Deloitte.

From high-end to high-security

Operational Technology (OT) cybersecurity transformation for a luxury goods leader.

Building resilience across OT and Information Technology (IT) to protect operations and enable digital growth.

Luxury consumer goods	Deloitte OT Cybersecurity Services
Industry	Solution

Cyber Stories

The starting point

Production downtime can be disastrous for manufacturers. For one maker of luxury goods, getting ahead of operational disruption has become a priority. The company has integrated more digital capabilities to support and enhance its traditionally manually intensive business. This digital transformation also supports its focus on crafting high-quality products for consumers worldwide.

In looking at the company's longer-term digital evolution, company leaders recognized that their traditional business was becoming more complex. Operational technology (OT) and information technology (IT) were intersecting in new ways resulting in new opportunities for cyber threat actors and others to disrupt operations— a common side effect of integrating IT and OT.

From ransomware attackers to hacker-activists ("hacktivists") targeting the luxury goods industry, there was no shortage of potential threats for the high-profile company and its 10 manufacturing sites and several repair centers across Europe.

Leaders understood that isolating risks across the OT/IT environment would be key to business resilience—to ensure that disruptions in one part of the business could be contained and remediated while having minimal impact on other business processes. They also understood that, to evolve with confidence and continue to operate efficiently, the business required a more strategic, end-to-end approach to OT cybersecurity, along with a greater understanding of its own technology environment.

Factors in focus

- Increased digitalization of the business
- Growing interdependencies across IT and OT
- Evolution and complexity of threats targeting the business

The way forward

To start transforming its security posture for a new digital landscape, the luxury goods maker enlisted the help of Deloitte's OT Cybersecurity team to begin mapping out its future. Creating a solid OT security policy and reference network architecture was the first step toward building a more secure environment and guiding future decisions about new OT or IT solutions. To jumpstart the transformation, Deloitte employed Factory Accelerated Security Transformation (FAST), its proven combination of technology and implementation that is designed to rapidly improve cybersecurity and fortify infrastructure within OT environments. Deloitte also drew on its global team of industry-specific OT specialists, ethical offensive hackers, network architects, and other cybersecurity professionals.

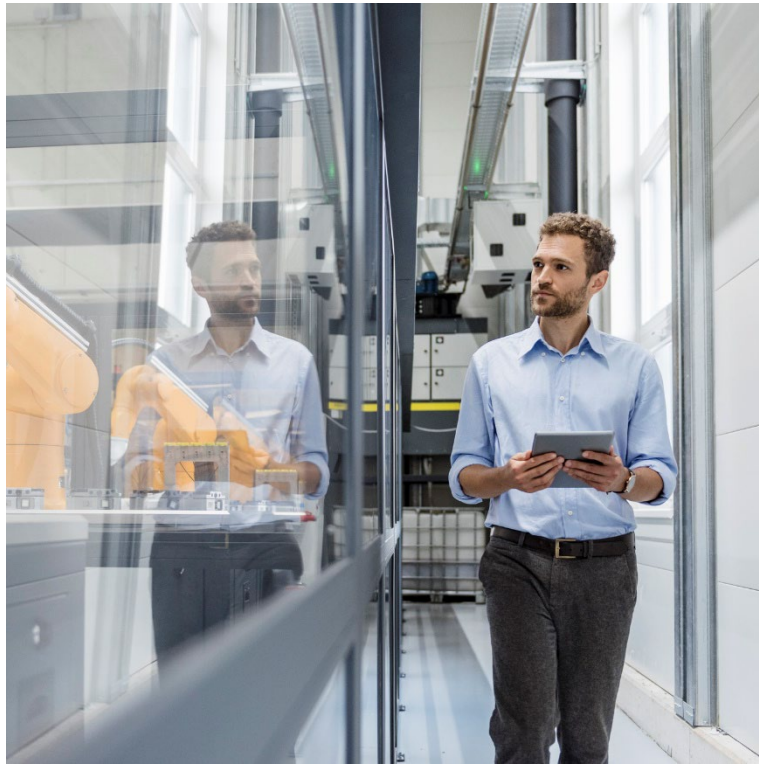
After helping to create a robust security policy and reference architecture as the foundation, Deloitte supported the company on automated asset discovery and business process inventory. Doing so helped the manufacturer understand its current OT environment and how various assets connected with other assets and systems—crucial for understanding interdependencies and risks, and for business continuity planning.

Insights to inspire

Know what you need to protect and where it is. Be curious. Conduct a thorough asset discovery and inventory process that can inform and support your security strategy.

Get into "island mode." After determining the interdependencies of your operations, know how you can disconnect them to keep certain assets and processes running—to avoid unnecessary downtime.

From high-end to high-security



Enabling “island mode” was also a vital need, to allow processes or assets to continue to operate effectively as isolated “islands” in the event of a disruption to a connected process or asset. Deloitte supported the segmentation of IT and OT environments through both high-level design (HLD) and low-level design (LLD), even working with the company on design needs for a planned factory.

With a new security reference architecture and guiding policy, a new view of its assets, and new segmentation across its environment, it was also critical for the company to train IT staff, OT engineers, and other internal users and operators. To set the company up for success, Deloitte developed detailed training materials to support implementation, as well as a broader set of educational resources to help drive policy compliance, ensure internal alignment on security objectives, and get ahead of potential employee questions or concerns.

The achievements

The combined team devised a comprehensive policy that addressed more than a dozen key topics in OT cybersecurity, including asset management, vulnerability management, backup management, secure remote access, account management, and password protocols. These focus areas were central to the design and implementation of a secure, effective future OT environment. The manufacturer was able to achieve its business goal of securing the IT and OT environments while maintaining business continuity and reducing the risk of production interruptions.

As a result of the work, the company has realized improvements in:

Cybersecurity

By conducting an OT asset discovery and designing a more secure OT network, the client would be better equipped to prevent cyberattacks in its industrial environment. This would help to protect its production capabilities and prevent potential financial losses.

Operational continuity

The design allowed sites to operate in "island mode," ensuring that operations could continue even if IT and OT environments needed to be isolated due to an attack.

Operational efficiency

The physical manual inventory and automated discovery of network traffic and characteristics of the remaining OT assets have provided the company with a comprehensive overview of its OT environment, helping optimize operations and identify areas for improvement.

Asset management

The process of discovering and registering OT assets is helping the company manage assets more efficiently. This enables it to track its assets, monitor performance, and identify any issues that may arise.

Training and compliance

Employees are well-equipped to comply with the new OT security policy and use the new processes and tools effectively. This has resulted in increased efficiency and productivity, reduced risk of security breaches, and improved compliance with industry leading practices.

Let’s talk cyber

How is your organization evolving—and how is it preparing for the new types of threats that are headed its way? Discover how Deloitte’s worldwide team of industry-focused OT cybersecurity specialists can help you get ahead of new challenges. Contact us to get the conversation started.

deloitte.com/cyber

Contacts

Dana Spătaru
Global Emerging Technology Cyber Leader
Deloitte Netherlands
dspataru@deloitte.nl

Cedric Nabe
Cyber Strategy and Transformation Leader
Deloitte Switzerland
cnabe@deloitte.ch

Guy Florian Seka
Senior Manager,
Industrial Cybersecurity Lead
Deloitte Switzerland
gfseka@deloitte.ch

Deloitte.

Cyber Stories