exabeam

Exabeam Unveils User Behavior Intelligence Platform, Delivers Future of Cyberattack Detection and Response

Technology uses existing log repository data to track user behavior, detect and qualify threats not recognized by SIEM

San Mateo, Calif. – October 6, 2014

Exabeam, a big data security analytics company, today announced the launch of its platform, which will enable enterprises to finally realize the full promise of their existing security information and event management (SIEM) deployments. Platform users will be able to detect cyberattacks and insider threats in real time, while simultaneously optimizing security operations. Exabeam adds a layer of user behavior intelligence on top of existing SIEM and log management repositories to give IT security teams a complete view of the full attack chain and spotlight valid attack indicators currently lost in a sea of security noise, allowing for better and more complete security response.

Attackers used authorized credentials in more than 76 percent of network intrusions in 2013, allowing them to impersonate legitimate users spanning across IT environments and conduct suspicious activities along the way. Current SIEM technologies can't detect subtle anomalies or correlate them across the entire attack chain, forcing IT and security teams to anticipate malicious behaviors, which is nearly impossible in today's hacker climate. Exabeam's platform removes the guesswork by providing access to real-time insights that tell users which indicators to look for in order to spot malicious behaviors.

"The challenge with SIEM solutions is that you can only find the threats you are actively looking for through a statistical or rule-based model," said Colin Anderson, vice president of information technology and chief information security officer at Safeway, an Exabeam beta customer. "Where Exabeam brings immense value is in identifying what we're not looking for by understanding 'normal' user behavior and alerting us when network activity deviates from that baseline. Without this type of solution, businesses are blind to these threats and waste time chasing the tails of false positive alerts."

Exabeam's user behavior intelligence platform provides security teams insight into which accounts are involved in attacks and provides a complete picture of user activity, greatly reducing attack detection times. The platform includes the following key capabilities:

- **Extraction and enrichment** of high-value log feeds, such as Windows, Unix, VPN and security events from existing log repositories.
- **Session tracking** of all user activities across multiple dimensions, from entrance to exit of the IT environment, regardless of the IP, devices and accounts used. It also connects discrete activities and security alerts back to the originating logon.
- **Behavior analysis** using unsupervised machine learning to automatically and continuously learn user and peer group behavior, as well as characteristics across multiple dimensions.
- **Risk scoring** to quantify the security importance of the anomaly, taking into consideration key security data, such as user access, asset priority and threat intelligence.

In the August 25, 2014 "Market Guide for User Behavior Analytics," written by Vice President and Distinguished Analyst at Gartner Avivah Litan and Managing Vice President Mark Nicolett, "User behavior analytics is transforming security and fraud management practices because it makes it much easier for enterprises to gain visibility into user behavior patterns to find offending actors and intruders." The report goes on to state, "While security information and event management (SIEM) supports activity monitoring with user context, UBA technologies augment SIEM by enabling more effective exception monitoring due to more advanced profiling and anomaly detection that is not dependent on IAM policy definitions for roles and authorization rights."

"For too long, security teams couldn't get ahead of hackers because they didn't know what to look for, had too many security alerts to process and didn't get the complete picture of what was happening in their network," said Nir Polak, Exabeam CEO and co-founder. "Exabeam fundamentally changes the way that cyberattacks are managed by addressing these challenges in an automated way and giving security teams the intelligence they need in real time. The future of cyberattack management starts with Exabeam, and the future is now."

Exabeam's beta customers include an impressive list of Fortune 500 companies in financial services, retail and more. To join this world-class group of industry leaders or learn more about Exabeam's technology, visit the company's booth during the Splunk Worldwide User Conference taking place October 6 – 9 at the MGM Grand in Las Vegas, or visit us at http://exabeam.com/resources.

About Exabeam

Exabeam, a leading provider of big data security analytics, is unlocking the potential of existing SIEM and log management repositories to fundamentally change the way cyberattacks are detected and greatly simplify security operations. The company's groundbreaking technology applies user behavior intelligence, focusing on attacker behavior rather than ever changing malware and tools to detect modern cyberattacks. Built by seasoned security and enterprise IT veterans from Imperva and Sumo Logic, Exabeam is headquartered in San Mateo, California and is privately funded by Norwest Venture Partners, Aspect Ventures and Investor Shlomo Kramer. Visit us on Facebook or Twitter and follow us on LinkedIn.

For more information,
please contact:

Megan Lieberman
Metis Communications
617-513-8315
exabeam@metiscomm.com

WHY EXABEAM

PRODUCT

- SUPPORT

- CASE STUDIES

PARTNERS

- PARTNER REGISTRATION

- PARTNER DEAL REGISTRATION

NEWS

- MEDIA KIT

ABOUT

- CONTACT US

- CAREERS

BLOG

GET EXABEAM NEWS

Email *

SUBMIT

CONNECT WITH US

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.