exabeam

SOLUTION BRIEF

REALLOCATING ADDITIONAL SIEM SPEND FOR BETTER DETECTION AND RESPONSE

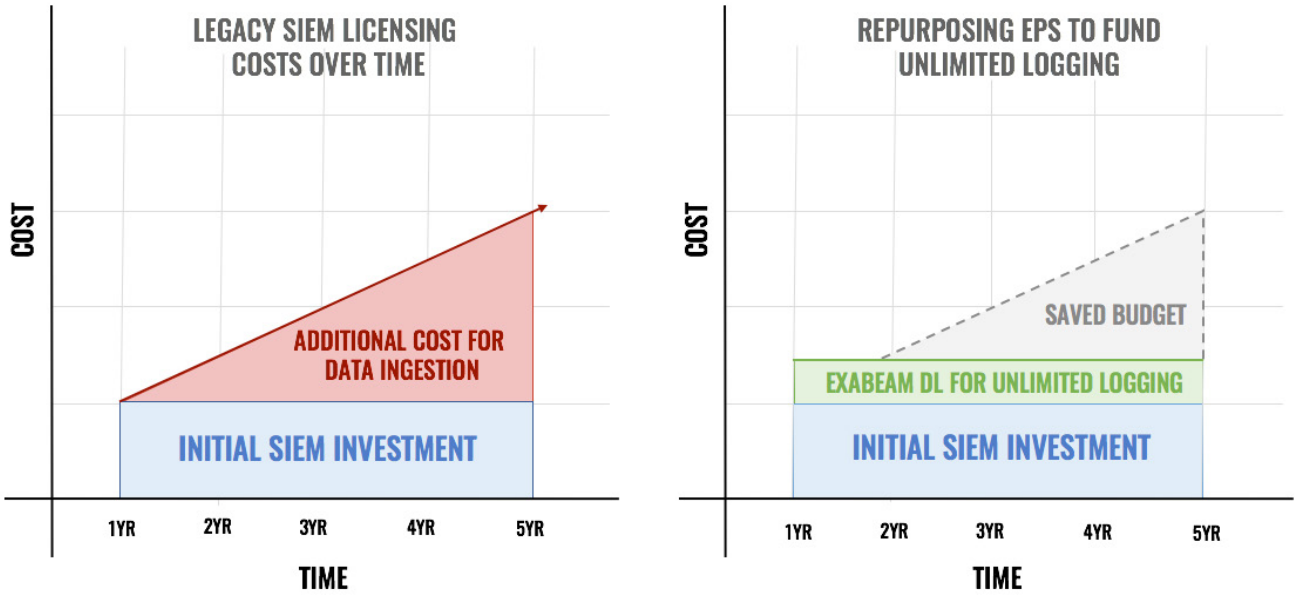
SIEM SPEND IS AN EVER-GROWING PROBLEM

When organizations initially implement a legacy SIEM they often plan their project around a handful of mission-critical use cases. Over time, as security teams conquer their initial use cases, they begin to broaden the use of their SIEM to tackle additional initiatives such as bringing in endpoint, web proxy, or firewall logs. This is typically where the conflict between security budgets and optimal use of a SIEM begins. Why? Because legacy SIEM vendors price their log management solutions by-the-byte, such that adding new data types, or ingesting greater volumes results in a higher SIEM bill. Data volume-based pricing forces security teams to choose between ingesting and analysing potentially valuable data sources—and thus increasing their data volumes or Events Per Second (EPS)—and adhering to their already tight security budgets.

GETTING THE MOST OUT OF YOUR SIEM BUDGET

Organizations find themselves in this predicament due to the consumption-based pricing model of their chosen SIEM vendors. The logical solution for savvy security leaders is to circumvent this pricing model by implementing an unlimited logging platform like Exabeam Data Lake (DL) to house their security data without the fear of a growing SIEM bill. This initiative can be in replacement of, or as a supplement to, their existing SIEM. Furthermore, the project virtually pays for itself, as budget that would have otherwise been spent on procuring additional EPS or ingestion capacity can be repurposed to fund this new unlimited logging initiative.

The following chart illustrates how additional ingestion fees can increase SIEM bills over time and how repurposing those funds toward unlimited logging solutions can save security budgets:



A REDISTRIBUTION IN SPEND YIELDS GREATER VALUE

While legacy SIEMs are ostensibly designed as comprehensive security management products, the focus of their business models and development efforts has largely been data collection. Once data has been collected, legacy SIEMs rely on antiquated technology like static correlation rules for threat detection, and case management for incident response. These tools consume valuable analyst time, while doing nothing to amplify analyst productivity in either area. Implementing an unlimited logging solution like Exabeam Data Lake frees up security budget, that can be repurposed to invest in modern technologies which provide greater value to security teams, such as behavioral analytics for threat detection and API-based security orchestration for incident response.

User and Entity Behavior Analysis (UEBA)
UEBA analyzes actual user and entity behavior to identify anomalous and risky activities which may be indicative of threat. This provides a powerful analytics layer on top of existing SIEM and log management technologies, detecting new attacks, prioritizing incidents, and guiding a more effective response. Exabeam's UEBA solution, Advanced Analytics, not only identifies risky user anomalies, it recreates entire attack chains including both normal and anomalous activities for related users.

Security Orchestration & Automated Response (SOAR)
Unlike the case management systems in legacy SIEMs, SOAR solutions like Exabeam Incident Responder, increase the productivity of security analysts and incident responders. API-based orchestration enables connection and coordination with other security and IT infrastructure tools. Automated response playbooks can be run at the click of a button to standardize response procedures and ensure swift, repeatable incident response that amplifies productivity, while minimizing human errors..

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

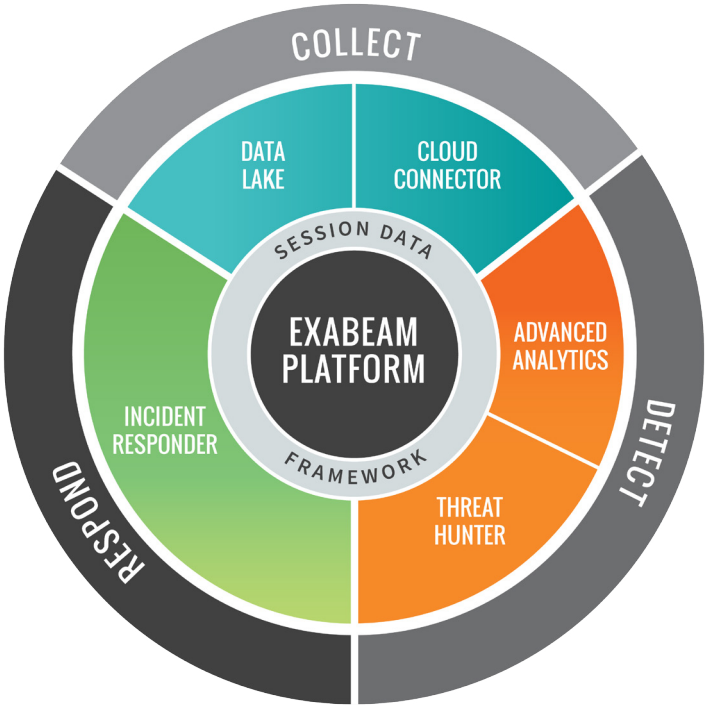
- **Data Lake** – Unlimited log data capture and search, based on open source big data technologies.
- **Cloud Connector** – Pre-built log collectors for popular cloud services such as Office 365, Box, Salesforce, and more.

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.



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