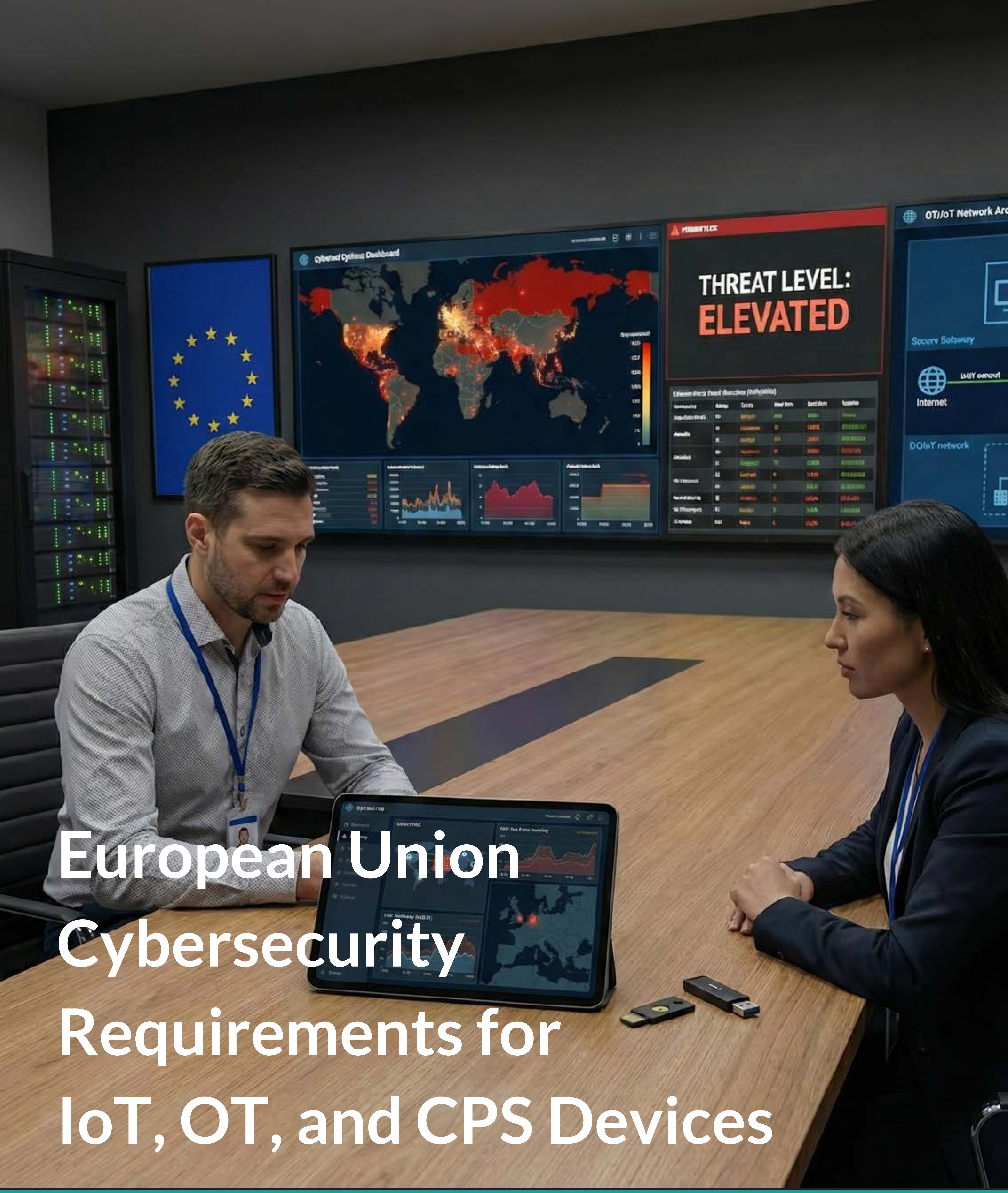


European Union Cybersecurity Requirements for IoT, OT, and CPS Devices

viakoo

(650) 263-8225 | sales@viakoo.com | viakoo.com

Table Of Contents

Introduction

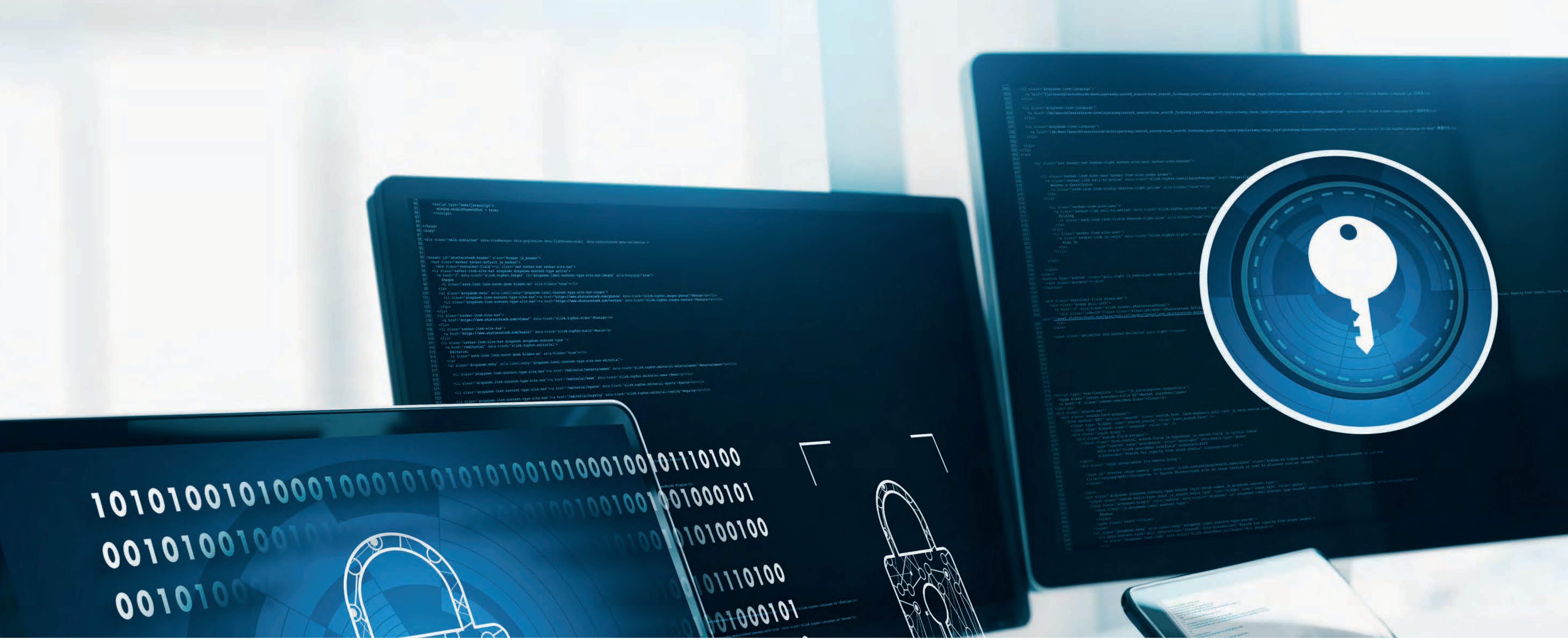
- ***European Union Regulations (NIS2 and CRA) have new mandatory requirements for IoT, OT, and ICS (CPS) cybersecurity***

- ***Key to achieving compliance is having detailed asset discovery combined with automation to perform firmware updates, password changes, manage certificates, and track actions taken.***

European regulators have been focused on reducing the risk of cyber incidents by crafting requirements for both manufacturers and operators of connected devices. The Cyber Resilience Act (a.k.a. CRA) is focused on requirements to manufacturers of connected devices (so that their products are designed with security built-in). The NIS2 (Network and Information Security Directive 2) is aimed at operators of connected devices to ensure they have ongoing security processes in place to keep these devices secure once they are put into operation.

This white paper will highlight how these new regulations apply to IoT (internet of things), OT (operational technology), and ICS (industrial control systems). These types of connected devices are often referred to as cyber-physical systems or CPS because they have (so to speak) one foot in the digital world by being network connected, and another foot in the physical world where they capture data, move actuators, close pipelines – in other words where a cyber attack can have a devastating physical impact. Throughout this white paper the terms IoT/OT/ICS and CPS will be used interchangeably.

Viakoo provides automated solutions to the most difficult part of achieving NIS2 and CRA compliance, with firmware updates, password changes, and certificate management. Using Viakoo also means that you will have push-button reporting to document the actions taken (when and by whom) in order to speed audit and compliance requirements. Viakoo's unique capability of being able to do all this across diverse networks and geographies overcomes one of the most difficult operational issues for organizations of all size.



Key Aspects of CRA and NIS2

The CRA ensures the "ingredients" (devices) are safe, while NIS2 ensures the "kitchen" (operations) is sanitary.

Aspect	Manufacturer Responsibility (CRA)	System Operator Responsibility (NIS2)
Primary Focus	**Product Security:** Ensuring the device itself is hardened before it is sold.	**Organizational Security:** Ensuring the entity using the devices is resilient against attacks.
Device Configuration	**Security by Design:** Must ship with no default passwords, encrypted interfaces, and minimized attack surfaces.	**Cyber Hygiene:** Must change default credentials, enable encryption, and configure devices securely upon installation.
Vulnerability Management	**Provide Updates:** Must fix vulnerabilities and push free security updates for the product's expected lifetime (min. 5 years).	**Apply Updates:** Must have a process to verify and install these updates promptly to mitigate risk.
Incident Reporting	**Exploits:** Must report *actively exploited vulnerabilities* to ENISA within **24 hours**.	**Incidents:** Must report *significant cyber incidents* (breaches/outages) to the national CSIRT within **24 hours**.
Supply Chain	**SBOM:** Must maintain a Software Bill of Materials tracking all third-party code.	**Vendor Risk:** Must assess the security of suppliers and is legally bound to purchase secure (CRA-compliant) tech.
Legacy/Retrofit	**Exemptions:** Legacy products sold before 2027 are exempt unless substantially modified.	**The "Trap":** If an operator heavily modifies a legacy device (e.g., retrofitting a sensor), they legally *become* the manufacturer.
Liability	**Market Ban:** Non-compliant products can be recalled or banned from the EU market.	**Personal Liability:** C-Level executives can be held personally liable (fines/suspension) for negligence.

1. Taking Action on NIS2 Compliance as an Operator of IoT/OT/ICS Systems

The NIS2 Directive (Network and Information Security Directive 2) is the European Union's sweeping law aimed at protecting critical infrastructure and essential services from cyber threats. For operators of IoT/OT/CPS devices and applications this is the most important regulatory directive to follow, as NIS2 forces operators to run secure organizations. If you are an operator of OT or IoT in a critical sector, NIS2 is the regulation that dictates your daily security operations.

NIS2 went into effect in October 2024, meaning that enforcement is just starting. Early enforcement is expected to focus on demonstrating that operational controls and processes are in place. This is exactly what Viakoo is designed to help you with.

Actively managing IoT/OT/CPS cyber hygiene is one of the key non-negotiable NIS2 requirements that organizations will have to increase efforts around, as many organizations currently leave IoT/OT/CPS outside of their IT-oriented cybersecurity policies. Mandatory policies on firmware, password and identity management must be implemented and maintained, with auditable records available. Viakoo, as the leader in IoT cyber hygiene at scale, supports all of these requirements.

NIS2 applies to a wide range of organizations (wider than CRA, which will be discussed later). These enterprises, if crippled or compromised from a cyber attack, could have a profound impact on the lives of European citizens. NIS2 is specifically is aimed at medium and large sized enterprises (>50 employees or >$10M euros in revenues) in these sectors:

- **"Essential" Entities** (High Criticality): Energy (electricity, oil, gas, hydrogen), Transport (air, rail, water, road), Banking & Financial Markets, Health (hospitals, labs), Drinking/Waste Water, Digital Infrastructure (cloud, data centers), and Public Administration.

- **"Important" Entities**: Waste management, Manufacturing (of chemicals, medical devices, computers, vehicles, machinery), Food production, and Postal services

Viakoo Makes NIS2 Compliance Fast & Cost Effective

- Built-in asset discovery makes setup fast
- Key device lifecycle information is automatically populated
- All devices are monitored for presence of new vulnerabilities
- Deploy firmware patches, password changes, and certificates across fleets of enterprise devices within hours
- Push-button reporting and historical data for audit/compliance

2. Taking Action on CRA Compliance as an Operator of IoT/OT/ICS Systems

The EU Cyber Resilience Act (CRA) is primarily a regulation for manufacturers (those who make software/hardware), but it significantly impacts operators (those who run/deploy these systems, like factory managers or CISOs). Under CRA, you are a "System Operator" (End User/Asset Owner) if you buy and run IoT/OT systems in a factory, power plant, or enterprise.

The CRA is designed to help enterprises become better consumers and “maintainers” of CPS deployments. It forces your vendors to give you the tools you need to secure your infrastructure (often required by NIS2, as discussed in the previous section).

For new devices, CRA-compliant vendors are required to carry the CE mark, tell you when security updates will stop (end of support date), not have default passwords, and be able to provide SBOMs (Software Bill of Materials). In addition, the security updates (firmware patches) will become frequently available.

Viakoo directly helps enterprises reduce risk by having an inventory that is CRA-compliant. Using Viakoo-generated detailed asset inventory information can identify devices that are behind in firmware updates or have reached end of support. As new devices are added, the vendor-supplied end of support dates can be easily added and tracked across the device lifecycle. Viakoo can also assess devices if they are using default or easily-guessed passwords, which CRA-complaint devices should not allow. Viakoo’s patented “last mile” capability allows firmware updates to be managed at scale without access to the open internet.

Here are key enforcement dates to be aware of:

- Late 2026: Reporting obligations start. Vendors must report vulnerabilities to the EU. (As an operator, expect to see more public CVEs for your gear).
- Late 2027: Full enforcement. Products without CRA compliance can effectively no longer be sold in the EU.

Viakoo Accelerates The Benefits of CRA

- Viakoo directly helps enterprises reduce risk by having an inventory that is CRA-compliant.
- Viakoo-generated detailed asset inventory information identifies devices that are behind in firmware updates or have reached end of support.
- As new devices are added, the vendor-supplied end of support dates can be easily added and tracked across the device lifecycle.
- Viakoo can also assess devices if they are using default or easily-guessed passwords, which CRA-complaint devices should not allow.
- Viakoo’s patented “last mile” capability allows firmware updates to be managed at scale without access to the open internet.

4. Additional EU Compliance Considerations

In addition to European Union regulations like CRA and NIS2 there are other compliance considerations to be prepared for (and can Viakoo can support).

1. The EU Machinery Regulation (2023/1230) is mandatory starting in January 2027 and redefines safe machinery as also including being cyber safe. For example, in addition to physical flaws that could injure person the updated directive includes cyberattacks and the physical consequences of them to be within the scope of the regulation. To be compliant organizations must include cyber risks in their Health & Safety risk assessments, and have mechanisms to keep equipment cyber safe.

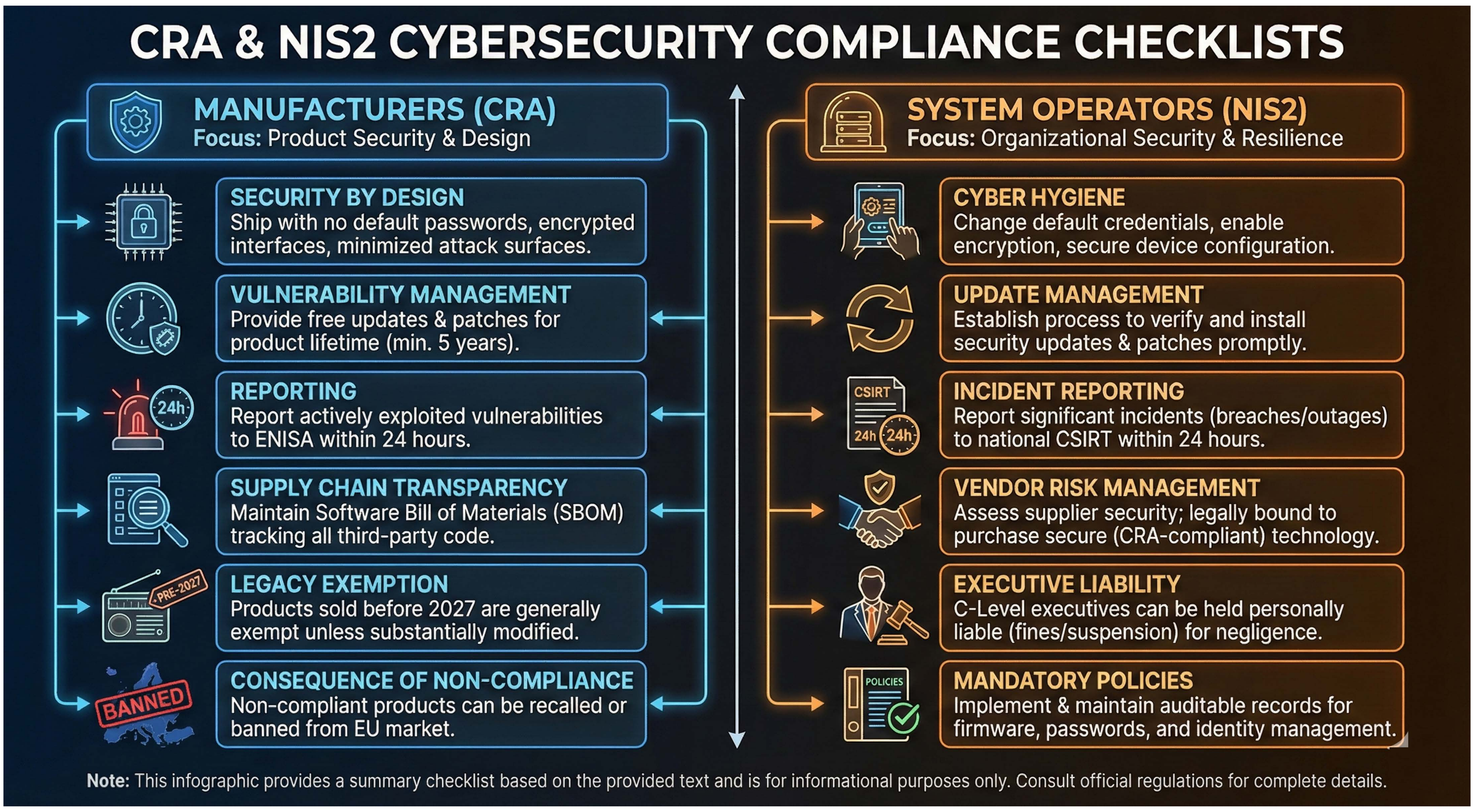
2. Internal or corporate Information Security (InfoSec) policies: Unless you have received a specific exemption for your IoT/OT devices they are subject to the same firmware, password, and certificate requirements as other network-connected devices.

3. Wireless devices (such as a WiFi connected IP cameras, sensors, or other assets) have mandatory requirements under the Radio Equipment Directive (RED) that went into effect in August 2025. These devices must be CE mark certified and conform to all CRA requirements.

Chart: Manufacturer vs System Operator Responsibilities

This white paper speaks to the responsibilities of operators, but there are many considerations for manufacturers as well. As a manufacturer, you are in a unique position because you are likely hit by both regulations simultaneously, but for different reasons.

- Under NIS2: You are regulated as an Entity (an organization that must keep its own factories and enterprise networks secure).
- Under CRA: You are regulated as a Product Maker (someone who must ensure the devices you sell are secure).



CRA & NIS2 CYBERSECURITY COMPLIANCE CHECKLISTS

MANUFACTURERS (CRA)
Focus: Product Security & Design

SECURITY BY DESIGN
Ship with no default passwords, encrypted interfaces, minimized attack surfaces.

VULNERABILITY MANAGEMENT
Provide free updates & patches for product lifetime (min. 5 years).

REPORTING
Report actively exploited vulnerabilities to ENISA within 24 hours.

SUPPLY CHAIN TRANSPARENCY
Maintain Software Bill of Materials (SBOM) tracking all third-party code.

LEGACY EXEMPTION
Products sold before 2027 are generally exempt unless substantially modified.

CONSEQUENCE OF NON-COMPLIANCE
Non-compliant products can be recalled or banned from EU market.

SYSTEM OPERATORS (NIS2)
Focus: Organizational Security & Resilience

CYBER HYGIENE
Change default credentials, enable encryption, secure device configuration.

UPDATE MANAGEMENT
Establish process to verify and install security updates & patches promptly.

INCIDENT REPORTING
Report significant incidents (breaches/outages) to national CSIRT within 24 hours.

VENDOR RISK MANAGEMENT
Assess supplier security; legally bound to purchase secure (CRA-compliant) technology.

EXECUTIVE LIABILITY
C-Level executives can be held personally liable (fines/suspension) for negligence.

MANDATORY POLICIES
Implement & maintain auditable records for firmware, passwords, and identity management.

Note: This infographic provides a summary checklist based on the provided text and is for informational purposes only. Consult official regulations for complete details.

5. Similar Regulations in Other Geographies

Directives similar to the EU's NIS 2 include:

* United Kingdom: The UK's NIS Regulations apply to critical infrastructure with a similar approach, though the upcoming Cyber Security and Resilience Bill is expected to bring it closer to NIS 2. The UK's NIS Regulations cover "Operators of Essential Services" (OES) who heavily rely on ICS/OT, and new rules address IoT devices directly.

* United States: The NIST Cybersecurity Framework (NIST CSF) provides a common set of best practices, and the SEC Cybersecurity Rule mandates stricter measures for financial institutions. The NIST CSF has dedicated programs and guidance for both IoT and ICS security. The SEC Cybersecurity Rule requires public companies to disclose risks, which explicitly involves identifying and managing risks from OT and IoT assets.

* Singapore: The Singapore Cybersecurity Act establishes a legal framework for securing critical information infrastructure and has strong enforcement powers. The Singapore Cybersecurity Act protects Critical Information Infrastructure (CII), which includes computer systems essential to services like energy and transport that use ICS/OT.

These frameworks all focus on enhancing cybersecurity, risk management, and incident reporting for key sectors.

Conclusions & Next Steps

Both NIS2 and CRA put a bright spotlight on the cybersecurity of IoT applications and device systems that organizations rely on. These systems are vulnerable, are being attacked, and lack the proper technology to secure them to the same level that traditional IT systems have been. To properly address these regulations many European enterprises will need accurate application-based discovery, remediation, and governance to ensure that IoT systems are always compliant.

Ready to take steps to improve your IoT security? Here are 4 key areas Viakoo can provide immediate value towards.

1. **Application-based Discovery:** Unlike any IT systems, most IoT systems are a tightly-coupled environment of devices and applications. Start with agentless application-based discovery to make visible the application, device, and port relationships, as well as vulnerabilities that exist in IoT devices or applications.
2. **Remediation Automation:** IoT devices exist in fleets spread across the organization. Manual approaches to firmware patching and password rotations simply do not scale or act fast enough to contain threats.
3. **Bring IoT into Zero Trust:** Ensure that all IoT devices have an automated method for certificate management, and use application-based discovery to ensure network segments are set up correctly.
4. **Repatriation and Compliance:** Increasing mandates, compliance requirements, and cyber insurance documentation means that your IoT security solution must be capable of tracking and reporting all cybersecurity operations over time.