The Missing Link Protects their SOC, and their Clients' SOCs, with Exabeam

50% to 100% reductions in Threat Detection, Investigation and Response (TDIR), SLA response times

The Missing Link, a leading managed security service provider (MSSP), needed a security toolbox update to achieve faster, more consistent Threat Detection, Investigation and Response (TDIR) results for their clients in ASX Top 20, Healthcare, NFP, Global Retail and FSI verticals.

While advanced detection and monitoring was a successful extension of their client's security operations, the MSSP set their own objective of reducing detection and response times to within 50% of their SLA for both themselves and their clients. The team partnered with a leading security solution platform — an industry pioneer who could boost their SIEM solution with the power of automation and user behaviour analytics — to achieve this goal.

After a robust internal Technology Comparison engagement by Nick Forster, the company's SOC Manager, The Missing Link selected Exabeam's security solution platform for the job. Nick identified user behaviour analytics as the key differentiator, stating, "No other technology provides insights and behavioural model customisation like Exabeam. They pioneered User and Entity Behavior Analytics (UEBA)."

The Exabeam platform significantly improved TDIR workflows for these security pros. The platform made it possible for the SOC to achieve their 50% SLA target for detections and response actions with more consistency and standardisation.

The implementation of Exabeam's Advanced Analytics and Incident Responder modules resulted in:

- Automated detection and response,
- Detailed analyst notes with actions; and,
- The provider running a much more efficient and polished service, both internally and for their clients.

Numerous challenges

Even professionals can get left behind by today's advancing technology — especially when it comes to keeping up with a dynamic threat landscape. Security teams face an uphill battle in promptly detecting and responding to potential threats, which is nearly impossible without automation and advanced behavioural analytics.

The Missing Link prides itself on keeping up to date with the latest and greatest technologies for their clients, and Extended Detection & Response (XDR) is no different. Faced with a looming licence expiry, ISO27001 recertification and the migration of multiple compliance reports and dashboards, The Missing Link were able to acquire SaaS licensing, deploy the solution and embed into their business as usual (BAU) operations within a matter of weeks, without delays or making an impact on operations. Overall, they experienced an improvement in detections, response and compliance reporting.

The Missing Link also wanted to improve the compliance component of their SIEM solution and embrace the power of automation-fueled user behaviour analytics to speed detection, investigation and response. The team aspired to the lofty goal of a one-hour SLA for incident response with consistent results.

Additionally, their team was pressed for time — their licence was expiring, and they wanted to transition to a SaaS option that would be easy for their team to learn and implement.

Fast, consistent, and customised solutions

Keep in mind that not just any security solution platform would be sufficient. The Missing Link needed a top-notch security platform which would position them as industry leaders. **Their clients depend on them for reliable and effective security solutions, so whom did they choose as a security partner? Exabeam.**

The Missing Link partnered with Exabeam's industry-leading user behaviour analytics fueled by automation and delivered with a quick, straightforward, prepackaged implementation. A team leader shared some of their decision-making logic: "We really liked the fact it's an emerging technology, a pioneer in the space, and the SIEM industry leader. We want a good understanding of what's normal in our network and, more importantly, to be able to recognise what's abnormal, and then effectively respond to that. Exabeam is extremely good at this, which means you're not burning resource time or, ultimately, money which can be better spent on our defences in other areas."

The Missing Link also sought a solution that was easy to implement and would seamlessly integrate with other vendors. Again, Exabeam had the most relevant and extensive range of out of the box integrations, therefore scoring highly in the comparison. From a partner perspective, Exabeam excelled by providing the client with an application helping their client base access and implement the platform. Simplifying the platform's use further, Exabeam Fusion SIEM easily integrates with more than 400 software vendor technologies, including multiple endpoint detection and response (EDR) vendors as well as the other member technologies in the XDR Alliance.

Possibly the most significant driver behind the decision to partner with Exabeam was the platform's ability to perform intermediate- to advanced-level tuning. This feature allows specialised customization based on the organisations needs, which sealed the deal for the client's team. "Lots of vendors have analytics engines, but you can't play with them, and with Exabeam you can tweak, tune and tinker to get what you need. I can't stress enough how impressive it is to have the ability to get it working correctly right away and create your own customised rules and models."

Results worthy of professionals

From the beginning of the partnership with Exabeam, The Missing Link diligently invested in implementing the technology, focused on core events and use cases, and established a solid path of maturity for the platform. They were well aware of the platform's required commitment, jumped in with both feet, and began to see tangible benefits after 60 days of working with the technology.

The Missing Link's team was pleased to notice a legitimate 100% reduction in detection and response times, both for clients and themselves. A team leader shared his thoughts on this accomplishment: "I don't know how anyone not using Exabeam can possibly meet a one-hour SLA, but with Exabeam's solution platform, it's all there and put together for you, so you can go directly back and find the data. I can credibly say to our clients, we meet your one-hour SLA goal, which also includes our team's analysis and notes."

Another positive result the client enjoyed was an improvement in the consistency of results, driven by the platform's automated workflows. Even if an incident doesn't turn out to be a breach, Exabeam's platform still provides details. For example, the security provider identified an incident where an external party accessed an environment through a known SSL VPN vulnerability. The Exabeam platform was able to detect initial access, reconnaissance and attempted lateral movement activity, before response actions were initiated. Post incident, The Missing Link were able to provide the client with assurances that no further indicators of compromise, or breach were present.

Thanks to the client's partnership with Exabeam, automated tools run processes, analysts add value with metric-driven insights, and this security solution provider is positioned to provide industry-leading protection. A team leader shared their enthusiasm for the future with Exabeam, saying, "I'm really excited about the Exabeam partnership this year and the potential future integrations. Exabeam is the perfect technology to monitor users and gives us the ability to leave no stone unturned."

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now →