exabeam

Data Sheet

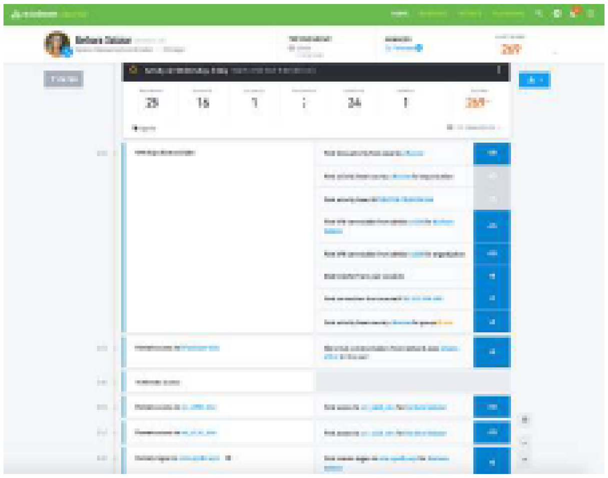
Exabeam Advanced Analytics

Shine a light on modern cyber-attacks

Today's credential based threats are complex, often touching many systems, using multiple log-ins, and spanning a period of several months. These insider threats involve the legitimate credentials and access privileges of real users, making them challenging for legacy security solutions to detect. In order to tackle these insidious threats, organizations need a solution built from the ground up using modern technologies such as machine learning, behavioral analysis and data science.

A smarter approach to detection and investigation

Exabeam Advanced Analytics is the world's most deployed behavioral analytics platform. Advanced Analytics automatically links and analyzes user and entity activity to better inform security analysts about threats and corresponding remediation. Advanced Analytics provides a powerful analytics layer on top of existing SIEM and log management technologies, detecting new attacks, prioritizing incidents, and guiding a more effective response.



Exabeam Advanced Analytics combines a purpose-built architecture with an investigation-focused user experience designed to fit the way security professionals actually work. Advanced Analytics uses a proprietary Session Data model that automatically stitches together event timelines, including both normal and abnormal behavior, before flagging potential threats. This reduces the manual effort security analysts spend on investigations and increases their productivity.

Rapid Time to Value

Regardless of the data type or source, Exabeam makes it easy for customers to make use of all of the information available to them in order to perform a truly comprehensive assessment of the threats on their network. Advanced Analytics can ingest logs from a SIEM or directly from the data sources themselves via Syslog. Customers are able to rapidly deploy and analyze historical logs for quick time to value, or analyze new log sources in Advanced Analytics which may be cost prohibitive to send to their existing SIEM. This flexible data handling delivers a fast time to value of unmatched by other behavioral analytics solutions.

Compounding Operational and Cost Effeciencies

The benefits of the Advanced Analytics solution are compounded by Exabeam Data Lake and Incident Responder which together provide full end-to-end coverage for data storage, access, analytics, and automated response. Advanced Analytics can be deployed as a standalone solution, or as part of the larger Exabeam Security Intelligence Platform.

Key Features

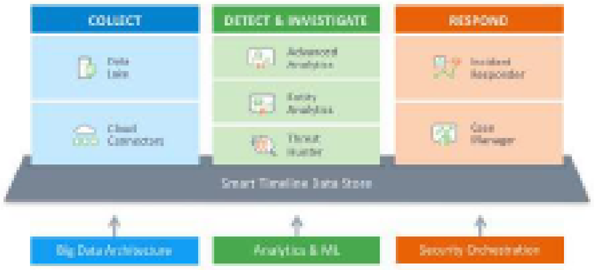
Exabeam provides world class threat detection, prioritizes analyst workloads, and greatly improves SOC productivity. Its key features include:

- User and Entity Behavior Analysis (UEBA) based detection for complex modern threats including credential-based attacks, insider threats, and ransomware
- Pre-constructed session timelines which automate analyst investigation, and make proactive analysis faster and easier
- Intelligent security alert prioritization to ensure analysts can easily find the alerts which require the most attention
- A unique session data model that automatically detects lateral movement including changes of credentials, IP addresses, or devices
- Detection methods within Advanced Analytics are now mapped to the MITRE ATT&CK Framework, offering a common taxonomy for security analysts to label adversary behavior and improving collaboration
- Interoperability with all major SIEM solutions, as well as Exabeam Data Lake and Incident Response solutions
- Ease of setup and use
- Scale-out multi-node architecture
- Supports 500+ data sources out of the box
- Ability to deploy on premises or in the cloud

Exabeam Security Management Platform

Exabeam's modular offerings can be mix-and-matched according to your organization's specific needs. Whether you're looking for a full SIEM replacement, or to enhance your current setup incrementally by augmenting it with improved threat detection, more cost effective logging, and improved productivity, we can help. The Exabeam platform includes:

- Data Lake
- Cloud Connectors
- Advanced Analytics
- Entity Analytics
- Threat Hunter
- Case Manager
- Incident Responder



About Exabeam

Exabeam is a global cybersecurity leader with the mission to add actionable intelligence to every IT and security stack. The leader in next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit exabeam.com.

exabeam™