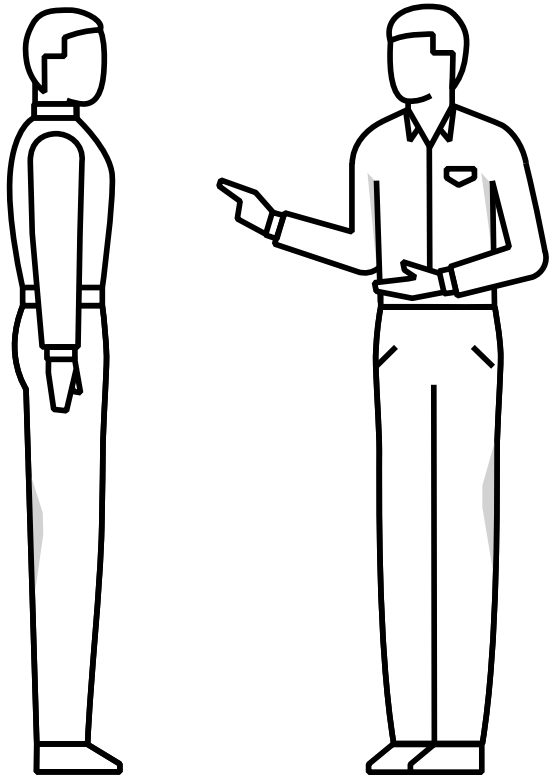
Multi-factor authentication or continuous authentication solutions, secured voice, video and text communications

What must suppliers and operators do now?

A mapping to a security standard and solutions can help

Standardization (Article 25 of the Directive)

To promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favor of the use of a particular type of technology, **encourage the use of European and international standards and technical specifications** relevant to the security of network and information systems



What do suppliers and operators have to do now?

	Europa	ISO	Operator	Supplier
	NIS 2.0, Art. 21, para. 2c	ISO 27002:2017, Cape. 17	Determination of crisis management and maintenance of information security and operations (business continuity management)	Contractual commitments of resources and response times; Support in the creation of technical recovery plans • ABB Care Framework • Incident Response • Cyber Security Backup & Recovery
	NIS 2.0, Art. 21, paragraph 2d	ISO 27002:2017, Cape. 15	Determination of the IS requirements for [NIS 2.0: direct] suppliers and their monitoring and verification (supplier audits)	Ensuring the implementation of IS requirements through certification (e.g., ISO/IEC 27001, IEC 62443-2-4); Monitoring of suppliers with regard to information security • ABB Cyber Security Requirements for Suppliers
			Display of the first use of a critical component	Submission of a manufacturer's declaration of trustworthiness (guarantee declaration); exact requirements for the declaration are still open

What do suppliers and operators have to do now?

	Europa	ISO	Operator	Supplier
	NIS 2.0, Art. 21, paragraph 2e	ISO 27002:2017, Cape. 14	Specification of requirements for the whole Information systems lifecycle (planning, development, testing, maintenance, replacement); adequate handling of vulnerabilities	Implementation of a development process based on standards and best practice; Vulnerability Disclosure and Addressing • ABB Approach to Software Vulnerability Handling • ABB Alerts and Notification • IEC 62443-4-1 Certified Development Organization • IEC 62443-4-2 Certified Components • **IEC 62443-3-3 Certified Systems** • **IEC 62443-2-4 ML2 Security Program Requirements for IACS Service Providers**
	NIS 2.0, Art. 21, para. 2f	ISO 27002:2017, Cape. 12.7 and 18.2	Establishing procedures for evaluating the effectiveness of protective measures in the area of information security Proof of compliance with IS requirements through audits, reviews or certifications	Support in comparing the status quo (actual) to the respective specifications (target) • GAP analysis • Individual Consulting • ISMS Support • CSWP

What do suppliers and operators have to do now?

	Europa	ISO	Operator	Supplier
	NIS 2.0, Art. 21, paragraph 2g	ISO 27002:2017, Cape. 10	Definition and documentation for use of cryptography or encryption and signing in information systems	Implementation of cryptographic measures in products and systems (e.g., encrypted communication protocols, signed software packages, encrypted remote maintenance access) • Remote Access Platform (Part of Care Contract) • IPSec at the HMI level
	NIS 2.0, Art. 21, paragraph 2ga	ISO 27002:2017, Cape. 7 to 9	Establishing IS requirements for employees and contractors before, during and after employment; Definition of asset management (IS assets) Definition of access control in information systems	Support through various services in the areas of training, asset management and access control • ABB University Classes • Cyber Security Asset Inventory • Cyber Security MFA Authentication • Remote Access Platform (Part of Care Contract)

Source: Draft NIS 2.0 (26.11.2021), https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf

Reporting obligations

Notify without undue delay and, in any event, within 24 hours after having become aware of the incident

An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

How can one notify without undue delay?

Designed solutions for reporting taking OT incidents into account, contracts with the proper reaction times covering the OT scope.

The act of the notification in itself shall not make the notifying entity subject to increased liability!

Cyber security information – sharing arrangements

Trusted communities of essential and important entities

What should be exchanged?

”Including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cyber security alerts and recommendations regarding configuration of cyber security tools to detects cyber attacks”

How?

Member States shall facilitate the establishment of cyber security information-sharing arrangements and ensure that the exchange of information occurs within communities of essential and important entities and, where relevant, their suppliers or service providers.

Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content, and conditions of the information-sharing arrangements.

Registry

Certain digital infrastructure entities and digital services providers

Entities are required to submit information to the competent authorities

the member states single points of contact shall forward the information to ENISA.

Based on the information received, ENISA shall create and maintain a registry for the entities. Upon request of Member States, ENISA shall enable access of relevant competent authorities to the registry.

Conclusion

From EU

Timeline

- Member states will have until October 17th, 2024, to adopt and publish necessary measures

Scope

- Nearly all kinds of industry
- No longer just NIS1 critical infrastructure

Measures to be implemented

- Obligation to report cyber security incidents
- Registration obligations with national authorities
- Duties for the Management Board
- Implementing cyber risk mitigation measures
- Possibly the obligation to use certified products (EU CSA schemes)

ABB's support

Timeline

- Legally, sharing the information with our clients to support early budgeting and project planning, establishing key competence centers/collaborative operation center

Scope

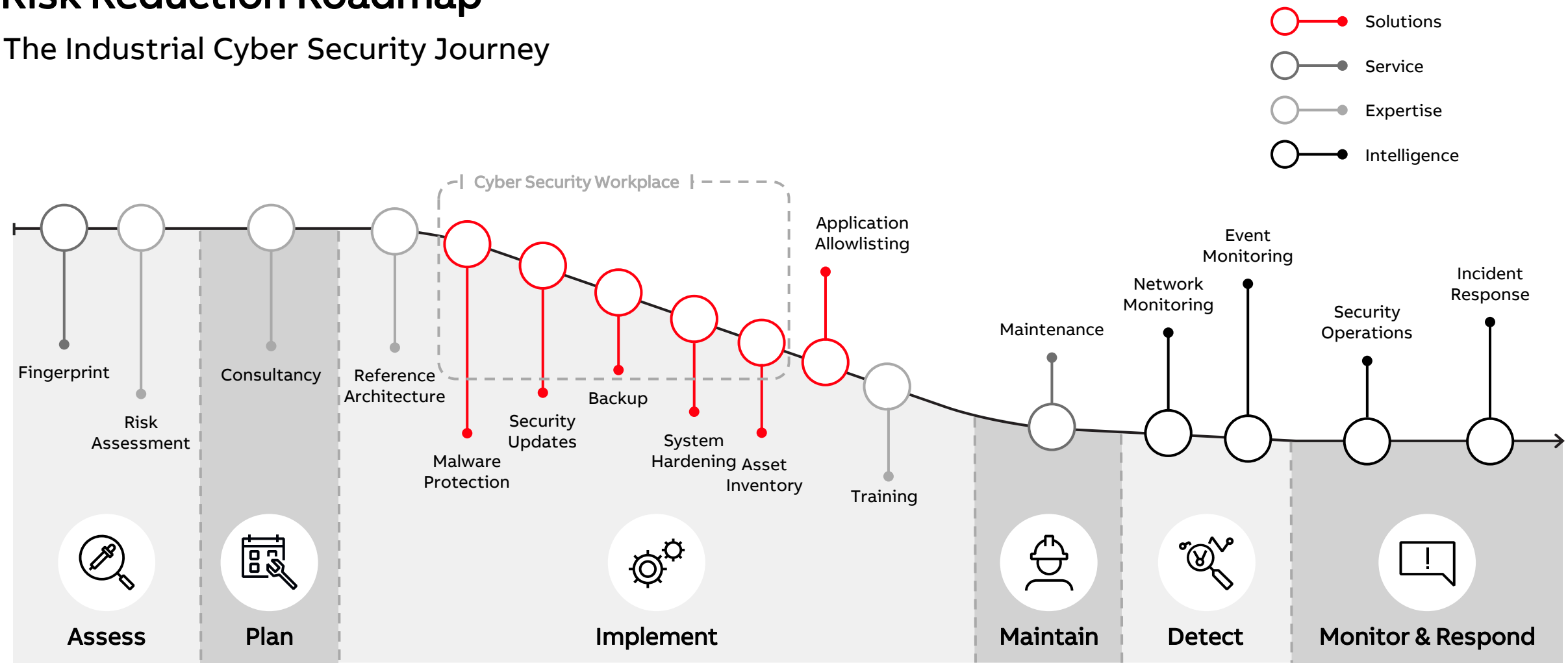
- Tailored cyber security product and service portfolio to implement all risk-mitigating measures for our customers from the manufacturer's hand

Resources

- With our collaborative Operation Centers and globally available experts, we help our customers meet their targets for detection, response, containment, eradication, and recovery, especially in OT environments
- Our care agreements help customers to be able to understand and report needed information within the regulated timespan

Risk Reduction Roadmap

The Industrial Cyber Security Journey



Challenges with Traditional Cyber Monitoring & Maintenance

Security Updates, Malware Protection, Backup & Recovery

Understanding Risks

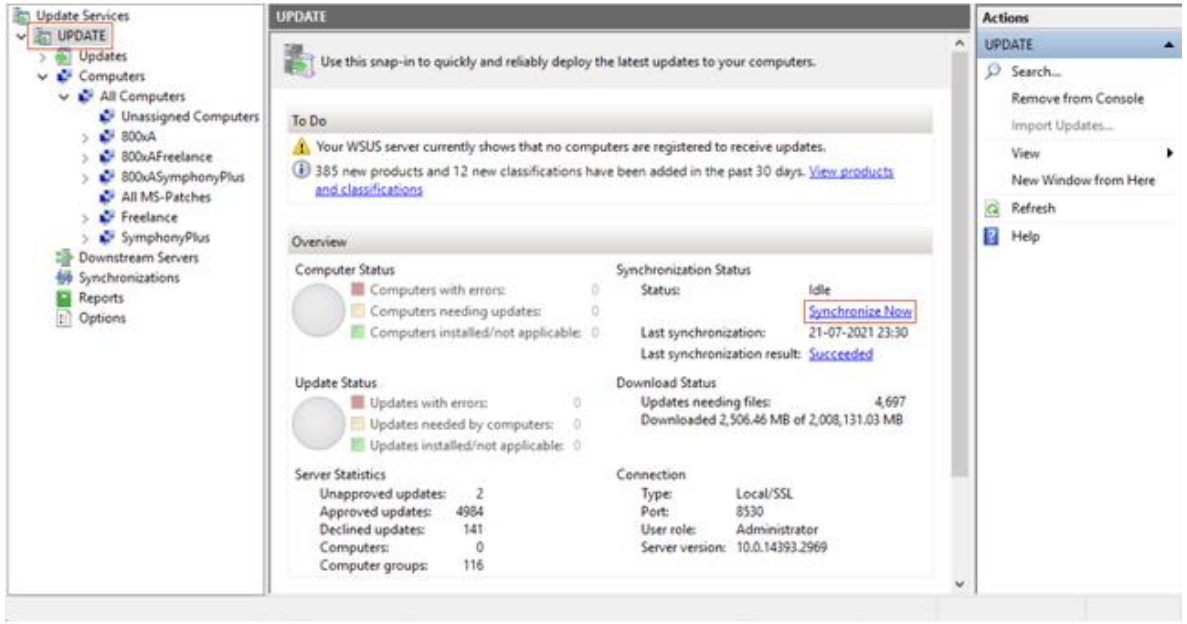
Security controls are only as effective as the team maintaining them. The lack of actionable data and expertise often results in missed threats and improperly maintained security controls.

Siloed Controls

Multiple complex and difficult to navigate consoles requires time and expertise to even understand what you are looking at, let alone know where to begin when one needs maintenance.

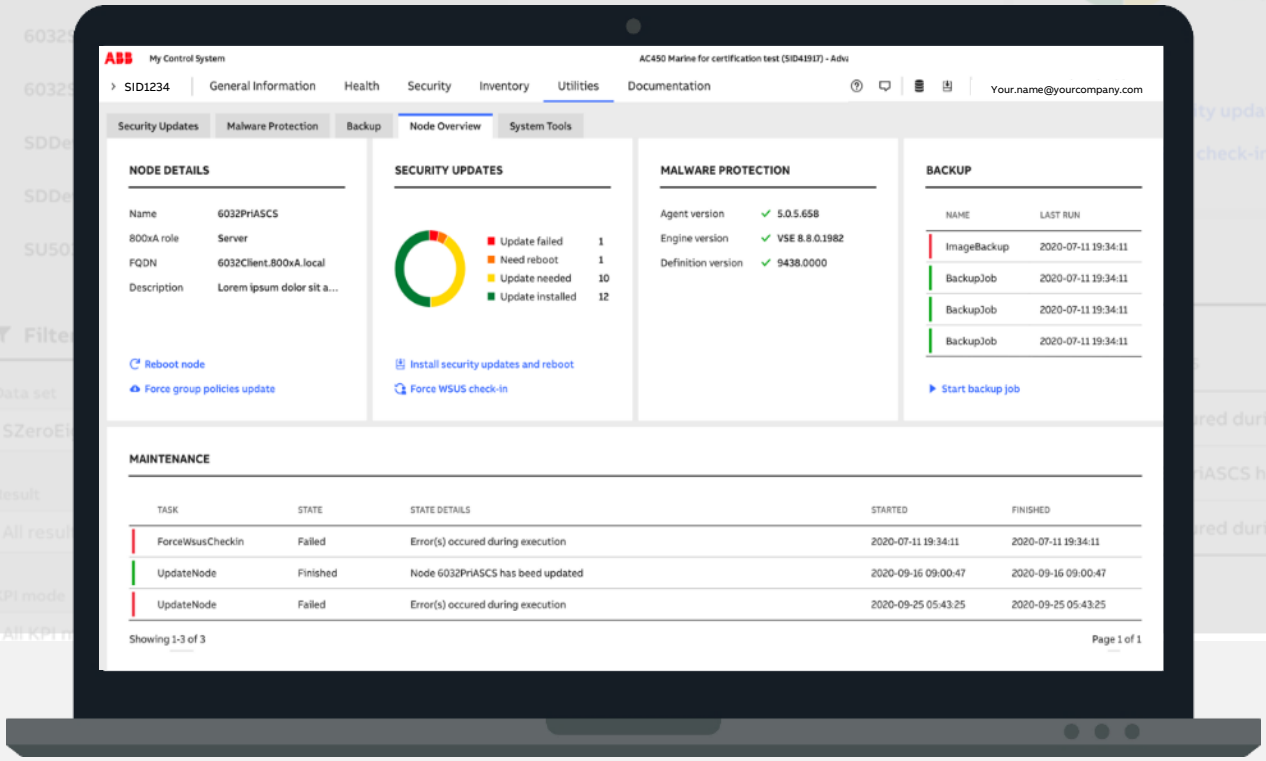
Lack of Visibility

Comprehensive visibility of your security controls status is required in order to identify your high-risk areas and remediate quickly.



Introducing ABB Ability™ Cyber Security Workplace

Security Simplified



- Monitor your security controls
- Get notified of increased risk
- Take action to protect your assets
- **All in one console**

Simplifies Security

Reduces Risk

Minimizes Effort

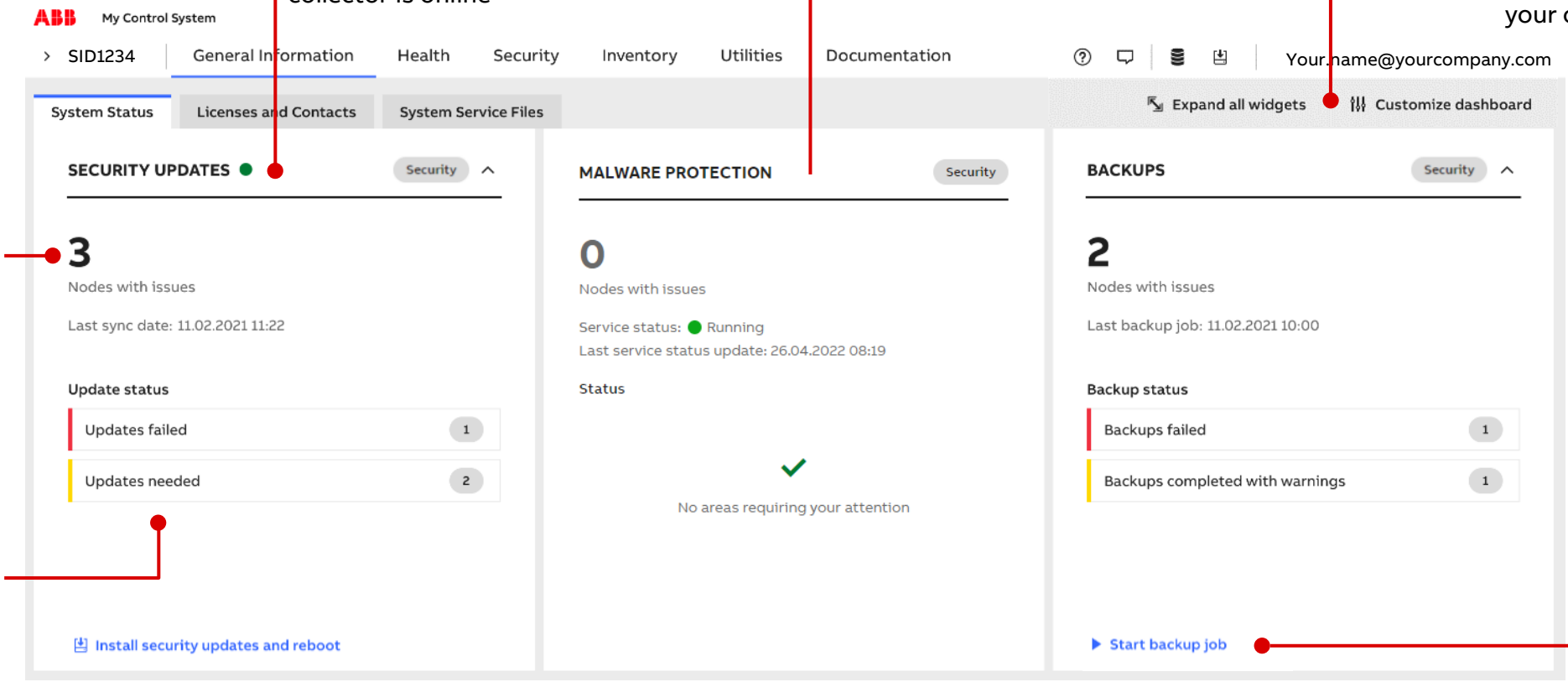
ABB Ability™ Cyber Security Workplace

Security Controls Dashboard

Service status indicator to ensure data collector is online

Single console of overall controls status

Flexible dashboard enables you to customize the page to work best for your organization



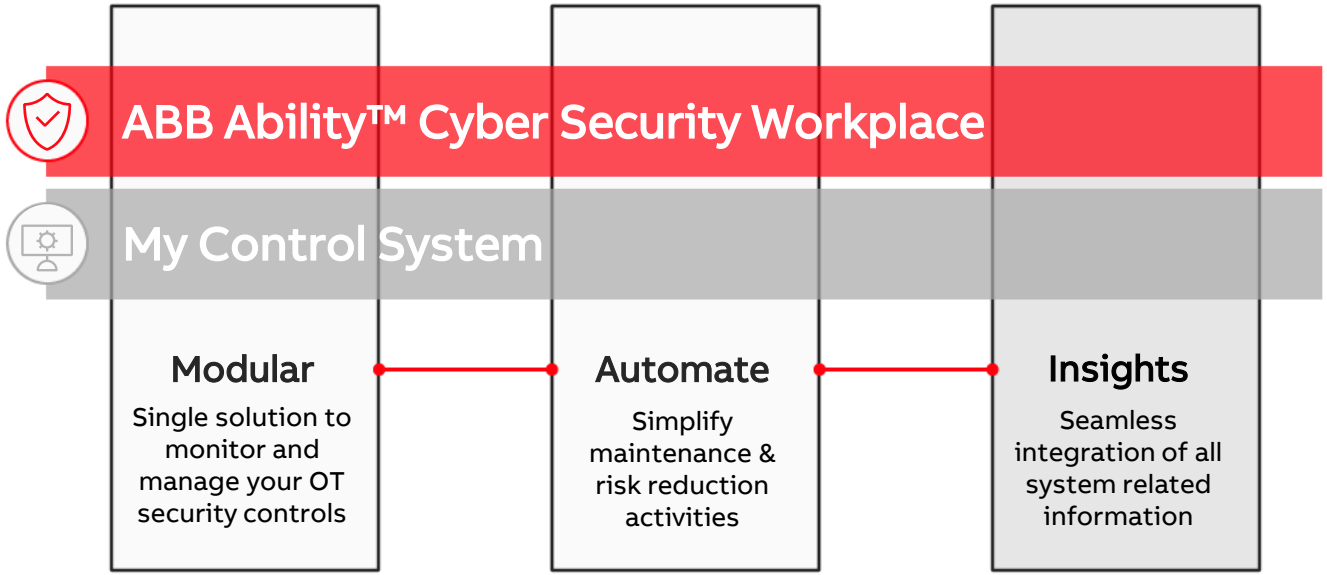
Identifies the number of nodes with **heightened risks**

Level 1 KPIs provide **early detection** of increased risk

Security maintenance actions to take to quickly remediate risk

ABB Ability™ Cyber Security Workplace

Scales with your cyber security program



Collaborative Solution for increased productivity


ABB

Agenda

13.00u-14.30u – plenaire sessie	14.45u-15.30 – subsessies ronde 1		
800xA update, NGT	Life cycle management	Cyber security	Asset Performance Management
Bedrijfsschool	**Bedrijfsschool**	**Het Strikkershuis**	**De Centrale**

15.30u-16.15u - break	16.15u-17.00 – subsessies ronde 2		
F2F-meetings, museumbezoek	**Life cycle management**	**Cyber security**	**Advanced Process Control + Energy Management**
Foyer, Museum	**Het Strikkershuis**	**Bedrijfsschool**	**De Centrale**

17.00u - dagafsluiting	17.15u-20.00u - Let's connect!	
Plenair einde	Borrel	Diner
Bedrijfsschool	**Perron Droomreizen**	**Perron Droomreizen**

Agenda

13.00u-14.30u – plenaire sessie	14.45u-15.30 – subsessies ronde 1		
800xA update, NGT	Life cycle management	Cyber security	Asset Performance Management
Bedrijfsschool	**Bedrijfsschool**	**Het Strikkershuis**	**De Centrale**

15.30u-16.15u - break	16.15u-17.00 – subsessies ronde 2		
F2F-meetings, museumbezoek	Life cycle management	Cyber security	Advanced Process Control + Energy Management
Foyer, Museum	**Het Strikkershuis**	**Bedrijfsschool**	**De Centrale**

17.00u - dagafsluiting	17.15u-20.00u - Let's connect!	
Plenair einde	Borrel	Diner
Bedrijfsschool	**Perron Droomreizen**	**Perron Droomreizen**