NIS2 Compliance for Industrial Operations with Cisco

The European Network and Information Security (NIS) directive outlines cybersecurity requirements for organizations operating in the European Union (EU) to ensure that there is a high, common level of protection across member states. It is designed to ensure cyber resilience across the region by requiring critical industries to adopt a set of cybersecurity best practices and procedures to drive governance, risk management, and reporting.

The second version of the directive (NIS2) applies to most organizations in many more industry sectors than the previous version. NIS2 makes compliance mandatory by imposing important financial penalties for noncompliance, mandating a strict incident reporting timeline, adding liability for senior management, and reinforcing the role of local cybersecurity agencies to monitor and control organizations. This solution overview describes how Cisco can help you protect your Operational Technology (OT) to drive NIS2 compliance.

NIS2 cybersecurity requirements

- Risk analysis and information system security policies
- Incident handling, including prevention, detection, response, and recovery
- Business continuity measures and crisis management
- Supply chain security
- Security in network and information systems, including vulnerability handling
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures for cryptography and encryption
- Human resources security, access control policies, and asset management
- Use of Multifactor Authentication (MFA) and secured communications

How can Cisco help?

Building infrastructures with secure components

NIS2 requires that "**entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their supplier and service providers, including their secure development processes.**" To ensure the security of Industrial Automation and Control Systems (IACS) throughout their lifecycle, the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have a globally recognized standard, ISA/IEC 62443.

ISA/IEC 62443 Part 4-2, Technical Security Requirements for IACS Components, delineates cybersecurity requirements for components that make up an industrial automation and control system. For the Cisco Catalyst industrial networking products, those security capabilities include:

- Hardware trust anchor and Secure Boot
- Run-time defenses
- Visibility and troubleshooting
- Modern cryptography
- Authentication, Authorization, and Accounting (AAA)

ISA/IEC 62443 Part 4-1, Product Security Development Life-Cycle Requirements, comprises process requirements for the secure development of products used to assemble an IACS. Cisco® software and hardware products are developed according to the Cisco Secure Development Lifecycle (SDL), which has obtained IEC 62443-4-1 certification, enforcing a secure-by-design philosophy from product planning through end of life.

Figure 1. Cisco Catalyst industrial networking products are certified for ISA/IEC 62443-4-2 and are developed according to the ISA/IEC 62443-4-1-certified Cisco Secure Development Lifecycle

Understand and minimize risk with Cisco Cyber Vision

Cisco Cyber Vision is an OT visibility solution embedded in Cisco industrial network infrastructure. It combines protocol analysis, intrusion detection, vulnerability detection, and behavioral analysis to help you understand your security posture. In doing so, it identifies the vulnerabilities within an OT network, detailing the Common Vulnerability Exposure (CVE) ID, Common Vulnerability Scoring System (CVSS), and associated risky activities to perform a risk analysis of the IACS network.

This type of analysis often identifies more vulnerabilities and configuration issues than an organization has the capacity to fix. IT teams struggle to understand what to prioritize, and are faced with long patch lists with little guidance. To help address this issue, Cyber Vision helps prioritize actions by applying a risk score to all devices and device groups discovered in the OT network. Using a combination of vulnerabilities, activities, and impact, risk scores provide guidance as to which devices should be addressed first when implementing risk-management measures.

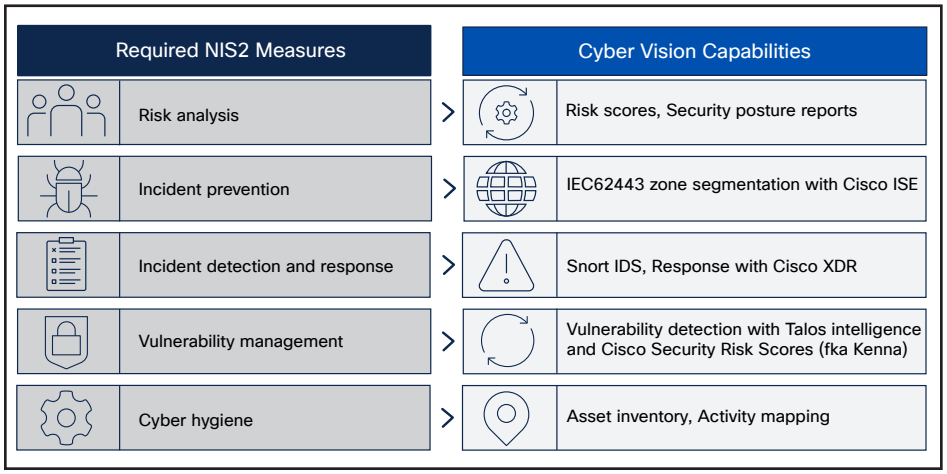

Figure 2. Understand and minimize risk with Cisco Cyber Vision

Prevent and minimize the impact of incidents

NIS2 also states that "**entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles" and "network segmentation.**" Zero trust in the IACS is achieved by grouping devices based on the role they have on the network within a trust zone and enforcing policies between zones.

For example, in an automobile plant, there is no reason equipment in welding would need to interact with equipment in the paint shop. Placing each in its own zone limits any damage if one zone gets infected. Conduits, the communication channels between zones, define the limited interaction allowed if equipment in different zones does need to communicate with each other. Access policies formalize zones and conduits in the OT network.

Cisco Cyber Vision, using an integration with Cisco Identity Services Engine (ISE), can assign IACS endpoints to the appropriate zones and tag their communications with Security Group Tags (SGTs) that enable Cisco network devices to define and enforce appropriate access policies.

In the unfortunate event that an incident does occur, Cyber Vision can use ISE to isolate a system under investigation to minimize the potential blast radius. This allows the system to stay on the network with minimal privileges to keep the control network operational, but traffic with malicious intent cannot leave the containment zone.

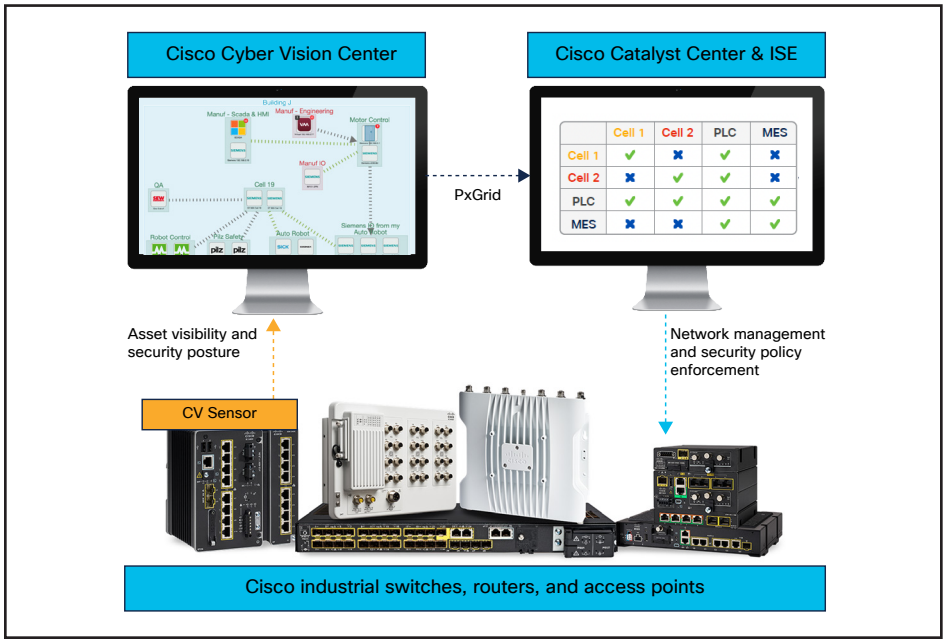

Figure 3. Cisco Cyber Vision together with Cisco ISE helps prevent cyber incidents in industrial networks

Minimizing risk from OT suppliers and service providers with Cisco Secure Equipment Access

Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is a critical NIS2 requirement. Industrial organizations often rely on providing remote access to their suppliers for support, maintenance, and upgrades which opens the most exploited attack vector to any organization: the remote access connection.

While zero trust is an important consideration within the OT network, NIS2 recognizes the need for Multifactor Authentication (MFA), which is a critical capability for any remote access solution.

To secure remote access to OT assets, Cisco provides a Zero-Trust Network Access (ZTNA) solution called Secure Equipment Access (SEA), which allows least privilege access policies based on identities, schedules, and context, and enforces strong cybersecurity controls such as Multifactor Authentication (MFA), remote user posture check, session monitoring and termination, and more.

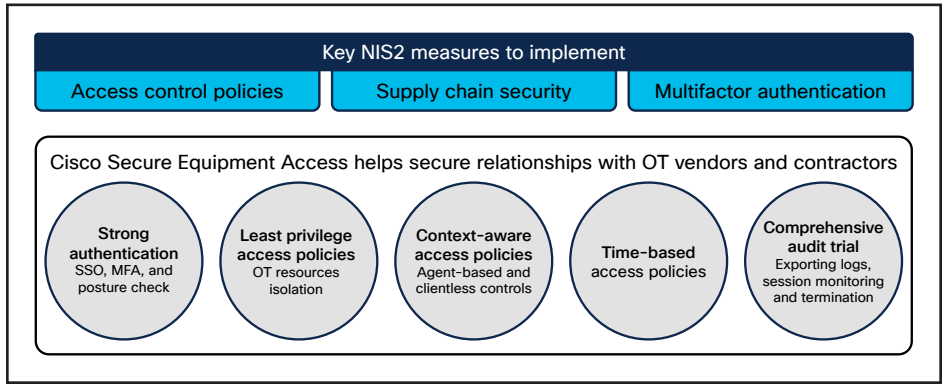

Figure 4. Minimizing risk from OT suppliers and service providers with Secure Equipment Access

Cisco SEA establishes trust by verifying user and device identity at every access attempt. Least privilege access is assigned to every user, meaning that only the applications that are required are permitted. Access to the full network is never granted. Additionally, remote access to a critical network should not be an always-on feature. SEA administrators can schedule their users' access, granting application access only during times of need. If a session expires, a new session must be created.

The Cisco Advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more.

Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. This rare combination makes Cisco an ideal partner to help industrial organizations secure their IACS to achieve compliance with the NIS2 standard.

Secure your OT and drive NIS2 compliance with Cisco

Talk to a Cisco sales representative or channel partner and visit these web pages to learn more:

- NIS2: Building OT Security Capabilities to Drive Compliance
- Cisco OT/ICS Security
- Cisco Cyber Vision
- Cisco Secure Equipment Access