exabeam®

CASE STUDY

SUPERCHARGING THE SOC TO HELP SITECH BETTER PROTECT ITS IT LANDSCAPE

EFFICIENCY PAIRED WITH VALUABLE INSIGHTS AND INSIDER THREAT CAPABILITIES. Sitech Services is a technology partner for the process industry and supports a large number of factories at the Chemelot site in Geleen, the Netherlands, by keeping chemical processes operational. A secure IT infrastructure is crucial for this. Thanks to Ilionx's Exabeam-powered Security Operations Center (SOC), Sitech can count on 24/7 protection of the IT landscape as well as proactive and timely detection of cyber threats.

ARMED AGAINST THE LATEST FORMS OF CYBERCRIME

Industry 4.0 has increasingly integrated IT and operational technology (OT) within factories. Technologies such as cloud computing IoT and AI are revolutionizing production methods, for example, by better utilizing data or smart machines.

"Projects and major maintenance are very tightly scheduled. When our systems go down, it affects the schedule. If downtime takes too long, people within Sitech cannot perform the scheduled maintenance. That's not really a viable option because it could cause the factories to run less optimally. That is why we do everything we can to prevent this. Thanks to Ilionx's Exabeam-powered SOC, we know that we can respond super-fast to a potential threat, preventing downtime as much as possible. And that is exactly what we need."

MARTIN REUMERS, IT SECURITY OFFICER AT SITECH.

INDUSTRY

Technology/Manufacturing

EXABEAM PRODUCTS

Advanced Analytics

Data Lake

Incident Responder

Cloud Connectors

Good monitoring and detection of internal and external threats is crucial for Sitech, especially since cyber attacks are becoming more advanced and the growing prevalence of insider threats. In Ilionx – a key European channel partner of Exabeam – Sitech has found an innovative partner for monitoring their entire IT landscape.

"With Exabeam, Ilionx deploys a detection method that uses the latest technologies. That is exactly what we look for in a security partner, so that we are armed against the latest forms of cybercrime," says Martin Reumers, IT Security Officer at Sitech.

PREVENT DOWNTIME

"The availability of our IT systems is very important for efficient and optimal production in the factories," explains Martin. "Projects and major maintenance are very tightly scheduled. When our systems go down, it affects the schedule. If downtime takes too long, people within Sitech cannot perform the scheduled maintenance. That's not really a viable option because it could cause the factories to run less optimally. That is why we do everything we can to prevent this. Thanks to Ilionx's Exabeam-powered SOC, we know that we can respond super-fast to a potential threat, preventing downtime as much as possible. And that is exactly what we need."

SELF-LEARNING SOLUTION WITH BEHAVIORAL MODELS

In order to deploy the latest technologies within the SOC, Ilionx works with Exabeam to detect threats based on user behavior models rather than rules. With the help of data science, deviations rapidly become apparent.

"Speed is what it's all about when limiting the impact of a security incident. That is why we automate as much as possible, such as the response to an incident (SOAR) and the investigation that precedes it. This allows the security experts in the SOC to detect and respond proactively, which minimizes an incident's impact for Sitech," says Joost Wanders, Benelux Channel Partner Manager.

UP AND RUNNING WITHIN THREE WEEKS

Leveraging Exabeam's Cloud Platform, Martin's team was able to take advantage of greater automation and subsequent speed of rollout to get their environment set up.

"The implementation of the solution went very quickly. This was because it is hosted in the cloud and because there is a high degree of automation. Of course, the solution took time to map out and analyze patterns, but we were fully up and running within three weeks," says martin, adding that " the security expertise at Exabeam and Ilionx and the excellent cooperation certainly contributed to this. The people have an open way of communicating, so we knew exactly where we stood. This means that we look forward to further cooperation. I am confident that with Ilionx and Exabeam at our side, we will be able to respond quickly to incidents and improve our security landscape even further."

KEY BENEFITS

- Reduced Downtime
- Faster Investigations
- Better Visibility
- Stronger Insider Threat Program

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.