exabeam

DATASHEET

EXABEAM SECURITY INTELLIGENCE PLATFORM

YOU CAN'T TEACH AN OLD SIEM NEW TRICKS

Legacy SIEMs no longer meet the needs of most organizations. While the premise of SIEM - to provide complete visibility into the threats unfolding on a network and enable automated, intelligent response to those threats - sounds as attractive as ever, SIEMs have become outdated and unable to fulfil that promise. They are built on aging, proprietary log data management technologies, (over)priced based on data volumes; lack intelligent, machine learning based analytic capabilities, and require deep technical skill to operate. To highlight the issues, nearly every company that suffered from a public breach in recent years had a large SIEM system in place at the time of breach. Modern security organizations deserve better.

Exabeam's Security Intelligence Platform (SIP) was built from the ground up on modern technology including machine learning, behavioral analysis, open source big data, and artificial intelligence in order to solve the problem of security management. Exabeam's SIP provides organizations of all sizes with comprehensive, end-to-end detection, advanced analytics, and automated response capabilities from a single security management and operations platform. Furthermore, this is achieved without surprise pricing based on data volumes.

EXABEAM SECURITY INTELLIGENCE PLATFORM

The Exabeam platform includes five key components, each of which can be purchased and deployed separately or as a complete solution:

COLLECT

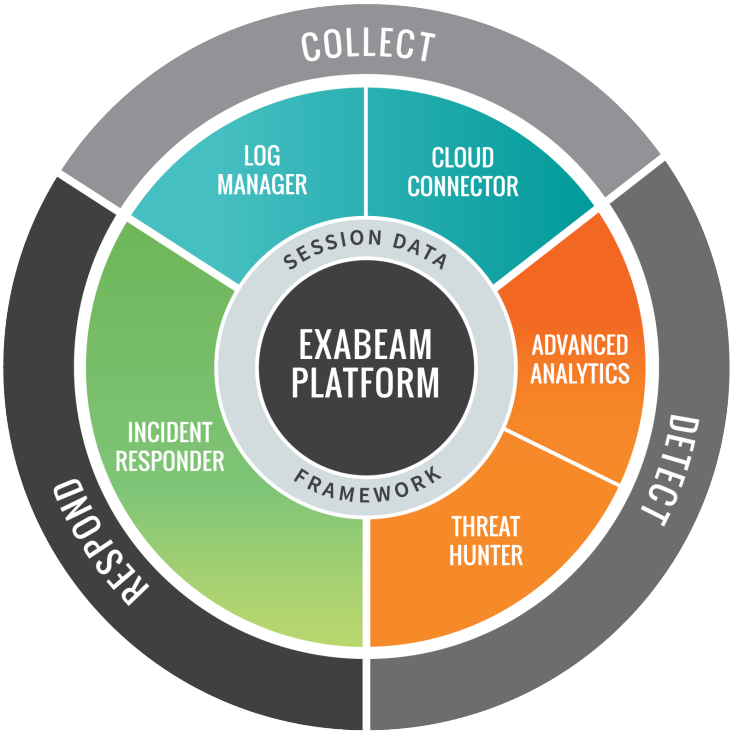
- **Log Manager** – Unlimited log data capture and search, based on open source big data technologies.
- **Cloud Connector** - Pre-built log collectors for popular cloud services such as Office 365, Box, Salesforce, and more.

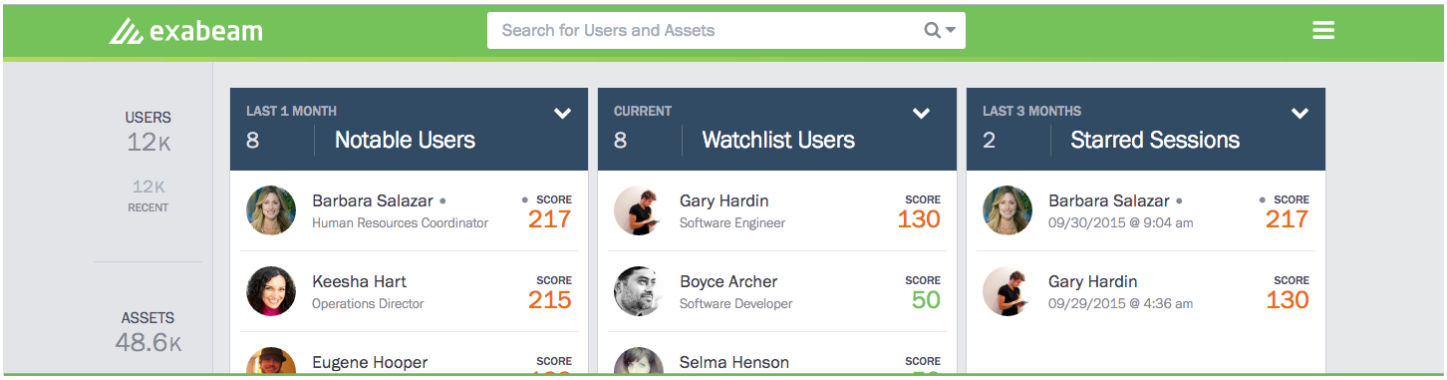
DETECT

- **Advanced Analytics** – Machine learning led threat detection based on Exabeam's market-leading User and Entity Behavioral analytics (UEBA) solution.
- **Threat Hunter** - Proactive, user session based threat hunting for the entire SOC; powered by an intuitive point-and-click interface.

RESPOND

- **Incident Responder** - Customizable incident management, API-based security orchestration, and automated security playbooks to amplify human abilities.





KEY FEATURES AND BENEFITS

Lightning Fast Log Management

Built on a customized version of the popular open source Elastic stack, Exabeam SIP provides lighting fast performance and proven scalability. Exabeam took the best parts of this battle-tested log management framework and them paired with the fit and finish that today's enterprises demand of their security solutions.

Unlimited Scalability at a Predictable Cost

Unlike Legacy SIEMs, Exabeam is not priced based on data volumes. Instead Exabeam SIP offers unlimited data ingestion using a predictable, user based pricing model. This means you no longer need to fear that chatty data sources such as web proxies will bloat your SIEM bill.

The World's Most-Deployed UEBA Solution

Exabeam detects complex insider threats using the Exabeam Advanced Analytics solution, the most-deployed User and Entity Behavior Analytics (UEBA) product in the world. SIP not only identifies risky user anomalies, it recreates entire attack chains including both normal and anomalous activities for related users.

Context-Aware Log Parsing

Digesting event logs can be dull and painful work for analysts. By leveraging a built-in context awareness, Exabeam is able to parse logs according to their type, highlighting the attributes of that specific log type which are most interesting for security analysts.

Security Orchestration and Automated Response

Increase the productivity of IR and SOC staff by leveraging automated playbooks and API-based orchestration. Pre-built or customized incident playbooks and workflows standardize response procedures from a self contained incident management system that ensures swift, repeatable incident response which amplifies productivity, while minimizing human errors.

End-to-End Analyst Collaboration

Built-in collaboration features including commenting, mentions, and bookmarking enable security analysts and incident response teams to effectively track and manage threats across teams and shifts. Exabeam's rich collaboration capabilities span the entire breadth of the SIP platform enabling efficient communication within and between each solution in the platform.

OPERATING INFORMATION

- Deployable as a physical appliance (in multiple sizes) or as a cloud-ready virtual machine
- Includes out of the box collection agents and parsers for over 500 security data sources
- Agents operate on Windows or Linux platforms

For more information, please contact Exabeam at info@exabeam.com