



ASSOCIAZIONE **IMPRESE ITALIANE**
DI **STRUMENTAZIONE**

Come rispondere alle nuova normativa europea NIS2

13/09/2024

HYDROGEN EXPO 2024 Piacenza



ABB Ability™ Cyber Security Services

Industrial companies face elevated cyber security risks

Key risk factors



Distributed systems



Asset complexity



Process complexity



Insufficient security visibility



Insufficient security awareness



Insufficient security expertise



Lucrative and attractive target that leads to...

Potential impacts



Health and safety



Environmental



Public



Production



Trust

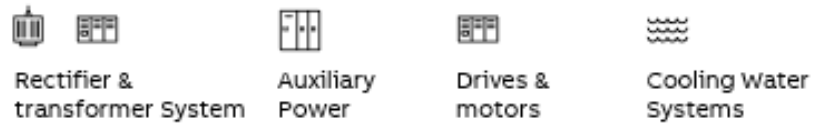


Revenue

ABB Energy Industries Division

Solutions maximizing the value of the hydrogen

Power to the Electrolyzer



Controlling and optimizing the process



Power to consumers

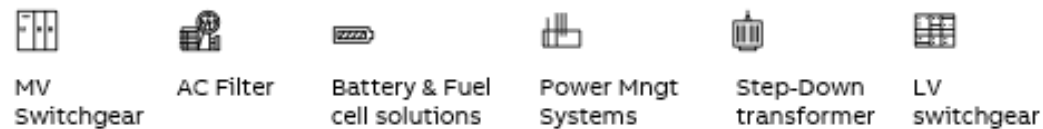


ABB Ability™



Remote Operation and Digitalization



Service and Asset Management



Production and Energy Optimization

The successful operation of a hydrogen plant is about efficient energy and process management

State of Cyber

Trends and Challenges



Cybercrime to reach
\$10.5 trillion
by 2025¹



Ransomware to
cost organizations
\$265 billion annually
by 2031¹



Cybercrime to grow
15% YoY
for next 5 years



On average it takes
organizations **277 days**
to identify and contain
a breach²



93% of OT organizations
had 1+ intrusions in last year;
78% had 3+ intrusions³



Cyber attacks impacted
61% of OT systems
causing outages, loss in
productivity and more³

Threat Landscape

Some of the Most
Common Threats



Phishing can now hide almost anywhere, emails, social media, messaging apps, or even video games³



30% of **extortion cases** were observed in the manufacturing industry⁴

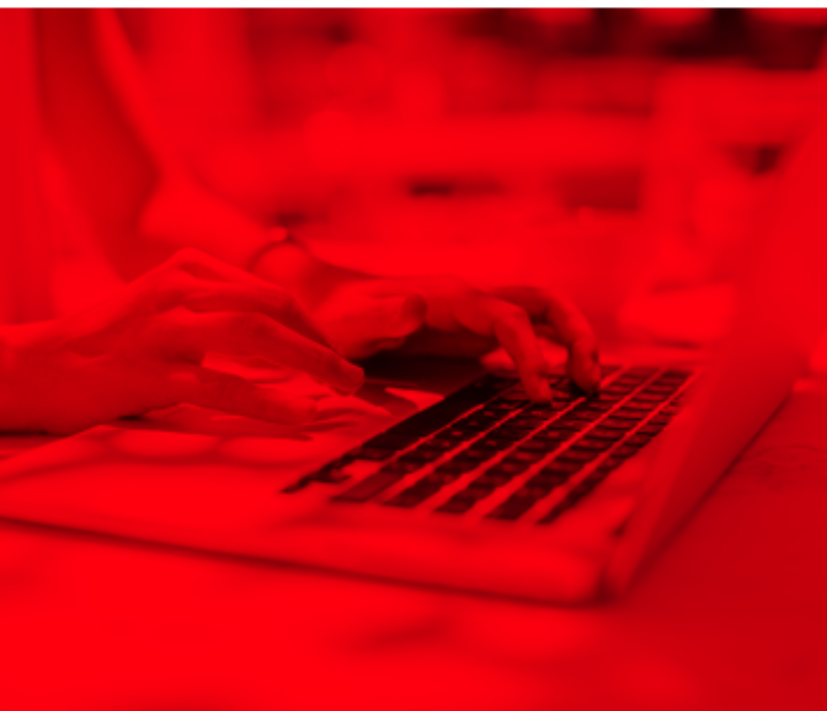


By 2025, 45% of organizations worldwide will experience **digital supply chains attacks**¹



The **ransomware** rollercoaster continued, ending 1H 2023 13x higher than it began²

1. Gartner (2022). Gartner Identifies top security and risk management trends for 2022.
2. Fortinet (2023). Global Threat Landscape Report
3. SOSAFE (2023). Cybercrime Trends 2023
4. Allianz (2023). Cyber security trends 2023



NIS 2 directive States applicability

From critical Infrastructure to much broader Industry coverage



Scope

- Large parts of industry are addressed, not limited to critical infrastructure
- Very small enterprises are excluded
- There will be no longer any threshold values like in NIS1
- **Small companies (up to 49 employees and up to €10 million turnover/balance sheet) are excluded. Digital infrastructures are regulated regardless of their size**



Fines

- **Essential entities** : in case of violation, fines of **up to 10 million euros or 2% worldwide annual turnover** may be imposed
- **Important entities** : in case of violation, fines of up to **7 million euros or 1,4% worldwide annual turnover** may be imposed

- EU States where NIS2 will be applicable
- Non-EU States, where NIS2 could be applicable depending on Customer dependency to EU



Critical sectors in the EU

Bolt is introduced in NIS2 (Scope Extends)



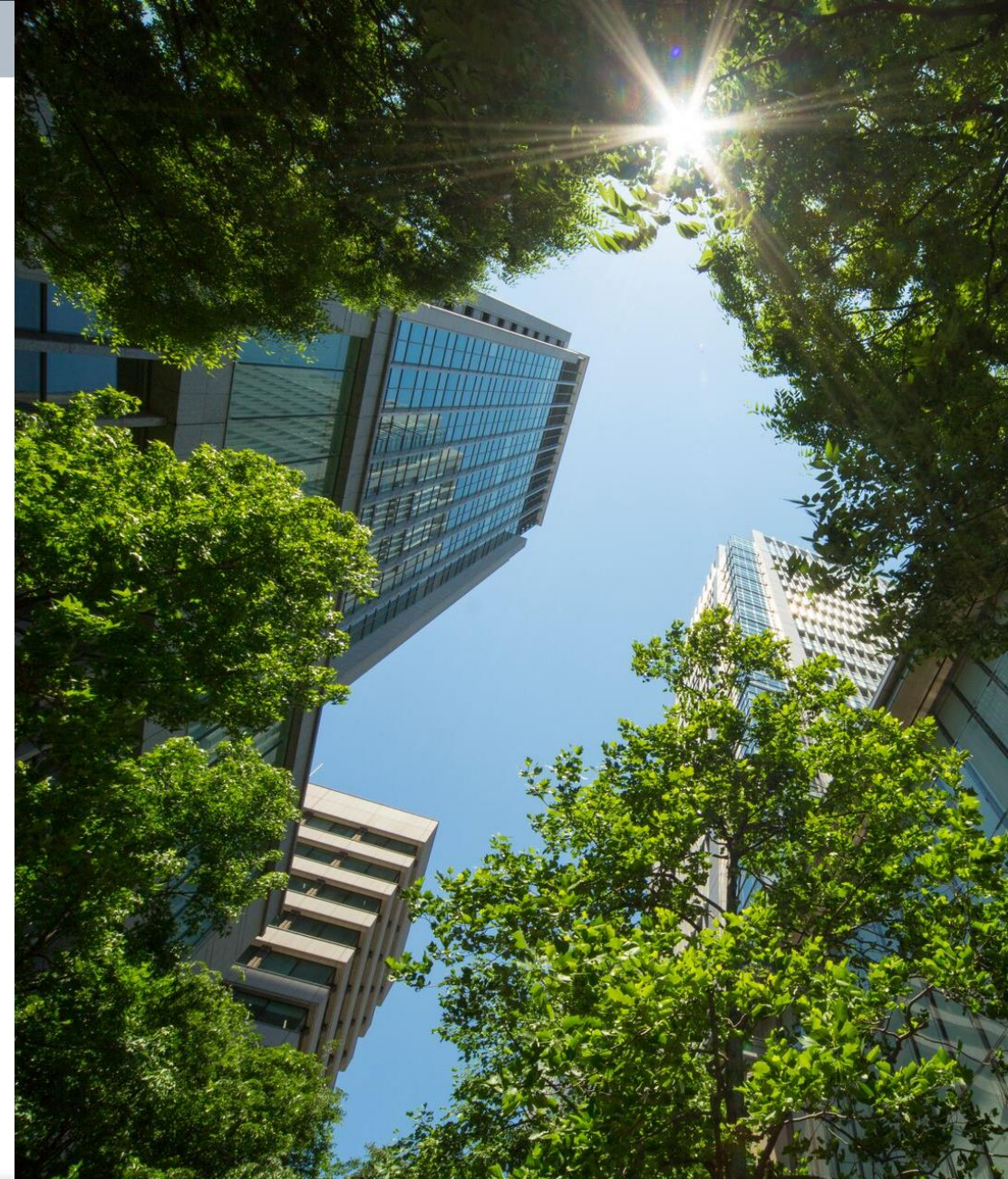
Essential Entities

- 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**



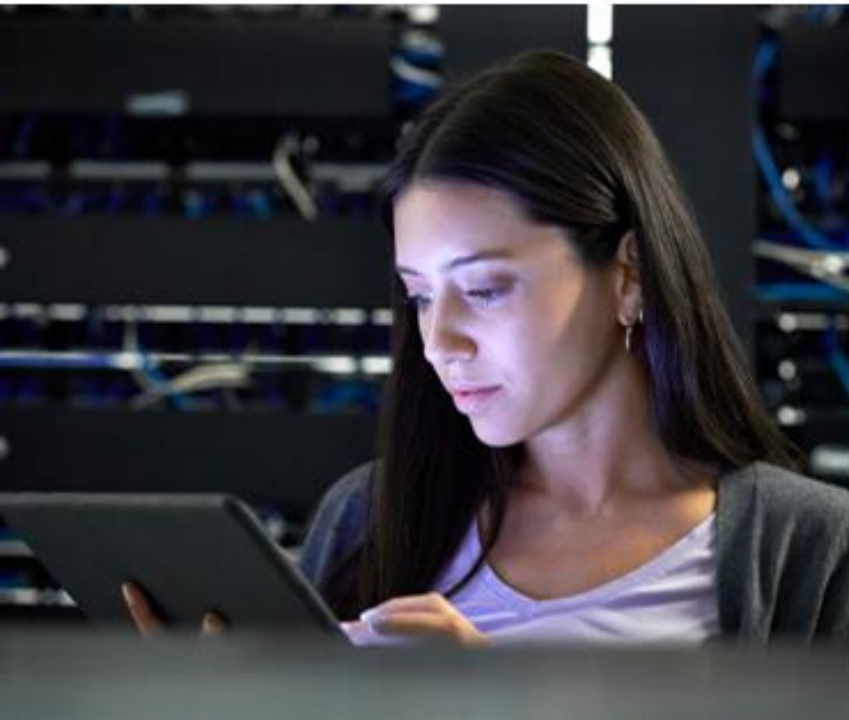
Important Entities

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



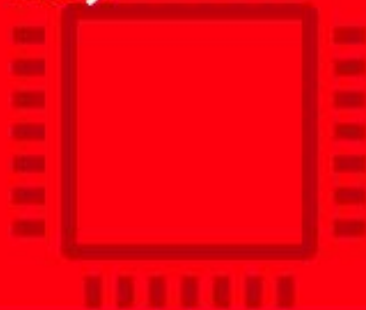
NIS 2 directive Operator duties

Four obligations are imposed on entity operators



Cybersecurity measures

(Art. 18)



Standards

(Art. 22)



Registration

(Art. 25)



Reporting

(Art. 20)



NIS2 – Art. 18/20 – What do suppliers and operators have to do now?

Cybersecurity risk management measures and Reporting obligations



| | Europa | ISO | Operator | Supplier |
|---|--------------------------------|--|--|--|
|  | NIS 2.0, Art. 20, paragraph 1 | ISO 27001:2015, Cape. 6.1, 8.2 and 8.3 | Immediate notification [NIS 2.0: within 24 hours] of significant disruptions in the information systems to authorities [NIS 2.0: and customers] | Contractual commitments of resources and response times; Support through technical solutions that have been specially tested and approved for the information systems used <ul style="list-style-type: none">• ABB Care Framework• Incident Response• Cyber Security Network Anomaly Detection, with the partnership of Nozomi or Forescout• Cyber Security Event Monitoring |
|  | NIS 2.0, Art. 18, Paragraph 2b | ISO 27002:2017, Cape. 16 | Definition and documentation of a process for the prevention, detection and management of IS incidents for information systems; effective and orderly response in focus Use of attack detection systems | Support through technical solutions that have been specially tested and approved for the information systems used <ul style="list-style-type: none">• Cyber Security Malware Protection• Cyber Security Application Allowlisting• Cyber Security Network Anomaly Detection, with the partnership of Nozomi or Forescout• Cyber Security Event Monitoring• Cyber Security Workplace |

ABB Industrial Security Domain Expertise

Trusted Partner – People and Processes



+160 Professionals

Industrial cyber security engineers & certified specialists

Certifications

- Security Development Lifecycle Assurance (SDLA) designated organization IEC 62443-4-1
- Certified Service Provider Certification Maturity Level 2 IEC 62443-2-4
- System Security Assurance (SSATM) Security Level 1 IEC 62443-3-3
- GSEC
- GCIH
- GSTRT
- GICSP
- GCFA
- TUV Cybersecurity
- CCNA
- CCNP Security
- ISA/IEC 62443 CFS
- ISA/IEC 62443 CRS
- ISA/IEC 62443 CDS
- ISA/IEC 62443 CMS
- ISA/IEC 62443 CE
- CISSP
- CISM



How to meet today's cyber security challenges

Implement a defensible architecture

Control communication between devices, zones, and levels.



Deploy foundational security

Deploy protection against malware and known vulnerabilities.

Monitor for malicious activity

Detect malicious activity early and give yourself time to respond.



The ICS Risk Reduction Roadmap

The Industrial Cyber Security Journey

- Consultancy
- Technology
- Service

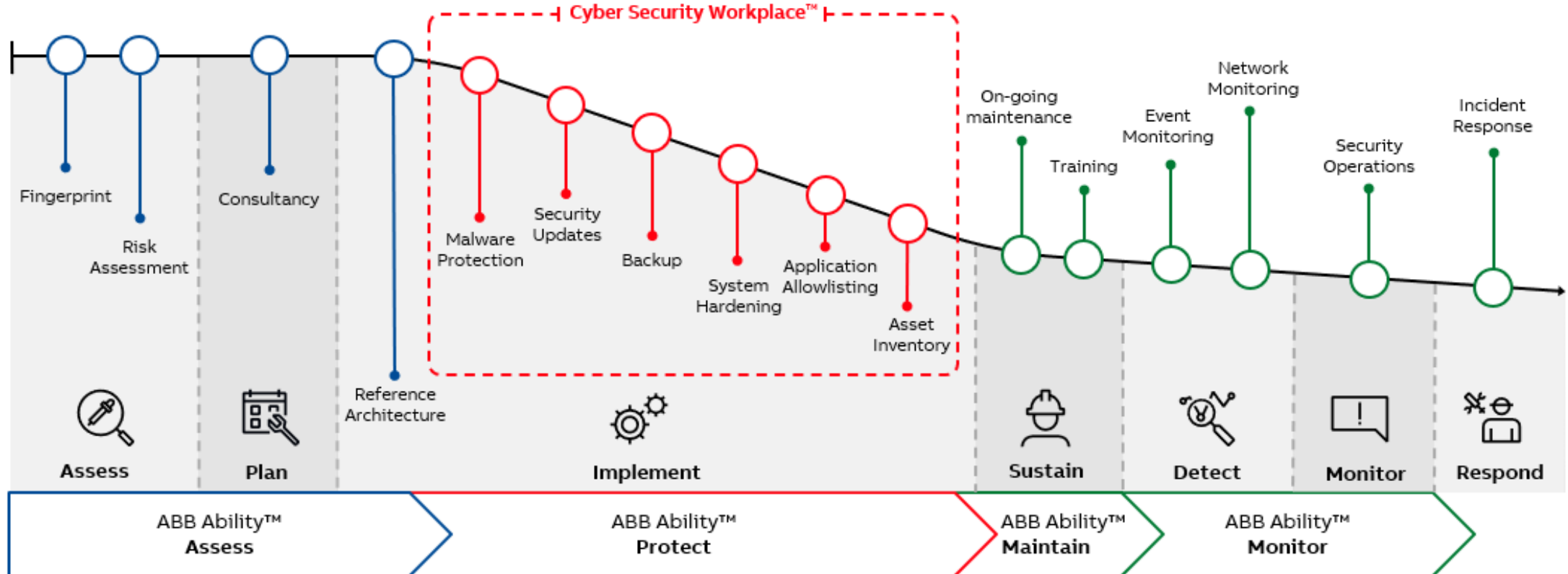


ABB Ability™ Cyber Security Workplace

Simplified Security for the Modern World

- Makes cyber security accessible to everyone
- Reduce risk with built-in recommended actions
- Automates security patching
- **All in one console**



Visibility



Simplified



Scalability

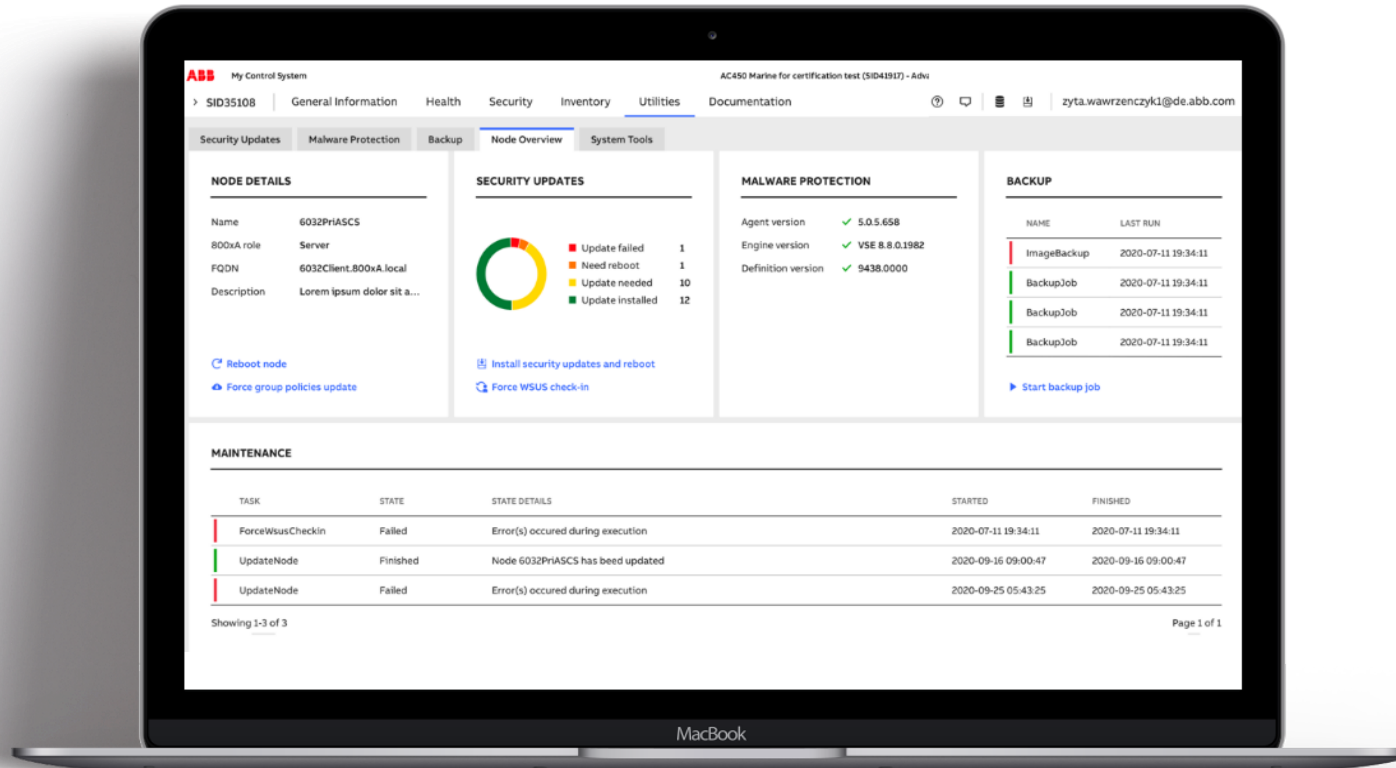


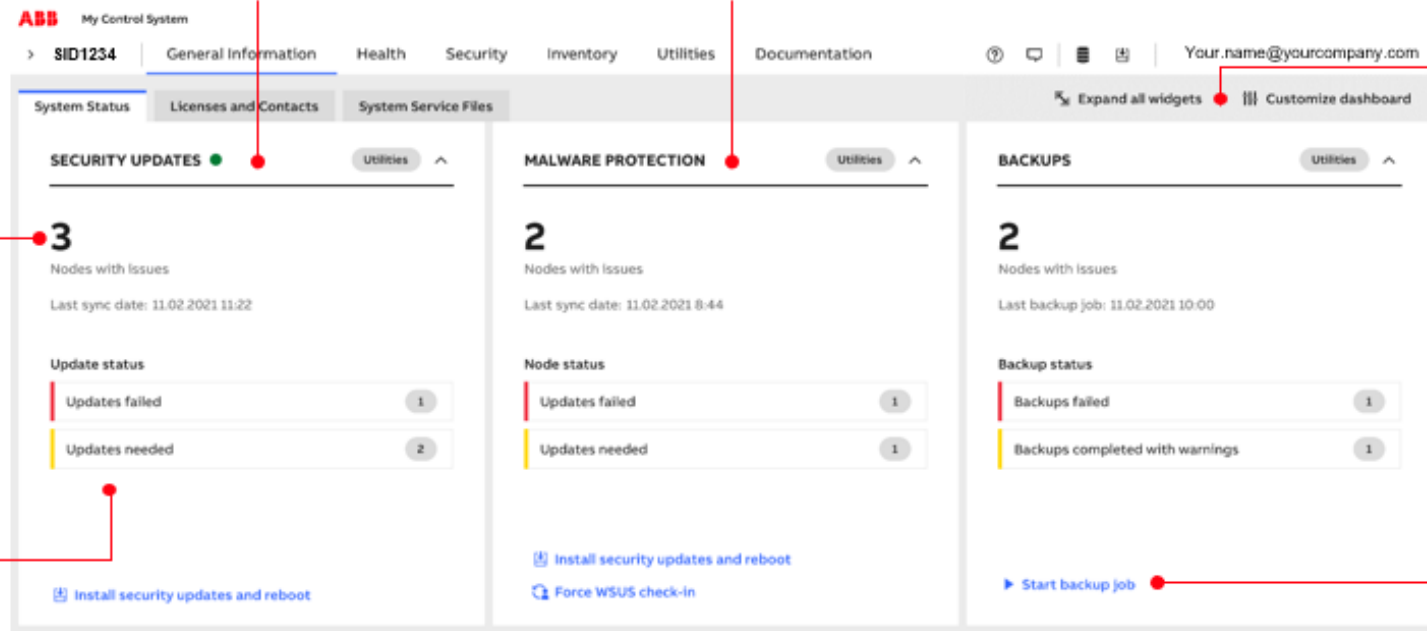
ABB Ability™ Cyber Security Workplace

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

Identify your Assets with Cyber Asset Inventory

Cyber Asset Inventory

- Automatically identifies and captures detailed information from cyber assets
- Provides updated information on control networks
- Non-intrusive system
- Facilitates compliance with standards

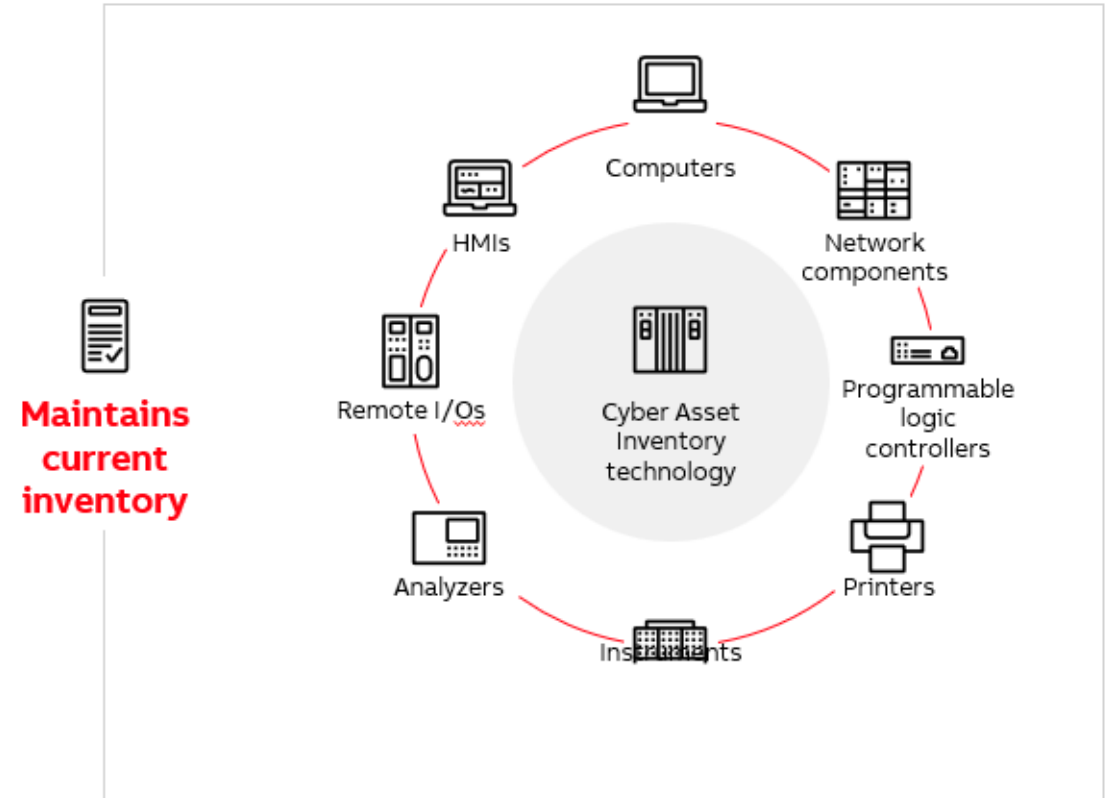


ABB Ability™ Cyber Security Workplace

Demo

Topics:

- Endpoint protection
- Backup solutions
- Patching
- Remote access
- Inventory

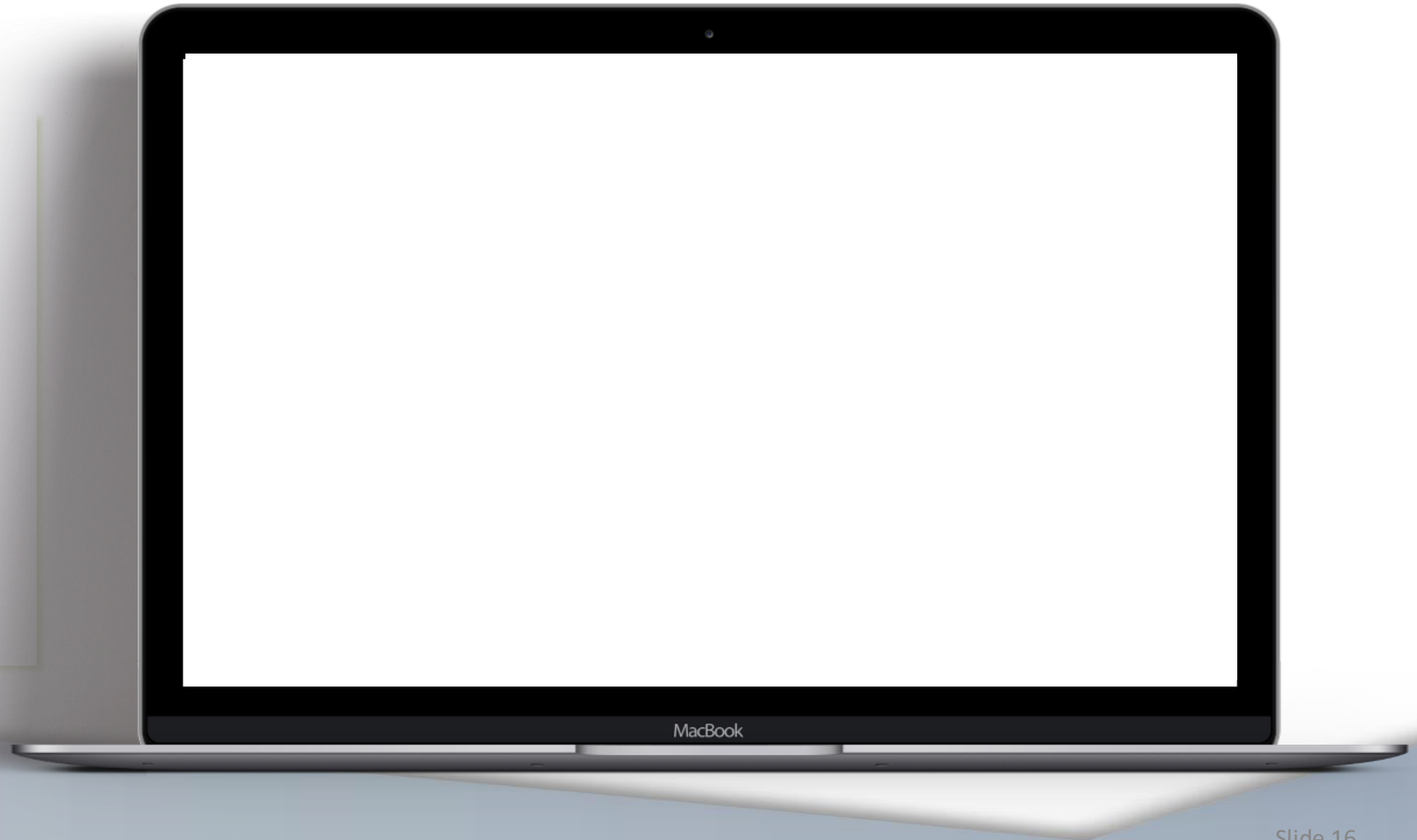


ABB Ability™ Cyber Security Workplace Architecture Fleet View

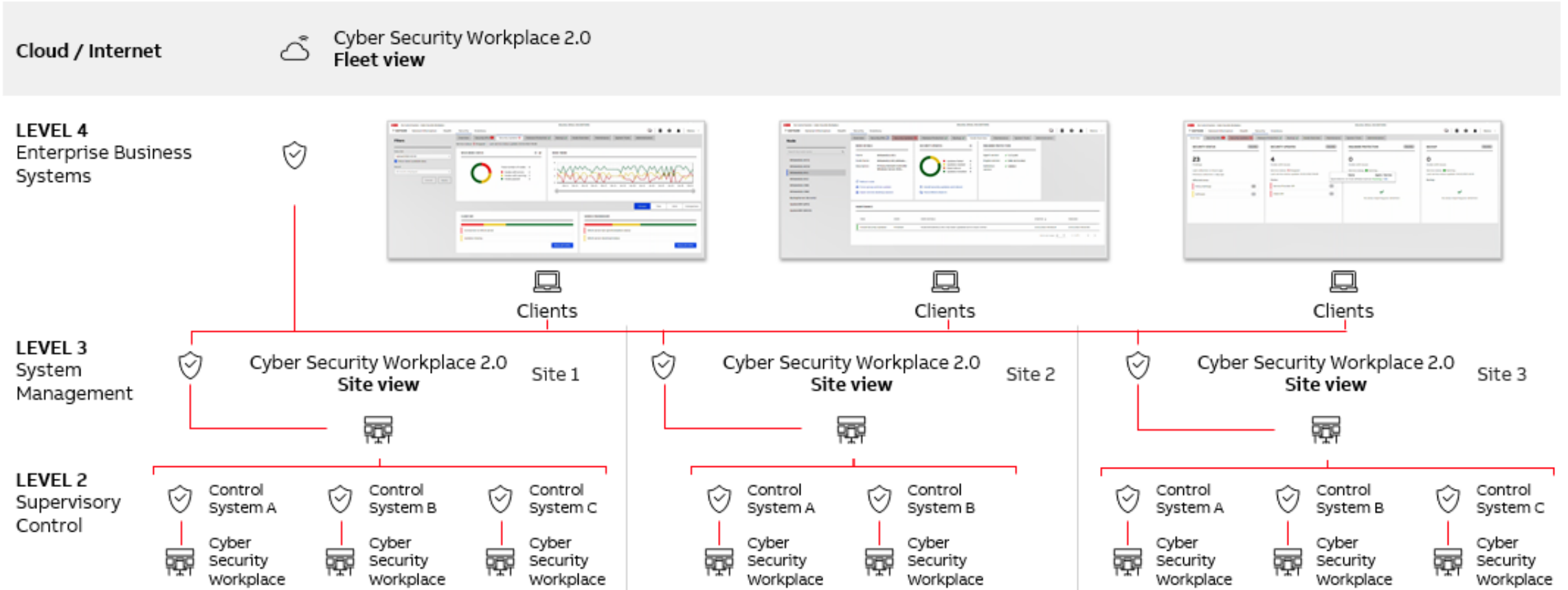


ABB Ability™ Cyber Security Workplace Architecture Fleet View

Partnership



FORESCOUT.



NOZOMI
NETWORKS

—
Collaboration with Nozomi and ForeScout to deliver the most comprehensive threat intelligence solutions



—
Integration with IBM security platform for digital threat visibility

Situational awareness

Difference between event and network monitoring



| | | |
|------------------------|--|---|
| Input data | System and device events | Network traffic |
| Detection | Directly - Based on defined rules | Indirectly - Based on heuristics |
| False positives | Low | High |
| Specificity | High - Detection is based on actual events | Low - Detection is based on score and confidence |
| Coverage | Supported systems | Any network-based system |
| Scope | Narrow - Only what is defined in the use-cases or manually detected | Wide - Anything that is abnormal |
| Technology | <ul style="list-style-type: none">• Security Information and Event Management system (SIEM)• Event collection technology• Use-cases & Runbooks | <ul style="list-style-type: none">• Network monitoring solution• Network TAPs or mirroring of network data |
| Example | Footsteps heard in the kitchen in the middle of the night following the opening of a window. | Noises are heard in the kitchen in the middle of the night when it is usually quiet. |

*Grazie per la Vostra
partecipazione e attenzione*



ASSOCIAZIONE **IMPRESE ITALIANE**
DI **STRUMENTAZIONE**