

Exabeam Security Investigation At a Glance

Overview

- Most SIEMs see endpoint or network traffic alerts only - no mapping to identity/users/services.
- Many parts of triage, investigation, and response are manual - especially where they include threats moving between network, cloud, endpoint

Market Drivers

Compromised Credentials - Today's breaches are rooted in compromised credentials. This has forced a shift in security investments from a focus on preventing threats to detecting abnormal behavior.

User and Entity Behavior Analytics (UEBA) - Legacy SIEMs use correlation rules for threat detection, which can lead to notable events (lateral movement) going undetected due to the lack of context about the event.

Security Orchestration and Response Automation (SOAR) - Analysts often lack sufficient expertise to consistently respond to an incident. Different analysts will approach the same incident differently, and junior analysts may lack the experience to know how to begin to tackle a ticket.

The Exabeam Solution

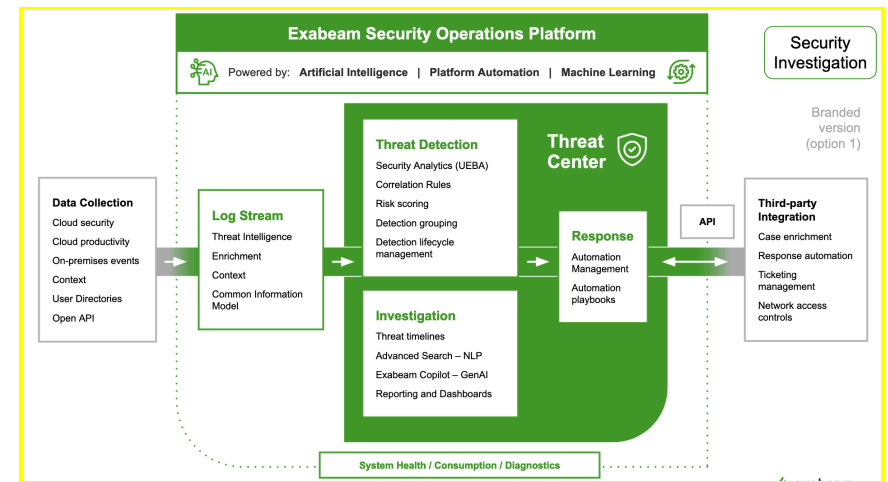
AI-Driven Exabeam Security Investigation can stand alone or run on top of a third-party SIEM or data lake, adding UEBA content, workflows, and automation to provide outcome-focused threat detection, investigation, and response (TDIR) capabilities. To help standardize around TDIR best practices, Exabeam Security Investigation includes prescribed workflows for ransomware, phishing, malware, compromised insiders, and malicious insiders and pre-built content (e.g., MITRE ATT&CK framework) that focus on specific threat types and techniques to achieve more repeatable and successful TDIR.

With Exabeam Security Investigation, analysts are able to run their end-to-end TDIR playbooks to allow security operations to accelerate investigations, reduce response times, and ensure consistent, repeatable results.

For Internal and Partner use only - NOT customer facing

What are the main benefits/value drivers for Exabeam Security Investigation?

- Faster investigation - hundreds of queries automated
- Do more with your existing team - uplevel your level 1 analysts
- Speed investigations and add consistency across shifts
- Improve processes – automate analyst workflows, including escalations/response activities



Ideal Customer Profile

Ideal customers will have a tiered SOC and an existing SIEM or data lake. While the customer may not be ready to replace their existing SIEM or data lake, they want better detection and automation to improve productivity and investigation processes.

Specific Buyer Questions

Economic Buyer (CISO/CIO)

- How many people monitor your SIEM and handle escalations, and how would you prioritize making them smarter and faster?
- If you gave your top two analysts the same alerts - do you think they would both come back with the same results?
- If you gave your top two incident responders the same incident - do you think their investigation and response would be identical?

Exabeam Security Investigation At a Glance

- How are you measuring your return on your SIEM investment? MTTR?
How can you see your team's scores?

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

- 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 for different threat types?

Other titles that may influence the buying decision:

Security Analyst, Engineer, Security Consultant

Qualify Out Questions

- Also interested in log storage – *position Exabeam Fusion*
- Does not like their SIEM and wants to replace it – *position Exabeam Fusion*
- Want visualization, a feature their current SIEM lacks – *position Exabeam Fusion*

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

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

For Internal and Partner use only - NOT customer facing

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 a budget 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.) Can you pick which logs you want your SIEM to save, and for how long?

Objection 2 - We already have a threat detection/UEBA solution.

Answer 2 - Oh? What are you using?

- Can it take every log from badge readers to CASB and public cloud threat detection sources?
- Does it give you a clear timeline of attacks across every source? How fast can you answer questions like, “How many systems/credentials are affected by this problem?”
- Can you automate your responses and integrate with your ITSM systems?
- Can you ask it questions about security and get informed, trusted responses?