CASE STUDY

Securing Supply Chain Operations

Swiss Retail Giant Coop Gains Full OT Visibility and Reduces Cyber Exposure Across Logistics, Warehousing, and Production

Overview

As one of Switzerland's largest retail and wholesale companies, Coop operates a diverse portfolio of businesses, including supermarkets, convenience stores, warehousing, logistics, and production facilities. This diverse operational footprint makes the security of Coop's OT environments essential to maintaining business continuity and safeguarding the supply chain.

Challenges

Coop recognized that its increasingly interconnected logistics and production infrastructure posed a significant security risk. Their core challenges were:

- **Limited Visibility:** Until now, Coop did not have a complete, unified inventory of all OT, IoT, and industrial control system (ICS) assets across its various sites.
- **Limited Insight Into the OT Attack Surface:** Without full asset visibility, identifying and prioritizing vulnerabilities and exposures within critical operational processes was very complex.

The Coop Group is a leading retail and wholesale powerhouse based in Switzerland, operating as a cooperative with a rich history spanning over 150 years. As one of the nation's largest employers with over 95,000 staff members, Coop maintains a dominant market presence through approximately 2,500 points of sale, including supermarkets, department stores, and specialty formats. Beyond its well-known retail footprint, the Basel-headquartered organization drives extensive international wholesale operations through the Transgourmet Group, making it a critical pillar of the European food service and supply chain infrastructure.

- **Segmentation Challenges:** To successfully implement zoning and segmentation, Coop needed greater transparency into device communications. This was essential for accurately defining trust zones while minimizing the risk of operational disruption.

Solution

Coop partnered with Claroty to implement a scalable, proactive security program designed for a retail OT environment. The Claroty xDome Platform was deployed across Coop's major production, warehousing, and logistics sites, with plans to extend protection to in-store operations.

Claroty guided Coop through a business-centric approach to securing their OT environment, ensuring that security priorities were directly aligned with business criticality.

- **Unified Asset Visibility:** Coop gained comprehensive visibility across its multi-site OT environment, establishing a continuously updated inventory of all OT, ICS, and IoT assets. This enabled Coop to define the criticality of assets and operational processes, creating a single source of truth for risk analysis.
- **Business-Centric Exposure Management:** Coop used contextual exposure insights to identify, assess, and prioritize vulnerabilities based on their potential impact on critical operational processes, reducing the OT attack surface while aligning remediation efforts with business risk.
- **Network Segmentation:** Coop applied Claroty-recommended policies to design, validate, and enforce granular network segmentation. Automated policy recommendations simplified segmentation design, while continuous monitoring ensured ongoing compliance and protection of critical asset zones.

> **"Claroty has given us complete visibility about our OT and IoT environment. With xDome, we can identify risks, define appropriate measures, and monitor them."**
>
> **Andreas W.,**
> Head of Operational Technology (OT/IOT)

Benefits

By adopting the Claroty xDome Platform, Coop achieved its primary security objectives, resulting in a significantly hardened logistics environment and enhanced operational resilience.

- **Complete Visibility & Inventory:** Gained 100% comprehensive visibility of all OT/ICS and IoT assets across multiple sites, with critical operational processes clearly defined.
- **Reduced Risk:** Shifted security efforts to a business-centric model, focusing remediation on the exposures that pose the highest risk to critical operational processes.

- **Stronger Network Protection:** Successfully implemented and enforced granular network segmentation between critical asset zones, significantly reducing the attack surface and containing the potential blast radius of any security incident.
- **Efficiency:** Leveraged Claroty's automated policy recommendations to accelerate the design and deployment of secure segmentation policies, saving engineering time and resources.

> **"Claroty xDome gives us an overview in the OT area. We were able to reduce the effort involved through manual maintenance and extensive research."**
>
> **Andreas W.,**
> Head of Operational Technology (OT/IOT)

Conclusion

With its core productions, logistics, and warehousing facilities secured, Coop is well-positioned to expand the Claroty deployment to additional in-person retail locations. This partnership has allowed Coop to build a foundation for their cyber-physical systems (CPS) protection program, enabling them to expand OT security initiatives across the entire organization.

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 claroty.com.