



SALINS THWARTS TWO TARGETED ATTACKS THANKS TO F-SECURE'S SERVICE

"To ensure its compliance with the French Data Protection Authority and to protect itself from zero day attacks, the Salins Group's La Baleine salt deployed sensors from F-Secure across its European sites."

Eugène Botella, Head of IT Security

Company name:
Salins Group

Industry:
Salt production

Country:
France

Solutions from F-Secure:
Rapid Detection and Response Service, F-Secure Radar



The Salins Group is one of the main European salt producers and the only one to dedicate itself exclusively to the production and marketing of salt. With 4 million metric tonnes of salt produced every year, it covers all possible applications: human food, agriculture, chemistry, de-icing, water treatment, and other industrial processes. For 150 years, the historic business in Aigues Morte has expanded internationally with an industrial presence in Spain and Italy. Among the brands of Salins Group are: Le saunier de Camargue, La Baleine, Salins Agriculture, Rock, Marine Salt etc. The Salins Group has 1,500 employees and a turnover of 300 million euros.

MAN & MACHINE

In 2018, against a background of GDPR compliance, Eugène Botella, Head of IT Security, Data Protection Office (DPO), and Head of Internal Control, expressed doubts over the ability of the Salins Group to detect zero day type of attacks. Therefore, he started researching a detection and response solution.

The Salins Group has been a client of F-Secure for over 20 years. After installing the F-Secure Radar vulnerability scanner in 2017, Eugène Botella accepted F-Secure's proposal to conduct a proof-of-concept to

test the F-Secure's managed detection and response service across several workstations.

"Of course, we considered other solutions, but what attracted us was that, in addition to the standard tools, F-Secure had its own sensors and its Service Operations Center (SOC); the security events, initially sorted and enriched by the algorithms, were seen by experts, which ensures highly detailed analysis of threats. Notably, the competition uses algorithms with no human analysis," clarifies Eugène Botella.

RAPID, DISCREET, AND LIGHTWEIGHT

The F-Secure team supported the group on the ground in defining the method of deployment that best suited the industrial environment and group's multi-site context.

"Deployment was very fast via the Active Directory: as soon as the user authenticated it, the agent was installed immediately. It is rapid, discreet, and lightweight to deploy," explains Eugène Botella.

The license was subsequently opened to all administrative and industrial sites in France, Italy, and Spain, totaling around 550 workstation and around one hundred servers. In case of growth, the Salins Group plans on expanding the deployment of the service to its new subsidiaries.

A VERY LOW RATE OF FALSE POSITIVES

When F-Secure sends an alert, the group's security team, consisting of some twenty people, confirms whether or not it is a real attack by changing the detection status on the platform.

In case of proven attack, the forensic and response teams collaborate with the security team to help them contain the threat. The information can be used as evidence in criminal investigations or sent to the French Data Protection Authority.

"With regards the support element, the platform service is in English but our contact at F-Secure France acts as an intermediary where necessary," adds Eugène Botella.

Operational since October 2018, the service has already issued 30 alerts, including 27 genuine threats, representing a false positive rate of just 10%.

TWO TARGETED ATTACKS CONTAINED

"Recently, our Italian operation was the subject of a targeted attack. We were able to reinforce our devices and warn employees to be vigilant. The phishing messages contained malicious files and were highly personalized with customer names, an order form matching our management software, with the names of genuine products. It is this type of situation which is not easy to intercept: we would not have been able to spot it without F-Secure," said Eugène Botella.

In total, two targeted attacks have been thwarted: their highly developed obfuscation techniques allowed them to bypass the other security solutions that were in place. The first attack was intended to paralyze some systems, while the second was intended to steal critical data about the business.

"Recently, our Italian operation was the subject of a targeted attack. We were able to reinforce our devices and warn employees to be vigilant. "

Eugène Botella

"The first results were very satisfactory, but it was also very concerning. We had the feeling that some attacks might have passed through the grid of our anti-virus solution: this enabled us to see that our intuition was accurate. Now, we know and we can respond rapidly," concludes Eugène Botella.

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

