WHITE PAPER

Securing Industrial Automation: A Joint Solution for NIS2 Compliance

INTRODUCTION

The NIS2 Directive marks a significant advancement in the European Union's cybersecurity framework, mandating that organizations in critical sectors, including manufacturing and distribution, enhance their cybersecurity measures. This directive aims to bolster the resilience of essential services against cyber threats. Compliance can be complex, requiring a multifaceted approach.

This whitepaper outlines how Copia Automation and Claroty, working together, provide a comprehensive solution to help manufacturers and distributors meet the rigorous requirements of NIS2, specifically addressing the challenges of securing industrial automation and operational technology (OT) environments.

COPIA CLAROTY

UNDERSTANDING NIS2 AND ITS IMPACT ON MANUFACTURING AND DISTRIBUTION

NIS2 expands the scope of its predecessor, the NIS Directive, by including more sectors and imposing stricter cybersecurity obligations. For manufacturing and distribution, this means that a broader range of entities must now implement robust security measures, report incidents promptly, and ensure business continuity in the face of cyberattacks.

KEY REQUIREMENTS OF NIS2

NIS2 outlines several key requirements, including:

- Risk Management: Organizations must adopt comprehensive cybersecurity risk management practices.
- Corporate Accountability: Management bodies are directly responsible for overseeing and approving cybersecurity measures.
- Reporting Obligations: Entities must establish processes for timely reporting of significant incidents.
- Business Continuity: Organizations must develop and implement business continuity plans.

These requirements are underpinned by **10 Minimum Security Measures**, which include:

1. Risk assessments and information system security policies
2. Policies and procedures to evaluate the effectiveness of cybersecurity risk-management measures
3. Policies and procedures regarding the use of cryptography and, where appropriate, encryption
4. Incident response plan
5. Security in the acquisition, development, and maintenance of network and information systems, including vulnerability handling and disclosure
6. Cybersecurity training and basic cyber hygiene practices
7. Security procedures for employees with access to sensitive data, including data access policies and asset management
8. Business continuity management plan, including backup management and disaster recovery

9. 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
10. Security of supply chains, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

THE CHALLENGES OF SECURING INDUSTRIAL AUTOMATION

Manufacturing and distribution rely heavily on industrial automation, including operational technology (OT) systems that control critical processes. However, these environments face unique challenges:

- **Increased Cyberattacks:** The convergence of IT and OT has expanded the attack surface, leading to a rise in cyberattacks targeting Industrial Control Systems (ICS).
- **Unplanned Downtime:** Cyberattacks and operational issues can cause significant financial losses due to unplanned downtime.
- **Legacy Systems:** OT environments often include legacy equipment not designed with security in mind and contain outdated software, making them vulnerable to cyber threats.
- **Lack of Visibility:** Inadequate visibility into OT assets and their configurations hinders effective risk management.
- **Siloed Teams:** The traditional separation of IT and OT teams can impede collaboration on security initiatives.

THE COPIA AND CLAROTY SOLUTION: A COMPLEMENTARY APPROACH

Copia Automation and Claroty offer a joint solution that addresses these challenges and helps manufacturers and distributors achieve NIS2 compliance.

CLAROTY'S ROLE: OT CYBERSECURITY

Claroty provides a comprehensive OT cybersecurity platform that delivers:

- **Asset Discovery and Inventory:** Claroty discovers and identifies all OT and IoT assets, providing deep visibility into industrial networks. This enables organizations to create a complete and accurate inventory of assets across their cyber-physical systems (CPS), which is crucial for effective cybersecurity and aligns with NIS2 requirements for asset management.
- **Exposure Management:** Claroty helps organizations identify, assess, and prioritize vulnerabilities and exposures in their OT environments. By comparing CPS assets to an extensive database of insecure protocols, CVEs, configurations, substandard security practices, and other vulnerabilities tracked by Claroty's award-winning Team82 researchers.
- **Network Protection:** Claroty protects industrial operations by applying zero-trust philosophies to OT devices to restrict unwanted access via policy enforcement and network segmentation. Claroty recommends policies and integrates with your existing NAC and firewalls to enforce and monitor policy compliance to safeguard against unauthorized access and threats.
- **Secure Access:** Claroty enables secure access to OT environments, ensuring that authorized personnel can connect and manage systems without compromising security.
- **Threat Detection:** Claroty continuously monitors the CPS environment for the earliest indicators of known and unknown threats, contextualizes all alerts to optimize response, and integrates with SIEM, SOAR, and related solutions to extend existing SOC workflows across all CPS.

Claroty's solutions support NIS2 compliance by:

- Minimizing attack impact and probability through network segmentation, ensuring secure access to remote assets, tailored prioritization and recommendations, as well as incident response playbooks for SOC teams.
- Discovering and assessing 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.

- Delivering 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.
- Correlating 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.
- Offering 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.
- Encrypting all user-, CPS-, and other system-related data in accordance with NIS2, GDPR, and other regulatory requirements.

COPIA AUTOMATION’S ROLE: INDUSTRIAL DEVOPS

Copia Automation provides an Industrial DevOps platform that complements Claroty’s cybersecurity solutions by focusing on:

- **Version Control and Backup:** Copia provides a Git-based version control system for industrial automation code, including PLC programs, HMI configurations, and other critical software. This ensures that all changes to automation code are tracked, providing a detailed history that is crucial for audits, incident investigation, and understanding system evolution. Copia also automates backups and stores them in secure, offsite cloud storage, for enhanced accessibility and redundancy.
- **Change Management:** Copia’s visual diffs allow you to compare versions of code quickly, so you can always see what’s changed.
- **Rollback Capabilities:** In the event of an incident, such as a cyberattack or system failure, Copia enables quick restoration to previous known-good versions of code, minimizing downtime and facilitating faster recovery.
- **Branching and Merging:** Copia facilitates secure development practices by allowing engineers to work on new features or fixes in isolation and then merge them into the main codebase after thorough testing and review.

- **User Access Control and Permissions:** Copia helps organizations establish roles and access rights, ensuring that only authorized individuals can make changes to automation code, thus enhancing security and aligning with NIS2 requirements for access control policies.
- **Centralized Repository:** Copia provides a single, secure location for storing all automation code, improving organization, accessibility, and security.

Copia's capabilities directly support NIS2 compliance by:

- **Enhancing Risk Management:** Copia's core function of managing the development and changes to automation code helps organizations track every change, identify potential vulnerabilities, and maintain accountability. This aligns with NIS2 requirements for security in the acquisition, development, and maintenance of network and information systems.
- **Strengthening Incident Handling:** While Copia doesn't directly handle incident response, it plays a vital role in recovery. If an incident involves compromised code, Copia enables organizations to quickly revert to a previous known-good state, minimizing downtime and facilitating faster recovery.
- **Improving Business Continuity:** Copia ensures business continuity by providing a robust and reliable backup and recovery mechanism for automation code. The Git-based system enables automated backup and retention of automation code for accessibility during disaster recovery scenarios.
- **Securing sensitive data and asset management:** Copia helps with the management of your automation systems through access control. Copia supports minimum necessary access and least privilege access to your automation code and supports preventing unauthorized or accidental changes. Copia is a central repository for your automation assets.

COVERAGE OF NIS2 REQUIREMENTS BY THE COPIA AND CLAROTY JOINT SOLUTION

The Copia and Claroty joint solution provides comprehensive coverage for several key aspects of the NIS2 Directive, enabling organizations to effectively meet their compliance obligations. Here's how the solution aligns with the main pillars of NIS2:

1. Cybersecurity Risk Management Measures:

- **Policies on risk analysis and information system security (21.2a):** Claroty discovers and assesses all assets, systems, vulnerabilities, and cyber and operational risks in CPS environments. This extensive visibility is crucial for risk analysis and enables the enforcement of policies to mitigate identified risks. Copia enhances this by providing detailed version control of industrial code, ensuring that changes are tracked and potential vulnerabilities introduced during development or maintenance are easily identified.
- **Incident handling (21.2b):** Claroty excels in continuous monitoring for early indicators of known and unknown threats, contextualizing alerts, and integrating with SIEM/SOAR solutions to extend existing SOC workflows across all CPS. Copia complements this by enabling rapid recovery from incidents involving compromised or corrupted code through its version control and rollback capabilities.
- **Business continuity and crisis management (21.2c):** Claroty delivers a comprehensive, real-time inventory of all CPS, logs all asset and network changes, and enables enforcement of network segmentation and access controls. Copia adds to this by providing a robust and reliable backup and recovery mechanism for automation code, ensuring that organizations can quickly restore operations after a cyber incident or hardware failure.
- **Supply chain security (21.2d):** Claroty correlates discovered assets against the latest CVEs and weaknesses, continually assesses risk, and provides secure remote access to OT for internal and third-party users. This helps customers assess, manage, and mitigate third-party risk across their supply chains.
- **Security in system acquisition, development, and maintenance (21.2e):** Claroty correlates discovered assets against CVEs, misconfigurations, and other weaknesses, and provides secure remote access. Copia's Git-based system ensures that all changes to automation code are tracked, providing a detailed history that is crucial for managing security in system development and maintenance.
- **Assessment of cybersecurity risk-management measures (21.2f):** Claroty offers a custom risk-scoring mechanism, the ability to simulate the impact of risk remediation measures, and proactive monitoring to measure how controls impact risk posture.

- **Basic cyber hygiene practices and training (21.2g):** Claroty's risk reporting and simulation include remediation recommendations that help inform cyber hygiene and training needs. Copia enhances security procedures for employees with access to sensitive data, including data access policies and asset management (21.2i).
- **Policies regarding cryptography and encryption (21.2h):** Claroty encrypts all data in accordance with NIS2, GDPR, and other regulations.
- **Use of multi-factor authentication and secured communications (21.2j):** Claroty xDome Secure Access 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.

2. Incident Reporting Requirements:

- Claroty provides continuous monitoring of the entire CPS environment, enabling rapid detection of potential incidents. Claroty also enriches each alert with granular details, including IoCs, root-cause analysis, affected assets, exploited vulnerabilities, and mitigation recommendations. These capabilities support compliance with NIS2's requirements for reporting incidents within 24 hours, 72 hours, and 30 days.

By combining the strengths of both platforms, manufacturers and distributors can:

- Gain comprehensive visibility into their OT environments
- Proactively manage and mitigate cyber risks
- Strengthen the integrity and security of their automation code
- Respond effectively to security incidents
- Maintain business continuity in the face of cyber threats
- Simplify compliance with NIS2 requirements

CONCLUSION

The NIS2 Directive presents a significant challenge for manufacturers and distributors, but it also provides an opportunity to enhance their cybersecurity posture and build more resilient operations. By implementing the joint solution from Copia Automation and Claroty, organizations can effectively address the requirements of NIS2, protect their critical infrastructure, and ensure business continuity in an increasingly interconnected and threat-filled world.

CALL TO ACTION

To learn more about how Copia Automation and Claroty can help your organization meet NIS2 requirements and secure your industrial automation environment, please contact us for a demo or email us to begin a consultation on your OT Cyber initiative today.

Copia:
Email: contact@copia.io
Demo: https://www.copia.io/request-demo

Claroty:
Email: info@claroty.com
Demo: https://www.claroty.com/request-a-demo

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit www.claroty.com.

About Copia Automation

Copia Automation delivers an Industrial DevOps Platform that empowers enterprises - large, mid-sized, and small - to effectively manage their operational technology, achieving industrial automation success. Copia's cloud-based Industrial DevOps Platform empowers companies with unparalleled visibility, governance, and control of automation code across multi-vendor devices. This provides a single source of truth, which enforces continuous quality control, increased uptime, automated backup, and preemptive crisis management. With the addition of AI-powered features like Copia Copilot, Copia Automation continues to drive the future of industrial automation forward. With its headquarters in New York City, Copia Automation is a member of the World Economic Forum as a Technology Pioneer in Manufacturing. For more information, visit www.copia.io.