exabeam

SOLUTION BRIEF

EXABEAM AND IMPERVA

Unleash the Power of Your Data While Detecting and Prioritizing Data Threats

Digital transformation initiatives are fueling unprecedented user access in the name of deriving greater insights and better decision making to drive business value. An unintended consequence of increased access is the risk of data breaches and sensitive data loss due to compromised credentials or insider threats. Even the most benign oversight, like poor policy management maintenance, can lead to unchecked user privileges and abuse by bad actors. In response to these risks, security teams have turned to data activity monitoring (DAM) solutions like Imperva to manage data breach risk and sensitive data loss.

Exabeam's user and entity behavior analytics (UEBA) solution uses behavioral modelling of users, peer groups, and devices to automatically baseline normal activity, assign a risk score to suspicious events and intelligently prioritize them for further evaluation – across all your security solutions of choice. The combination of Exabeam and Imperva bridges the gap between DAM data and other security and IT infrastructure tools to build a complete picture of an attack. By combining DAM data with data from other solutions—like data loss prevention solutions—security teams benefit from more accurate risk scoring and a lower rate of false positives. This enables security teams to efficiently collect, detect, investigate, and respond to suspicious activity that may indicate a data breach without compromising business agility.

imperva

UNCOVER SUSPICIOUS DATA ACCESS EVENTS

Given the massive volume of database activity events, it's difficult for resource-strapped security teams to accurately pinpoint and prioritize suspicious behaviors. The Exabeam-Imperva integration identifies unusual behaviors such as a user's sudden interest in a database they've not previously accessed, a single user logging into multiple accounts, multiple authentication attempts, logins from unfamiliar locations, abnormal volumes of data downloaded or exported, and other unusual data alteration activity that might denote a compromised insider or other activity by a bad actor.

By creating a baseline for normalized behavior of users, peer groups, and devices, Exabeam's machine-built timelines and response playbook templates make it possible for security analysts to quickly and efficiently analyze, detect, and respond to threats eliminating time-consuming threat hunting across multiple tools and standardizing incident response actions to ensure timely and consistent action.

INTEGRATION BENEFITS

COLLECT

Collect unlimited Imperva DAM data—from heterogeneous environments (such as relational databases, mainframes, data warehouses, and PaaS) with full context, including all user and device access activity log data and anomalies, as well as those identified by Imperva — using a flat, predictable pricing model.

DETECT

Exabeam baselines "normal" credential and database access activity for all users, including privileged users, as well as anomalies identified by Imperva to detect suspicious activity, even if the attack has never been seen before. By applying user and entity behavior and analytics, Exabeam helps teams analyze massive volumes of DAM data to more quickly and accurately identify and anomalous activity. With analytics based risk scoring, Exabeam helps highlight risky behavior such as possible attempts to steal, alter, or delete database records and evaluate DAM data in the context of other solutions. In addition, Exabeam monitors activity from other security tools for greater confidence levels in threat identification - for example, by analyzing suspicious data from a data loss prevention (DLP) solution with data activity monitoring logs, security teams can identify a data exfiltration attempt with greater confidence.

INVESTIGATE

Dramatically reduce the time analysts spend investigating incidents with Exabeam Smart Timelines that automate the manual assembly of evidence from multiple, disparate systems, including detailed audit trails from Imperva, into machine-built timelines. Exabeam accurately pinpoints anomalous events and improves analyst productivity while significantly improving response times. .

RESPOND

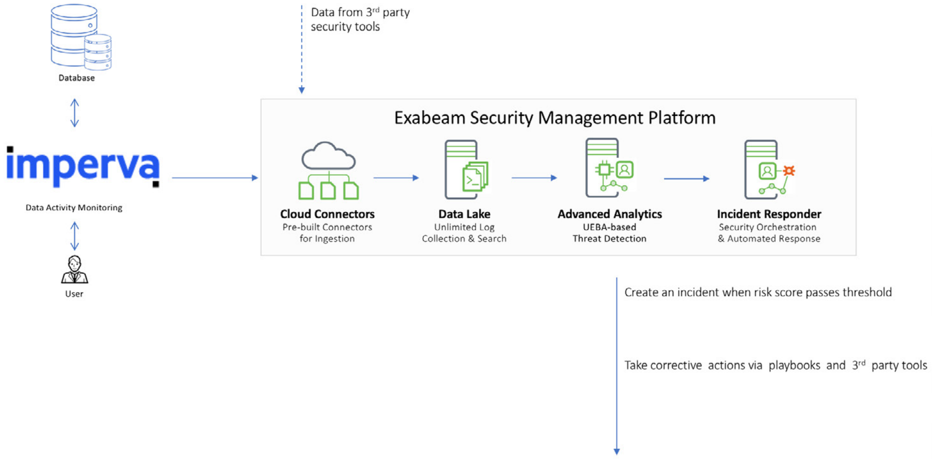
Reduce human error and response times with pre-built, out-of-the-box playbooks that automate and standardize incident response actions including threat containment, investigation and mitigation. Exabeam's existing third party integrations lets analysts employ pre-defined containment actions, such as those with identity access and privileged access management providers, to take corrective steps like suspend user access or prompt for re-authentication to restrict database access.

> "In the digital transformation era, companies are storing more sensitive data than ever before. Exabeam and Imperva allow users to understand who, what, where, and when access occurred and focus on anomalous activity warranting further investigation."

CHRIS STEWART, SR. DIRECTOR OF BUSINESS DEVELOPMENT, EXABEAM

TOP USE CASES

Compromised credentials
Data exfiltration
Malicious insider
Compliance reporting


Database
imperva
Data Activity Monitoring
User
Data from 3rd party security tools
Exabeam Security Management Platform
Cloud Connectors
Pre-built Connectors for Ingestion
Data Lake
Unlimited Log Collection & Search
Advanced Analytics
UEBA-based Threat Detection
Incident Responder
Security Orchestration & Automated Response
Create an incident when risk score passes threshold
Take corrective actions via playbooks and 3rd party tools

EXABEAM ANALYZES IMPERVA DATA ACTIVITY MONITORING DATA GIVING SECURITY TEAMS GREATER CONFIDENCE IN IDENTIFYING SUSPICIOUS DATA EVENTS AND THREATS.

HOW IT WORKS

- Imperva monitors all database activity across a variety of environments to identify anomalous behavior.
- Exabeam ingests the event log, and data activity monitoring data from Imperva. Exabeam parses, normalizes and enriches the data with context from your environment.
- Exabeam parses, normalize, and enriches the data with context from your environment and then performs behavioral analytics to automatically detect deviations from those behavioral baselines. Anomalous activity is assigned a risk score and added to the relevant user or device for each incident detected.
- Concurrently, Exabeam Smart Timelines stitch together Imperva DAM data with third party security solution data to create machine-built incident timelines for rapid threat investigation
- When user risk scores surpass a pre-defined risk threshold, security teams can use automated response playbooks to automatically trigger predefined containment actions (suspending user access, rotating credentials, or prompting for re-authentication via 2-factor/multi factor push) to restrict database access using Exabeam integrations with third party identity access management or privileged access management solutions.

exabeam

ABOUT IMPERVA

Imperva is an analyst-recognized, cybersecurity leader on a mission to protect customers' digital assets by accurately detecting and effectively blocking incoming threats, and empowering customers to manage critical risks, so they do not have to choose between innovating for their customers and protecting what matters most.

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures.

Exabeam is continuously adding new integrations with best of breed security vendors to its offering. These integrations are included as part of the solution at no additional cost, supporting organizations as they expand their security ecosystem, and providing peace of mind that Exabeam integrations will support your unique environment as it evolves over time. For more information, visit https://www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.