All'attenzione delle Commissioni riunite I e IX

Il Consorzio PI Italia raggruppa in Italia le 93 aziende che condividono le tecnologie più influenti nel campo dei protocolli e delle tecnologie di comunicazione industriale, per dare il proprio contributo al dibattito in corso in Parlamento ha accolto la richiesta di memoria scritta da lasciare agli atti delle Commissioni riunite I (Affari costituzionali, della Presidenza del Consiglio e interni) e IX (Trasporti, poste e telecomunicazioni) al fine di acquisire utili elementi di conoscenza e di valutazione relativamente Atto del Governo n. 164, recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (cd. NIS2).

Per quanto riguarda il contenuto tecnico dettagliato si rimanda ai due documenti seguenti, ma il senso di quanto si vuole portare all'attenzione delle Commissioni impegnate in questo importante lavoro di recepimento della direttiva europea è la richiesta di porre attenzione in particolare alla componente OT (operation technology) delle reti industriali che la stessa direttiva si propone di proteggere. Gli stessi dati di KPMG presentati durante il Main Event 2024 del Consorzio hanno evidenziato come nel settore manifatturiero è stato registrato, nell'ultimo anno, un aumento del 25% degli incidenti occorsi, e del 12% dei danni operativi conseguenti ad attacchi sui sistemi di controllo industriali. Questi dati, senza un impegno chiaro del Legislatore, possono peggiorare progressivamente e mettere a rischio il sistema industriale italiano se non si trova un equilibrio tra l'attenzione alla cybersicurezza nell'IT e nell'OT.

Vi ringraziamo per l'attenzione,

Cristian Sartori, presidente del Consorzio PI Italia".

SIEMENS

Support and solutions for the **NIS 2 Directive**

https://siemens.com/nis2-directive

Solutions to meet the reqirements of NIS 2

Get ready for NIS 2! Here, you'll find a brief overview of our consulting, hardware, and software offerings. Additionally, we provide in-depth information on cybersecurity that aims to protect network and information systems and their physical environment from incidents.
In addition to this selection, you will find other useful solutions in our portfolio.

↗ **Further information on NIS 2, including Article 20, Governance and Article 21 Cybersecurity risk-management measures**

SOLUTION

Develop the right security policies for your customers

In addition to technical measures, policies and procedures are mandatory as part of a security concept. Policies are equally important to meet the requirements of cybersecurity standards and regulations. You need to ensure that you develop the right policies for specific OT applications and define a set of policies that meet your customer's needs for their OT environment. Policies need to cover multiple solutions from multiple vendors and multiple stakeholders (asset owners, integrators, suppliers, maintenance partners, etc.).

Expert support to meet the specific needs of your customers

Policy Consulting, performed by experienced Siemens consultants, ensures that the customer gets the right policy that fits their organization and OT environment, based on our experience in various projects. The Security Consulting is based on Siemens' global experience to limit the effort for our customers and to get the required quality.

Industrial Security Consulting provides support from experienced consultants on security policies, consulting and engineering for the various cybersecurity measures that are part of a holistic cybersecurity approach to meet the requirements of cybersecurity standards and legislation.

SOLUTION 1

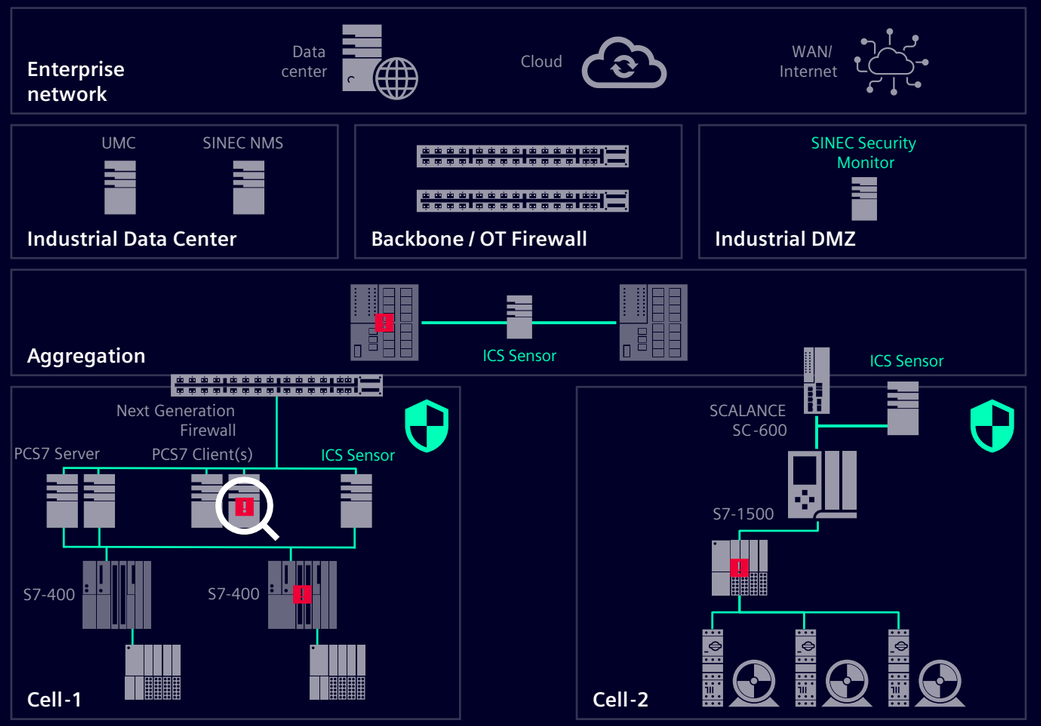
Detect threats at an early stage to increase security and availability

Cyber-attacks on industrial enterprises are on the rise. However, the lack of visibility into the security status of industrial control systems leads to increased cyber risk. Late detection of industrial cybersecurity incidents results in plant downtime and additional recovery costs. In addition, regulated industries are required to report security incidents.

Anomaly detection helps operators to act earlier

SINEC Security Monitor monitors network traffic, creates a baseline of normal operations, and detects anomalies from that baseline. This enables operators to react quickly and address threats at an early stage. The software automatically analyzes network traffic and correlates current traffic against a baseline or threat database to detect anomalies, such as hacker intrusion, data theft, etc.

The monitoring solution can be configured as 100% passive and integrates seamlessly into industrial networks and control systems. Local sensors collect the data in the different networks by mirroring the network traffic, pre-processing it and forwarding it to the central instance in the industrial DMZ. SINEC Security Monitor enhances the data quality with an agent for Windows-based endpoints.



SOLUTION 2

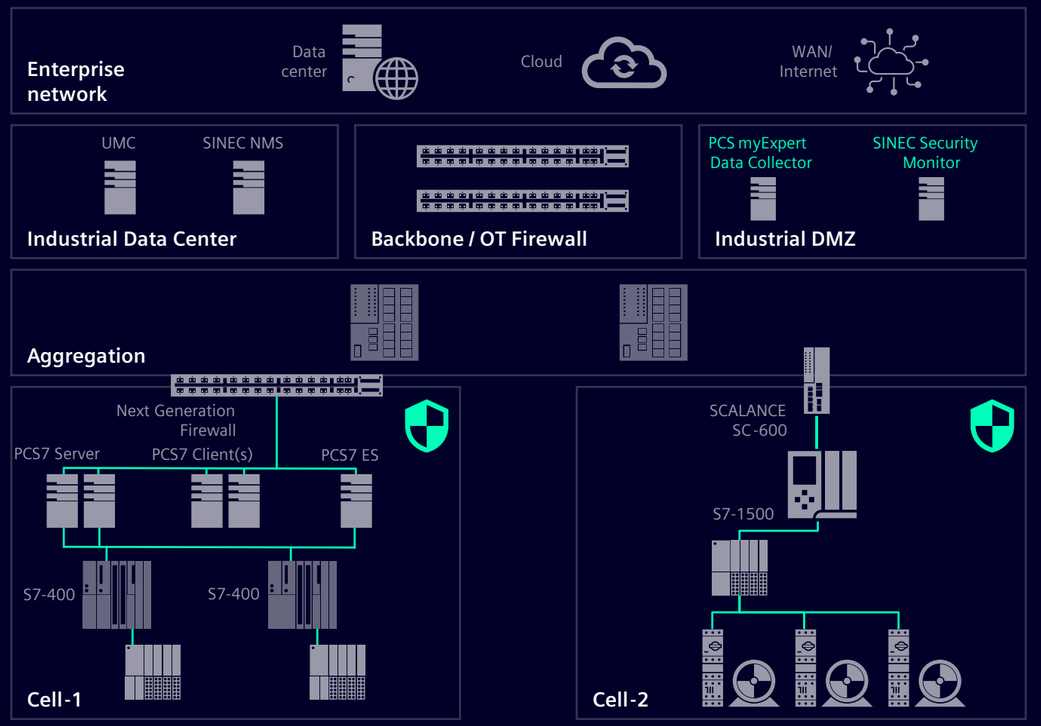
Collect and share security-relevant event data from OT devices

Due to increasing regulatory requirements such as IEC 62443-3-3, security-related event data must be collected and analyzed. Customer requirements for IT-OT integration do not require a dedicated solution, but rather the integration of OT safety events into the existing monitoring solution.

OT systems without direct connection to higher-level networks are required to provide security event data to the top-level security information and event management (SIEM) for further investigation. Even systems that are not capable of syslog must provide security event data to the top-level SIEM. Often, IT departments lack knowledge about the details of extracting security events from OT systems.

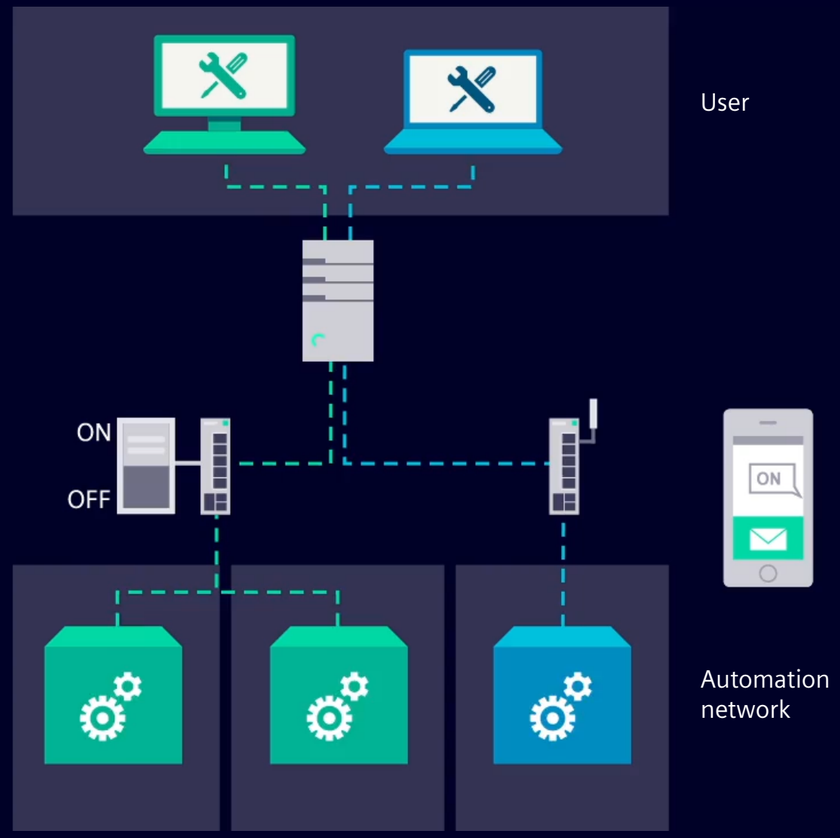
Integrate OT systems into an existing IT SIEM

SIMATIC PCS myExpert is a web-based application that monitors security events in a e.g. SIMATIC PCS 7 environment and forwards them to an existing IT top-level SIEM system. Security events are transferred to a central plant collector in the OT DMZ. This approach collects all OT security events in one place, normalizes data and adds location-specific information, sends consolidated data to the top-level SIEM, and meets all known regulatory and standards requirements.



SOLUTION

Ensure business continuity with backup management and secure remote access for recovery



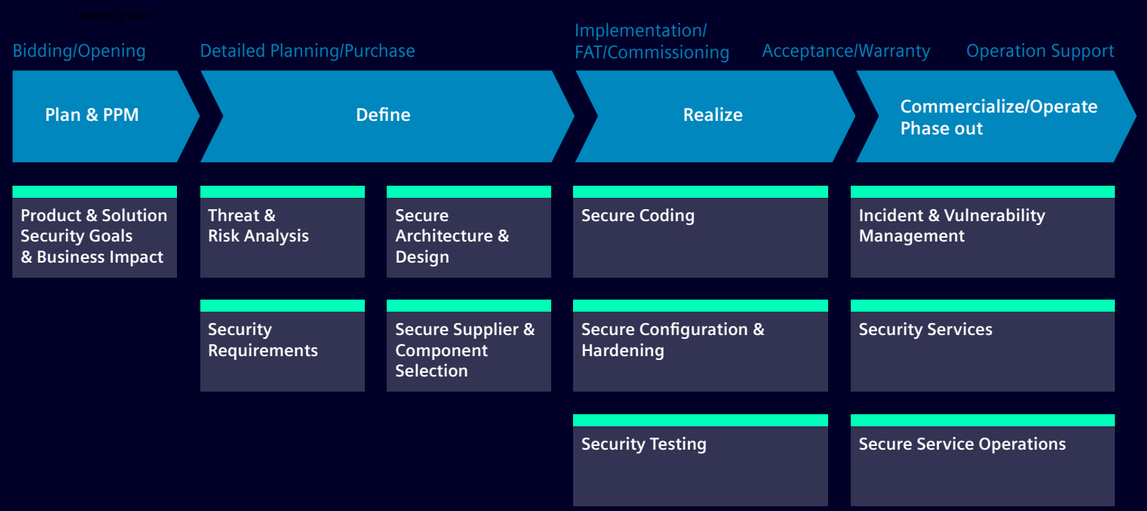
Industrial plants are typically distributed, sometimes across national boundaries. During the operation and optimization phases, maintenance and recovery from incidents in an operational distributed industrial plant and machinery must be performed without delay to avoid downtime for operations and services. Disaster recovery systems and remote recovery support address these challenges. At Siemens, we offer disaster recovery systems with online/offline backup options with a variety of local and offsite backup options, e.g. SIMATIC DCS SCADA Infrastructure.

How to establish secure remote connections

Establishing the connection for secured remote access is very easy with our VPN management platform SINEMA Remote Connect or the common Remote Service Platform cRSP. The service technician uses a SINEMA Remote Connect Client or cRSP, the system or the machine to be serviced, is equipped with a SCALANCE S Industrial Security Appliance, a SCALANCE M industrial router or Industrial Next Generation Firewalls. Secure remote access to the OT environment is also provided by the Zero Trust OT Access Service with the local processing platform SCALANCE LPE.

SOLUTION 1

Secure products and services along their lifecycle



A robust supply chain involves several key factors. It includes integrating cyber secure components into your products, ensuring that all applications involved in the process adhere to security standards, and being able to rely on your service providers in times of crisis. As manufacturers are also part of the supply chain, it's vital to establish a chain of trust through practices that lead to cyber resilience. Incorporating robust supply chain and product security measures throughout the lifecycle can help meet new laws and regulations and set high standards.

Consideration of the entire product lifecycle

Experts in automation, digitalization and cybersecurity identify vulnerabilities and risks in product lifecycle management, project management and engineering, and work with you to develop a security roadmap with specific supply chain security measures. Our supply chain security consulting services are delivered by consultants who draw on our own factory experience and take a holistic approach to risk management in product lifecycle management, project management, and engineering.

SOLUTION 2

Continually identify and evaluate vulnerabilities

Application cybersecurity requires a structured software bill-of-material (e.g. CycloneDX) to gain the ability to identify vulnerabilities, license compliance, and monitor the software supply chain. Throughout the application cybersecurity lifecycle, continuous assessment of risk and applicability of identified vulnerabilities is measured. However, this requires an understanding of cybersecurity risks and impacts throughout the lifecycle of software applications.

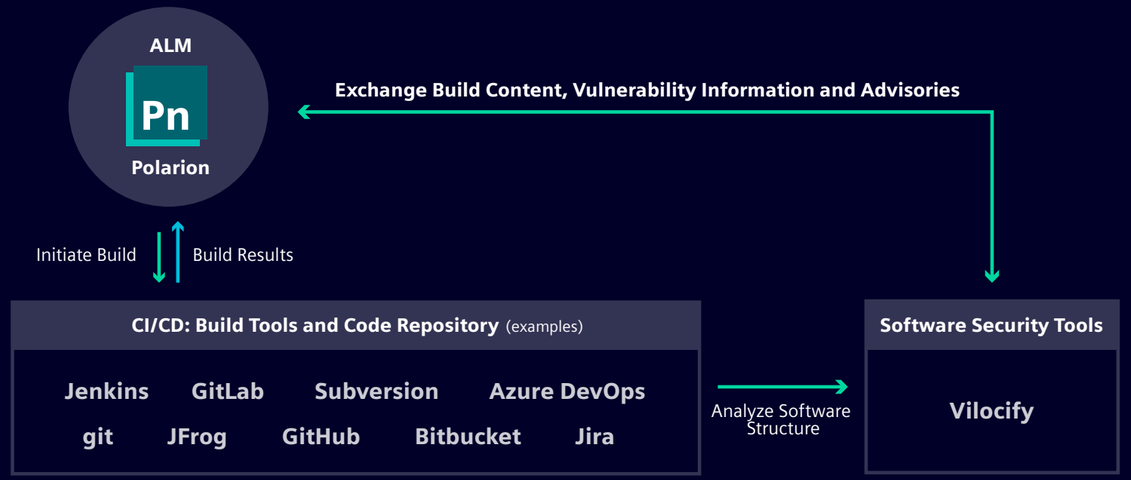
Control, manage, and maintain a cybersecurely developed application

Our comprehensive solution ensures complete product traceability by tracking industry requirements, performing threat and risk analysis, and documenting remediation efforts and product changes.

Polarion orchestrates the software cybersecurity ecosystem that connects build tools (CI/CD), code repositories, and test environments.

Software security tools such as Vilocify Vulnerability Services continuously identify and assess vulnerabilities and monitor the software supply chain.

Integrating Polarion into the process enables automated vulnerability management and compliance testing of software components



SOLUTION

Manage vulnerabilities and patches to increase security and availability

During the operations and optimization phase, systems must be updated on a regular basis. New vulnerabilities are reported daily for many systems. Vulnerabilities can be exploited by attackers if proper mitigation is not implemented. Identifying new vulnerabilities as soon as possible and minimizing the time to patch is critical. One of the NIS 2 Cybersecurity Risk Management (CRM) obligations is the handling and disclosure of vulnerabilities.

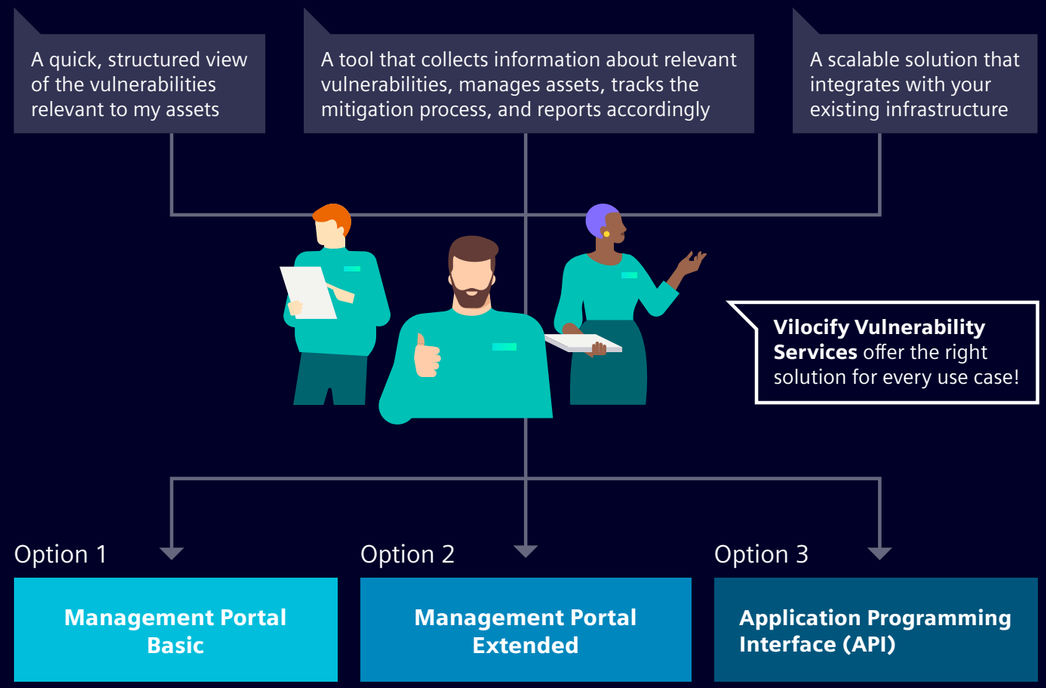
Secure your infrastructure and product portfolio

Vilocify Vulnerability Services empower you to secure your infrastructure and product portfolio by providing relevant, actionable vulnerability intelligence. You receive vulnerability alerts for your individual system via different options:

- Management Portal: Web-based application offering a structured overview of relevant vulnerabilities for your components
- Application Programming Interface (API): Seamless interface to integrate the vulnerability intelligence into your existing vulnerability management tools and processes

With its vulnerability scanner, SINEC Security Inspector also checks the network for potential gateways that could be used for cyber-attacks to compromise systems and data. Patch Management helps you manage critical Microsoft product updates.

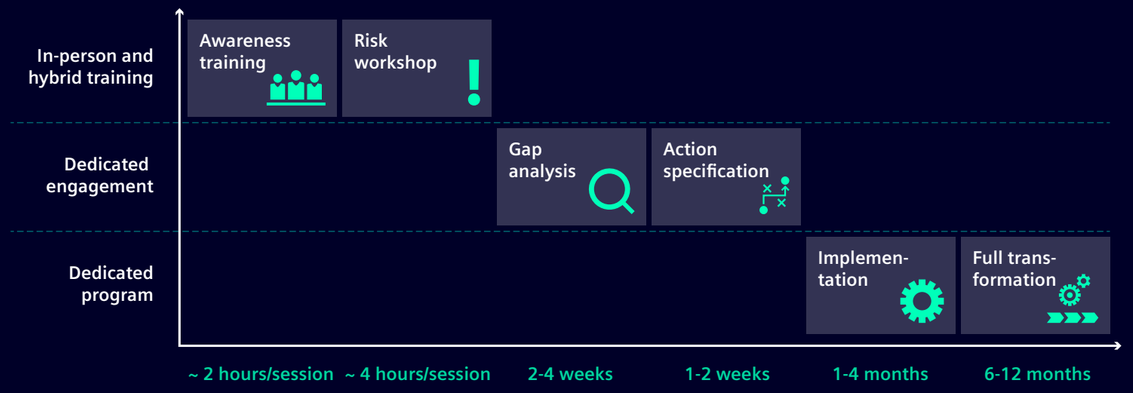
Requirements



SOLUTION

Help the board and CEO deal with NIS 2 requirements

The executive team and employees must acquire sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the organization. The board and CEO must also evaluate whether and how to disclose a cyberattack internally and externally to customers and investors. However, finding the right training provider with appropriate knowledge of processes, procedures and cybersecurity solutions in IT and OT is challenging. It's important to find a modular training offering that fits your organization's unique needs, and to work with a training provider that will be with you for the long haul of the NIS 2 journey.



Build cyber resilience in your organization

Cybersecurity Training delivered by experienced Siemens consultants ensures that the organization receives the right training content, tailored to the needs of the organization and the IT and OT environment, based on our experience in various projects. Our step-by-step approach ensures that we guide organizations from the first NIS 2 awareness training to the implementation of NIS 2 compliance. Our experienced trainers are always responsive to your individual needs.

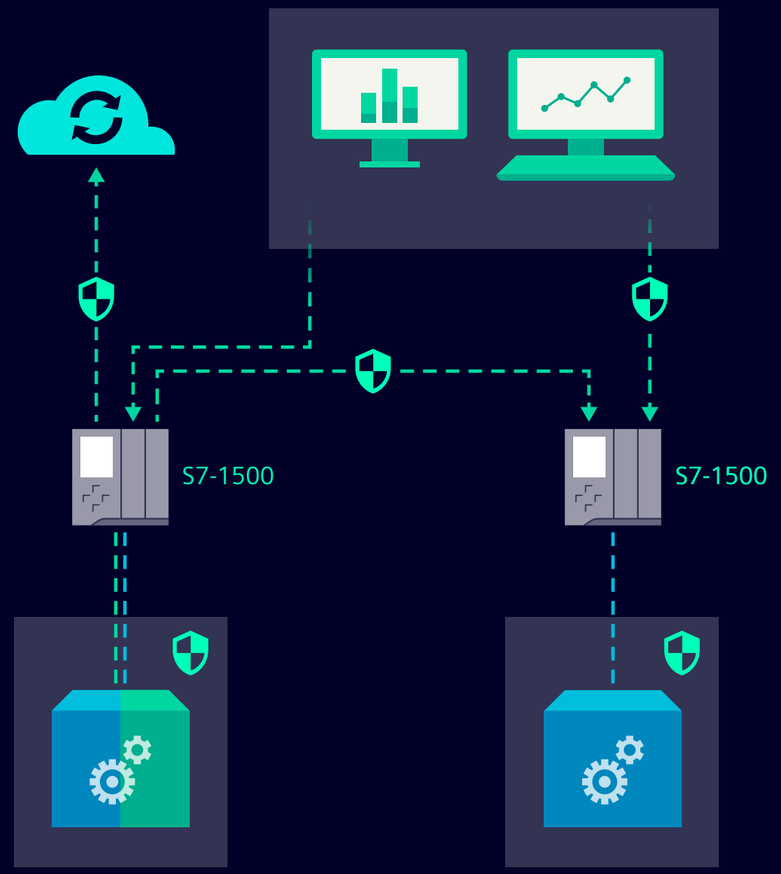
SOLUTION

Mitigate cyber risks with encrypted communication for OT

As manufacturing becomes more dynamic, data access throughout the product lifecycle becomes critical. Devices, systems, and users exchange data continuously or on demand without proper data access management or identification mechanisms. Without these mechanisms, anyone can connect to the network, making the system vulnerable to man-in-the-middle attacks. Because the data is in clear text, it is vulnerable to theft, manipulation, espionage, and sabotage. One of the NIS 2 Cybersecurity Risk Management (CRM) obligations is the use of cryptography and, where appropriate, encryption.

Secure communication and system integrity factors

Ensure system integrity through authentication and encryption, for example with end-to-end encryption between TIA Portal, S7-1500/1200 controllers, and HMI stations thanks to state-of-the-art secured communication based on Transport Layer Security (TLS) V1.3.



SOLUTION 1

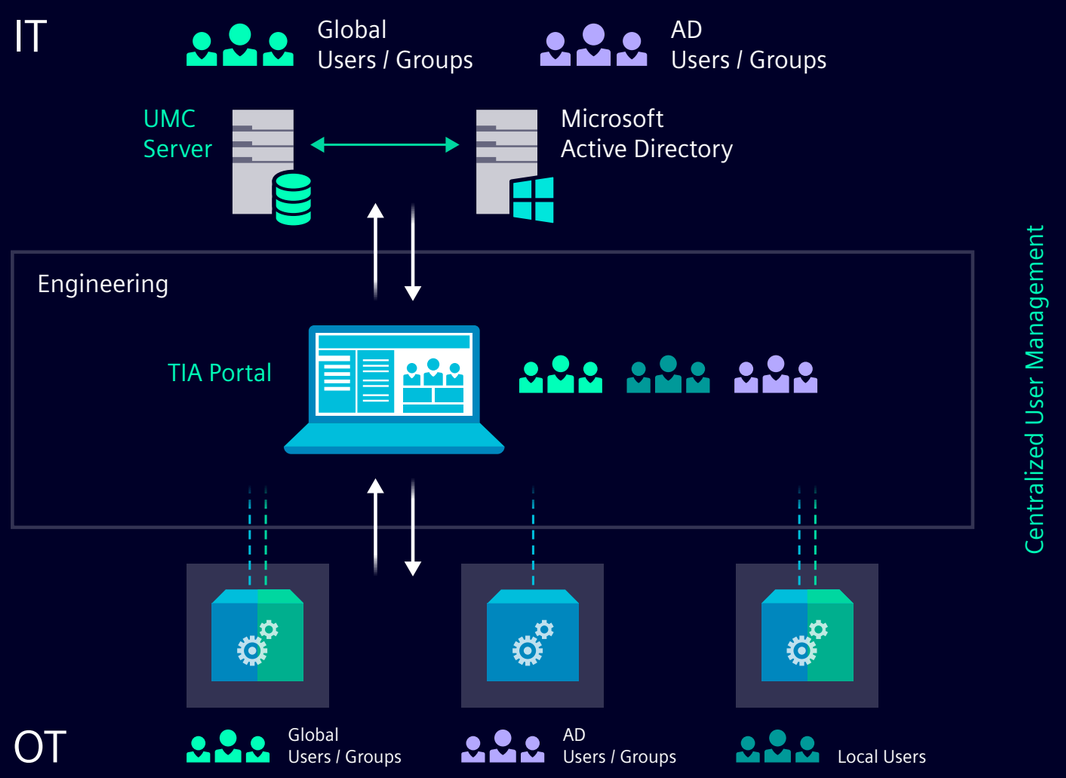
Easily and centrally manage users, roles and access rights

Preventing unauthorized access to user programs, the automation system, and data during the design and maintenance phases requires granular configuration of user privileges and access management. Often, user management is not centralized during engineering and especially during operations.

Engineering projects require user management and access control to prevent unauthorized access, resulting in increased effort. Individual access rights for each user should be based on their role. This results in even more effort to keep each project consistent and to update projects according to user changes.

Efficient user management at the OT level

Implementing a centralized user management requires just a few steps. Import users and groups from Microsoft Active Directory to the UMC server and connect the TIA Portal engineering station to the UMC server. Import users and groups from the UMC server to TIA Portal, then assign rights and roles locally.



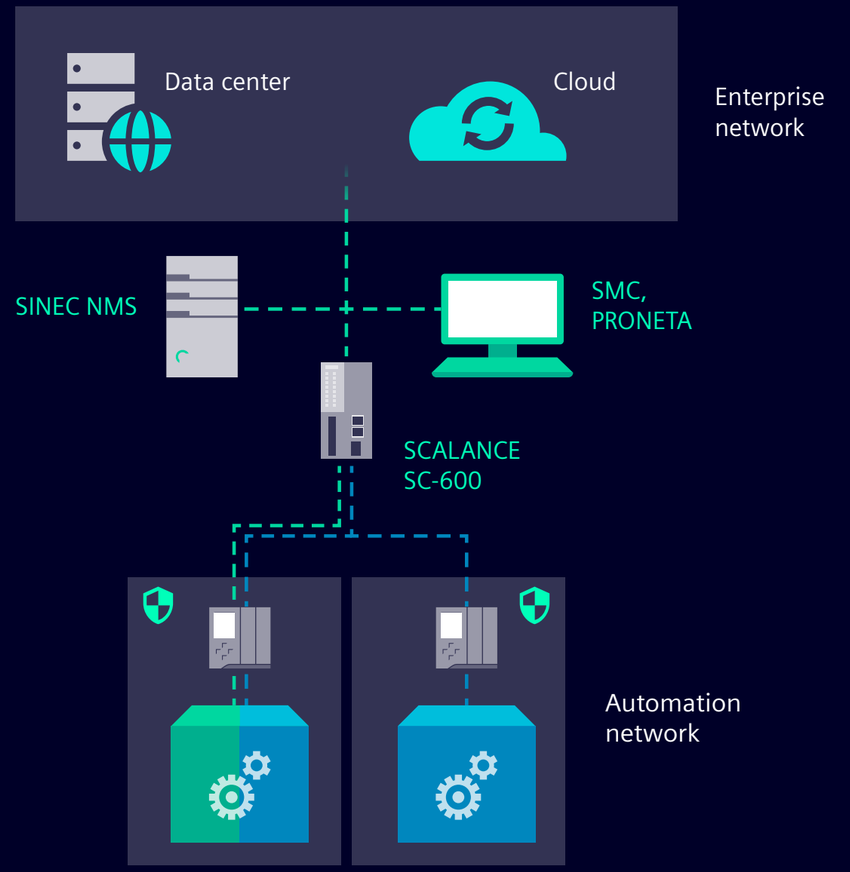
SOLUTION 2

Improve security with asset discovery and management

As manufacturing becomes more dynamic, data access throughout the product lifecycle becomes critical. Devices, systems, and users exchange data continuously or on demand without proper data access management or identification mechanisms. Without these mechanisms, anyone can connect to the network, making the system vulnerable to man-in-the-middle attacks. Because the data is in clear text, it is vulnerable to theft, manipulation, espionage, and sabotage. One of the NIS 2 Cybersecurity Risk Management (CRM) obligations is the use of cryptography and, where appropriate, encryption.

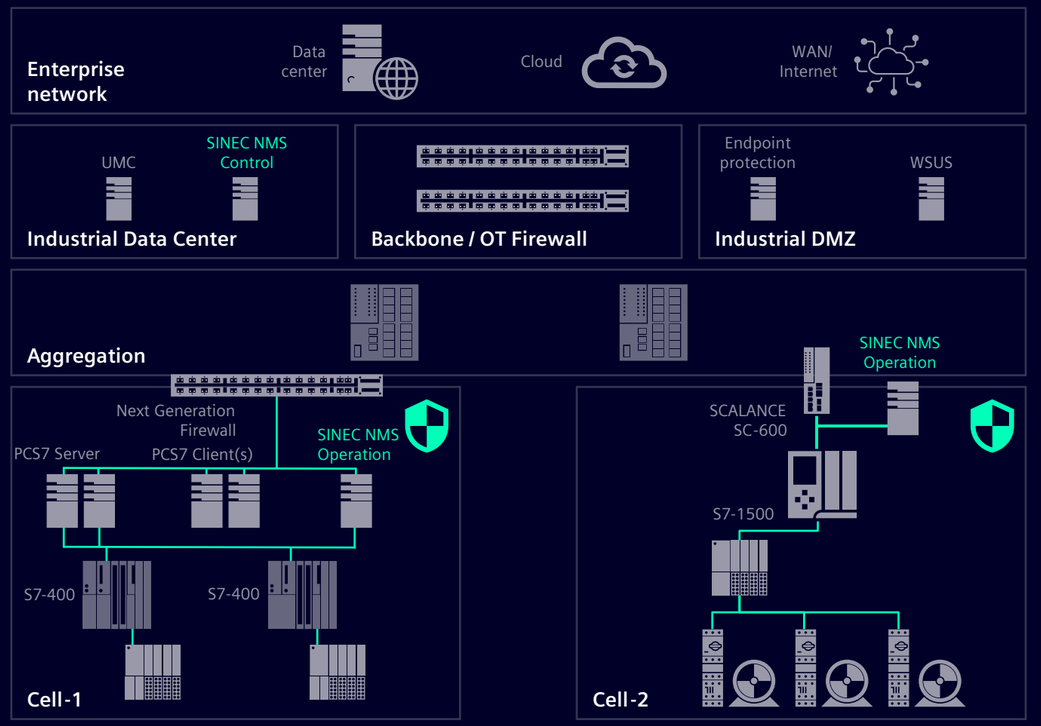
Get a comprehensive view of all your assets

Our solution makes use of the centralized SINEC NMS (Network Management System), SMC (SIMATIC Management Console), and PRONETA to provide network monitoring, topology discovery, diagnostics and firmware management. Additionally, SINEC Security Inspector features a high performance, nonintrusive, vendor independent scans to generate easy to manage installation overview.



SOLUTION 3

Gain a comprehensive view of all your network assets across the plants



A holistic approach to cybersecurity requires the ability to discover, monitor, operate and manage all OT assets, including critical ones. Throughout the cybersecurity lifecycle, a detailed view of OT assets is required to effectively manage these assets and reduce their attack surface.

The challenge is that plants contain many network assets from many different vendors and may also contain legacy assets. Equipment upgrades and the latest firmware updates are not included in network asset lists. Network assets with outdated firmware are a particular cybersecurity risk.

Support for discovery of your network assets

Our solution seamlessly and comprehensively assist customers in network asset discovery and management:

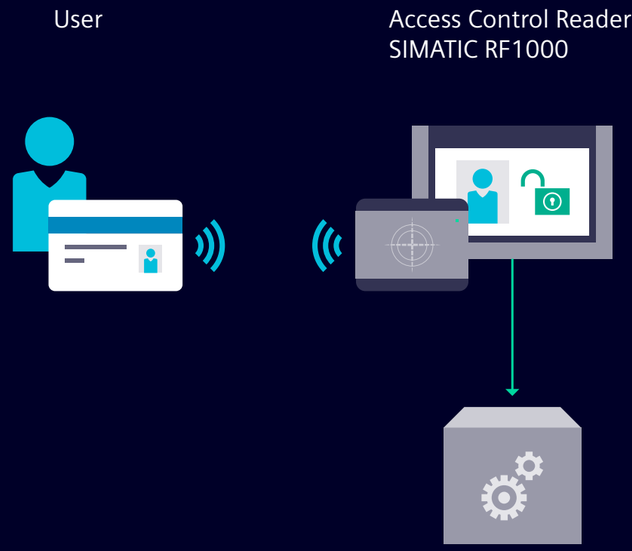
- Inventory and visibility: Maintain an up-to-date inventory of all devices, equipment and software in your plant's network.
- SINEC NMS automatically discovers network assets and manages them in an inventory list or network topology view, providing a complete, up-to-date view of all components in the network, including their properties.
- In addition, various network areas can be monitored, including automation products such as PCS 7/neo, PLCs, PROFINET-IO and third-party assets.

SOLUTION

Prove and verify a user’s ID to a system

A variety of applications are important sub-elements of a production or process. Different people have access to these applications. It must be ensured that only authorized persons have access to these applications. Availability of production systems is a top priority. Unauthorized access to machines can cause downtime. Ensure that only authorized and trained personnel have access at all times.

Brownfield environments are often an obstacle, and stakeholders don’t pay enough attention to authentication. There is a lack of visibility into where multi-factor authentication makes sense in production, and many organizations haven’t developed processes to enable multi-factor authentication and don’t know what solutions are available on the market to help them implement it. In addition, local and remote access to the HMI is required to operate the machine.



Reliable access control protects system integrity

The solution is the explicit identification of operators at machines and plants, including:

- Access control
- Audit trail

The SIMATIC RF1000R access control reader supports one-time and permanent RFID card logon, as well as RFID card logon with user credentials:

- One-time reading of the ID card
- Permanent reading of the ID card
- One-time reading of the ID card with additional user-specific password authentication

SOLUTION

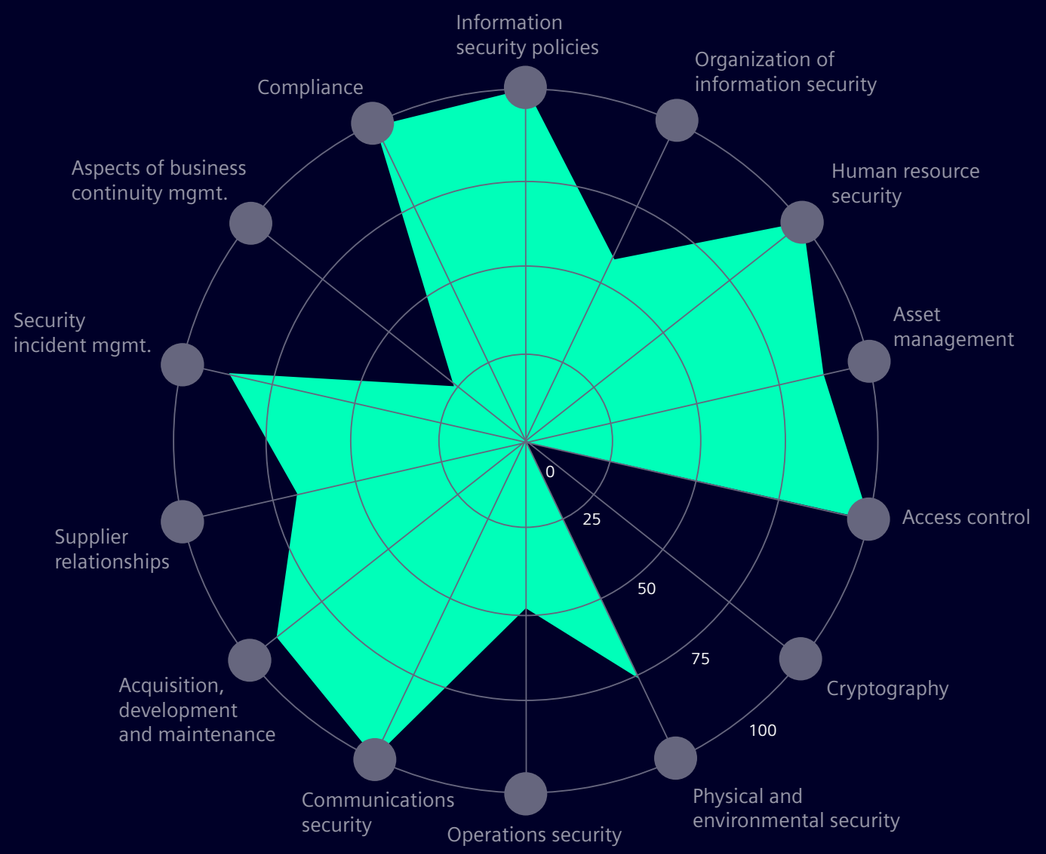
Gain transparency and develop a security roadmap

Implementing effective security measures is critical. The pressure on industrial companies to comply with national laws and regulations, such as NIS 2 and NIST, and standards, such as IEC 62443 and ISO 27001, is increasing significantly. Capacity for industrial cybersecurity and industrial cyber-security expertise is scarce, and IT staff need support from security experts with automation expertise. Time pressures are increasing due to new compliance requirements and legislation. In addition, conducting comprehensive assessments and developing customized security plans is not easy and often requires deep knowledge of both OT and IT.

Leverage the expertise of cybersecurity and industry experts

Security Assessments include a holistic analysis of threats and vulnerabilities, identification of risks, and recommendations for closing identified gaps. They maximize transparency and provide a complete overview of the current security status of your automation systems. You can choose between a compact one-day on-site assessment (Industrial Security Check) or an in-depth assessment of compliance with IEC 62443 (IEC 62443-3-3 / NIS 2 and IEC 62443-2-1 Assessment).

Industrial Security Consulting provides on-site support from experienced consultants on security policy and plant-specific network design, as well as customized implementation support for the Industrial Security portfolio.



Contact

Published by

Siemens AG
Digital Industries
Factory Automation
P.O. Box 4848
90026 Nuremberg
Germany

For the U.S. published by

Siemens Industries Inc.
800 North Industry Parkway
Suite 450
Alpharetta, GA 30005
United States

TXOne Networks

2023 /Q2

Mastering the NIS2 Directive: Achieving Cybersecurity Compliance

txOne networks

TXOne Networks

Mastering the NIS2 Directive: Achieving Cybersecurity Compliance

txOne networks

Mastering the NIS2 Directive:
Achieving Cybersecurity Compliance

Table of Contents

Introduction

The "**Network and Information Security (NIS) Directive**" is the first EU-wide legislation on cybersecurity, with the specific goal of achieving a standardized level of cybersecurity between EU member states, with a focus on protecting critical infrastructure. After the EU adopted the NIS1 Directive in 2016, EU member states were required to transpose it into domestic law by May 9, 2018.[1]

However, since the adoption of the NIS1 Directive, the threat environment has undergone significant changes, considering the increasing dependence of the economy on digital technology, and the growing importance of network resilience for essential services such as healthcare and energy due to the Covid-19 pandemic. Moreover, not all industries that were originally expected to be covered by the NIS1 Directive are included, and at this point NIS1 has been shown to lack effective enforcement and supervision during implementation.[2]

Due to these internal and external factors, the European Commission proposed replacing NIS1 with NIS2 to address the shortcomings of certain provisions or methods in the past NIS Directive, introduce more entities and sectors, instate stricter regulatory measures, and establish stricter enforcement requirements to raise the baseline level of digital security in Europe and ensure future economic resilience. In November 2022, the Network and Information Systems (NIS) 2 Directive was approved by the European Council and published in the EU Official Journal. Member states must adjust their national legislation to comply with the new rules by October 17, 2024.[3]

As the scope of the NIS2 discipline is broader, more entities will be subject to European cybersecurity discipline in the future, and companies that have already been bound by previous rules should reassess their status to determine whether they will comply with the new law. It seems that there is still a long way to go before member states complete implementation (i.e., before October 2024). However, given the detailed obligations of the NIS2 Directive and the timeline for implementing directive measures, companies must implement internal safeguards in technology and organization as soon as possible to protect themselves from potential cyber attacks and prepare for the strict requirements that will be imposed on relevant departments. In this article, we will first highlight the shortcomings of the NIS1 Directive discussed during the review process (Part 1), then analyze the main policy objectives of the NIS2 Directive and discuss the changes compared to the NIS1 framework (Part 2). Then, we will conduct a technical analysis of the core principles of the NIS2 Directive and how the industry should respond (Part 3). Finally, we will summarize (Part 4).

The Necessity of NIS2

Due to some issues exposed during the implementation of the NIS1 Directive, including significant changes in the threat environment, flaws in certain provisions, ineffective supervision and enforcement systems, and a lack of systematic information sharing among member states, it was necessary for the EU to update the NIS Directive and take more comprehensive measures. Therefore, NIS2 became an important component of the EU's cybersecurity strategy, and aims to replace NIS1 in order to better combat current and future cybersecurity challenges.

The threat environment has undergone significant changes

Since the outbreak of the COVID-19 crisis, the EU's economy has become more dependent than ever on networks and information systems, and industries and services are increasingly interconnected. The COVID-19 crisis has demonstrated the need for the EU's digital transformation, especially in improving network resilience for critical operational services such as healthcare and energy. In recent years, the level and variety of cyberattacks have also greatly increased, further highlighting the need for the EU to have a higher level of network. In addition, the NIS Directive's coverage of industries is too limited and needs to be updated and expanded to address current and future risks, with the security of 5G technology posing one of the larger challenges.

Certain provisions of the NIS1 Directive have flaws

A major shortcoming in the NIS1 Directive is the lack of a unified approach, resulting in significant inconsistencies among member states in compiling lists of operators of essential services (OESs) and digital service providers (DSPs). Therefore, companies of the same type may face different requirements depending on their member state. The EU's NIS assessment found that the old Directive did not provide sufficiently clear OES scope standards or national responsibilities for digital service providers. This has resulted in certain types of entities not being identified in some member states, and therefore not being required to take security measures or report incidents. For instance, large hospitals in some member states lay outside the scope of the NIS Directive and are therefore not required to implement corresponding security measures, while in another member state, almost every healthcare institution is covered by NIS security requirements. These differences have a negative impact on implementing fair competition, as an entity in one member state may face operational costs to comply with this framework while a similar entity in another member state may not.

In addition, the NIS Directive gives member states wide discretion in formulating OES security and incident reporting requirements. The EU's NIS assessment showed that member states' implementation of these requirements is markedly different in some cases, adding an additional burden to companies operating across multiple member states. Therefore, most survey participants agreed that common EU rules are needed to address cyber threats, as today's cyberattacks can quickly spread across borders (such as in the cases of NotPetya, LockBit, etc.).

The supervision and enforcement systems of the NIS Directive are ineffective

There is a significant difference in financial and human resources allocated by member states to perform their tasks (such as OES identification or supervision) and the ability to handle cybersecurity risks. The inconsistency in ability from one organization to another comes from, among others, different capability requirements. One company may set very strict capability requirements, and another might have unclear or loose requirements, leading to a larger gap between companies. This is just one example. Situations like these further exacerbate the differences in cybersecurity resilience among member states. Additionally, there is no deterrent to this because there are no minimum standards for administrative penalties under the NIS1 Directive.

There is no systematic information sharing among EU member states

This has a negative impact on the effectiveness of cybersecurity measures and the level of joint situational awareness at the EU level. This also affects information sharing among private entities and the participation of private entities in collaboration structures at the EU level, again adding to the inconsistencies of cybersecurity levels across different member states.

NIS2 Directive: Critical Updates for Cybersecurity in the EU

NIS2 is not just a simple revision of the previous regulations, but includes many important differences aimed at achieving better coordination of security standards and reporting obligations. In 2020, the EU's "Cybersecurity Strategy" laid the foundation for future measures, including the "Network and Information Systems Security Directive" (NIS2).

1. The Scope of NIS2

Although both NIS1 and NIS2 have the same goal of requiring EU member states to implement measures to achieve a high level of common network and information system security within the Union, the NIS1 framework focuses on "network and information system security", while the NIS2 directive focuses on the broader holistic concept of "cybersecurity", including operational systems and content defined by the cybersecurity law.

The Scope of Sectors

In terms of scope, one change in NIS2 is the replacement of the operators of essential services (OES) and digital service providers (DSP) categories in NIS1 with technology-independent proprietary terms "essential entities" and "important entities". In addition, the industries covered under the purview of NIS2 have been further expanded, as detailed in Directive Appendices 1 and 2.

To summarize, it is evident that many more industries have become the focus of this framework, and there has been significant expansion in comparison to the industries covered by NIS1. By April 17, 2025, member states should establish lists of essential entities, important entities, and entities that provide domain name registration services. To this end, member states should require entities to submit at least the following information to the competent authorities: the entity's name, address, email address, IP range and so on, and member states should periodically review and update that list at least once every two years. The European Commission and the European Union Agency for Cybersecurity (ENISA) will provide guidance and templates to guide member states in reporting relevant content.

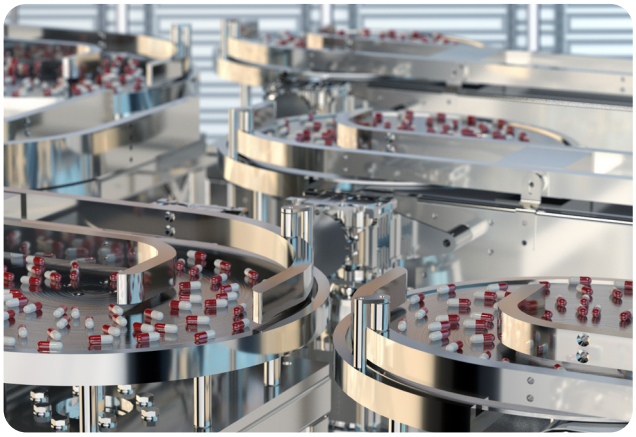


Table 1. Sectors of Essential Services

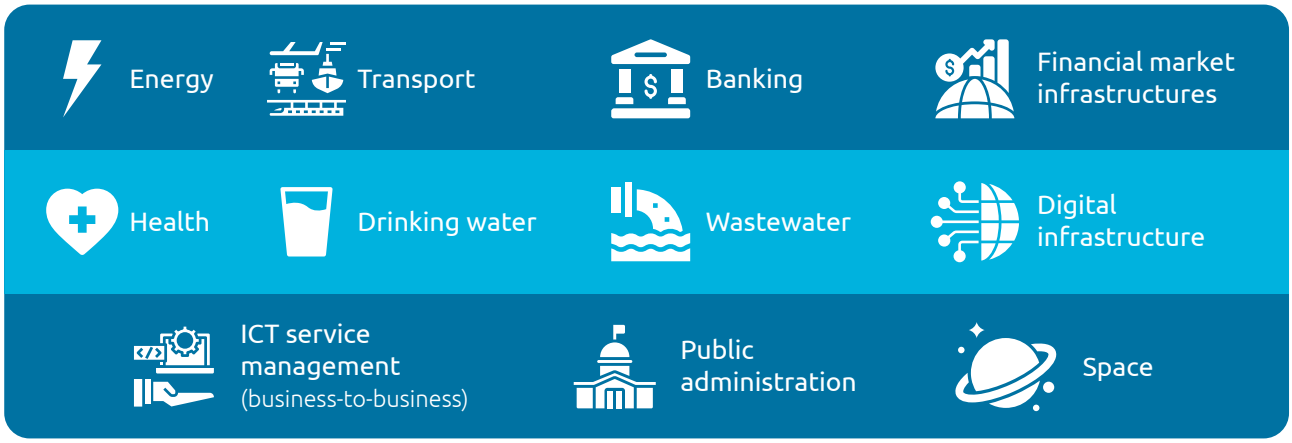
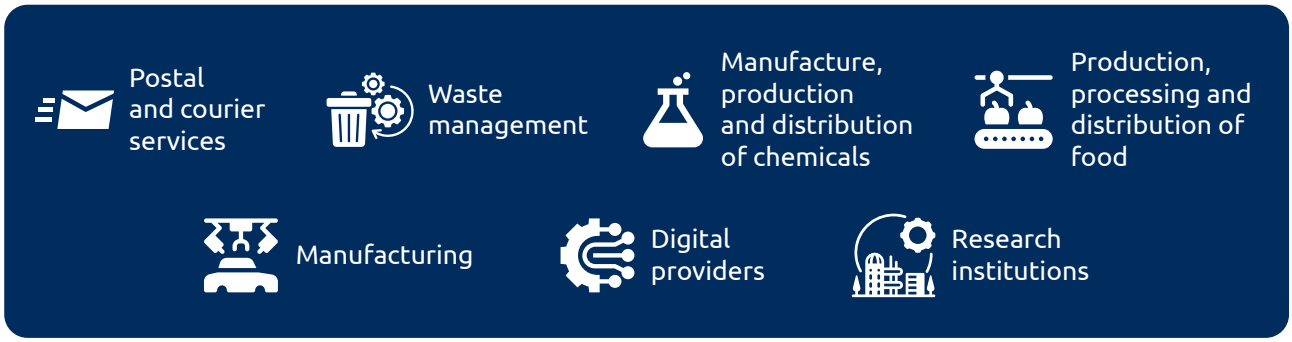


Table 2. Other Important Sectors



The Scale of Enterprises

In terms of scale, NIS2 applies to public and private entities that meet the requirements for medium-sized enterprises or above and belong to the essential entity category specified in Appendix I or the important entity category specified in Appendix II, excluding micro and small enterprises. That is to say, entities that are not listed in the appendix or, even if listed in the appendix, have fewer than 50 employees and an annual revenue of less than 10 million euros, are excluded from the scope of NIS2. It is worth noting that certain types of entities, because of their unique industry attributes, are subject to the influence of NIS2 regardless of their size. When an entity meets specific conditions listed in Appendix I and Appendix II, NIS2 can apply to entities of any size, including entities that:

a) Are considered essential entities under Directive (EU) 2022/2557 (The Critical Entities Resilience Directive; CER)

b) Are providers of public telecommunications networks or publicly available electronic communications services, trust service providers, or top-level domain name registries and domain name system service providers

c) Are the sole providers of necessary services for a specific key social or economic activity within a specific member state

d) May have a significant impact on public safety, public security or public health, or may produce significant system risks, especially for cross-border effects when their services are interrupted

e) Are crucial because of their importance to a particular industry or service type or to other interdependent industries

f) Provide domain name registration services

g) Might fall into the scope of this directive if they are member states that are: (a) public administrative entities at the local level; (b) educational institutions

This directive does not apply to public administrative entities engaged in activities related to national security, public safety, defense or law enforcement (including prevention, investigation, detection and prosecution of criminal offenses). The coverage of NIS2 is becoming increasingly broad, and uncertainties exist in the interpretation of certain standards, as well as the broad definition of certain industries, which may lead to an increase in the number of entities that need to comply with the new directive and related requirements.[3] For example, the automotive industry is now listed as another critical industry in Annex II of NIS2, which means that existing entities in Europe need to comply with the new requirements should North American electric vehicle manufacturers and battery manufacturers decide to produce their vehicles or parts in the EU. The same applies to Asian manufacturers such as Toyota and Hyundai. Similarly, the scope of the health sector has been expanded, including research and manufacturing of EU-sanctioned laboratories, medicines, and medical devices, which was particularly important during the Covid-19 pandemic. Therefore, investments in the health sector will also be subject to NIS2 regulations.

Specific Sectors of EU Regulations Should Cooperate with NIS2

Another regulation to consider is the new Critical Entities Resilience Directive (CER Directive), which replaces the 2008 Critical Infrastructure Directive. The resilience of the "critical entities" category in the CER Directive is demonstrated in that it includes entities from 11 sectors, which have significant overlap in NIS2. The main difference is that the CER Directive addresses the physical security of these entities, while NIS2 addresses their cybersecurity. Given the interdependence of these two aspects, NIS2 and the CER Directive establish a consistent approach. Therefore, entities may need to comply with both frameworks, and supervisory authorities under both frameworks should closely cooperate on certain issues.[4]

Another new approach is the Digital Operational Resilience Act (DORA) for the financial industry. DORA specifically lists 21 types of regulated entities, including credit institutions, payment and electronic money institutions, investment firms, insurance and reinsurance companies, and crowdfunding service providers. In addition to the financial entities themselves, DORA also applies to some extent to third-party providers that provide ICT-related services to them. The framework aims to establish common requirements for their digital operational resilience, including cybersecurity. DORA mainly focuses on risk management, testing, managing third-party risks, and supervising critical third-party providers. NIS2 can serve as a generic cybersecurity law, while DORA operates specifically as cybersecurity law for the financial industry.

2. A Coordinated Cybersecurity Framework

Originally, NIS1 focused solely on cybersecurity strategies for networks and information systems. However, NIS2 expanded its focus to include national cybersecurity strategies. According to Article 7, each member state should develop a national-level cybersecurity strategy that includes strategic objectives, the resources required to achieve these goals, and corresponding policies and regulatory measures to achieve and maintain a high level of cybersecurity [Article 7]. To ensure the specific content of each member state's national cybersecurity strategy, NIS2 explicitly requires that the strategies cover supply chain cybersecurity, vulnerability disclosure, and information-sharing tools, among others, and that they be reassessed at least once every five years.

National Cyber Crisis Management Frameworks

In light of the Colonial Pipeline and Ukrainian power grid attacks, NIS2 introduces a new requirement that member states must designate or establish one or more specialized organizations responsible for large-scale cybersecurity incidents and crisis management (cyber crisis management organizations). The goal is for member states to develop national large-scale cybersecurity incident and crisis response plans, which outline the objectives and arrangements for managing large-scale cybersecurity incidents and crises. These plans should specifically include:

a) objectives of national preparedness measures and activities.

b) missions and responsibilities of cyber crisis management authorities.

c) cyber crisis management procedures, including integration into national crisis management frameworks and information exchange channels.

d) national preparedness measures, including exercises and training activities.

e) relevant public and private stakeholders and infrastructure.

f) national processes and arrangements to ensure relevant national authorities and institutions effectively participate in and support joint management of large-scale cybersecurity incidents and crises.

Computer Security Incident Response Teams (CSIRT)

As with NIS1, member states must designate Computer Security Incident Response Teams (CSIRT). NIS2 primarily adds some requirements for CSIRT capabilities, such as:

a) monitoring and analyzing cyber threats, vulnerabilities, and events at the national level, and providing assistance for real-time or near-real-time monitoring of networks and information systems for relevant essential and important entities when necessary.

b) issuing early warnings, alerts, announcements, and information about cyber threats, vulnerabilities, and events to relevant important and essential entities, relevant supervisory authorities, and other stakeholders, if possible, in near-real-time.

c) responding to incidents and providing assistance to relevant important and essential entities.

d) collecting and analyzing forensic data and providing dynamic risk information about cybersecurity.

ENISA to Maintain an EU Vulnerability Database

Furthermore, a new requirement in NIS2 addresses vulnerability disclosure with the aim of comprehensively addressing the cyber resilience issues of ICT products and services. Any security vulnerabilities, be they unintentional or intentional weaknesses, attack-prone vulnerabilities, or flaws, should be included in the database. Additionally, manufacturers of these products and providers/ developers of services should be compelled to promptly address these vulnerabilities upon receiving reports.

The European vulnerability database, developed and maintained by ENISA, streamlines the reporting process and increases efficiency, minimizing the efforts required by all participants. Additionally, CSIRTs act as trusted intermediaries for reporting and disclosing vulnerabilities. If a reported vulnerability has significant implications for other member states, CSIRT can notify the CSIRTs network. ENISA will maintain an EU vulnerability database where known vulnerabilities can be voluntarily disclosed.[4]

In other respects, similar to NIS1, the competent authorities and CSIRTs of member states need to cooperate at the national level and exchange information regularly to ensure they receive notifications of significant events, routine events, cyber threats, and near-misses in networks and information systems.

3. EU and International Cooperation

NIS2 retains the NIS1 Cooperation Group, which consists of representatives from the member states, the Commission, and ENISA. Although the specific formulation of its tasks has been updated to reflect new challenges and the new framework, the group's mode of operation essentially maintains the principles of NIS1. The national CSIRTs remain members of the CSIRT Network.

A new institution introduced in NIS2 is the European Network Crisis Liaison Organization (EU-CyCLONe) [Article 16]. This organization is responsible for coordinating operational-level management of large-scale cybersecurity incidents and crises and ensuring regular exchange of relevant information between member states and Union institutions, agencies, offices, and bodies. EU-CyCLONe are responsible for:

a) enhancing preparedness for the management of large-scale cybersecurity incidents and crises.

b) developing shared situational awareness for large-scale cybersecurity incidents and crises.

c) assessing the consequences and impacts of relevant large-scale cybersecurity incidents and crises, and proposing possible mitigation measures.

d) coordinating the management of large-scale cybersecurity incidents and crises and supporting decision-making at the decision-making level.

e) discussing national large-scale cybersecurity incident and crisis response plans.

Another new requirement is peer review. In the past, the principle under NIS1 regulations was that member states could freely develop their national strategies with little involvement from others. Under NIS2, national strategies can be voluntarily submitted for peer review by cybersecurity experts designated by at least two member states. The peer review can cover aspects such as: the implementation level of cybersecurity risk management measures in Article 21, the operational capabilities of CSIRTs, the implementation level of mutual assistance, and the implementation level of cybersecurity information sharing, among others.

4. Risk Management and Reporting

In order to implement the requirements of Article 21 of the NIS2 Directive, Article 20 appoints the management of essential and important entities the task of approving risk-management measures, implementing them, and ensuring that those entities are in compliance. This also means they are liable for the entities' infringements of Article 21. To that end, member states shall ensure that these management bodies follow training and that they should offer their employees similar training on a regularly updated basis so as to equip them with the knowledge and skills required to identify risks and adeptly assess cybersecurity risk-management practices for their efficacy and their impact on the entity's services. Within this training, employees should be made aware of commonly encountered cyber threats, phishing and social engineering techniques.

Cybersecurity awareness and cyber hygiene are necessary for raising the level of cybersecurity within the Union, especially with the increasing digitalization of devices and the Internet of Things. In particular, conscientious efforts should be made to increase the level of risk awareness related to these devices. Cyber hygiene policies are the foundation of an entity's protection of network and information system infrastructures, hardware, software and online application security and end-user or business data. A standardized baseline set of practices should include software and hardware updates, password changes, the principle of least privilege when it comes to administrator-level access accounts, backup of data, and supervision of new installations or assets. Good cyber hygiene also includes zero-trust principles, device configuration, network segmentation, software updates, and identity and access management.

Moving on to Article 21, essential and important entities are required to manage the risks posed to the security of network and information systems which those entities use to provide their services or to stay in operation by taking appropriate and proportionate technical, operational, and organizational measures. To determine the proportionality of those measures, three areas of consideration are:

a) The divergent risk exposure (including societal risks) or criticality of the entity

b) The entity's size

c) The likelihood of cybersecurity incidents occurring, their severity, and their societal and economic impact should they occur

In addition to accounting for the cost of implementation and the relevant European and international standards, these measures ought to establish a level of network and information systems security commensurate with the risks posed. Proportionality is important here so as to avoid unduly burdening essential and important entities financially. These measures shall be based on an all-hazards approach, which is geared towards protecting not only network and information systems but also the physical environment of said systems. This means protecting network and information systems and their physical environments from events like theft, fire, flood, power failures or unauthorized physical access that enables attackers to damage an entity's information and information processing facilities with the intent to compromise the availability, integrity or confidentiality of stored, transmitted, or processed data or of the services underpinned by these systems. This entails, at minimum, the following security measures:

a) Policies on risk analysis and information system security

b) Incident handling

c) Business continuity, which includes crisis management, disaster recovery and backup management

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

e) Security in the acquisition, development and maintenance of network and information systems, including vulnerability handling, and vulnerability disclosure

f) Policies and procedures that assess the effectiveness of cybersecurity risk-management measures

g) Basic cyber hygiene practices and cybersecurity training for the employees of the entity

h) Policies and procedures regarding the use of cryptography, and encryption (as needed)

i) Human resources security (to ensure that sensitive information doesn't leak), access control policies and asset management

j) The use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications and secured emergency communication systems within the entity where appropriate

When it comes to supply chain security, listed as measure 'd' above, entities shall take a few things into consideration, e.g. vulnerabilities specific to each direct supplier and service provider, their overall product quality, cybersecurity practices, secure development procedures, as well as the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22, wherein it is explained that, along with the Commission and ENISA, the Cooperation Group are permitted to "carry out coordinated security risk assessments of specific critical ICT services, ICS systems, or ICT products supply chains, taking into account technical, and where relevant, non-technical risk factors". These security risk assessments should identify measures, mitigation plans, potential single points of failure, best practices to counter critical dependencies, vulnerabilities and other risks associated with the supply chain. Aside from these technical risk factors, there are also non-technical risk factors such as concealed vulnerabilities or backdoors, or undue influence by a third country on

the suppliers and service providers' side of the equation. The principle is to avoid systemic supply disruptions that can be caused by technological lock-in or provider dependency (if one supplier is compromised, the entire supply chain is at risk of disruption).

Should an entity find that it does not comply with the measures listed above, then that entity must promptly take all necessary corrective measures, proportionate with its level of severity.

When it comes to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, of online search engines and of social networking services platforms, and trust service providers, the Commission has until October 17, 2024 to adopt acts of implementation that clearly delineate the technical and methodological requirements of the aforementioned measures. These may extend to sectoral requirements as well. However, entities that were not listed above (DNS service providers, TLD name registries, etc.) can also have these implemented acts applied to them. Those acts will be adopted in accordance with Article 5 of Regulation (EU) No. 182/2011.

Important and essential entities have reporting obligations. They should notify, without undue delay, their CSIRT or the competent authority and the supervisory body established under Regulation (EU) No. 910/2014 of any significant cyber threat or incident affecting trust services. By and large, member states can use an established single entry point to facilitate common and automatic incident reporting to both the supervisory body under Regulation (EU) No. 910/2014 and the CSIRT or the competent authority designated by this Directive. Entities shall also notify the recipients of their services that could potentially be impacted by the incident. Measures or remedies that those recipients are able to take in response to that threat or incidents should be communicated to said recipients by the member state.

An entity can determine the incident to be significant if it fulfills one of the two following conditions:

a) It has caused or is capable of causing severe operational disruption of the services or financial loss for them.

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

If the incident is deemed significant, the entity shall, for the purpose of notification, submit to the CSIRT or competent authority:

a) An early warning in any event within 24 hours of becoming aware of the significant incident which, if possible, shall indicate whether it seems to be caused by unlawful or malicious acts or could have a cross-border impact.

b) An incident notification in any event within 72 hours of becoming aware of the significant incident which shall update the information referred to in point (a) and indicate an assessment of the significant incident's severity and impact and, where possible, the indicators of compromise.

c) An intermediate report on relevant status updates, furnished upon the request of a CSIRT or the competent authority.

d) A final report not later than one month after the submission of the incident notification under point (b). This final report should include the following information:

   1) A detailed description of the incident, including its severity and impact.

   2) The type of threat or root cause that is likely to have triggered the incident.

   3) Applied and ongoing mitigation measures.

   4) Where applicable, the cross-border impact of the incident.

e) If the time has come for the submission of the final report and the incident is still ongoing, member states should instead provide a progress report at that time and a final report within one month of their resolution of the incident.

Conversely, the CSIRT or the competent authority is obligated to provide, where possible, a response to the notifying entity within 24 hours of receiving the early warning referred to in point (a). This response should contain initial feedback and, if requested by the entity, guidance or operational advice on implementing possible mitigation measures. If the CSIRT is not the initial recipient, the guidance would be provided by the competent authority instead and the CSIRT shall provide further technical support upon the entity's request. Should the significant incident be suspected to be criminal, the CSIRT or competent authority is also obligated to advise the entity on how to report the incident to law enforcement. When it is called for, especially when the significant incident affects two or more member states, the CSIRT, the competent authority, or the single point of contact shall inform the other affected member states and ENISA of the significant incident, including the information that was listed above. This should be done while preserving the entity's confidentiality, security and commercial interests. If public awareness of this incident is necessary to prevent security breaches, or to help mitigate an ongoing incident, a member state's CSIRT or competent authority can inform the public about the significant incident after consulting with the entity concerned.

Upon request by the CSIRT or the competent authority, the single point of contact shall forward these notifications to the single points of contact of other affected member states. The single point of contact shall also submit a summary report to ENISA every three months that contains aggregated and anonymized data on significant incidents, incidents, cyber threats, and near misses. The ENISA shall report its findings based on these reports every six months to the Cooperation Group and the CSIRT's network. The CSIRTS or the competent authorities shall provide information about incidents, significant incidents, cyber threats, and near misses to the competent authorities under Directive (EU) 2022/2557.

Again, the Commission shall adopt implementing acts further specifying the cases in which an incident shall be categorized as significant with regards to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, etc. Those acts will be adopted in accordance with Article 5 of Regulation (EU) No. 182/2011.

In the interests of standardizing implementation of Article 21, member states shall encourage the use of European and international standards and technical specifications relevant to the security of network and information systems without imposing or discriminating in favor of this technology. ENISA

shall cooperate with member states after consulting relevant stakeholders and draw up advice and guidelines regarding the technical areas while retaining already existing standards, including national standards.

5. Jurisdiction and Registration

Mainly, an entity that this Directive applies to falls under the jurisdiction of the member state they were established in, save for entities that are classified as:

a) Providers of public electronic communications networks or providers of publicly available electronic communications services. In this case, they are under the jurisdiction of the member state in which they provide their services.

b) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines, or of social networking services platforms. These entities shall be considered to fall under the jurisdiction of the member state in which they have their main establishment in the Union.

    1) An entity's main establishment in the Union is in the member state where the decisions related to cybersecurity risk-management measures are predominantly made. If it cannot be determined or if such decisions are not made in the Union, then its jurisdiction lies in the member state where cybersecurity operations are carried out. If there isn't such a member state, the main establishment would be in the member state where the entity hosts the highest number of employees in the Union.

    2) If it is not established in the Union but instead offers services within the Union, it shall designate a representative in the Union. This representative shall be stationed in one of those member states in which the entity's services are offered. The entity is then under the jurisdiction of this member state where the representative was established. Crucially, if no representative in the Union is designated, then the entity is considered to be infringing on this Directive, and any member state wherein they provide services will be capable of taking legal actions against the entity.

    3) The designation of a representative by an entity shall be without prejudice to legal actions.

    4) If a member state has received a request for mutual assistance in relation to an entity, they can take appropriate supervisory and enforcement measures in relation to the entity that provides services, or which has a network and information system on their territory.

c) Public administration entities. These fall under the jurisdiction of the member state which established them.

The ENISA is responsible for creating and maintaining a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines, or of

social networking services platforms. Should the competent authorities request it, ENISA shall allow them access to that registry, while protecting the confidentiality of information where applicable. They shall populate this registry using the information sent to them by single points of contact. By January 17, 2025, entities are required by member states to submit the following information to the competent authorities:

a) The name of the entity

b) The relevant sector, subsector and type of entity referred to in Annex I or II, where applicable

c) The address of the entity's main establishment and its other legal establishments in the Union, or of its designated representative

d) Current contact details, including email addresses and telephone numbers of the entity and its designated representative (where applicable)

e) The member states in which the entity provides services

f) The entity's IP ranges

Should there be any changes to the information they submitted above, member states shall ensure that the entity notifies the competent authority without delay and in any event within three months of the date of the change. Once the information has been received, the single point of contact of the member state shall forward it to ENISA without undue delay. If applicable, this information, and any changes thereof, shall be submitted through the national mechanism established by member states in order for entities to register themselves.

In order to enhance the security, stability and resilience of the DNS, TLD name registries and entities providing domain name registration services must collect and maintain accurate and complete domain name registration data in a dedicated database. They should exercise due diligence and abide by Union data protection law when it comes to data that is considered personal data. This database of domain name registration data must include information that is necessary for identifying and contacting the holders of the domain names and the points of contact (administrators of the domain names under the TLDs) which includes:

a) The domain name

b) The date of registration

c) The registrant's name, contact email address and telephone number

d) If it is not the same as the registrant, the contact email address and telephone number of the point of contact administering the domain name

The registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines, or of social networking services platforms must have policies,

procedures and verification procedures in place to certify that the information within is complete and accurate. These policies and procedures should be available to the public. In addition to that, TLD name registries and the entities providing domain name registration services must make the domain name registration data publicly accessible, so long as it isn't personal data.

Upon lawful and duly substantiated request by legitimate access seekers, these registries and entities must provide access to specific domain name registration data while abiding by Union data protection law. TLD registries and the entities providing domain name registration services are required to reply within 72 hours of receipt of the access request. The policies and procedures related to the disclosure of such data will also be available to the public.

To reduce redundancy, there will be no duplication of domain name registration data. Therefore, member states shall require that TLD name registries and entities providing domain name registration services cooperate with each other fully.

6. Information Sharing

NIS2 places a greater emphasis on information sharing, requiring in Article 29 that member states ensure various entities can "voluntarily share information" relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts, and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, in order to achieve the following two objectives:

a) Prevent, detect, respond to, or recover from, incidents or mitigate their impact.

b) Enhance the level of cybersecurity, particularly by increasing awareness of cyber threats, limiting or hindering the spread of these threats, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies or response and recovery phases, or promoting cooperation between public and private entities in the study of cyber threats.

In addition to the reporting obligations under Article 23, member states should ensure that key and significant entities, or those related to major cyber threats and near-miss incidents, can voluntarily submit threat or vulnerability intelligence to CSIRTs or competent authorities. However, due to the sensitivity of the information, proper arrangements are needed for sharing cyber threat information. These arrangements are to be promoted by member states, with the EU's ENISA responsible for providing best practices for intelligence exchange and guidance. Although NIS2 places a greater emphasis on sharing cybersecurity threat intelligence, as previously mentioned, the provisions of Article 29 are still voluntary, so the actual impact remains to be seen.

7. Supervision and Enforcement

NIS2 more explicitly expresses the supervision of compliance with the framework. As with NIS1, relevant parties must cooperate with data protection authorities in cases involving personal data. New aspects include the fact that authorities can prioritize tasks based on risk, and for significant entities, the powers of competent authorities have been expanded, allowing them to take measures such as:

a) Conducting on-site inspections and remote supervision

b) Regular and targeted security audits by independent bodies or competent authorities

c) Special audits based on significant violations or infringements of this directive by important entities

d) Security scans based on objective, non-discriminatory, fair, and transparent risk assessment standards, cooperating with relevant entities when necessary

e) Requiring the provision of information necessary for assessing the cybersecurity risk management measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to submit information to competent authorities under Article 27.

f) Requiring access to necessary data, files, and information to carry out their supervisory tasks

g) Requiring evidence of the implementation of cybersecurity policies

In addition, competent authorities have specific enforcement powers for significant entities, including:

a) Issuing warnings

b) Adopting binding instructions, including measures needed to prevent or remedy incidents

c) Ordering important entities to cease certain conduct

d) Ordering compliance with cybersecurity risk management measures

e) Ordering notification of potentially affected natural and legal persons

f) Ordering the implementation of security audit recommendations

g) Appointing monitoring officers

h) Ordering the public disclosure of illegal conduct

i) Imposing administrative fines

If these measures prove ineffective, authorities may temporarily suspend part, or all, of the relevant services or activities provided by the entity, or suspend its certification or authorization. At the same time, competent authorities have the right to prohibit the CEO or legal representative of the entity from exercising management functions within the entity. These temporary suspensions or prohibitions are a last resort in extreme situations and should comply with the general principles of EU law and the Charter, including the right to an effective remedy, the right to a fair trial, the presumption of innocence, and the right to a defense. However, the competent authorities' tracking of individual responsibility for senior management may become an incentive for cooperation.

Penalties in NIS2

In terms of administrative fines under NIS2, when essential entities and important entities infringe on Article 21 (cybersecurity risk-management measures) or Article 23 (reporting obligations), for essential entities, the maximum administrative fine amount is the higher of 2% of the global annual turnover in the previous financial year or at least 10 million euros. Moreover, for significant entities, the maximum administrative fine amount is the higher of 1.4% of the global annual turnover in the previous financial year or at least 7 million euros. Penalties may also include periodic fines to force entities to cease violations. When multiple member states are involved, competent authorities must provide mutual assistance in enforcement, with joint supervisory actions possible, and the European Commission being granted the power to adopt delegated and implementing acts.

If the infringement also constitutes a violation of personal data, the relevant data protection authorities will be notified. In summary, member states must further develop penalty measures. In case of non-compliance, entities may face the worst-case scenario including costs of violation reporting, GDPR fines, NIS2 fines, negative company news, and loss of operational availability, among others.[5]

Adoption Timeline for NIS2

The NIS2 Directive was officially adopted on December 14, 2022. It came into effect 20 days later. Member states must finish transposing the directive by October 17, 2024, and begin applying these measures from October 18, 2024. After the implementation of the NIS2 Directive, the NIS1 framework will also be abolished. The European Commission will review the operation of the NIS2 Directive on October 17, 2027, and report to the European Parliament and the Council. The report will specifically assess the scale, industry, sub-industry, and entity types of entities related to cybersecurity, as well as their relationship to the functioning of the economy and society, with a similar review conducted every 36 months thereafter.

Cracking NIS2.0 with TXOne Networks Solutions

In this chapter, we focus on applying the Cyber Assessment Framework (CAF) to analyze the NIS2 Directive and explain its importance in OT environments as well as the measures taken. From our perspective, the guidelines in the NIS2 Directive should not only cover ISMS but also extend to the concept of OT/ICS CSMS, to help essential and important entities prepare for compliance.

TXOne Networks is committed to "keep the operation running" and can accelerate the risk assessment process by providing visibility of the OT environment, defense capabilities, and our advanced cyber threat detection expertise.

1. Objective A: Managing Security Risks

Find below the recommended organizational structures, policies, and processes necessary to understand, assess, and systematically manage security risks to networks and information systems supporting essential and important entities.

Principles under Objective A include:

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Governance	• Policies on risk analysis and information systems security policies (Article 21.2(a))	• OT Cybersecurity policy • RACI Charts • KPI's and Senior management buy-in • Risk assessment process	• EdgeOne allows large-scale and remote management of all Edge Series devices in different facilities. It organizes alerts, assets, and incident events, permitting direct monitoring of the enterprise's industrial control system security, in addition to providing insight into the shadow OT environment. • Stellar locks down modernized and legacy assets running side-by-side and allows management from a single pane of glass via StellarOne. • ElementOne creates a holistic view for risk assessment during routine scans, allowing verification of vulnerability status, version information, and compliance with regulations.
Risk Management	• Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (Article 21.2(f))	• Risk assessment records • IACS drawing(s) • Risk assessment review records and improvement management plan	

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Asset Management	• These should all be clearly identified and recorded so that it is possible to understand what tools are important to the delivery of the essential service and and why (Article 21.2(i))	• IACS simple network drawing(s) • Asset register(s) • Plan for ageing and obsolete hardware and software	• Scan assets with Portable Inspector before onboarding, enabling stakeholders to confirm digital hygiene while also tracking asset security status throughout the entire asset lifecycle. • The Edge Networking defense solution detects and regularly monitors the connectivity status of assets.
Supply Chain	• Security-related aspects concerning the relationships between each entity and its direct suppliers or service providers (Article 21.2(d)) • Vulnerabilities specific to each direct supplier and service provider (Article 21.3) • Their overall product quality and cybersecurity practices (Article 21.3) • Secure development procedures (Article 21.3) • The results of the coordinated security risk assessments of critical supply chains (Article 21.3)	• List of third parties used, their roles, and responsibilities • Definition of cybersecurity requirements for the third parties • Reports of completed assessment and assurance of third parties	• Scan every OT asset or device that comes onto the work site for regulatory compliance with Portable Inspector, including service vendors' and contractors' laptops. • Use Portable Inspector's asset scan logs to create an "OT health check", or a record of digital hygiene for both internal and external use that helps organizations create a secure supply chain.

2. Objective B: Protecting Against Cyberattacks

Proportionate security measures in place to protect essential and important entities and its systems from cyberattack or system failures.

Principles under Objective B include:

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Service Protection Policies and Procedures	• Basic cyber hygiene practices and cybersecurity training (Article 21.2(g)) • Policies and procedures regarding the use of cryptography and, where appropriate, encryption (Article 21.2(h))	• Published and controlled policies, procedures and work instructions, etc. • Personnel security records (recognizing data protection requirements) • Configuration records (e.g., for firewalls, etc.) • Management of change records • Organizational and procedural change control records • Validation test records • Audit reports, review reports and management of resulting actions	• EdgeOne manages the policies of networking and endpoint security assets, ensuring operational integrity across distant sites. It allows administrators to modify OT protocol allowlists for asset interoperability and to conduct deep L3-L7 network analysis. EdgeOne employs Virtual Patching, a signature-based threat prevention solution, to protect OT networks from known threats. • Incorporate Portable Inspector into the work site's cybersecurity plan to mitigate the risk of malicious code landing with asset scans and asset inventories that include standalone and air-gapped assets as well as networked assets.

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Identity and Access Control	• Access control policies (Article 21.2(i)) • The use of multi-factor authentication or continuous authentication solutions (Article 21.2(i))	• Authentication and authorization • Records of current authorized users / assets and the level of access / privilege, etc. (noting data security requirements) • Records of change management for users, control of physical tokens / cards, etc. • Records of physical access control authorization and physical access control measures, e.g., key distribution or electronic access control records	• Use business intention to model routine tasks and network traffic, then make rules for intra- and inter-segment traffic with Edge series products. • EdgeIPS series supports the principle of least privilege, allowing businesses to minimize the OT attack surface, restrict OT network attacks, enhance operational performance, and mitigate the impact of human error. By implementing fine-grained access control at different levels, businesses can strike a balance between availability and security while safeguarding critical data and systems. • Use Portable Inspector to periodically scan OT assets and service vendors' or contractors' laptops for regulatory compliance. Conduct scans of incoming and outgoing devices for both insider threat elimination and supply chain security purposes.

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Data Security	• Any innovative technology, including artificial intelligence, must comply with Union data protection laws, including principles such as data accuracy, minimization, fairness, transparency, and data security with state-of-the-art encryption (NIS2 Directives (51)) • Fully leverage the data protection requirements set by Regulation (EU) 2016/679 (GDPR) for data protection by design and by default (NIS2 Directives (51))	• Relevant procedures for identification of sensitive data and assets containing this data and how this is protected • Specification of encryption algorithms and keys used • Records of essential data, services and connections identified and how these are protected where required	• Deploy Edge networking defense solution to segment the network based on understanding of regulations, data sensitivity requirements, and work group productivity – this prevents attackers from moving within your network or accessing any sensitive devices. • Apply Edge series network-based virtual patch technology to create a shield around legacy OS or unpatched assets that prevents attackers from exploiting a vulnerability to access sensitive data. • Define roles using trust list-based lockdown software Stellar to secure mission critical systems data against disruption. • Portable Inspector scans sensitive air-gapped or standalone assets that sometimes cannot accept installations or even light modifications, creating an inventory of them and ensuring they are threat-free while still adhering to their sensitivity needs. • Portable Inspector includes secure storage equipped with AES-256 encryption to completely safeguard file transfers in your work site.

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
System Security	• Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure (Article 21.2(e)) • Required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme (Article 24)	• Procedures setting out requirements for network architecture, segregation, and access • IACS simple network drawings • Asset-hardening procedures, instructions, and templates • Vulnerabilities and threat records • Patch management procedures and records, as well as records of management of associated change	• Conduct system hardening with the Stellar series lockdown software – use machine learning and trust lists to prevent all unapproved or suspicious applications and operations from deploying. • Edge series virtual patching addresses even unpatchable asset vulnerabilities at a network level without requiring any re-configuration or changes to the asset being fortified. The streaming-based anti-virus solution can prevent malware files from landing. • Streamline management and reference of records with the inventory of scanned assets automatically created by Portable Inspector's scan process.
Resilient Networks and Systems	• Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure (article 21.2(e)) • Secured voice, video and text communications and secured emergency communication systems within the entity (Article 21.2(j))	• Records of review of limitations, constraints, and weaknesses • Disaster recovery strategy • Software / firmware / application / configuration libraries and safes • Restoration test records	• Segment networks with the Edge series to make OT environments inherently more defensible, preventing lateral movement and other malicious actions by hackers. • Use Edge series appliances to create special rules for traffic which are based strictly on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity. • The Stellar series prevents unapproved USB device connectivity, script execution, and changes to configurations or data.

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Staff Awareness and Training	• Basic cyber hygiene practices and cybersecurity training (Article 21.2(g)) • Human resources security (Article 21.2(i))	• Definition of competence requirements for defined IACS roles and responsibilities • Cybersecurity awareness training program • Competence management records	• Solutions based on OT zero-trust increase the efficiency of cybersecurity planning and execution, enabling more economical manpower usage while streamlining oversight and management concerns. • Portable Inspector is an easy to operate scanning device, requiring no special training or education to use.

3. Objective C: Detecting Cybersecurity Incidents

Appropriate capabilities to ensure network and information system security defenses remain effective and to detect cybersecurity events affecting, or with the potential to affect, essential and important services.

Principles under Objective C include:

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Security Monitoring	• Monitoring and analyzing cyber threats, vulnerabilities, and incidents at the national level, and offering real-time or near real-time assistance to essential entities concerned (Article 11.3) • Collecting and analyzing forensic data and providing dynamic risk and incident analysis for cybersecurity situational awareness (Article 11.3) • Offering real-time or near real-time assistance to essential entities concerned with monitoring their network and information systems (Article 11.3)	• Procedures setting out security monitoring requirements, including malicious code detection • Records of periodic monitoring (e.g., of security logs, virus detection logs, intrusion detection logs etc.) • Analysis and interpretation of threat intelligence, periodic monitoring • Records and management of resulting actions	• Network segmentation with the Edge series streamlines monitoring and inspection of OT traffic, network vulnerability attacks, malware file landing over regular file transfer protocol, even when specialized ICS protocols are in use. • Portable Inspector creates centrally recorded asset inventories during every scan.

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Proactive Security Event Discovery	• Proactively scan the entity's network and information systems to detect significant vulnerabilities (Directive (43)) • Establish a proactive framework for preparedness and overall safety and security to respond to cyber incidents and threats (Directive (49))	• Relevant proactive security event discovery procedures • Analysis and interpretation of associated test and / or monitoring records and management of resulting actions	• Network segmentation with the Edge series brings unusual or suspicious activity directly to the attention of stakeholders on a need-to-know basis to prevent alert fatigue. • Identify and remove any malware brought onto the premises via third-party assets with the Portable Inspector, and use security records to get to the root of any recurring issues quickly. • Stellar disallows all activities that are not specifically trust listed while providing threat detection, including machine learning that identifies suspicious or malicious actions that are often part of unknown attacks.

4. Objective D: Minimizing Impact of Security Incidents

Capabilities to minimize the impacts of a cybersecurity incident on the delivery of essential and important entities including the restoration of those services where necessary.

Principles under Objective D include:

Key Subdomain	NIS2 Requirements	Tips for Application in OT	TXOne Products
Incident Response and Recovery Planning	• Incident handling (Article 21.2(b)) • Business continuity, such as backup management and disaster recovery, and crisis management (Article 21.2(c))	• Incident response plan • Incident response exercise plans and records	• Use Portable Inspector's threat detection and quarantine functions to identify, analyze and initiate a strategic response to a cybersecurity incident. • Detailed scan logs and reports from TXOne solutions allow you to understand the target, nature, and potential impact of a threat. Determine the appropriate amount of time to retain logs based on your needs. • Scan logs can also be exported to CSV files and then stored as evidence for nonrepudiation purposes or transferred to an SIEM (such as QRadar or Splunk) or Rsyslog server.
Improvements	• To exchange views on the policy for responding to large-scale cybersecurity incidents and crises, using lessons learned from the CSIRTs network and EU-CyCLONe (Article 14.4(m))	• Post-incident and post-exercise root cause analysis • Management plan for improvement • Evidence of review of incident response plans	• Conduct precise forensics with highly detailed scan logs and reports generated by the Edge series, Stellar, and the Portable Inspector.

Conclusion

This article primarily explores the significant impact of the implementation of the NIS2 Directive on European enterprises, as well as the improvements made in NIS2 compared to NIS1, including addressing disparities among member states that led to unfair competition, imbalanced supervision, and varying levels of enforcement. As a result, NIS2 reduces member states' discretion, enabling a more consistent application across the EU. With the rising rate of cyber incidents and the growing dependence on information and communication technology services and products, cybersecurity has become increasingly important. In this context, the NIS2 Directive emphasizes the cybersecurity level of essential and important industries more than NIS1, having a much larger scope that includes many new types of entities, enhanced supply chain security, and the adoption of the EU cybersecurity certification scheme. Moreover, it emphasizes the need for effective coordination among EU member states, strengthening national large-scale incident management, reporting, and response obligations, clarifying the functions and tasks of CSIRTs organizations in member states, and even establishing a new institution, EU-CyCLONe, to coordinate large-scale events and crisis management at the EU level.

Furthermore, although the NIS2 Directive does not impose mandatory requirements for threat intelligence sharing, it's evident that it encourages member states to adopt more incentive measures. At the same time, the NIS2 Directive significantly expands supervision and enforcement, with competent authorities being given clearer tasks and powers. The NIS2 Directive now stipulates thresholds for administrative fines, employing a carrot-and-stick approach to help prevent, detect, respond to incidents or recover from them, or mitigate their impacts, as well as improve the common cybersecurity level.

Finally, we explored how to strengthen preventive measures for OT/ICS using the NIS2 Directive, as it has a broader applicability in the CSMS framework and is even interconnected with the new Critical Entities Resilience Directive (CER). TXOne's OT zero trust solutions for simplifying compliance with the NIS2 Directive effectively protect the endpoints and network systems of critical and essential entities' OT/ICS, ensuring operational availability, integrity, and confidentiality, while safeguarding entities from supply chain attacks.

a) **Security Inspection:** Portable Inspector uses a removable approach to provide effective malware scanning with independent computer and physical isolation. It can detect and remove malicious software by being inserted into the USB port of any Windows and Linux device without the need for software installation or rebooting the target system. In addition, Portable Inspector can collect asset information to generate an inventory list to increase IT/OT visibility and eliminate shadow IT/OT. With its use of an AES 256 hardware encryption engine and scanning of all files before storing data, it ensures that data is free from malware before being securely stored in storage.

b) **Endpoint Protection:** Stellar offers organizations an all-in-one OT solution for long-term endpoint security coverage, securing modernized assets with a library of ICS applications and certificates. For fixed-use and legacy systems, Stellar locks them down so that they can only conduct tasks related to their role, and StellarOne empowers smooth management throughout the asset lifecycle from a single pane of glass.

c) **Network Defense:** Edge series employs baseline auto-rule learning technology to assist organizations in automatically generating a network trust list, and allows organizations to create and edit L2-L3 network policies strictly based on which assets need to communicate in order to do their work, highlighting all suspicious or potentially harmful activity. The Edge series also supports a wide range of industrial protocols and deeply analyzes network packets, enabling organizations to effectively block malicious behavior and errors without affecting production line operations. To protect legacy devices and production systems that are vulnerable to attack due to unpatched vulnerabilities, Edge series uses industry-leading signature-based virtual patching technology. And the Edge series supports market-leading anti-virus solutions for preventing malware files from landing in field environments. In addition, Edge series minimizes the time required to configure and manage devices and can be easily deployed in an organization's existing OT environment.

In conclusion, the NIS2 Directive has improved upon NIS1 in many aspects. However, in addressing cybersecurity challenges, enterprises and government sectors require more effective, faster, and automated solutions to adapt to new threats, regulatory changes, and to reasonably adjust their cybersecurity strategies to meet evolving requirements. The TXOne Networks' solution helps essential and important entities make significant progress in managing cybersecurity risks, creating a more secure and reliable cyberspace for European citizens and businesses.

Reference

[1] NIS1 Directive, *"Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union."*, Official Journal of the European Union, July 2016.

[1] NIS2 Directive, *"Directive (EU) 2022/2555 of the European Parliament and of the Council, Official Journal of the European Union"*, December 2022.

[2] Briefing, *"The NIS2 Directive A high common level of cybersecurity in the EU"*, European Parliament, February 2023.

[3] Valentino Lucini, *"The Ever-Increasing Cybersecurity Compliance In Europe: The NIS2 And What All Businesses In The Eu Should Be Aware Of"*, Russian Law Journal, 2023.

[4] Niels Vandezande, *"Cybersecurity in the EU: how the NIS2-Directive stacks up against its predecessor"*, Timelex, March 2023.

[5] Alkiviadis Giannakoulias, *"NIS2 Directive: Implications for System and Infrastructure Security"*, University of Piraeus, 2023.

txone.com

txOne networks *The Leader of OT Zero Trust*

NIS 2 Directive

Cybersecurity Risk Mitigation & Enabler for OT networks

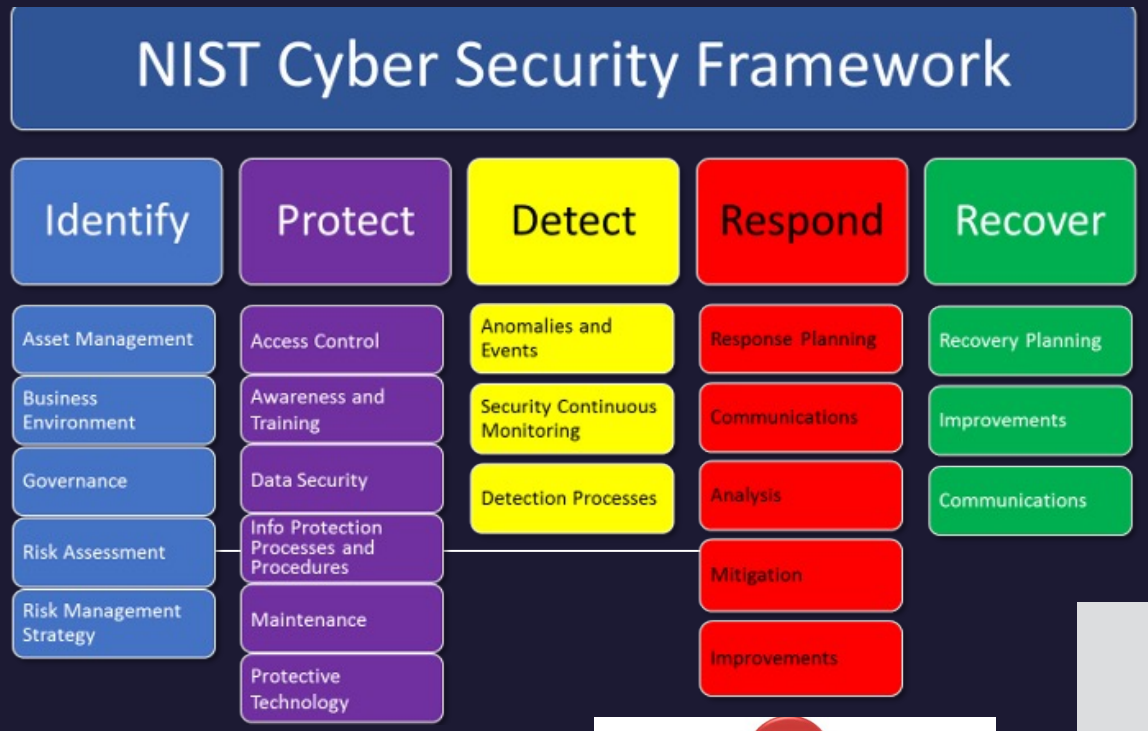
Giorgio Santandrea - OEM & Machine Builder Director Europe

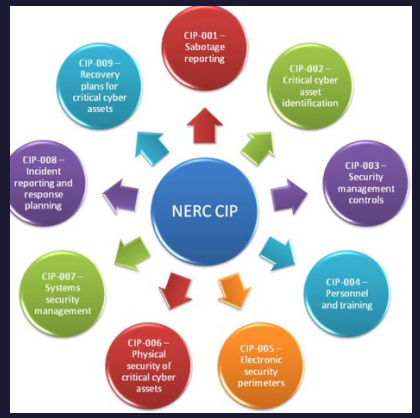
NIS Directive 2

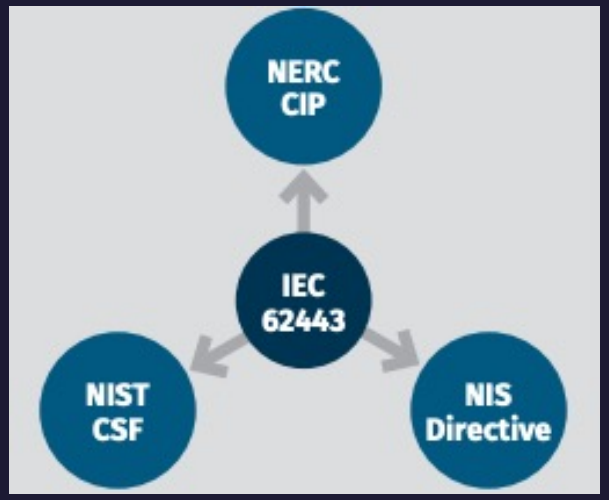
- Introduction
- Key provision of NIS Directive 2
- Impact to NIS Directive 2
- How TXOne could help?

OT Different Standards & Good Practices in the world

txOne networks *The Leader of OT Zero Trust*







NIST Applicable to OT Security Community

txOne networks *The Leader of OT Zero Trust*

- NIST SP 800 Series
- NIST SP 1800 Series
- NIST IR Report Series

Series	Title
NIST SP 800-82	Guide to Operational Technology (OT) Security
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations
NIST SP 800-40	Guide to Enterprise Patch Management Planning: Preventive 4080 Maintenance for Technology
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program
NIST SP 800-53	Security and Privacy Controls for Information Systems and 4084 Organizations
NIST SP 800-70	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

Series	Title
NIST SP 800-98	Guidelines for Securing Radio Frequency Identification (RFID) Systems
NIST SP 800-116	Guidelines for the Use of PIV Credentials in Facility Access
NIST SP 800-123	Guide to General Server Security
NIST SP 800-125	Guide to Security for Full Virtualization Technologies
NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
NIST SP 800-150	Guide to Cyber Threat Information Sharing
NIST SP 800-160 Vol.1 an 2	Systems Security Engineering, Developing Cyber-Resilient Systems

Series	Title
NIST SP 1800-25	Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events
NIST SP 1800-26	Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events
NIST SP 1800-27	Securing Property Management Systems
NIST SP 1800-30	Securing Telehealth Remote Patient Monitoring Ecosystem
NIST SP 1800-32	Securing Distributed Energy Resources: An Example of Industrial Internet of Things

Series	Title
NIST SP 1800-2	Identity and Access Management for Electric Utilities
NIST SP 1800-7	Situational Awareness for Electric Utilities
NIST SP 1800-8	Securing Wireless Infusion Pumps in Healthcare Delivery Organizations
NIST SP 1800-10	Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector
NIST SP 1800-11	Data Integrity: Recovering from Ransomware and Other Destructive Events
NIST SP 1800-23	Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry
NIST SP 1800-24	Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector

Series	Title
NISTIR 7628	Guidelines for Smart Grid Cybersecurity
NISTIR 8011, Vol.1/2/3/4	Automation Support for Security Control Assessments:
NISTIR 8183	Cybersecurity Framework Version 1.1 Manufacturing Profile
NISTIR 8183A Vol.1/2/3	Cybersecurity Framework Manufacturing Profile Low Impact Level 4154 Example Implementations Guide
NISTIR 8212	ISCMA: An Information Security Continuous Monitoring Program Assessment
NISTIR 8219	Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

Why we need the Standard and NIS background

- Next Generation Technology Machine Learning, Artificial Intelligence etc.
- Computers & Networks are critical for right functioning of environment
- We regulate with Cyber Physical Systems (CPS)
  - Electricity & Communications
  - Health-care, Transport, Banking & Finance
- We need to regulate this computer and networking information as we all are heavily dependent on it.
- NIS directive is all about
  - Co-operation of member state within and outside EU
  - Good practices and Information Exchange between each other
  - Notification of Cyber incident and Breaches
  - Cybersecurity measures

Introduction to NIS Directives

A. Definition of NIS Directive

- The NIS Directive 2, also known as the Network and Information Systems Directive, is a piece of European Union (EU) legislation that was implemented to increase the security of critical infrastructure Essential entities (OES) and Important entities within the EU.

- New Directive proposed because of the deficiencies of NIS-D in 2018
  - Some EU countries took it very seriously whereas other countries did not list any of their sectors
  - Inconsistent resilience across Member States and sectors
  - Insufficient common understanding of the main threats and challenges among Member States
  - Lack of joint crisis response and notification of breaches
  - Unclear Fines & Regulatory patchwork

1st Introduction to NIS2 Directives

- The NIS Directive is not a regulation yet and becomes a minimum baseline for local regulations/law in different European Countries
- Full definition by October 2024 and in operation by Jan 2025
- Simpler Scope: Essential Services (OES) & Important Services

- Internet Exchanges
- ccTLD operators
- Large scale authoritative servers
- Large scale resolvers
- Data center service providers
- Content Delivery Networks
- **Root servers**

txOne networks

NIS2 - Entities in Scope and shall it apply to me

- Medium and Large organisation providing services within European Union

- Large Annex I entities are considered as Essentials entities
- Medium and Large Annex II entities are considered Important entities

- Entities of Directives NIS1 are considered essential

- Exempt “Small” and “Micro” enterprises as defined by commission recommendation 2003/361/EC

Annex I	Sub-Sectors
Energy	Electricity, District heating and cooling, Oil, Gas
Transport	Air, Rail, Water, Road
Health	Pharma, Manufacturing, Laboratories, Services
Water	Drink and waste
Space	Infrastructure, Services
ICT	MSP, MSSP

Annex II	Sub-Sectors
Waste Mgmt.	all
Food	Production, Processing, Distribution
Manufactu-ring	Chemicals, Medical Dev., Computer Electronics, Optical Products, Electrical Equipment, Machinery & Equipment, Motor Vehicles, Trailers, Transport equipment
Postal/ Courier	all

txOne networks

Purpose / Goals / Requirements of the Directive

- The purpose of the NIS Directive 2 is to ensure the Availability, Reliability, and Security of essential services and critical infrastructure, such as energy, transportation, health, and banking, in the EU. It aims to:

  - Improve the cybersecurity posture of essential services and critical infrastructure in the EU
  - Ensure a consistent level of security across all Member States
  - Encourage the sharing of information and best practices among Member States and organizations

  - Two High level Requirements

Requirements of NIS Directive 2

- A - Cybersecurity Risk Management Services
  - Risk Analysis & Security policies
  - Incident Handling and reporting procedures
  - Business continuity & Crisis management plan
  - 3rd party dependencies and security compliance on your service suppliers
  - Vulnerability management & disclosure
  - Security Audits and Testing of effective cybersecurity measures
  - Use of Cryptography and encryption for security hardening
- B - Incident reporting

" If you are **Essential** you need to have all the above plan ready for inspection and if you **Important** you better have the plans ready if you have an incident"

Consequences for if you don’t care

- If you don’t care
  - 1st level Warnings
  - Orders to Fix and improve your cybersecurity postures
  - If not Fixed, then Fines
  - Criminal Procedures
  - Orders to cease doing business
  - Bans on persons from Management (CEO)

“ Surprised On-site Security inspections if suspicious of any problems or security incidents ”

Compliance requirements

BAD: No one wants to be regulated and get certified

Good: NIS 2 provides every CISO's Wishlist

- Minimum Requirements
  - Establish cybersecurity risk-management measures
  - Reporting obligations of severe cybersecurity incidents
- Governance
  - Supervision, enforcement, penalties related to entities
  - Establish legislation, systems, guidelines, collaboration

txOne networks

A – Cybersecurity Minimum Risk-Management Measures

- Establish Risk and Security Management System
  - Security policies, risk analysis
  - Policies and Procedures for NIS2 compliance, cryptography / encryption, access control
  - Personnel: HR security, roles, training and accountability
- Endpoint and Network Security
  - Asset and lifecycle management
  - Cyber hygiene, patch and vulnerability management
  - Backup management
  - Secure and continuous authentication, data protection
- Incident Handling
- Supply Chain security
  - Direct suppliers, service providers vulnerabilities, product security, assessments
- Business Continuity, disaster recovery
  - Backup management, crisis management, secure emergency communication

“ Members state has the flexibility to add on to minimum requirements and greater detail would be added by October 2024”

txOne networks

B- Incident reporting

Report	Description?	Deadline
Early Warning	• Cross-border impact? • Unlawful or malicious act?	Within 24 hours after being aware
Incident notification	• Update to early warning data? • Initial assessment? • Severity and impact? • Indicators of compromise? (if available)	Within 72 hours after being aware
Intermediate report	• Relevant status updates ?	Government requested
Final Report (Progression report if attack is ongoing)	• Detailed description of the incident including severity and impact • Type of threat or root cause • Applied and ongoing migration measures • Cross-border impact of the incident	One month after submission of initial notification
Final report after ongoing attacks	• see above	Within one month of handling the incident

A severe incident is:

a) Severely impacting services or
b) Imposing significant financial loss, or
c) Significant material impact to natural or legal person

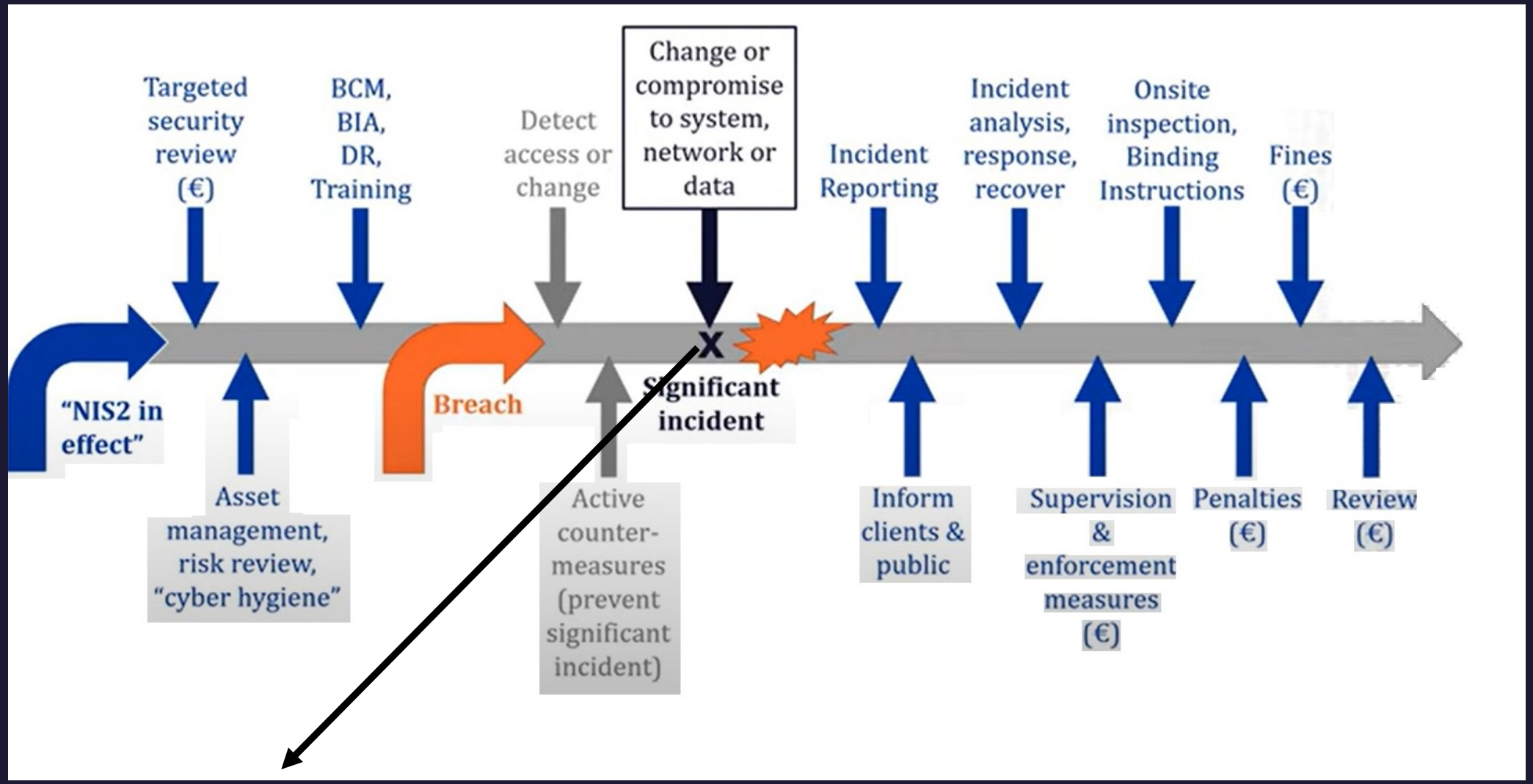
txOne networks

B - Incident reporting

- Comparable to the GDPR (General Data Protection Regulation)'s
- Reporting requirements, Company must notify their competent authority of NIS incidents with a "significant" impact on the continuity of the service they provide "without undue delay"

- They must consider three factors when determining whether an incident is "significant":
  1. The number of users affected by the disruption;
  2. The duration of the disruption; and
  3. The size of the geographical area affected by the incident.

NIS2 – Lifecycle process



If breach is not detected you shall loose control and shall have severe consequences

Supervision, Enforcement and Penalties

	Supervision	Enforcement of Violations	Fines/Penalties
Baseline **(Important & Essential)**	• Coordinate with legal representative • **On-site inspections** • **Off-site inspections** • Request information to assess compliance • **Request evidence** of security policy implementation	• **Issue warnings** • Binding instruction to **remediate** incident within deadline • Orders to cease and make **infringement public** and provide guidance • Order to implement **security audit** recommendations within deadline • Imposed administrative **fines**	• A maximum of at least 1.4% of global turnover or **7 Million Euro** whichever is higher • Additional imposed periodic penalty payments to cease infringements • **Additional sanctions** to be effective Jan 2025
Additional Fines **Only for Essential entities**	• Regular and **Ad-hoc audits** • Random checks	• Initiate **temporary prohibition** to exercise managerial function at **CEO** or **legal representative** level • Designate **monitoring officer** to oversee compliance • Binding instruction to **prevent incidents** with deadlines for implementing and reporting	• A maximum of at least 2% of global turnover or **10 million Euro** whichever is higher

txOne networks

Key Challenges

- Challenges and limitations
  - Prepared to be reviewed
  - Prepared to establish a cybersecurity risk management system, **including OT systems** (OT networks, Cyber Physical Systems in production area, etc.)
  - Prepare to report but also react on the receive third party incident reports
  - Tough timeline to prepare a security programme for NIS2
    - Three months between detailed requirements made public (October 2024) and NIS2 been effective (January 2025)
    - 18 months approx to prepare process is procedures and select supporting technologies
- How to get started?
  - Select a related framework and perform a self-assessment
  - **NIS2 requires IT and OT to work in collaboration**
  - Knowing what to **Protect**
  - Manage cyber security risk and orchestrate the remediation
  - **Prepare for compensating controls in OT**
  - Monitoring and identification of potential breaches

Conclusion & Take-Away

- See impact on entities
  - Audit ready requirements are here to stay so be prepared to be compared with your industry peers
  - Requires active security and risk management organisations
  - Requires integrated approach and capabilities to take action
  - Maximum penalties at least five to seven days of production revenue or 7 to 10 million pounds
- Impact for member state/EU
  - Directive is designed to allow flexible extension in all directions
  - Part of a bigger cyber security effort (GDPR, CER-Directive, upcoming embedded security.)

Technological Elements To Effectively Address The NIS2 Prerequisites Of OT Cybersecurity

OT Native Environment Fit

NIS 2 Article 21 & 25

Support legacy and modernized operation system

NIS 2 Article 21 & 25

ICS/OT Network protocols support

NIS 2 Article 24

It can be operated in the harsh conditions

NIS 2 Article 12 & 21

Ability to protect unpatched assets

NIS 2 Article 12 & 21 & 25

Persevere ICS/OT Applications running as the priority

OT Native Operation Fit

NIS 2 Article 12 & 21

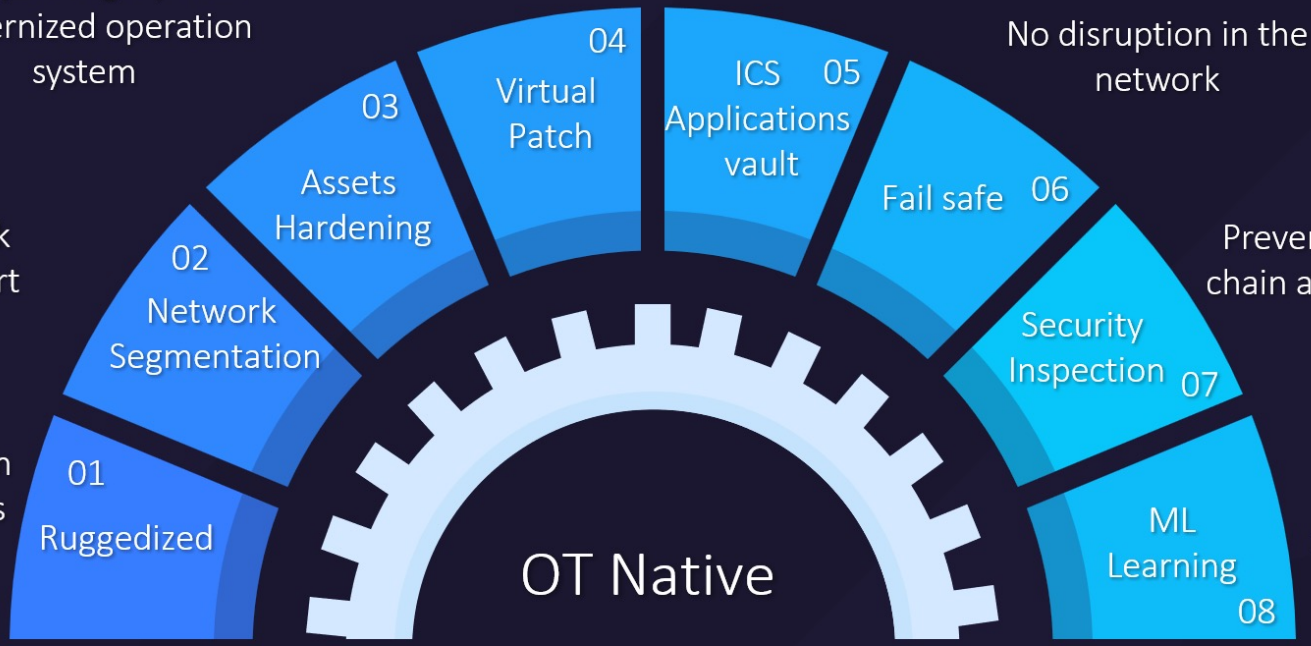
No disruption in the network

NIS 2 Article 22 23 & 25

Prevent the supply chain attack thru the assets

NIS 2 Article 20 & 21

The solution can not introduce more management/operation efforts



"Let's keep the Business Growing and Operations Running all the time"

txOne networks

High Level Mapping against NIS2 requirements

	NIS2 High Level Requirements	TXOne Technology Stack
NIS 2 Article 12 – Coordinated vulnerability disclosure and a European vulnerability database	Risk analysis and information system security policies	SageOne
NIS 2 Article 20 – Governance	Incident Handling	SageOne
NIS 2 Article 21 – Cybersecurity risk-management measures	Business continuity and crisis management	EdgeOne & StellarOne and ElementOne
NIS 2 Article 22 – Union level coordinated security risk assessments of critical supply chains	Supply Chain Security	Portable Inspector & Safe Port
NIS 2 Article 23 – Reporting obligations	Vulnerability Handling and Disclosure	Edge Series – Virtual Patching & ElementOne
NIS 2 Article 24 – Use of European cybersecurity certification schemes	Policies and procedures to evaluate cybersecurity risk management efficacy	EdgeOne & StellarOne and ElementOne
NIS 2 Article 25 – Standardisation	Basic cyber hygiene practices and cybersecurity training	TXOne OT Zero Trust Solutions
	Policies and procedures for cryptography and encryption	Portable Inspector includes secure storage of AES 256 encryption
	Human resources security, access control policies and asset management	Edge Series, ML-Auto-Learning, Trust-listing, Stellar CPSDR Asset fingerprinting
	Use of multi-factor authentication and secure communication systems	Edge Series

txOne networks