exabeam®

Exabeam Data Sheet

Exabeam Security Analytics

Complement a SIEM or data lake with automated threat detection powered by user and entity behavior analytics (UEBA) with correlation and threat intelligence.

Most security operations teams lack standard procedures and expertise to detect and cope with credential-based threats, resulting in an inability to efficiently and effectively operationalize their legacy security information and event management (SIEM) solution or data lake for threat detection, investigation, and response (TDIR). Meanwhile, the sophistication and pace of attacks is multiplying.

Cloud-scale threat detection

Exabeam Security Analytics is the only threat detection UEBA product in the market that can run on top of an existing third-party legacy security information and event management SIEM solution or data lake to upgrade an organization's defenses and contend with complex, sophisticated, and credential-based attacks.

Exabeam Security Analytics ingests, normalizes, and parses logs using a common information model (CIM) with automated data enrichment and threat intelligence. This helps build and correlate events that automatically learn normal user and device behavior to detect, prioritize, and respond to anomalies based on risk. Smart Timelines™ convey the complete history of an incident, showing full event flows and activities and scoring the risk associated with each event. This eliminates the writing of hundreds of queries and transforms the way analysts do their jobs.

Flexible integration to augment your security stack

Exabeam Security Analytics enhances your existing security stack by absorbing your SIEM data and layering on analytics through hundreds of pre-built integrations covering dozens of key technologies. The result? Uplevel your security team's confidence, speed, and performance while maximizing the potential of your existing security investments as you unify them into a single console for monitoring and operations.

Understand normal; Detect and prioritize anomalies

Normal keeps changing. With Exabeam, baselines are established for all user, peer group, and device activity. Risk-based prioritization powered by machine learning (ML) automatically assigns risk scores to all events, facilitating triage, investigation, and response for key incidents. ML helps classify entity context like workstation versus server or service account versus human user, identifies personal email addresses, and more.

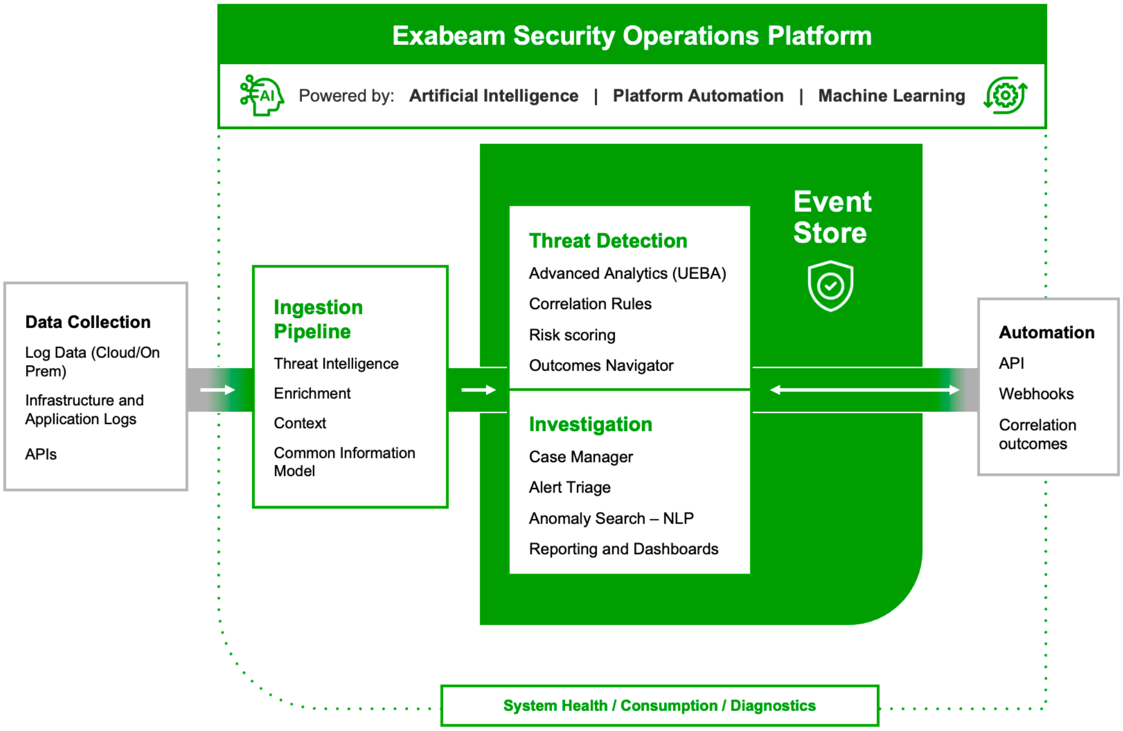

Figure 1.

The Exabeam Security Operations Platform powers Exabeam Security Analytics.

Exabeam UEBA capabilities include ML-based behavior analytics, correlation rules, and models to find advanced threats like credential-based attacks and other insider threats, and external threats missed by other tools. Automatically detect lateral movement and organize events across your technology stack into Smart Timelines that follow attacks no matter where they move or which credentials they use within your environment.

- Natural language anomaly search pairs behavior-based tactics, techniques, and procedures (TTPs) detection with known IoCs from integrated threat intelligence to enhance an analyst’s threat hunting capability.
- Smart Timelines dynamically gather evidence and assemble it into a cohesive story that can be used to perform an initial investigation. Each event registering as anomalous behavior is assigned a risk score.
- Extensive rule mapping enables analysts to perform behavior-based threat hunting on abnormal TTPs and use Outcome Navigator to evaluate coverage against the most common use cases and get suggestions for additional log sources that may contribute to detection.
- Existing SIEM, extended detection and response (XDR), and logs from other cloud data lakes or resources like cloud access security brokers (CASBs) and web gateways are brought in to consolidate views, add depth, establish normal baselines, and create correlation potential to see end-to-end attack event strings.
- Correlation rules can be customized to trigger on complex, multi-stage attacks and escalate into a ticketing system, Slack, or Teams notifications.

Built on the Exabeam Security Operations Platform

Bringing a cloud-native experience built to scale with your organization, the Exabeam Security Operations Platform allows you to collect and search log data, leverage behavioral analytics to detect attacks, and automate incident response. Visualize the health of your security log feed for every service, log, and application with dashboards showing uptime, health, and data flows. The Exabeam Security Operations Platform supports measurable, continuous, outcomes-focused security posture improvement by recommending information, event stream, and parsing configuration changes to close any common security use case gaps.

Benefits of Exabeam Security Analytics:

- **See threats across your environment:** Identify associated events and reduce the need for manual builds of hundreds of queries. Automated Smart Timelines stitch events together into a timeline with associated risk scores.
- **Bring your own SIEM or data lake:** Exabeam integrates UEBA with any SIEM solution, offering fast threat detection and streamlined search.
- **Enhance coverage with the right data:** Absorb and monitor new security log inputs, and collect and parse log sources quickly using a CIM.
- **Improve time to value:** Prepackaged content reduces time spent on building and maintaining hundreds of thousands of correlation rules.
- **Identify high risk, anomalous user and entity behavior:** Learn normal user and entity activity to detect deviations that may indicate threats.
- **Threat hunt:** Hunt on known indicators of compromise (IoCs), correlated events mapped to the MITRE ATT&CK® framework, use cases, and anomalous activity within a single Search application.
- **Identify gaps in coverage:** Map security data sources to the most common use cases and receive recommendations on data sources, actions, and improved correlations or visualizations.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. The company was the first to put AI and machine learning in its products to deliver behavioral analytics on top of security information and event management (SIEM). Today, the Exabeam Security Operations Platform includes cloud-scale security log management and SIEM, powerful behavioral analytics, and automated threat detection, investigation, and response (TDIR). Its cloud-native product portfolio helps organizations detect threats, defend against cyberattacks, and defeat adversaries. Exabeam learns normal behavior and automatically detects risky or suspicious activity so security teams can take action for faster, more complete response and repeatable security outcomes.

exabeam®

Detect
Defend
Defeat™

Get a demo →

Speak with an Expert →

Join a CTF →