Exabeam's Next Gen SIEM/UEBA tool

For further help contact the Exclusive Networks team at Exabeam_UK@exclusive-networks.com

SIEM has the 3rd largest industry budget behind Firewall and Endpoint

The SIEM market is expected to reach $3.7 billion by 2023

68% of attacks go unnoticed for months

THE NEXT GEN SIEM/UEBA TOOL IN A NUTSHELL

The modular Exabeam platform allows analysts to collect unlimited log data, use behavioural analytics to detect attacks and automate incident response with two deployment paths to choose from - augmentation, enhancing current SIEM solutions, and replacement, a swap out of the entire existing platform.

Exabeam differentiate themselves from the competition with:

- A predictable and scalable cost model, price per user as opposed to data ingestion.
- Behaviour based analytics for anomaly detection enables complex use case detection, such as Insider Threat and Compromised Credentials.
- Automatic Host-to-IP user mapping stitches all log data together to give a comprehensive view of user and entity activity.
- Automatically built smart timelines created to increase analyst productivity and reduce time to answer.
- The ability to augment and enhance the capabilities of existing and legacy SIEMs using Exabeam's Advanced Analytics.
- Incident Response automation with Case Management and Playbooks.
- A Modular Platform which allows for a phased SIEM migration.

TARGET MARKET

- Customers with legacy SIEM vendors
- Customers with no SIEM/UEBA
- Customers with over 1000 users
- Customers with busy networks, generating large numbers of logs

THE BUSINESS NEED

What does a SIEM/UEBA tool do?

Everything on a network generates a log whenever it performs an action. A SIEM tool ingests and collates these logs in an organised and presentable way. Analysts can then use this data and Exabeam's UEBA to detect threats and remediate with a lower time to action.

WHY ENTERPRISES NEED EXABEAM'S NEXT GEN SIEM/UEBA TOOL

SAVE MONEY ON LOGGING

IMPROVE THREAT DETECTION

INCREASE ANALYST PRODUCTIVITY

WHO SHOULD YOU BE TALKING TO?

You need to find the people who care about logging costs, analyst productivity and infrastructure efficiency. Go as high as you can because the final decision is made or approved at the executive layer or CISO.

You'll often find that more than one department is involved in the purchase, so nurture your relationship across departments:
Department VPs/Directors - IT Security (IT Security Architect), InfoSec, Network IT/Security (Network Security Architect), DLP (DLP Manager), Risk & Compliance, Information Recovery

Next Gen SIEM/UEBA tool

For further help contact the Exclusive Networks team at Exabeam_UK@exclusive-networks.com

DISCOVERY QUESTIONS

1. Do you currently have a SIEM/Log Collector? If so, what?
2. Do you currently have a SOC? If so, is it managed in-house? How many SOC/general analysts do you have looking at this?
3. How many IT Users do you have/number in your AD? (If you have multiple accounts but one user, we only look at the user).
4. What cyber threats are you concerned about?
5. What security projects are on your roadmap?
6. What security toolsets are you using/any cloud apps?
7. Competition - who else are you considering?
8. What's your biggest concern with not having a SIEM in place/that you're not getting from your SIEM today?

THE MOST COMMON OBJECTIONS

"I already have a SIEM"
We can also augment SIEM using our UEBA offering. Improving threat protection by detecting threat correlation rules cannot find and remove a heavy number of false positives. Would you like to explore this option?

"We have analysts who sit in the SOC and manage this"
If analysts were able to work more efficiently and utilise their time across more projects – would that be useful to you? How do they prioritise alerts to ensure they're looking at attacks as opposed to false positives? Exabeam's smart timelines can automate the manual processes and increase your analysts' productivity.

How does Exabeam compare to the competition?

Exabeam is a market leader in the Gartner Magic Quadrant for both SIEM and UEBA. They are the 2nd fastest company to go from start up, to top right (behind Palo Alto Networks). Exabeam have also won the 'Gartner Customer Insight Award' two years in a row. This is a highly coveted award that is voted for by end prospects themselves and is based on direct feedback.

Competitors include:
Splunk, QRadar, AlienVault, Microsoft Sentinel, McAfee Nitro, LogRhythm, ArcSight, RSA, Secureonix and Forcepoint.

Exabeam vs. Splunk and QRadar

Legacy SIEM with volume based pricing, poor UEBA tool

- Splunk's pricing is based on data ingestion which creates large, unpredictable bills without appropriate value. Only Exabeam uses a flat, user-based pricing model so customers can log unlimited amounts of data for a fixed price.
- Splunk doesn't have any response capabilities. No timelines, no API based orchestration or playbooks. Slower and more cumbersome process that Exabeam's automated collation.
- Long POCs that require heavy manual handling with high intensity logs.
- Little detection value from UEBA offering.

Legacy SIEM now platform focused; UEBA as a feature; resilient for response

- QRadar's pricing is based on data ingestion which creates large, unpredictable bills without appropriate value. Only Exabeam uses a flat, predictable, user based pricing model so customers can log unlimited amounts of data for a fixed price.
- UEBA based on correlation rules resulting in heavy false positives.
- Running UEBA often requires additional hardware at an additional cost.
- Incident response based on IBM Resilient - low degree of automation focused on ticketing and compliance and industry specific reporting rather than incident response automation.

1400+ Vendor Integrations:

Data Lake tools e.g. Splunk, QRadar

Visibility tools e.g. Ixia, Forescout

EPP/EDR tools e.g. SentinelOne, Crowdstrike

Firewalls e.g. Fortinet, Palo Alto Networks, Checkpoint

DLP e.g. Symantec, WatchGuard, Forcepoint