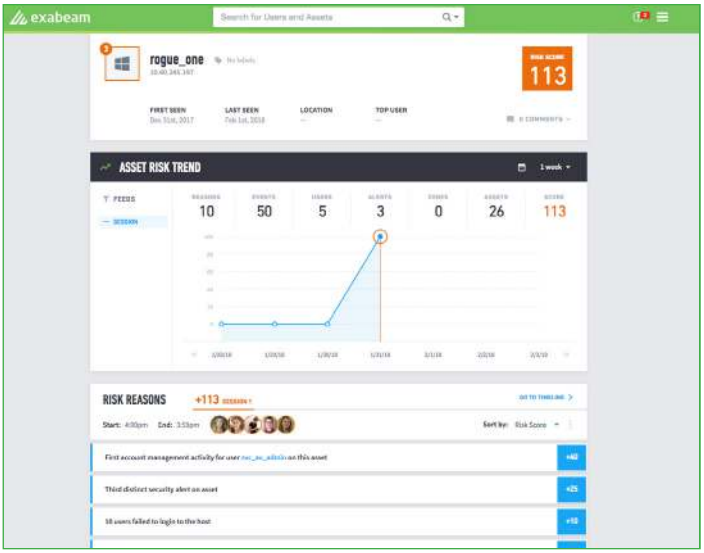
exabeam

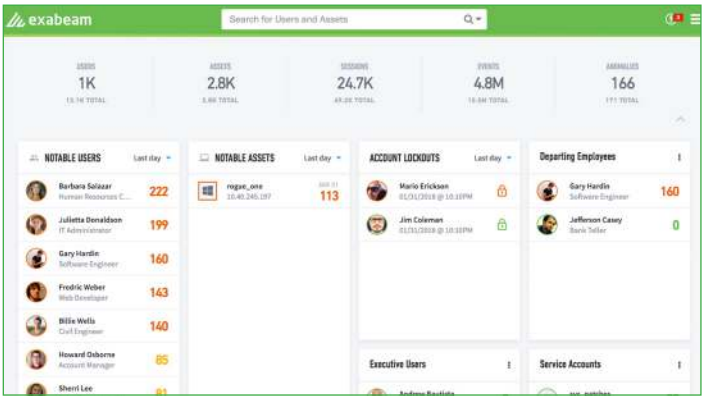
DATASHEET

EXABEAM ENTITY ANALYTICS

ENTITY BEHAVIOR ANALYSIS

Advanced threats often traverse laterally though a network, leveraging multiple users and machines in their search for high value data. Seemingly innocuous machines like medical devices, office printers, manufacturing machinery, and database servers often fall victim and are used by bad actors as stepping stones; thus, they demand the same level of security monitoring and control as their human counterparts. Entity Analytics establishes a baseline of normal behavior for all assets in an organization—including communication patterns, ports and protocols used, and operating activity. It automatically identifies risky, anomalous device activity that may be indicative of a security incident or compromise.





PREBUILT INCIDENT TIMELINES

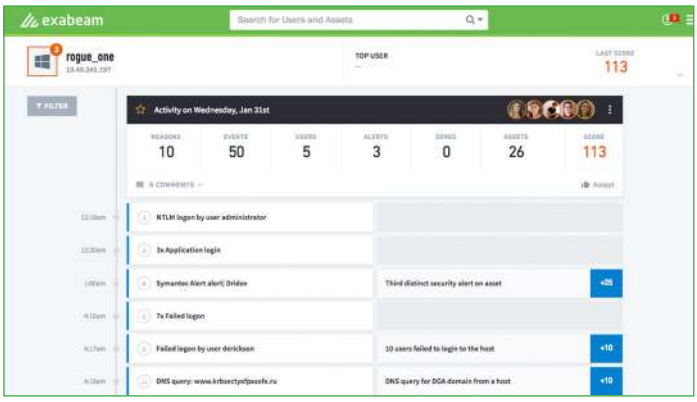
Entity Analytics automatically creates prebuilt timelines for all discovered incidents. Unlike competitive solutions, Exabeam's timelines include all lateral movement—there are no gaps or manual steps required to follow the attacks as they move between users or entities.

Our timelines detail what happened during an incident, as well as surrounding behavioral context to determine if the activity is normal. For your security analyst team, this greatly reduces the tedious steps and manual effort required to gather evidence and perform an investigation.

ENTERPRISE-WIDE VISIBILITY

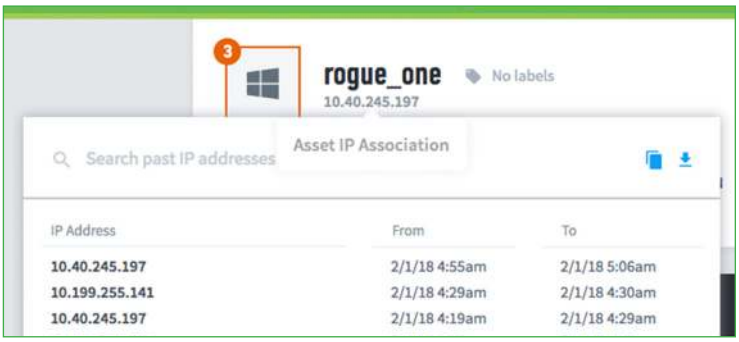
Exabeam Advanced Analytics is the only "pure-play" behavioral analytics solution that combines a purpose-built architecture with an investigation-focused user experience designed to perfectly fit the way security professionals want to work.

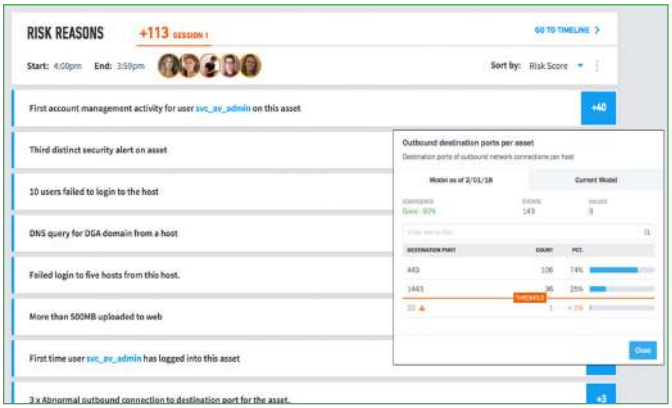
Our patented Session Data Model automatically stitches together the disparate events that comprise both normal and anomalous activities, highlighting in seconds the critical entities security professionals normally spend weeks collecting.



AUTOMATIC IP MAPPING

In most IT environments machines are dynamically assigned IP addresses by way of DHCP. If an incident occurs, security teams must match which assets correlate with the targeted addresses. This can be a tedious, manual process. Entity Analytics not only performs IP association on current addresses, but also all past DHCP IP addressing over time.





RULE AND SIGNATURE-FREE DETECTION

Correlation rules and threat signatures create false positives due to their lack of user or machine context. They suffer from false negatives as they cannot detect unknown attacks; maintenance consumes large blocks of analysts' time.

Instead of leveraging basic pattern matching or correlation rules, Entity Analytics uses behavioral modeling and machine learning to look for abnormal activity. Sensing potential compromise and risk, this method detects anomalous events—without the tuning, maintenance, and false positives that drain analyst productivity.

KEY FEATURES

Entity Analytics provides advanced threat detection for the myriad of internet connected devices scattered throughout your environment. By modeling the behavior of these machines, Entity Analytics is able to baseline every asset in your organization, then automatically identify risky, anomalous activity that may be indicative of compromise or malicious use. Key features include:

- Behavioral analytics-based detection eliminates false positives, reduces false negatives, and slashes security management overheads
- Patented lateral movement detection that follows attacks as they move between devices, IPs, or credentials
- Prebuilt incident timelines automate the manual steps involved in investigations to boost analyst productivity
- Interoperability with SIEM solutions, as well as Exabeam's Log Management and Incident Response Solutions
- Intelligently prioritized security alerts to ensure high scoring alerts best reflect business priorities
- Ability to deploy as a pre-sized physical appliances or as a cloud-ready VM

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**

To learn more about these products, please visit www.exabeam.com/products to download whitepapers, datasheets, etc.