

Exabeam SIEM At a Glance

Overview

SIEM Challenges

Of all the products in an organization's security architecture, the SIEM plays a central role in monitoring, alerting, threat detection and compliance. Unfortunately, SIEM cost-effectiveness is low for many organizations — especially as data, exposure points, credential-based attacks, alerts, and cost of people and storage continue to rise.

Market Drivers

Compliance- Many organizations must adhere to one or more compliance regulations. Creating and maintaining compliance reports is both time-consuming and expensive. Whether subject to GDPR, PCI-DSS, HIPAA, NYDFS, NERC, or utilizing a framework such as NIST.

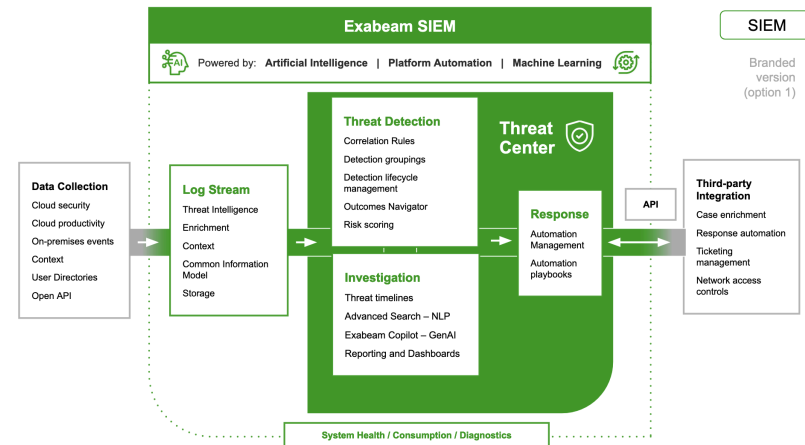
Alert and Case Management- Most organizations receive alerts from multiple security point products such as EDR, IdPs, and DLP. Additionally, a SIEM also produces alerts via correlation. Each product has its monitoring console and notification engine. However, triggered events without context cause more pain to manage than it helps.

The Exabeam Solution

Exabeam SIEM is a scalable cloud-native offering providing advanced capabilities for log management and SIEM. It delivers a limitless scale to ingest, parse, store, search, and report on petabytes of data — from everywhere. Exabeam SIEM includes over 165 pre-packaged correlation rules and a rule builder, allowing analysts to easily create, deploy, and manage environment-specific rules. Integrated threat intelligence improves the fidelity of detections, adding context to rules and allowing some of the most accurate and efficient threat management.

What are the four main benefits/value drivers for Exabeam SIEM?

- Cloud-native, limitless scale- Ingest, parse, store, and search more data – from everywhere — on-premises and cloud; over 2M EPS sustainable per tenant on a platform that scales to hundreds of petabytes.
- Threat Center combines case management with the ability to research threats and events, providing clear summaries of risk.
- Fast, modernized search and visualization — See instant results over petabytes or years of data without reloading or moving data.
- Integrate from anywhere — 650+ integrations with existing tools and over 9,500 log parsers to bring in data from on-premises or cloud



Ideal Customer Profile

Ideal customers will be first-time SIEM, bare-bones functional SIEM vendor replacements, or customers transitioning to cloud offerings. No UEBA- or SOAR-specific needs, mostly questions will arise in discovery on log sources.

Specific Buyer Questions

Economic Buyer (CISO/CIO)

Exabeam SIEM At a Glance

- What are you looking to get out of the SIEM solution? What is lacking in your current SIEM solution?
- How much data do you need to store and maintain?
- How long does it take to search your security data?
- What are your costs to manage alerts from your security stack?

Technical Buyer (Security Analyst)

- What kind of logs do you want to bring into your SIEM?
- What challenges do you have in searching your security data today?
- What data do you wish you had to add context to your alerts?

Other titles that may influence the buying decision:

Security Analyst, Architect, Engineer

Qualify Out Questions

- Do you need analytics/UEBA? (Send to Exabeam Fusion)
- Are you happy with your current log storage costs and just looking for UEBA or analytics/timelines? (Send to Exabeam Security Investigation)

Competitors and Complements - and how we do it better:

Splunk (Not a great feature match, but)

- Requires heavy amounts of manual tuning and config
- Steep learning curve for new Splunk users

Devo

- Limited out-of-the-box detection content for SecOps
- Lacks other next-gen functionality
- Threat hunting and log search are very challenging.

Chronicle

- Static-correlation-based detection with no baselining
- Disjointed alert and case management experience
- Glorified threat hunting platform with no automation

Microsoft

- Limited support and content for non-MS data sources
- Poor automation with many features in “Preview” mode
- Rules engine relies on static-based correlation rules

Objection Handling

Objection 1 - We don't really have the budget / initiative / time for this right now.

Answer 1 - Do you mind me asking if you have a budget that covers the ingest and storage costs? (Keep the conversation alive by pointing out that we may be a cost savings initiative.)

Objection 2 - We don't really have a cloud strategy at present, and data sovereignty is very much a concern.

Answer 1 - When a customer chooses which region for us to deploy their service, the data stays in that region. For example, if the customer is deployed in the US, we do not copy/move/backup that data to any region outside of the US. This is true for the EU and other regions as well.

Objection 3 - We already have a SIEM

Answer 3 - Do you mind me asking if you have a budget that covers expanding ingest and storage costs? (Keep the conversation alive by pointing out that we may be a cost savings initiative.)

Objection 4 - We already have a SIEM and UEBA

Answer 4 - That's fantastic. How are you managing your long-term storage costs? Do you know how long you'll need your logs, and what it will cost every year? Can you selectively save only the logs you need to?

Objection 5 - We outsource our SIEM

Answer 5 - Legacy SIEMs are hard. We work with a lot of MSPs on managing them for you, if you want to keep on with that strategy.