Exabeam and Vectra AI

Uncover Hidden Threats With AI-Driven Detection and Response

Executive Summary

Security teams use network detection and response (NDR) to detect and contain post-breach activity such as ransomware, insider threats, and lateral movement. Unlike traditional rule-based tools, NDR uses heuristic and behavioral modeling to detect unusual activity. It complements other security operations center (SOC) tools like security orchestration, automation and response (SOAR); security information and event management (SIEM); endpoint detection and response (EDR); and managed detection and response (MDR) by identifying threats that evade signature-based detection.

The Exabeam New-Scale Security Operations Platform uses AI and automation to unify threat detection, investigation, and response (TDIR). By integrating with Vectra AI, you gain deeper visibility across cloud environments, consolidating data and improving situational awareness.

Market Challenge

Security teams struggle to detect advanced threats that move laterally across cloud environments. Tools built for on-premises detection often miss these signals, leaving gaps in visibility and response.

Complete Threat Detection, Investigation, and Response

The New-Scale Platform combines SIEM, user and entity behavior analytics (UEBA), and automated workflows to give you full visibility into threats across your environment. Its cloud-native design supports rapid data ingestion, lightning-fast queries, and automated investigations—empowering analysts to detect, investigate, and respond faster and more accurately.

The integration with Vectra AI strengthens these capabilities by enabling log ingestion and automated response actions. Exabeam ingests Vectra AI's

Key Integration Benefits

- → **Faster threat detection by consolidating security data and automating workflows across tools**
- → **Stronger visibility into network-based risks across your cloud infrastructure**
- → **Streamlined operations through prebuilt mappings, a preconfigured Vectra AI tile, and webhook collectors**

network detections and enriches them with UEBA and correlation, helping SOC teams spot attacker behavior early, understand it faster, and act decisively. Built-in low-code and no-code SOAR capabilities in Exabeam Automation Management allow security teams to build, test, and deploy playbooks that automate containment, ticketing, and incident triage.

Together, Exabeam and Vectra AI simplify security operations, reduce manual work, and improve cloud security posture so your team can focus on what matters: stopping threats before they escalate.

Top Use Case: Situational Awareness

- **Definition:** The ability to quickly understand your current threat landscape, identify risks, and measure how well your defenses are working.
- **Challenge:** Without centralized visibility, analysts must manually pivot between Vectra AI, Exabeam, and other tools—slowing response times.
- **Solution:** Ingest Vectra AI network detections into Exabeam to see cloud threats from one console. Track investigations and remediation in real time.

Integration Overview

Integrated Product: New-Scale Security Operations Platform (sold as Exabeam Fusion)

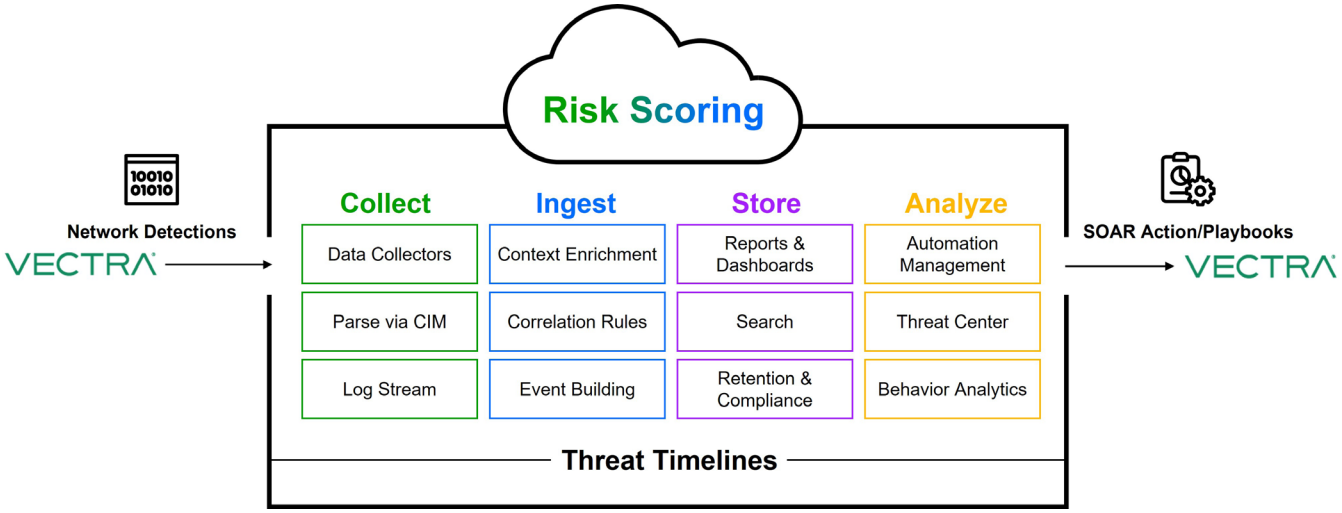

Figure 1. Vectra AI data flows into Exabeam and is enriched with behavioral context for UEBA and correlation-based threat detection and prioritization. Automation Management allows custom notification and sends webhooks back to Vectra AI systems.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at
www.exabeam.com →

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

2025 Exabeam, LLC. All rights reserved.