exabeam

Case Study

Improving Threat Detection, Investigation and Response

How SA Power Networks teamed with Exabeam for faster, analytics-driven cybersecurity results

SA Power Networks is the sole electricity distributor for the state of South Australia, supplying electricity to about 1.7 million South Australians. Like many of today's organizations, their threat detection and response capabilities weren't meeting expectations, and the small but mighty cyber security team was challenged to keep up with numerous responsibilities, including preventive controls, patch management, and detect/respond functions.

SA Power Networks wanted to boost its threat detection, investigation and response (TDIR) capabilities with advanced technology capable of expediting processes, reducing manual workload, and aligning security with the company's business goals.

After weighing their options, they chose to implement Exabeam's TDIR analytics software solution in January 2021. Over more than a year later, SA Power Network's partnership with Exabeam has delivered the anticipated value: streamlining and accelerating the company's TDIR function, strengthening security team bonds and collaboration, and cementing the critical link between security and business initiatives.

Challenges along the way

In May 2020, the cyber security operations team at SA Power Networks realised their in-house threat management technology needed an uplift. While aligning security posture and business objectives, they were looking to replace their existing Security Information and Event Management (SIEM) product with a technology solution that complemented their current capability without introducing a single risk point.

The small team shouldered many duties and, like far too many security teams today, was struggling to monitor an overwhelming volume of alerts. Major incidents took up extensive time and sometimes resulted in unidentified root causes. Response times lagged due to the need to monitor multiple interfaces. On top of this, the team was preparing for the looming compliance requirements of the soon-to-be legislated Australian Energy Sector Cyber Security Framework (AESCSF).

Previously, SA Power Networks had outsourced threat detection and response duties to a managed security service provider, who did not meet expectations. They didn't receive the anticipated service value and risk mitigation, and business correlation stumbled. The team now faced a critical choice –– try another managed service provider or invest in developing an in-house detection and response skillset. For SA Power Networks, the choice was easy, and in January 2021, they began a direct partnership with Exabeam, sparking a critical shift in their threat management strategy.

Analytic solutions

Right out of the gate, Exabeam's easily integrated, cloud stack-based solution, with its ability to quickly index and search data, provided a proactive, structured approach, driven by the unique capabilities of analytics. No more time-intensive searching for alerts –– with Exabeam's Smart Timeline feature, necessary event details were presented in a structured, linear, easily-consumable format. The team immediately noticed the convenience of checking a Smart Timeline whenever an incident occurred.

With Exabeam Fusion SIEM on the job, the team no longer felt overwhelmed by alert volume. Exabeam's solution provided a structured format of standardisation, eliminating multiple interfaces. Watch lists could now be broken down to specific areas so teams could easily and quickly prioritise response actions.

Analytics helped the SA Power Networks team even the playing field –– expediently detecting and identifying more alerts for faster response times and a superior level of security.

Checking all the boxes

SA Power Networks validated the value of the partnership by conducting a series of fully simulated penetration tests to confirm the effectiveness of Exabeam's threat management technology. This confirmed the significant boost in threat detection and response capability, saving valuable time and resources while enjoying the peace of mind delivered by superior network protection. Numerous use cases were now caught that would have slipped by in the past, and significant business risks, like data breach system unavailability and reputational damage, were avoided.

"We've enjoyed some profound, systemic benefits using Exabeam Fusion SIEM," said Lindbergh Caldeira, Cyber Security Operations Manager, SA Power Networks.

"We've strengthened our processes with workflows that have helped our team become far more effective as a result of the Exabeam partnership. Our team members can now ask the critical questions connecting security to business function."

Thanks to Exabeam, SA Power Networks has received a needed technology uplift with a TDIR function, gaining speed and efficiency all while positioning the company for a secure future as South Australia's regulated electricity distributor.

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. The leader in Next-Gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR), from common security threats to the most critical that are difficult to identify. Exabeam offers a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. We design and build products to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and best protect their organizations.

For more information, visit exabeam.com.

exabeam™