STORMSHIELD

BUSINESS CASE

A large-scale industrial project for a secure architecture and well-protected business processes

AGRO-INDUSTRY

In 2017, the WannaCry ransomware affected more than 200,000 computers, exploiting a flaw caused by failures to apply Windows security updates. This caused panic in many of the industrial infrastructures affected, across more than 100 countries.

It also resulted in a growing awareness in the industrial world of the obsolescence of their infrastructures and operating systems, particularly for critical and sensitive infrastructures.

One of these industries, a major French agricultural industry player, decided to implement a plan to secure more than 40 production sites around the world. To this end, its management enlisted the help of all its Operational Technology (OT) teams.

This extraordinarily ambitious project began in 2017, and is expected to take 10 years to complete. It covers two major aspects, the first of which is a complete revamp of the entire network infrastructure. More specifically, it involves modifying or replacing obsolete equipment to modernise it and incorporate the administration layer essential for protecting the industrial network. This is followed by the implementation of all the safety functions across every production line.

Given the scale of the project, an industrial team with network administration skills was specially formed. The aim was to involve high-performance professionals with both expertise in the company's business processes and cyber skills. Naturally, this team worked very closely with the local teams at each site to ensure that the project ran smoothly and that all employees were on board.

"This international group has implemented a truly high-performance architecture and ensured an optimum level of protection for all its processes worldwide. This is a large-scale project that greatly reduces the risk of failure and ensures business continuity in the event of an attempted compromise."

Vincent Nicaise
Industry Team Leader at Stormshield

Efficient administration of industrial systems, in line with best practice

To reinforce the level of protection, the customer wanted the technologies used on the operational network to be from a different publisher to those used on the IT network. As a result, the teams chose solutions from Stormshield, a company strongly committed to the cybersecurity of industrial systems: its solutions incorporate most industrial protocols, and are ANSSI-qualified and IEC62443-1 certified.

The teams chose solutions from Stormshield, a company strongly committed to the cybersecurity of industrial systems: its solutions incorporate most industrial protocols, and are ANSSI-qualified and IEC62443-1 certified.

A double barrier of clusters, i.e. four Stormshield firewalls, were installed at each of the production sites

The first cluster provided secure communications from the outside, while the second ensured secure communications within the industrial network.

A double barrier of clusters, i.e. four Stormshield firewalls, were installed at each of the production sites. The first cluster provided secure communications from the outside, while the second ensured secure communications within the industrial network.

Then, in order to segment and secure the different activity zones, several hundred VLANs per site were implemented. With more than 30 sites involved, in order to save time and set up a clear and identical infrastructure across all production plants, the teams created a secure architecture model upstream, which was deployed in an identical way across all sites.

With the same objective of following best practice, the “IT for OT” networks – including all server and PC-type equipment – were segmented, as were all the lower layers of the industrial processes, including all the PLCs on the production lines.
For this task of securing the lower layers, certain critical systems required the implementation of a process for analysing industrial protocols, such as the Modbus protocol, in order to ensure that the command instructions sent to the production lines are not maliciously altered, which could completely compromise the processes.

SNi20 firewalls were installed to analyse the instructions or variables sent and prevent any unauthorised commands. In particular, the SNi20 model enables in-depth packet inspection, via contextual packet analysis (Stateful DPI) in operational network traffic. This avoids modifications to data flows, particularly control orders, and guarantees a high level of protection for industrial communication protocols. Logs of unauthorised commands are automatically sent by the firewall to the company’s SIEM for in-depth analysis.

SOLUTION USED

→ SN-M-Series

→ SNi20

In addition, SNi20 enclosures are able to withstand the specific conditions of operating environments and can be adapted to DIN-rail, for deployment in close proximity to the PLCs themselves.

Thanks to their high-availability system and their “bypass” mode for operational security on the networks, all the deployed firewalls guarantee operational security for optimum business continuity at all times – even in the event of failure.

Streamlined deployment and maintenance processes

During the project implementation phases, the in-house teams also used the Stormshield Management Center centralised security management solution.

This solution provided operational simplicity, cut deployment times by limiting repetitive tasks through the automated implementation of security and filtering policies, and also limited the risk of configuration errors.

The platform enables very fine-grained rules management, offering the option of pushing both global rules for the centralised architecture and specific local rules tailored to the various business lines and production plants.
It continues to be used by teams on a daily basis for maintenance operations, freeing up more time for higher added-value safety operations.