STORMSHIELD

INDUSTRY

FRENCH INDUSTRIAL AND TECHNOLOGICAL GROUP

GLOBAL VISIBILITY OF INFORMATION SYSTEMS TO IMPROVE CYBERSECURITY

+ more than 84,000
EMPLOYEES

+ more than 1 ,300
EXPERTS WORKING TOWARDS THE INNOVATION STRATEGY

+300
ESTABLISHMENTS ALL OVER THE WORLD

The cyber challenges of industry 4.0

Analysis of data provided by sensors, automation of logistics, product customisation... The industry is gradually migrating to the "smart factory" model to increase productivity, anticipate predictive maintenance and improve the customer experience.

But the multiplying connections to the IT world via IP networks and machine-to-machine communications are generating new cyber security risks and increasing attack surfaces. However, Industrial Control Systems (ICS) are complex elements that require a security policy suited to their particular constraints.

The challenges are many. It is necessary to ensure the integrity of the data sent to the different devices, avoid rebound attacks and secure communications between the different information systems. This exhaustive visibility is essential to ensure the sustainability and the resilience of the industrial activity.

The context

The digital transformation at the service of industry 4.0 requires manufacturers to have a true 360° vision of their activity. In particular, data on production quality, machine utilisation rates, downtimes and maintenance frequencies. Collecting information in real time therefore implies a permanent connection between the IT and OT information systems.

Ensuring this IT/OT interconnection is the primary concern of a major French manufacturer in the aeronautics field. Initially, the company wanted to interconnect three plants in France, each with more than a hundred pieces of equipment. Of course, they also wanted to take into account the security aspect to avoid the increasingly varied and sophisticated cyber-attacks that manufacturers are encountering and their consequences: infection by malicious software, taking control of a machine, theft of critical data, economic espionage, etc.

This industrial group also wanted to guarantee access to technical (company directories, time servers, DNS servers, etc.) and operational (administration, backup and remote maintenance) facilities for employees working in the plants.

The chosen solution

To secure its information systems, the customer chose the Stormshield Network Security solution and set up a cluster of SN2100s on each of the three sites to protect all the entry points and interconnections between the different networks.

Thanks to its unrivalled modularity, this next-generation firewall optimises the segmentation and separation of the OT networks of each site from the rest of the information system, where all the industrial data related to operations are uploaded and centralised.

Specifically designed to protect programmable logic controllers (PLCs), a dozen Stormshield SNi40 firewalls were also deployed to closely secure each piece of equipment.

These boxes also allow IP address plans to be standardised via Network Address Translation (NAT), in particular for the so-called "approved" machine islands supplied by external equipment manufacturers which have their own IP addresses which cannot be modified to maintain the manufacturer's warranty. SNi40 firewalls can translate the equipment address at the Internet connection gateway between the internal address of the machine and the IP address of the gateway, which allows a PLC to be seamlessly integrated into the client's addressing scheme.

By deploying Stormshield equipment, the customer was also able to improve the visibility of its industrial information system thanks to the "Intrusion Detection System" (IDS) mechanism, which can detect malicious traffic and raise an alarm.

In addition, choosing Stormshield was motivated by several other determining factors:

- application plug-in technology for maximum protection against known threats and zero-day attacks,
- protocol inspection capabilities to harden industrial protocols to avoid attacks and human error,
- a small equipment footprint on latency in the industrial network,
- easy installation thanks to a simple configuration procedure,
- a single software for a one-step administration process, regardless of the protection domain (OT or IT).

The customer is now fully satisfied by the interconnection of these IT and OT networks, which allows them to fully exploit all industrial data and thus improve its efficiency, while providing a better service offer to operational staff.

Watch this

This major industrial group continues to place its trust in Stormshield, recognised for its experience and knowledge of the constraints and challenges specific to industrial environments, to equip all its European sites in the coming months and, in the longer term, all of its sites worldwide.

Integrating new protocol plug-ins is also planned and is currently being studied by Stormshield R&D to meet future operational needs.

STORMSHIELD

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider. To find out more: **www.stormshield.com**