Reveelium INC

Case study:
AGRIBUSINESS
REVEELIUM

The implementation of an expert behavior analysis & APT-combat system in the case of an organic food manufacturer

"The growing use of the internet within enterprises has significantly raised risk levels where IT security is concerned. Without crossing the line into insanity, instating a global security policy, meant to reduce these very same risks, is absolutely necessary", the IT Director explains.

FOOD INDUSTRY LEADER

Today, this dietetic and organic food industry giant, leader in France and in Europe, employs over 1500 collaborators. Consequently, it attempted to equip itself with the means to secure its data, wanting to protect the know-how and the competences that help maintain its position as a global leader.

ISSUE

High-tech industries nowadays are facing substantial needs concerning the security of their information system:

+ Protect their knowledge and their R&D.
+ Guarantee the confidentiality of exchanged data: DMS, inbox, shared platforms with constraints (extended enterprise).
+ Guarantee production chain availability.
+ Guarantee the confidentiality of commercial proposals and negotiations.

In an environment so highly restrained, they must protect their knowledge and trade secrets in order to maintain their technological advance, to ensure production cycles keep running and to turn their investments into profit.

In tackling these stakes, the enterprise was looking for ways of protecting itself against APTs (Advanced Persistent Threats) and data extraction.

SOLUTIONS

At the end of the "Security Club" quarterly meeting, the IT Director was seduced by ITrust's pragmatically-constructed speech and entrusted us, in a first stage, with auditing the company's information system. Successive audits conducted since then led to the discovery of security vulnerabilities, even though the company was protected by an antivirus and firewalls. These weaknesses were quickly resolved thanks to the reports ITrust provided, reports that detailed and prioritized recommended countermeasures.

Satisfied by these audits, the IT Director expressed his wish to deploy on the entire network the continuous vulnerability management presented by ITrust – the IKare solution. Strongly aware of the importance of data security, the Director realized that the systems he had at his disposal were not enough to fight against unknown threats (APT).

Nevertheless, these unknown threats leave traces, but that are difficult to detect with the current technology, which generates too much noise and false positives. SIEM tools collect data, but cannot push unknown threat alerts forward. This is why the company has opted this year for an expert system, capable of detecting in real-time viruses, unknown attacks, APTs...

Reveelium was quickly integrated within the company's SOC (Security Centre). It processes security assets' logs, Windows domains, DNS and proxy servers, as well as applications. It can detect weak signals predicting the existence of APTs by identifying behavioral abnormalities within the supervised system and enriching and filtering information to produce qualified and prioritized alerts.

Reveelium is a next generation security solution. Its performance and adaptability to so many "use cases" in various and diverse businesses arises from the combination of three complementary technologies. 1 / the weak signal scanner, which is the result of advanced research in statistical algorithms and artificial intelligence. Its findings are enriched by a 2 / logical correlator that integrates business rules and detectors extracted from the expertise of ITrust's engineers and security consultants. The system then uses an 3 / overall knowledge base, Reveelium's memory, which collects information from various Reveelium bodies, enabling each customer to benefit from each other's experience.

RESULTS

Deploying Reveelium enabled the enterprise to:
- Detect an APT that had been present within its IS for several weeks or that had never been detected before.
- Reduce the time dedicated to the detection of unknown threats to a few days (instead of several months).
- Reduce significantly the number of false positives and, thus, reduce 50-fold the supervision time.

www.reveelium.com/en

Join us on LinkedIn

Reveelium Inc.

Headquarters
4200 Regent Street, Suite 200
Columbus, OH 43219, USA

Telephone
+1-614-944-5771

Mail
sales@reveelium.com