THE PATH TO NIS2 COMPLIANCE

Understanding version two of the Network and Information Security Directive (NIS2) and how Claroty enables in-scope organisations to achieve NIS2 compliance

Introduction

The NIS2 Directive is a piece of legislation that aims to enhance the cyber resilience of critical infrastructure in the European Union (EU) by establishing a minimum set of cybersecurity requirements that all EU member states must impose on their respective in-scope entities. NIS2 replaces and builds upon its predecessor, the original NIS Directive, with an expanded scope and additional requirements developed in response to increases in the frequency and impact of cyberattacks against EU critical infrastructure in recent years.

This solution brief provides a high-level overview of NIS2, details the Claroty portfolio's support for NIS2 compliance, and offers related guidance for security and risk practitioners in the EU and beyond.

NIS2 Basics

Scope

Member states must identify and impose NIS2 requirements on all organisations in their jurisdiction that:

1. Employ at least 50 people or generate at least €10,000,000 in revenue*; and
2. Provide services deemed "essential" or "important" to the health, safety, and/or stability of the EU. In-scope essential and important organisations include those in the following sectors:

ESSENTIAL	IMPORTANT
• Energy • Transportation • Banking and financial infrastructures • Healthcare • Drinking water and wastewater • Digital infrastructure • Public administration • Space	• Postal and courier services • Waste management • Chemical manufacturing, production, and distribution • Food production, processing, and distribution • Manufacturing of medical, electronic, transportation, or related equipment • Digital providers • Research

**Member states may extend NIS2 requirements to organisations that do not meet these personnel or revenue criteria but that do play a key role in supporting the health, safety, and/or stability of the EU.*

NIS2 Compliance Requirements

The minimum requirements for NIS2 compliance for in-scope essential and important entities are as follows:

- **Cybersecurity risk management measures:** Entities must implement 10 key measures to manage and mitigate cyber risks posed to any networks, systems, and/or other digital or physical assets involved in delivering essential or important services in the EU. These measures include:
    1. Policies on risk analysis and information system security
    2. Incident handling (prevention, detection, and response to incidents)
    3. Crisis management and business continuity, such as backup and recovery management
    4. Supply chain security for relationships between each entity and its suppliers or service providers
    5. Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosures
    6. Policies and procedures to assess the effectiveness of cybersecurity risk management
    7. Basic cyber hygiene practices and cybersecurity training
    8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption
    9. Human resources security, access control policies, and asset management
    10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems
- **Incident reporting requirements:** Entities must report cyber incidents to their designated CSIRT (Computer Security Incident Response Team) or other national authority per these specifications:
    - Within 24 hours of detection: Known details of the incident must be communicated
    - Within 72 hours of detection: A full notification report containing an assessment of the incident and its severity, impact, and any indicators of compromise must be communicated
    - Within 30 days of detection: The final report on the incident must be communicated

Noncompliance Penalties

- **For essential entities:** Fines up to €10,000,000 or at least 2% of the total annual worldwide turnover in the previous fiscal year of the company to which the entity belongs (whichever amount is higher)
- **For important entities:** Fines up to €7,000,000 or at least 1.4% of the total annual worldwide turnover in the previous fiscal year of the company to which the entity belongs (whichever amount is higher)

Timelines & Deadlines

- NIS2 entered into force on **16 January 2023**
- Member states must transpose NIS2 into national law by **17 October 2024**
- Member states must identify and register in-scope essential and important entities by **17 April 2025**

How Claroty Supports NIS2 Compliance

The Role of Cyber-physical Systems (CPS)

Claroty's cyber-physical systems (CPS) cybersecurity portfolio both supports and simplifies NIS2 compliance by extending robust protection, monitoring, and other cyber risk management controls to all CPS — including those that underpin the essential and important services provided by EU entities deemed in-scope for NIS2.

As an often-overlooked risk blindspot for critical infrastructure entities and other industrial, healthcare, commercial, and public sector organisations, CPS are imperative to secure not only because doing so is required by NIS2 and other regulations — but also because the health, safety, and stability of our society rely on CPS. Common types include:

- **Operational technology (OT)** assets, such as the programmable logic controllers (PLCs) that drive power generation and manufacturing processes
- **Internet of Things (IoT)** and **Industrial IoT (IIoT)** devices, such as the security cameras and motion sensors that help keep hospitals safe and comfortable
- **Building management system (BMS)** equipment, such as the digitised HVAC controllers and elevators that enable us to breathe clean air and easily move throughout buildings
- **Internet of Medical Things (IoMT)** and other clinical devices, such as the infusion pumps and MRIs that monitor our vitals, diagnose our ailments, and help us keep us healthy

The aforementioned, as well as all other, types of CPS are inherently challenging to secure (including in the context of NIS2 compliance and otherwise), largely because they are incompatible with traditional security tools and approaches. Claroty tackles this challenge with a comprehensive-yet-flexible cybersecurity portfolio that is purpose-built to protect — and support NIS2 and other regulatory requirements for — all CPS.

About the Claroty Portfolio

Claroty supports all use cases and objectives on the full CPS cybersecurity journey. Portfolio solutions include:

Claroty xDome

Claroty xDome is a flexible SaaS platform purpose-built for all use cases & types of CPS on the entire industrial cybersecurity journey.

Medigate by Claroty

Medigate by Claroty is a SaaS-based healthcare cybersecurity platform that safeguards the devices that underpin patient care.

Claroty SRA

Claroty Secure Remote Access (SRA) delivers frictionless, reliable, secure remote access for internal & third-party OT personnel.

Claroty CTD

Claroty Continuous Threat Detection (CTD) offers robust, on-premises cybersecurity controls for industrial environments.

Mapping Claroty Capabilities to NIS2 Requirements for Cybersecurity Risk Management

The following table outlines the extent that the capabilities provided by solutions within Claroty's portfolio map to the cybersecurity risk management requirements set forth by the NIS2 Directive:

	NIS2 REQUIREMENT	SUMMARY OF CLAROTY SUPPORT	SOLUTION(S)
1.	**Policies on risk analysis and information security**	Claroty discovers and assesses all assets, systems, vulnerabilities, and cyber and operational risks in CPS environments and uses this extensive visibility to automatically define and enable the enforcement of policies that mitigate exposure to such risks.	**Claroty xDome, Medigate, & CTD**
2.	**Incident handling**	Claroty continually monitors the entire CPS environment for the earliest indicators of known and unknown threats, contextualises all alerts to optimise response, and integrates with SIEM, SOAR, and related solutions to extend existing SOC workflows across all CPS.	**Claroty xDome, Medigate, & CTD**
3.	**Crisis management and business continuity**	Claroty delivers a comprehensive, real-time inventory for all CPS, logs all asset and network changes and anomalies, defines and enables enforcement of network segmentation policies and access controls that help protect against and contain incidents, and offers ready-made integrations with backup and recovery tools — all of which help drive and improve entity-wide crisis management and continuity efforts.	**Claroty xDome, Medigate, SRA, & CTD**
4.	**Supply chain security**	Claroty correlates all discovered assets against the latest CVEs and other weaknesses, continually assesses risk in the CPS environment, and provides secure-yet-frictionless remote access to OT for all internal and third-party users, enabling customers to effectively and efficiently assess, manage, and mitigate third-party risk across their supply chains.	**Claroty xDome, Medigate, SRA, & CTD**
5.	**Security in network and information systems**	Claroty correlates all discovered assets against the latest CVEs, misconfigurations, and other weaknesses in real-time, continually assesses risk exposure in the entire CPS environment, and provides highly secure-yet-frictionless remote access to OT for all internal and third-party personnel, enabling customers to effectively and efficiently assess, manage, and mitigate cyber risk across their environments.	**Claroty xDome, Medigate, SRA, & CTD**
6.	**Policies and procedures to assess the effectiveness of cybersecurity risk management**	Claroty offers a custom risk-scoring mechanism, the ability to simulate the impact of risk remediation measures, proactive monitoring and historical assessments to measure how respective controls impact enterprise-wide risk posture over time, and flexible reporting to simplify the communication of this information for stakeholders across disciplines.	**Claroty xDome, Medigate, & CTD**
7.	**Basic cyber hygiene practices and cybersecurity training**	Claroty's risk reporting and simulation include remediation recommendations that help inform cyber hygiene and training needs. Additionally, Claroty's SRA solution enables easy enforcement of RBAC, password policies, and other cyber hygiene practices among both internal and third-party personnel.	**Claroty xDome, Medigate, SRA, & CTD**
8.	**Policies and procedures for cryptography, encryption**	Claroty encrypts all user-, CPS-, and other system-related data in accordance with NIS2, GDPR, and other regulatory requirements. Claroty also alerts on events in which sensitive data, such as personal health information (PHI), is processed against policies or otherwise, enabling customers to preempt incidents involving potential data exposure.	**Claroty xDome, Medigate, SRA, & CTD**
9.	**Human resources security, access controls, and asset management**	Claroty's risk mitigation recommendations help inform and prioritise cyber hygiene and access control policies. Additionally, Claroty's SRA solution enables easy enforcement of RBAC, password policies, and other cyber hygiene practices for internal and third-party personnel. Claroty's seamless integration with CMDB, CMMS, and related solutions enables easy extension of existing asset management workflows to all CPS entity-wide.	**Claroty xDome, Medigate, SRA, & CTD**
10.	**Multifactor authentication and secured communications**	Claroty SRA offers Zero Trust-based access controls including granular RBAC and MFA for all internal and third-party OT personnel, as well as secure remote and onsite access to all CPS within OT environments with the added peace of mind of high availability, an OT purpose-built UX, and full recordings to support audits, forensics, and related use cases.	**Claroty xDome, Medigate, SRA, & CTD**

Mapping Claroty Capabilities to NIS2 Requirements for Incident Reporting

The following table outlines the extent that the capabilities provided by any solution(s) within Claroty's portfolio map to the incident reporting requirements set forth by the NIS2 Directive:

	NIS2 REQUIREMENT	SUMMARY OF CLAROTY SUPPORT	SOLUTION(S)
1.	**Within 24 hours: Communicate all known details of the incident**	Claroty continuously monitors the entire CPS environment, enabling rapid detection of the earliest indicators of potential incidents. All events related to the same incident are bundled into a single, fully contextualised alert with all relevant details that can be quickly and easily exported and shared with relevant authorities to satisfy this requirement.	**Claroty xDome, Medigate, & CTD**
2.	**Within 72 hours: Submit a full notification report with an assessment of the incident and its severity, impact, and any IoCs**	The granular details with which Claroty enriches each alert typically include the incident's IoCs, a full root-cause analysis, involved or otherwise affected assets, exploited vulnerabilities, their severity, and their risk to the environment, mitigation recommendations, logs, and more — all of which support further impact assessments and can be quickly and easily shared with relevant authorities to satisfy this requirement.	**Claroty xDome, Medigate, & CTD**
3.	**Within 30 days: Submit the final report on the incident**	In addition to the above monitoring, alert enrichment, and assessment capabilities, Claroty's portfolio integrates seamlessly with SIEM, SOAR, EDR, CMDB, and other IT, operational, and security technologies. Such integrations further support forensics investigations, audits, and related workflows across IT and CPS environments, enabling customers to more effectively and efficiently assess and report on incidents entity-wide.	**Claroty xDome, Medigate, & CTD**

Conclusion

Claroty's cybersecurity portfolio is especially ideal for security and risk practitioners at industrial, healthcare, commercial, and public sector organisations that are in-scope for NIS2. The portfolio offers extensive support for the directive's cybersecurity risk management and incident reporting requirements — particularly in the context of cyber-physical systems (CPS). By harnessing and seamlessly integrating Claroty's CPS cybersecurity solutions with their existing IT security tools and workflows, practitioners will gain full coverage and support for all NIS2 requirements across all IT and CPS environments entity-wide.

About Claroty

Claroty empowers industrial, healthcare, commercial, and public sector organisations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organisations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.