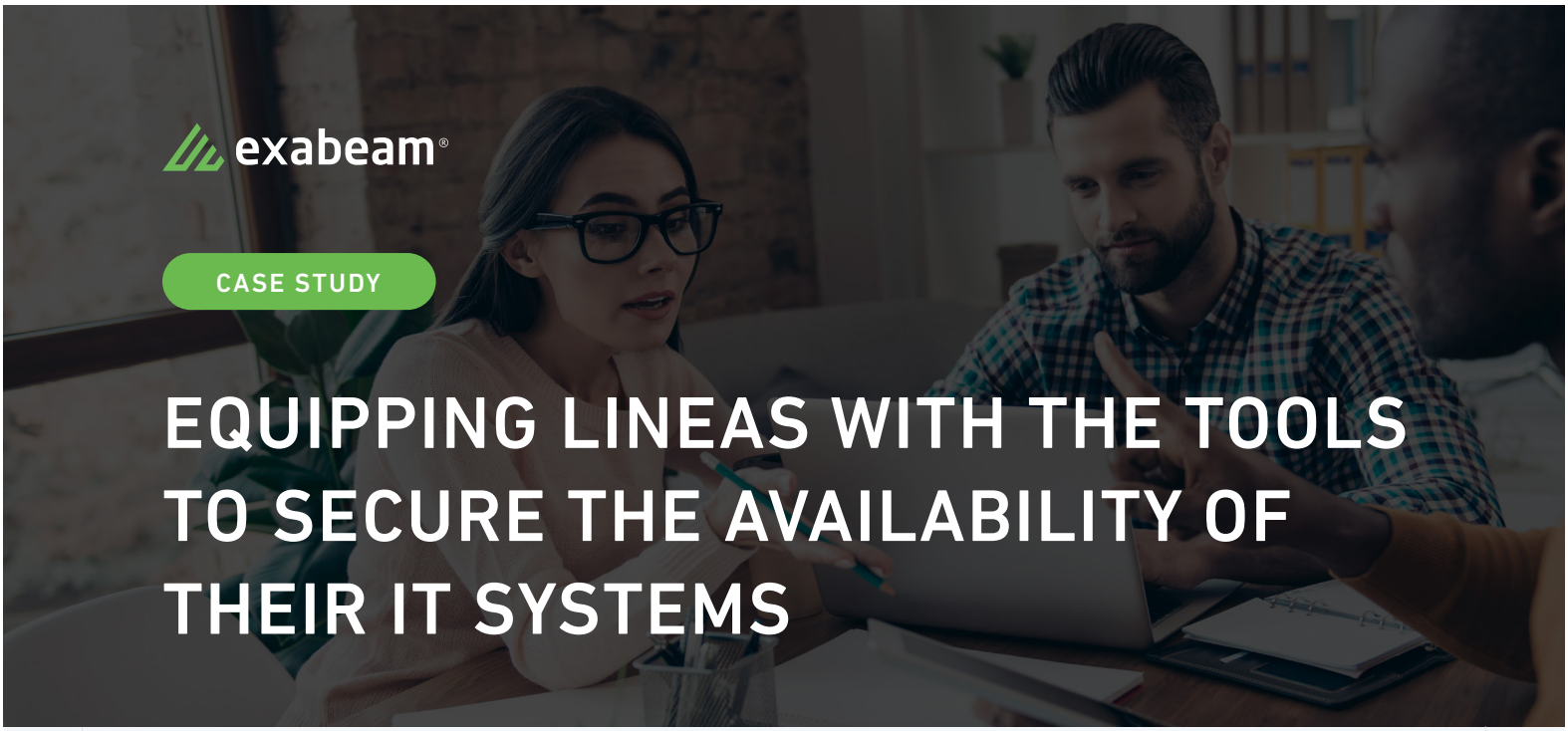

exabeam®

CASE STUDY

EQUIPPING LINEAS WITH THE TOOLS TO SECURE THE AVAILABILITY OF THEIR IT SYSTEMS

PROTECTING THE SYSTEMS BUILT TO MAKE SURE EUROPE'S LARGEST PRIVATE RAIL FREIGHT FLEET STAYS ON TRACK.

Headquartered in Brussels, Lineas is the largest private rail freight operator in Europe offering premium rail products and total door-to-door logistics solutions across the continent.

MOVING TARGETS

Vital infrastructure is a prime target for bad actors, with attacks on Israeli water facilities and critical infrastructure in Australia just some examples. This holds true for the railway transportation industry as well, and Lineas is well aware of the threats out there.

That said, there is one key difference in this industry; with a fleet of locomotives constantly on the move and dispersed across the continent, the team at Lineas had to have a security solution that would guarantee round the clock availability of IT systems to make sure that the backbone of the business remained safe, and arrived on time.

> "The alerts we're seeing are not coming out of there because it's defined use cases, but rather from the behavioral aspects, this is something that we wouldn't catch with traditional solutions."
>
> CHRISTOPHE ROME, CHIEF INFORMATION SECURITY OFFICER, LINEAS

"We own a lot of locomotives, and trains, and our core business relies on the fact that these trains keep on running, period. If for some reason they stop, we lose business and rather quickly. So anything impacting the availability of our IT systems has a direct impact on our revenue," says Christophe.

INDUSTRY

Transportation

A BIRD'S-EYE VIEW OF THE ENVIRONMENT

Straight off the bat, Christophe knew that whatever security solution they chose had to be able to bolster their capabilities, with a small team of security experts in-house. He also knew that, with a very young security program, much of the heavy lifting would have to come from whichever tool they went with.

"The number one priority was making sure that our applications would keep on running. So you need to keep your network running and free of compromise," says Christophe, adding that at the time, there wasn't much in the way of threat detection and response.

Visibility then was another major deciding factor, with user entity and behavior analytics (UEBA) at its core so that whoever was using it would be able to to focus on behavior and not simply rely on logs and established use cases. Additionally, building a security program almost from scratch meant that Lineas needed functionality at a reasonable cost, with a small team.

WHY EXABEAM?

Lineas ultimately decided on Exabeam, with an eye on capability vs SOC team size, the cost benefit in relation to what Christophe can achieve and the visibility they're able to get into how people are interacting with their environment.

With these tools, Christophe is able to look at how people operate inside of their environment, establish a baseline of what is normal behavior, in order to quickly identify and respond to threats accurately.

"The alerts we're seeing are not coming out of there because it's defined use cases, but rather from the behavioral aspects, this is something that we wouldn't catch with traditional solutions," says Christophe.

PUNCHING ABOVE THEIR WEIGHT

UEBA is an integral element in Lineas' toolkit, helping Christophe maintain a robust posture without bloating his security team. He was able to bring people on board who didn't have to spend their time sifting through volumes of logs, but rather focus on genuine insights with valuable outcomes.

"What makes Exabeam valuable for us is the fact that you can add a multitude of logs and get real insights, which is a big time-saver for us because the output that we get is really tangible, there are almost no false positives after going through the learning periods," says Christophe, adding that from an inventory and an analysis perspective, "it just takes all the burden away. So, I mean, it's a lifesaver, right? It's not even a time-saver. I mean, how can you do this with a small team? It's not going to work."

KEY BENEFITS

- Cost savings
- Time savings
- Visibility across the environment
- Powerful insights with a small team

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.