How the Exabeam SOC Utilizes Exabeam to Set the Security Standard

About The Exabeam SOC

As a global cybersecurity leader, Exabeam not only provides industry-proven security solutions to its customers but also rigorously applies them in its own internal Security Operations Center (SOC). The Exabeam SOC is responsible for protecting the company's corporate environment, customer data, and infrastructure from the ever-evolving threat landscape. With a mission to lead by example, the Exabeam SOC leverages the Exabeam New-Scale Security Operations Platform to provide complete visibility and automated threat detection, investigation, and response (TDIR).

The Challenge

For a leading cybersecurity vendor like Exabeam, internal security is not just a best practice — it is the foundation of customer trust. The company is acutely focused on protection against adversaries seeking to compromise its platform and, by extension, its customers. Because the New-Scale Platform integrates deeply into customer environments, a breach of Exabeam systems could create a "superhighway for threat actors" into its clients' networks. This high-stakes environment means that defending against sophisticated threats is paramount.

> "A focus on security for a company like Exabeam is key and critical. My main concern as a CISO is those individuals that are inside the company...If you look at the statistics, you'll see that more than 70% of attacks come from an insider."
>
> — Kevin Kirkwood
>
> Chief Information Security Officer (CISO) at Exabeam

The members of the Exabeam SOC team also bring a wealth of experience from previous roles, including a deep understanding of the frustrations common to legacy SIEMs. In their past positions at other companies, they were confronted with overwhelming alert volume, the time-consuming manual effort required to correlate events, and the steep learning curves of complex query languages. This environment created a high risk of analyst burnout and the potential for critical threats to be missed.

The Solution

This collective past experience gives the team a unique appreciation for the Exabeam New-Scale Security Operations Platform, which stands in stark contrast to the tools they used previously. A key differentiator was the platform's rapid time-to-value.

> "With other platforms, it would have taken us months to get from bare bones out-of-the-box to a completely efficient, tuned platform. With the Exabeam New-Scale Security Operations Platform, it's days."
>
> — Saul Ibarra
>
> Senior Security Operations Analyst at Exabeam

The platform's core technical capabilities driving this transformation include:

- **Exabeam Nova:** Exabeam Nova is the multi-agent AI infrastructure built into the foundation of the New-Scale Platform, which includes the Analyst Assistant agent. The Exabeam Nova Analyst Assistant Agent fundamentally changes the investigation process — instead of the complex, proprietary query languages analysts had to master in past roles, they can now ask Exabeam Nova questions in plain language. The Analyst Assistant Agent then automates the process of gathering context, correlating logs, and building a threat narrative. Its agentic AI use cases extend to proactive guidance; analysts can ask Exabeam Nova, "How would you investigate this type of alert?" and receive a step-by-step plan that mirrors the actions of a seasoned expert.
- **User and Entity Behavior Analytics (UEBA):** At its core, the platform automatically establishes a baseline of normal behavior for every user and device — and now AI agents — in the environment. It then uses machine learning to detect meaningful deviations. This behavioral approach is crucial for detecting the insider threats and "low and slow" attacks that the team saw bypass traditional, signature-based tools at their previous companies.

The Results

Adopting the New-Scale Platform has yielded measurable benefits for the Exabeam SOC, and also made a profound impact on day-to-day operations for the team's analysts.

The machine learning capabilities embedded within the platform directly combat one of the industry's biggest challenges: burnout. By automating the monotonous task of sifting through endless logs, Exabeam has fostered a more fulfilling work environment.

"With other platforms, the burnout was real, but with the Exabeam New-Scale Security Operations Platform, it's basically non-existent," elaborated Ibarra.

The intuitive, AI-powered workflow provided by Exabeam Nova and the Analyst Assistant Agent also empowers junior analysts to be effective almost immediately. This operational efficiency has strategic implications for staffing: the platform's ease of use broadens the available talent pool, alleviating the pressure of the cybersecurity skills gap.

> "I wish I had had this when I was first starting out as an analyst. It makes everything so much easier. It kind of shows you how to connect the dots...it's a great training tool."
>
> — Gabrielle Hempel
>
> Security Operations Strategist at Exabeam

A Commitment to Continuous Innovation

Exabeam's use of its own product is a collaborative journey, with the SOC team continuously providing feedback to engineering, helping to refine and innovate the platform. The experience of struggling with legacy tools in past careers to building the future of security operations at Exabeam ensures that the platform is battle-tested and aligned with the real-world needs of security professionals.

"My journey here at Exabeam has really changed my perspective on security operations. I've become a lot more confident in my incident response capabilities... I'm able to focus on more advanced processes such as threat hunting because of the flexibility that the platform has to offer," concluded Ibarra.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →