TACKLING THE INSIDER THREAT

Pharmaceutical enterprise Allergan is proactively protecting its data with a security solution from Exabeam. The company has implemented Exabeam’s User and Entity Behaviour Analytics solution to uncover potential threat indicators before they happen, providing a mitigation to data exfiltration and insider theft.
Pharmaceutical company Allergan is proactively protecting its data with a security solution from Exabeam. The company has implemented Exabeam's User and Entity Behaviour Analytics (UEBA) solution to uncover potential threat indicators before they happen, providing a mitigation to data exfiltration and insider theft.

TACKLING THE INSIDER THREAT

THE CHALLENGE

Allergan is a multinational leader in the pharmaceutical industry with operations in more than 100 countries.

Michael Towers, CISO at Allergan, said that there are two unique threats to the industry. "Number one is intellectual property protection that goes into our medicines, our biologics and our new treatments," he said.

"The second is reputational risk for the company; making sure that people trust what we're doing for health management and the overall experience of dealing with our company and our brands."

Allergan operates in an ever-changing environment, which requires ongoing protection from complex threats like malicious insiders and compromised accounts. Towers said that the threat comes from insiders either "taking the data themselves or somehow their accounts being compromised and data exfiltrated." Towers explained how over the last few years, the range of transactions Allergan has undertaken presented an increased risk.

"We've done 50 transactions, some of them acquisitions, some of them buying brands or products, some of them domestic," he said.

"They all carry with them a little bit of uncertainty or angst with the employees and the contingent workers that we have. It makes Allergan more susceptible to the insider threat risk generally."

Allergan looked to Exabeam to fill a specific gap in its analytics programme. Towers said that previously, the company's analytics programme comprised mostly of traditional security information and event
Our gap was proactive risk analytics; being able to look for indicators of compromised or potential issues before they happen.

management (SIEM) software, as well as "environmental indicators and stuff that goes on in the media or social media."

Towers added: "Our gap was proactive risk analytics; being able to look for indicators of compromised or potential issues before they happen, whether that's behavioural or based on access patterns. We thought Exabeam was the best fit for that gap."

THE SOLUTION

Allergan implemented Exabeam's User and Entity Behaviour Analytics (UEBA) solution to proactively protect itself from insider threats by ingesting security data from its myriad of security solutions and holistically analysing that data to baseline normal behaviour for its operations.

The key to effective security is to take a user-centric approach, understanding each and every user's normal or baseline behaviour. This allows businesses to answer some of the key questions that cannot be resolved by network monitoring tools alone. These include: Who is accessing the network? What are they accessing? Is the person displaying normal user behaviour?

Once implemented, Exabeam was able to proactively detect any deviation from normal use or machine activity that might indicate a potential security event was emerging.

Towers said: "Exabeam looks at behavioural patterns, access patterns; basically how an individual works with the environment. The analytics allow us to build some sort of picture of normality for the users, both collectively and individually. Then, if we see anything that puts us in a higher risk scenario we look into it more deeply to find any potential compromises before they happen."

Machine learning techniques can discover important connections between seemingly unrelated parts of identities, creating a detailed map of a user's activity, even if various identity components are not explicitly linked. Machine learning algorithms analyse
Allergan requires ongoing protection from complex threats like malicious insiders and compromised accounts.

Trends and create behaviour baselines which provide the much-needed context required to spot and flag any activity that deviates too far from what is considered acceptable or normal. Constantly learning and self-improving, these algorithms help Allergan stay one step ahead of its evolving threat landscape.

**THE RESULT**

Through the use of Exabeam advanced analytics, Allergan can easily and proactively detect insider threats and compromised credentials before they develop into security breaches or loss of intellectual property.

Towers described one specific example that underscores the value Exabeam’s solution is delivering.

"We had a handful of users that we know based on the analytics, and behavioral and access patterns, were behaving differently than they had in the past."

"We knew these users weren’t likely to steal data or to do anything nefarious intentionally, so our theory was their credentials had been compromised. Based on the access patterns, we investigated and found out what actually had happened and there was an attempt to steal some data. We were able to stop this before it happened."

Exabeam’s behavior-based approach to threat detection delivered value for Allergan out of the box, without the need for extensive customization or lengthy professional services engagements. Towers said: "One of the things we liked about Exabeam frankly was that it was by far the quickest to deploy any of the technologies that we looked at. We were able to see value in it, and evidence that it was actually doing its analytics — and giving us potential alerts — within a few days."

After seeing how its solution works in practice for Allergan, Towers identified three primary benefits and value propositions Exabeam is delivering:

"Number one, it’s proactive. We had really good capability to respond to incidents after they happened; Exabeam now allows us to look at potential indicators before they happen."

"Number two, it provides a mitigation to two of our most challenging risks: data exfiltration and insider theft."

"It does so without a lot of tweaking, configuration or consulting time. You plug it into the network and it works."

**TWO PIECES OF ADVICE**

Following Allergan’s experience with Exabeam, Towers offered two pieces of advice for other CISOs looking to mitigate the risk of insider theft:

"The first is to work with a partner that can plug into your network, adding value from the start and allowing you to convince your stakeholders that you’re mitigating this risk very, very quickly."

"The other piece of advice I would give is to try not to configure every possible scenario. Don’t overcomplicate it. Let the technology do its work and even if you only get 80% to 80% of the value that you were originally intending, it’s better than nothing and will be a really strong indicator to your stakeholders."

Towers concluded with the critical importance of a proactive solution that pre-empts potential issues. He said:

"There are plenty of options out there in the security world if you’re looking for technologies to help you respond to incidents quicker. But there are only a few I think – and Exabeam being the best – that will help you look for things and incidents before they happen."