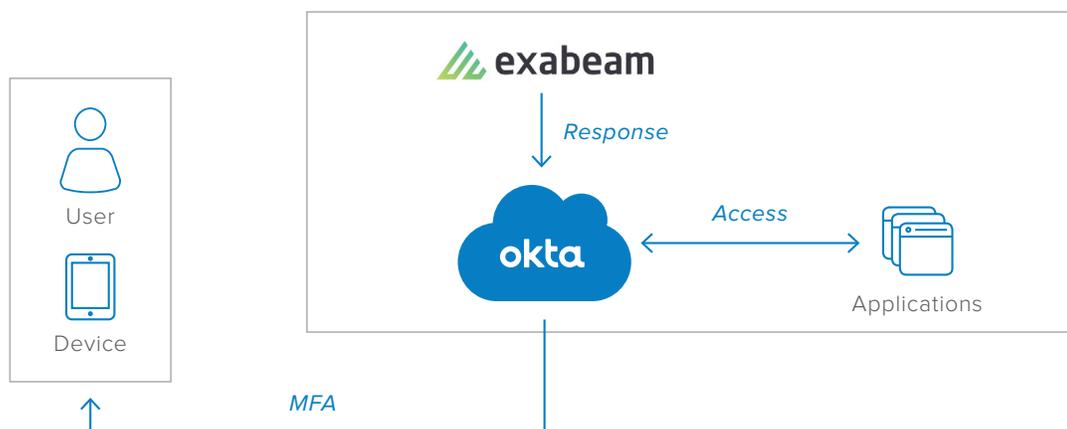# okta + exabeam

Advanced Detection and Response for Identity-Based Threats

SecOps teams are tasked with the mission-critical job of resolving security alerts to keep the enterprise safe. But triaging credential-based attacks—by far the most common threat vector for data breaches—can be a manual and inexact process. To effectively respond to credential-based attacks, you need a sophisticated, orchestrated security solution. Okta has now partnered with Exabeam to quickly identify and remediate compromised user accounts, to empower your SecOps team to stay ahead of the bad guys.

Okta, the leading independent provider of identity for the enterprise, deeply integrates with Exabeam, the next-generation SIEM company, to offer a powerful, identity-driven security solution to keep your enterprise safe. The Okta Identity Cloud supplies rich user data, which Exabeam's Security Intelligence Platform indexes to create a detailed baseline of user behavior. Exabeam's detects anomalies from this baseline, indicating suspicious account behavior, and then coordinates with Okta to remediate against the compromised account by prompting for Okta MFA or moving the user to a higher-risk group in Okta.

Okta + Exabeam join forces to provide user-based security detection, analysis and response.

- Gain deep insights into user activity informed by broad visibility across your environment

- Quickly spot suspicious account behavior with advanced behavior modeling and analytics

- Remediate credential-based threats immediately via an adaptive response framework

Okta provides:

- Rich identity context based on user attributes and authentication activity from Okta

- Okta Adaptive MFA to verify authorized users and remediate against threat actors

- Powerful APIs that enable flexible enforcement based on risk scores (for example, killing the session for low-risk groups or suspending accounts for high-risk groups)

Exabeam provides:

- A consolidated Data Lake to compile security logs, evaluated by Advanced Analytics intelligence to parse suspicious activity from baseline behavior

- Quick, intelligent threat remediation through Exabeam Incident Responder

- End-to-end collection, detection and response capabilities from a single platform

An effective, automatic response

Okta + Exabeam integrated together lets you collect a comprehensive baseline of user behavior across your environment, deeply informed by Okta's contextual identity information. Exabeam stores and indexes aggregated security logs, adding authentication activity and user context from Okta. Then after forming a baseline of user behavior, Exabeam uses incident timelines and a risk engine to detect true threats.

Okta can then take action against the affected user account by applying policy-based enforcement measures, such as prompting for step-up auth, killing a session, or suspending an account altogether. The result is a complete view of security events across your entire environment, contextualized with user identity information, in a unified security management system that detects suspicious from normal behavior, surfaces real alerts instantly to your team's attention with clarifying contextual data, and initiates automated remediation measures where appropriate.

With Okta + Exabeam working together, your company will be able to:

- Arm your SOC with best-in-breed user intelligence, analytics, and response capabilities

- Gain deep insights into account activity and a comprehensive understanding of security events

- Spot and prioritize suspicious user behavior of all kinds from the moment it emerges

- Respond with automated, policy-based remediation processes

For more information on this integration, go to okta.com/partners/exabeam.
If you have more questions, please contact our sales team at okta.com/contact-sales.