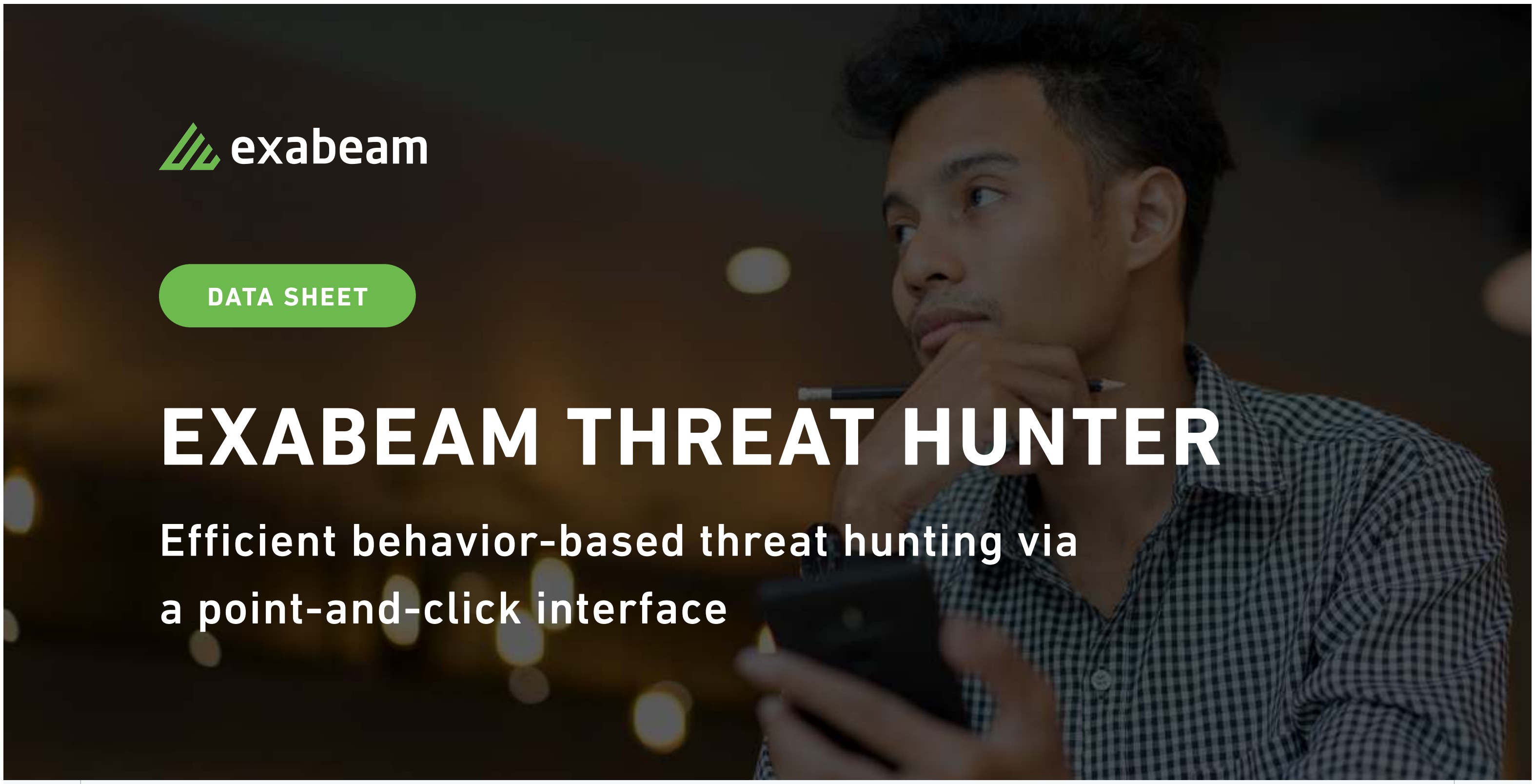


exabeam

DATA SHEET

EXABEAM THREAT HUNTER

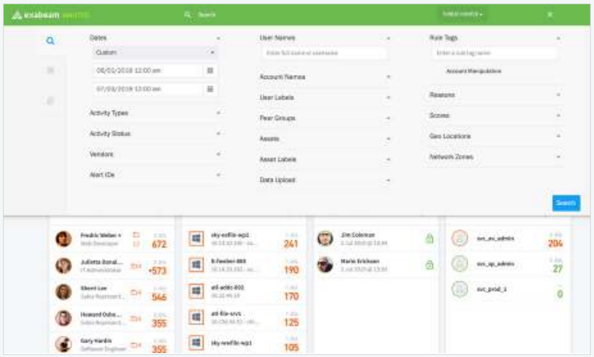
Efficient behavior-based threat hunting via a point-and-click interface

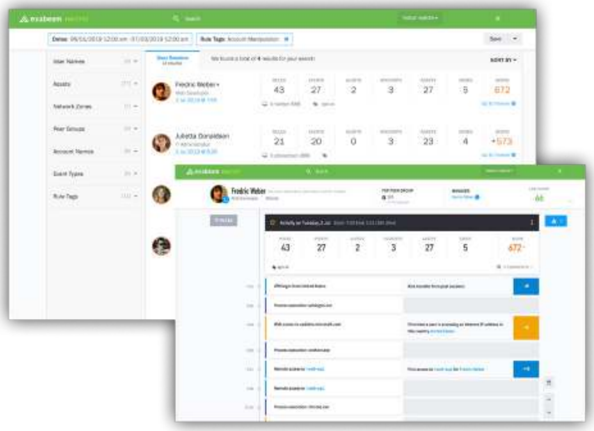
THREAT HUNTING INVOLVES CONTINUOUSLY SEARCHING SECURITY DATA FOR PATTERNS IN AN ATTEMPT TO DISCOVER THREATS THAT HAVE EVADED EXISTING SECURITY TOOLS. Many analysts run manual, query-based searches within a SIEM to find adversaries. However, these searches require a deep understanding of the specific threats being searched for, thus relegating the activity to seasoned analysts. Once a threat is discovered, they must perform a tedious and inefficient investigation process, which makes it difficult for them to quickly understand the scope of the threat and identify any users or entities that may have been compromised.

Protecting your business from security threats on an ongoing basis requires a modern approach to threat hunting. Exabeam Threat Hunter combines threat hunting with behavioral analytics and a point-and-click interface to position you well ahead of adversaries when it comes to protecting your organization's assets.

Efficiently hunt for anomalous behavior

Threat Hunter allows analysts to easily search for abnormal behaviors in their environment, which may be indicative of threat. Taking a behavioral approach to threat hunting is more efficient than searching for indicators of compromise (IoCs) because a single behavior can be responsible for hundreds or thousands of IoCs. Moreover, identifying abnormal behavior saves analysts time, as they no longer have to identify risky, unusual behavior hiding in a sea of day-to-day activity. This can help prevent alert fatigue resulting from triaging too many false positives.





Automate investigations with pre-built incident timelines

Threat Hunter returns machine-built incident timelines, that outline both normal and anomalous activity that happened before and after the threat, as search results; instead of raw logs. By contrast, in a traditional SIEM, when threat hunters uncover an attack, they must kick off an investigation to understand the surrounding context; which can take hours, days or weeks. With machine-built incident timelines, analysts can save time on investigations and easily interpret results, reviewing any suspicious activity that was uncovered.

Simplify search queries with easy-to-use point-and-click interface

Threat Hunter leverages a point-and-click interface that simplifies the process of creating complex search queries. Analysts can easily string together conditions from available menus like activity type, vendor, or peer group, without needing to learn a complicated search query language. This allows analysts at all levels to quickly and easily perform threat hunting by developing searches that otherwise may have been extremely difficult or impossible to create using traditional querying.

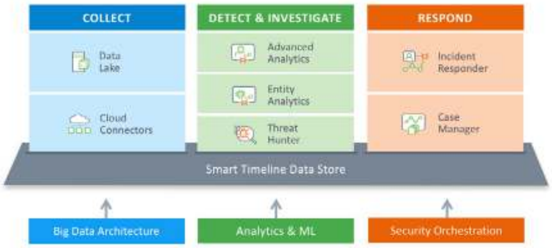
Threat Hunt using MITRE ATT&CK tactics, techniques and procedures

With Threat Hunter, analysts can easily search for anomalous tactics, techniques, and procedures (TTPs) from a drop-down menu. Traditionally, security experts searched for indicators of compromise (IoCs) to identify known threats. This left organizations with a large amount of IoCs to hunt for but no effective way to investigate them all. However, IoCs largely rely on historical data, making them unsuccessful in identifying unknown threats, since you cannot search for an attack you have yet to see. Exabeam replaces legacy discovery methods with threat hunting that leverages the MITRE ATT&CK framework to detect recognizable attack patterns within their infrastructure. This allows analysts to search for relevant TTPs in their environment after learning of a new attack.

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.