HWG Sababa

GRUPPO multicedi

Multicedi Secures a €2.1B Retail Ecosystem with HyperSOC™ Across IT and OT



Executive Summary

Multicedi, one of Southern Italy's leading companies in large-scale retail distribution, operates approximately **600 affiliated supermarkets** supported by **5 distribution centers** and a highly distributed digital infrastructure.

To strengthen cybersecurity across its expanding **IT and OT environment**, Multicedi partnered with **HWG Sababa**. By implementing **HyperSOC™** managed security operations and expanding visibility across thousands of connected devices, the company improved threat detection and response capabilities, reduced operational risk, and strengthened readiness for NIS2 compliance.

Key Results

- **Continuous security monitoring across 600 retail locations and 5 distribution centers**
- **50% faster threat detection and response (MTTD / MTTR)**
- **Centralized visibility across IT and thousands of connected OT devices**
- **Strengthened governance and NIS2 readiness**

Company Background

Multicedi is a major player in Southern Italy's large-scale retail distribution sector. The company operates a network of approximately 600 affiliated supermarkets under multiple brands, supported by five logistics centers across the region.

The organization employs more than 1.300 users, including approximately 300 office staff and 1.000 warehouse operators, and generated €2.1 billion in revenue in 2025.

The company's digital infrastructure reflects the scale and complexity of its retail operations, combining traditional IT systems with a growing number of connected operational devices supporting logistics and retail activities.

Key Challenges

Multicedi faced several cybersecurity challenges typical of large and highly distributed retail environments.

Highly Distributed Attack Surface

The company operates 5 distribution centers connected continuously with ~600 retail locations for fiscal reporting, logistics coordination, and operational management. Each store, warehouse, and remote system represents a potential entry point into the corporate environment.

Hybrid and Multi-Cloud Infrastructure

Multicedi runs a hybrid architecture where part of the infrastructure remains on-premises while most applications operate across 4 different cloud environments, increasing complexity in monitoring and governance.

Limited Visibility into Operational Technology

Thousands of operational devices – including scanners, warehouse systems, Android terminals, refrigeration systems, and facility controls – support daily operations. Many of these assets historically fell outside traditional IT monitoring.

Lean Internal Security Resources

Despite the scale of its operations, the internal IT team consists of 10 professionals, managing infrastructure, applications, and security, with only 2 generalists dedicated to cybersecurity.

Regulatory Pressure

As a large food-sector operator, Multicedi must comply with evolving European cybersecurity regulations such as NIS2, which require stronger governance, monitoring, and cyber risk management capabilities.

Unlike many organizations, Multicedi chose not to wait for a cyber incident before taking action.

"When you operate at our scale, risk management is not theoretical. If operations stop for even a short time, the cost is immediate."
– Livio De Prisco, CIO of Multicedi

The Solution: Integrated Security Operations Across IT and OT

To address these challenges and support its digital transformation roadmap, Multicedi partnered with a cybersecurity integrator specializing in IT and OT environments with 25 years of industry experience supporting large retail enterprises across Italy. Together they defined a multi-year cybersecurity evolution roadmap for Multicedi.

In 2023, Multicedi selected **HWG Sababa as its SOC provider**, introducing managed security operations through **HyperSOC™**.
The initiative established a coordinated security architecture combining continuous monitoring, threat detection, asset visibility, and close operational collaboration between the SOC and Multicedi's internal IT team.

Unlike alternative proposals focused on autonomous implementation of individual technologies, Multicedi chose an **integrated ecosystem approach**. The partner led infrastructure design and endpoint security integration, while HWG Sababa delivered managed detection and response through HyperSOC™, ensuring continuous monitoring and operational support.

"In an environment this distributed, the real value is not adding more tools, but building a coherent framework that gives you control over the entire ecosystem."
– Livio De Prisco, CIO of Multicedi.

Implemented Capabilities

Managed Security Operations through HyperSOC™
Deployment of 24/7 SOC monitoring with SIEM-based correlation across the IT perimeter and centralized log management. HyperSOC™ serves as the central platform for monitoring, detection, and response, acting as the operational backbone for the security technologies deployed across the environment. SOC analysts work directly with Multicedi's IT team, providing continuous operational oversight and specialized cybersecurity expertise.

Endpoint Threat Detection and Response
Managed detection and response capabilities were deployed across the endpoint environment using SentinelOne, enabling rapid identification and containment of suspicious activity.

OT Asset Discovery and Visibility
Deployment of Armis Centrix™ for Asset Management and Security, an advanced OT cyber exposure management platform delivering complete asset awareness, enabled Multicedi to achieve real-time visibility across thousands of connected operational devices within its distributed infrastructure. The platform automatically identified and classified a broad range of assets – including barcode scanners, warehouse management systems, Android terminals, refrigeration units, and facility control systems – eliminating blind spots and uncovering previously unmanaged devices.

Supply Chain and Third-Party Monitoring
Continuous monitoring of supplier connections and third-party access points strengthens oversight of the extended partner ecosystem. Controls include automated VPN session limits, account lockouts after repeated failed attempts, and monitoring of anomalous third-party activity.

Hyperautomation within the SOC
Automation mechanisms were gradually introduced within HyperSOC™ to accelerate incident investigation and response processes, reducing manual effort and improving response times.

The Results: Operational Stability and Measurable Resilience

Since implementing HyperSOC™, Multicedi has strengthened its cybersecurity posture while maintaining uninterrupted operations across its retail network.

Continuous monitoring and coordinated SOC operations improved detection and response capabilities while expanding visibility across the organization's IT and OT infrastructure.

Operational Outcomes

The project delivered measurable improvements across security operations:

- **Reduced operational risk across 600 retail locations and 5 distribution centers,** supporting Multicedi's growing retail network
- **50% reduction in MTTD and MTTR**, improving threat detection and response times
- **Centralized visibility across IT and OT assets**, including thousands of operational devices
- **Stronger oversight of supplier and third-party access**, enabling faster detection and prevention of unauthorized activity
- **Greater readiness for NIS2 compliance**, supported by stronger governance and continuous monitoring capabilities

Continuous SOC support has also increased the **effectiveness of the internal IT team**, allowing resources to focus on infrastructure evolution and strategic initiatives rather than reactive incident response.

Strategic Impact

Beyond operational improvements, the initiative strengthened cybersecurity governance across the organization. Cyber risk is now treated as a business risk, regularly discussed at executive and board level. Management participation in security awareness initiatives aligned with NIS2 requirements has further improved governance maturity and organizational readiness.

By combining the partner's architectural expertise with HWG Sababa's HyperSOC™ managed security operations, Multicedi established a centralized security model capable of supporting its distributed retail infrastructure.

Next steps in the cybersecurity roadmap include conducting penetration testing across all affiliated stores, further strengthening security across the company's retail ecosystem.

"No organization is untouchable. The key lesson is not to attempt to manage cybersecurity alone. Internal IT teams are rarely specialized cyber defenders. Without experienced partners, organizations risk spending more while achieving less protection."

– Livio De Prisco, CIO of Multicedi