exabeam

Data Sheet

Entity Analytics Data Sheet

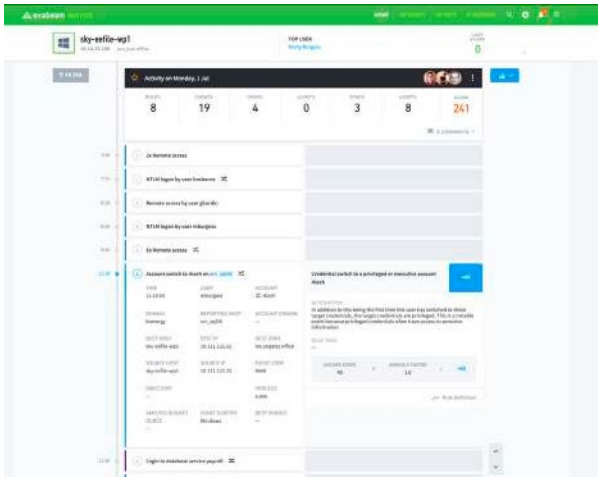
Behavioral Analytics for Interconnected Devices to Complete your UEBA Solution

According to a recent Gartner report, between 2018 and 2023 the world will see a three-fold increase in internet connected devices—which equates to a growing attack surface that security must defend. Unfortunately, a lack of visibility into device based threats leaves organizations vulnerable to advanced threats that span both users and assets. These threats frequently move laterally through a network, leveraging users and machines in their search for high value data. Devices of all types—for example, laptops, servers, printers, along with specialized devices like medical equipment, heavy machinery, and power grid infrastructure—are prime targets for attackers, thus they require the same monitoring and security controls as their human counterparts.

Exabeam Entity Analytics improves detection and investigation of advanced device-based threats through the use of behavior analytics, leveraging machine learning and behavioral modeling to identify anomalous, high-risk activity indicative of complex threats.

Behavioral Analytics for Threat Detection

Modern attacks involve both users and devices. While user behavior analytics can stitch together how an attacker advances across a network from the perspective of a user, it lacks visibility into the attack from the perspective of the entity: an asset, device, server etc. Entity Analytics detects threats by identifying high risk, anomalous entity activity. This happens by using machine learning to baseline normal activity for all entities in an environment. Once a baseline has been created, the system automatically detects deviations compared to that baseline—and assigns that activity a risk score. Analysts can easily identify deviations in entity behavior: like anomalous machine to machine communication or a machine sending out anomalous data flow. These could all be indicators that an attack is in progress, and without a baseline understanding of that entity's normal behavior, an analyst could easily miss all or a part of the attack.



Machine-Built Incident Timelines for Rapid Investigation

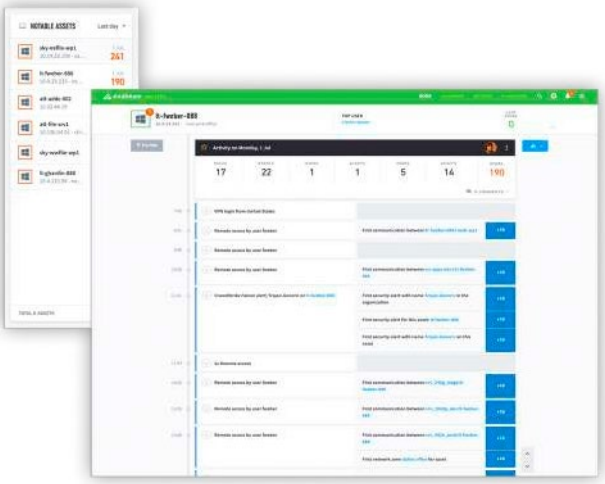
Analysts must perform manual, time-consuming investigations to stitch together a timeline of events preceding and following an attack to determine whether the attack needs further investigation or if it is a false positive. For all anomalies detected by Entity Analytics, Exabeam's machine-built incident timelines, stitch together both the normal and abnormal behavior for entities. These timelines include all information an analyst needs to perform a rapid investigation, including: normal and abnormal activity, as well as the surrounding context, like what happened before and after an alert, or whether this alert maps to a MITRE tactic, technique, or procedure. Exabeam Smart Timelines™ automate entity investigation and improve SOC productivity, helping SOCs handle staffing shortages.

Automated User Attribution for Enhanced Visibility

Modern attacks involve both entities and users. However, it is often difficult to pivot between user and entity investigation timelines to find additional points of compromise. This is because security alerts and logs frequently do not contain the data needed to perform user attribution or to associate the attack to a set of credentials and thus to other activity taken elsewhere in the environment with those credentials. Entity Analytics automatically identifies the users associated with devices. Associating users to entities automates a difficult, manual step in investigation and allows analysts to easily follow the lateral movement of attacks and see entire attack chains.

Risk-Based Prioritization for Increased Productivity

SOC teams must triage and respond to an overwhelming number of alerts. However, analysts have no way to efficiently determine whether an alert indicates a compromised entity, without performing a lengthy investigation. With Entity Analytics, risk scores are assigned to each anomalous event or alert and then aggregated within an entity's timeline, escalating the highest risk assets to analysts for review. Prioritizing which entities SOC analysts should investigate helps SOC managers run a more effective and efficient SOC. Identifying notable assets that present the highest risk for an organization, decreases the likelihood that a critical alert, which could lead to a breach, is overlooked.



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 how Exabeam can help you visit exabeam.com today.