

Exabeam Fusion - At a Glance

Overview

SIEMs play 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

- **TDIR/SOC/Outcomes** - Need a single interface for threat detection, investigation, and response (TDIR) that makes it all “easy”.
- **Compliance** - Many organizations must adhere to one or more compliance regulations for both storage length and visibility into credential use.
- **Automation and Cloud Initiatives** - “Business Transformation” and cost-savings consolidation
- **Customer maturity** - “We want more.” “We’re building an Insider Threat team.”

Exabeam Fusion

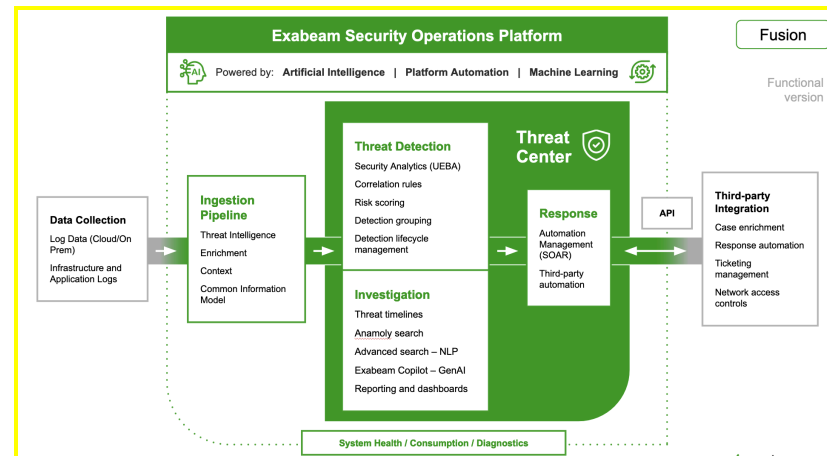
Exabeam Fusion applies AI and automation to security operations workflows for a holistic approach to combating cyberthreats, delivering the most effective TDIR. AI-driven detections pinpoint high-risk threats by learning normal behavior of users and entities and prioritizing threats with context-aware risk scoring. Automated investigations simplify security operations, correlating disparate data to create threat timelines. Playbooks document workflows and standardize activity to accelerate investigation and response. Visualizations map coverage against the most strategic outcomes and frameworks to bridge data and detection gaps. Exabeam empowers security operations teams to achieve faster, more accurate, and more consistent TDIR.

Main benefits/value drivers for Exabeam Fusion

- Cloud-native, limitless scale — Ingest, parse, store, and search more data at 2M+ EPS - Transform data ingestion, transformation, storage, and search speed and economics.

For Internal and Partner use only - NOT customer facing

- Integrate from anywhere- collect from 600+ products, with over 9,500. log parsers to bring data from on-premises or cloud
- Faster investigation - thousands of (total) pre-built queries and anomalies
- Threat Center combines case management with the ability to research threats and events, providing clear summaries of risk
- Improve processes – automate analyst workflows, including response activities



Ideal Customer Profile

- Competitive Takeout: Has Splunk/QRadar etc. – wants better visualization of attacks, more easy/user-friendly
- Growing from UEBA: Looking at diving into the SIEM world from threat detection or UEBA only – wants the best of all worlds.
- Growing from SLM/SIEM: Has log management (commercial or home grown) but needs analytics too.
- Needs options and flexibility – may want extended retention of select logs, etc.

Specific Buyer Questions

Economic Buyer (CISO/CIO)

- Do you feel that your teams have the tools they need to investigate and respond quickly to a breach/new attack/zero-day exploit?

Exabeam Fusion - At a Glance

- How many people monitor your SIEM and handle escalations, and how would you prioritize making them smarter and faster?
- How are you measuring your return on your SIEM investment? MTTR? How can you see your team's scores?
- Are you struggling with the costs of long-term log data storage – and having multiple tools doing the same tasks? (SIEM + UBA + Defender...)

Technical Buyer (*SOC manager, Security Architects, Director of IT/IS, Network Architects, Security Analyst/Engineer*)

- Where do you see the gaps in your SIEM coverage?
- Do you have a problem with prioritization – deciding which events and incidents to review first?
- Walk me through the process of investigation. How do you see what each user did as part of the issue?
- Walk me through the process of response. Do your incident responders know which steps to take to address the different threat types?
- How would you measure success when handling an incident?

Other titles that may influence the buying decision:

Security Consultant, Auditors

Qualify Out Questions

- Just interested in log storage – *position Exabeam SLM*
- "Can't get rid of Splunk/QRadar yet" = *ask what features they are using*
-> *if not a security installation, maybe help them contemplate log sizes, storage, etc.*

Competitors and Complements - and how we do it better:

Securonix

- Securonix focuses solely on abnormal activities
- Limited rule set breadth leaves gaps in detection content
- Non-competitive EPS limitations and data management

Splunk

- Requires heavy amounts of manual tuning and config
- Out-of-the-box content leaves customers with gaps
- Steep learning curve for new Splunk users

For Internal and Partner use only - NOT customer facing

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

IBM QRadar

- Manual, query-driven workflows with little automation
- UBA offerings restricts users to only 17 ML-based models
- Disjointed interface experience with migration issues

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 Have a SIEM "we're all set" / Happy with what they have.

Answer 2 Agree and even congratulate the prospect/ congratulations for taking the steps to secure your business.

- What do you like about your current solution?
- What do you wish your current solution did better?
- Are there any logs your current solution is not collecting?
- Are your costs predictable for the 3rd year of log storage and beyond?