exabeam

SOLUTION BRIEF

EXABEAM AND CYBERARK

Behaviorally Analyze Privileged Access Security Data for Efficient, Accurate Threat Identification, Investigation and Response

PRIVILEGED ACCOUNTS A PRIME TARGET FOR ATTACKERS

Privileged accounts, and the sensitive access they provide, represent a major security vulnerability for organizations. In the wrong hands, privileged access can be used to take over and disrupt an organization's IT environment, steal sensitive information, or commit financial fraud with the potential to cause irreparable damage by damaging critical systems. While privileged access security (PAS) solutions provide rich insights into privileged users' permission levels, application access and activity, security teams can identify, investigate and block threats more efficiently by collecting and behaviorally analyzing PAS data in combination with a broad set of data from other security solutions.

Exabeam's user and entity behavior analytics (UEBA) solution uses behavioral modelling of users, peer groups, and other tools 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

CYBERARK®

choice. The powerful combination of Exabeam and privileged access security provider, CyberArk, helps bridge the gap between PAS and other security and IT infrastructure tools as part of a modern security management strategy looking to take a risk-based approach to cyber-security.

IDENTIFY SUSPICIOUS AUTHENTICATION ATTEMPTS AND UNUSUAL ACTIVITY

The Exabeam integration with CyberArk allows security professionals to monitor privileged access and application activity across the enterprise, including on-premise, hybrid, and cloud environments, and analyze it in the context of baseline user and device behavior. Security teams can rapidly identify anomalous behavior such as suspicious authentication attempts, including logins from unfamiliar locations, or unusual application activity. By bringing together

normal and abnormal behaviors for users and devices, with their surrounding context, Exabeam's machine-built incident timelines automate the manual process of gathering evidence and assembling a timeline, resulting in significant time savings for incident investigation and threat hunting. When combined with the core capability of CyberArk to generate risk scores for each privileged session, security and operations teams can quickly identify the activities that present the most risk to the organization. Incident response playbooks automate response to ensure timely and consistent action reducing human error and further increasing productivity of security staff.

INTEGRATION BENEFITS

COLLECT

Collect an unlimited amount of privileged account access and application activity data from other security solutions using a flat, predictable pricing model. This data enables the analysis of advanced threats including privileged account access, lateral movement, and insider threats, without large unpredictable logging bills.

DETECT

Baseline normal activity for all privileged accounts using CyberArk data including anomalies identified by CyberArk Core Privileged Access Security that may indicate a security compromise. Behaviorally analyze PAS data from cloud, hybrid or on-premise application access activity, in addition to data from a wide assortment of third-party security and infrastructure tools, to detect suspicious activity and provide automated remediation actions focusing on the most critical or anomalous activities within the network.

> "The combination of CyberArk and Exabeam provides joint customers a powerful tool to effectively combat insider threats of all types, including those involving privileged credentials."
>
> **CHRIS STEWART, SR. DIRECTOR OF BUSINESS DEVELOPMENT, EXABEAM**

INVESTIGATE

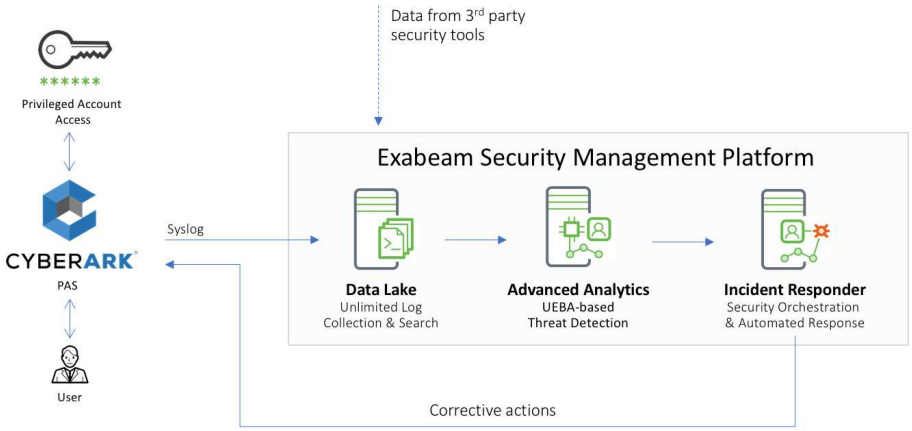
Dramatically reduce the time analysts spend investigating incidents including attacks not seen before. Exabeam Smart Timelines automate the manual assembly of evidence from multiple, disparate systems, including suspected incidents uncovered by CyberArk, into machine-built incident timelines that accurately pinpoint anomalous events and improve productivity while significantly reducing response time.

RESPOND

Reduce human error and incident response times with pre-built or user generated playbooks and policies that automate and standardize incident response actions including enabling/disabling users or rotating account credentials.

TOP USE CASES

- Misuse of credentials
- Anomalous access or activities
- Unmanaged privileged access
- Privilege escalation
- Malicious or compromised user detection



CYBERARK DATA IS INGESTED INTO EXABEAM FOR ANALYTICS-BASED INCIDENT DETECTION AND PRIORITIZATION. NOTABLE USERS ARE AUTOMATICALLY SENT BACK TO CYBERARK FOR CORRECTIVE ACTION.

HOW IT WORKS

- CyberArk Privileged Access Security monitors privileged user account access and application activity.
- Exabeam ingests privileged user account access and application activity along with log data from CyberArk's API and analyzes it alongside data from other security and context sources.
- Exabeam uses behavioral analytics to parse, normalize, and enrich the data with context from your environment and then automatically detects deviations from those behavioral baselines. This anomalous activity is assigned a risk score and added to the relevant user or device for each incident detected.
- Concurrently, Exabeam stitches together CyberArk data with third party security solutions' data to create machine-built incident timelines for rapid threat investigation.
- When user risk scores surpass a pre-defined risk threshold, your security team can use automated response playbooks to employ predefined containment actions through CyberArk including automatic credential rotation, unmanaged account onboarding and session suspension and/or termination.

exabeam

ABOUT CYBERARK

The CyberArk Privileged Access Security Solution provides a comprehensive approach to securing privileged access on-premises and in the cloud, from every endpoint and application, and throughout the DevOps pipeline. A global leader in privileged access security, CyberArk delivers the industry's most complete solution to reduce risk created by privileged access across the enterprise. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, to protect against external attackers and malicious insiders.

ABOUT EXABEAM

Exabeam empowers enterprises to detect, investigate and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. With Exabeam, 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 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.

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