exabeam

SOLUTION BRIEF

EXABEAM AND OKTA

Leverage Identity Analytics for Adaptive Authentication Using Exabeam and Okta

THE CHALLENGE OF CATCHING COMPROMISED CREDENTIAL ATTACKS

Attackers often use stolen user credentials to gain access to enterprises' critical data when committing breaches. Even though the risk of data breaches continues to grow, many organizations still struggle with credential-based threats, because they aren't using a security solution that closes the gap between identity management and security controls.

Identity and access management (IAM) solutions are valuable tools for collecting rich insights into users' authentication and access activities, but they aren't sufficient for identifying the larger universe of risks, on their own, because they don't offer a complete picture of threats. Security teams need to analyze identity data in conjunction with information from other security solutions including servers, endpoints, badge readers and cloud services in order to collect, detect, investigate and respond to suspicious activity.

Exabeam's user and entity behavior analytics (UEBA) solution uses behavioral modelling of users, peer groups and other tools to automatically baseline normal activity and detect anomalous behaviors indicative of a threat – across all your security solutions of choice. The powerful combination of Exabeam and Okta uses behavior to bridge the gap between IAM and other security and IT infrastructure tools as part of a modern security management strategy. The integration between Exabeam and Okta also extends security monitoring and controls to ensure uniform scrutiny across cloud services, on-premise systems and mobile applications.

okta

MONITOR ACCESS AND AUTHENTICATION ACTIVITY ACROSS YOUR ORGANIZATION

Using Okta identity context and authentication data, Exabeam monitors account access and authentication activity across your enterprise and analyzes it in the context of user behavior to identify suspicious authentication attempts including multiple password reset requests, logins from unusual locations or compromised accounts.

Machine-built incident timelines bring together normal and abnormal behaviors for users and devices, giving SOC analysts a unified perspective to quickly and efficiently analyze and respond to threats using incident response playbooks that ensure timely and consistent action. The Exabeam-Okta integration also gives security teams the option of using multiple automated containment responses through Okta Adaptive Multi-Factor Authentication, thereby increasing productivity and extending stretched security resources.

INTEGRATION BENEFITS

COLLECT

Collect unlimited Okta identity and security data for threat detection and eliminate unpredictable volume-based expenses with Exabeam's flat pricing model. Analyze data from all your sources without being forced to choose, based on your budget, which ones to import into Exabeam. Combine Okta identity data with other security and infrastructure data sources for analysis and centralized compliance reporting.

DETECT

Behaviorally analyze IAM data from account and application access activity in conjunction with other security and infrastructure solutions to detect anomalous activity. Generate behavioral baselines unique to your organization using Okta Identity Cloud data and automatically identify threats with a higher degree of confidence using Exabeam user and entity behavioral analysis and risk scoring – even for attacks that have never been seen before.

INVESTIGATE

Dramatically reduce the time analysts spend investigating incidents with Exabeam Smart Timelines that automate the manual assembly of data from multiple, disparate systems. Accurately pinpoint anomalous events and improve productivity while significantly reducing response time.

> "Identity Analytics, the combination of powerful machine learning-based analytics and identity access management, provide joint Exabeam and Okta customers with a formidable weapon to combat today's most challenging cyber threats."
>
> CHRIS STEWART, SR. DIRECTOR OF BUSINESS DEVELOPMENT, EXABEAM

RESPOND

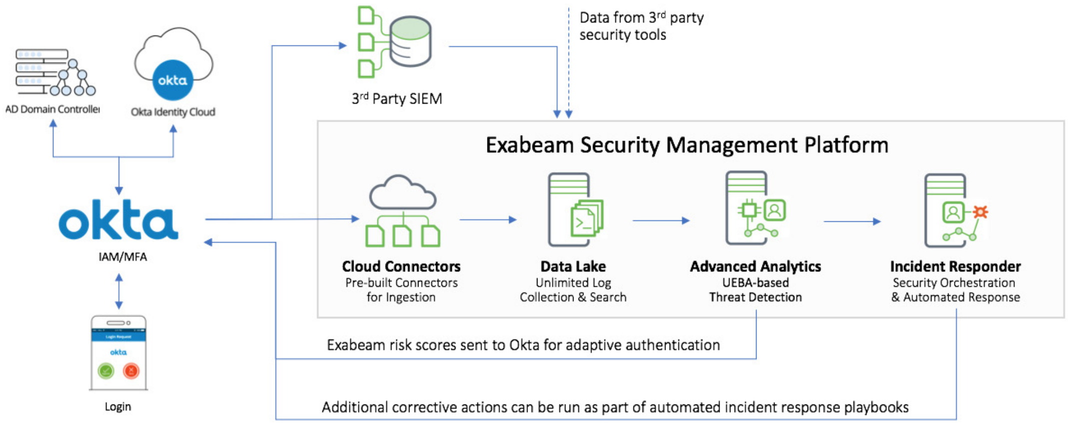
Reduce human error and boost response productivity with pre-built playbooks that automate and standardize actions, including threat containment, investigation, mitigation and response to take corrective actions specific to the Exabeam-Okta integration.

TOP USE CASES

- Adaptive/step-up authentication
- Identity analytics
- Compromised credentials

Analysts can run seven actions in Okta directly from Exabeam including:

- Get User Information
- Add User to Group
- Remove User from Group
- Reset Password
- Suspend User
- Unsuspend User
- Send 2FA Push


AD Domain Controller
Okta Identity Cloud
okta
okta
IAM/MFA
Login
3rd Party SIEM
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
Exabeam risk scores sent to Okta for adaptive authentication
Additional corrective actions can be run as part of automated incident response playbooks

OKTA IDENTITY CONTEXT AND AUTHENTICATION DATA IS INGESTED INTO EXABEAM FOR ANALYTICS-BASED THREAT DETECTION. RISK SCORES FOR NOTABLE USERS ARE SENT TO OKTA FOR AUTOMATED STEP-UP AUTHENTICATION OR OTHER CORRECTIVE ACTION.

HOW IT WORKS

- Okta Identity Cloud monitors user account and application access activity
- Using Okta's API, Exabeam ingests Okta user account and application access data and security alerts. Exabeam parses, normalizes, and enriches the data with context from your environment.
- Logs are sent to Exabeam Data Lake for unlimited log collection and search and then ingested into Advanced Analytics for behavioral analysis-based threat detection.
- Exabeam baselines normal user and endpoint activity using UEBA and then automatically detects deviations from those behavioral baselines.
- Risk is added to the relevant users and entities for each anomalous activity detected.
- Concurrently, Exabeam stitches together Okta 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, Exabeam initiates a response by prompting the Okta Adaptive Multi-Factor Authentication to verify the user. If the user validates their account, the incident is closed. If not, security teams can define several containment actions through Okta using SOAR integrations such as disabling the account, reducing the user's access, adding the user to a watch list, revoking user credentials and/or sending an email alert to the SOC team.
- Response playbooks in Exabeam Incident Responder, a SOAR solution, include seven pre-built actions specific to the Okta integration such as getting user information, adding or removing users, resetting passwords, suspending/unsuspending users, and sending two-factor (2FA) notifications to your Okta analysts using Okta and other security and infrastructure tools.

exabeam

ABOUT OKTA IDENTITY CLOUD

The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business.

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.