exabeam®

Detect
Defend
Defeat™

Eliminate your blindspots and respond to threats faster and more accurately with Exabeam.

Welcome to New-Scale SIEM™

Exabeam can help you detect, investigate, and respond more quickly and accurately to threats and mitigate damage.

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM for advancing security operations. Built for security people by security people, we reduce business risk and elevate human performance.

The powerful combination of our **cloud-scale security log management, behavioral analytics, and automated investigation experience** gives security operations an unprecedented advantage over adversaries including insider threats, nation states, and other cyber criminals.

We understand normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more at exabeam.com →

Products

Exabeam Security Log Management

Cloud-scale log management to ingest, parse, store, and search log data with powerful dashboarding and correlation.

Exabeam SIEM

Cloud-native SIEM at hyperscale with fast, modern search, and powerful correlation, reporting, dashboarding, and case management.

Exabeam Fusion

New-Scale SIEM, powered by modern, scalable security log management, powerful behavioral analytics, and automated threat detection, investigation, and response.

Exabeam Security Analytics

Automated threat detection powered by user and entity behavior analytics (UEBA) with correlation and threat intelligence.

Exabeam Security Investigation

Threat detection, investigation, and response powered by user and entity behavioral analytics, correlation rules, and threat intelligence, supported by alerting, incident management, automated triage, and response workflows.

Exabeam Security Operations Platform

One cloud-native platform, five all-new products: Exabeam Security Log Management, Exabeam SIEM, Exabeam Fusion, Exabeam Security Analytics, and Exabeam Security Investigation.

Common Information Model (CIM)
Provides a schema to simplify the normalization, categorization, and transformation of raw log data into actionable events in support of security use cases.

Threat Intelligence Service
Available on all products at no additional cost, ingests multiple commercial and open source threat intelligence feeds, then aggregates, scrubs, and ranks them every 24 hours, using proprietary machine learning algorithms to produce a highly accurate, up-to-date stream of IoCs.

Outcomes Navigator
Maps the feeds and parsing against the most common security use cases, suggesting ways to improve coverage.

Service Health and Consumption
Dashboards show uptime and health of all your log parsers, applications, data flow, and connections, as well as your total license volume consumption to help with long-term storage and capacity planning.

Product Features

Cloud-scale Security Log Management

Collectors
A single interface to securely configure, manage, and monitor the transport of data from thousands of on-premises, cloud, and context sources into the Exabeam service.

Log Stream
A central console enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features.

Correlation Rule Builder
An intuitive UI to write, test, publish and monitor up to 1,000 custom rules.

Search
A simplified search experience with faster query and instant results over petabytes (PB) and years of data; search hot and cold data at the same speed.

Powerful Behavioral Analytics

Advanced Analytics
Automated UEBA with over 1,800 rules, including cloud threat detection, and over 750 behavioral models to baseline normal behavior of users and devices with histograms to detect, prioritize, and respond to anomalies based on risk.

Alert Triage
Automates both Exabeam and third-party alert prioritization, offering dynamic alert prioritization to filter views by high priority, low priority, observational, or all alerts.

Anomaly Search
A single interface to search for Exabeam-triggered anomaly events in the data repository across a variety of different objects such as sessions, rules, users, assets, MITRE TTPs, anomaly identification, and cases.

Automated Investigation Experience

Alert and Case Management
Centralizes events and alerts sourced from Exabeam and/or third-party products, letting an analyst review alerts individually or at volume — or set conditions to automate the alert triage workflow and escalate events and alerts into incidents.

Turnkey Playbooks
Automate repeated workflows with playbook response actions. Includes granular options such as semi-automation (i.e., running at the push of a button) or full automation.

Incident Responder
Allows analysts to orchestrate and automate repeated workflows to 100 third-party products with 576 actions and operations, from semi to fully-automated activity.

exabeam

Comprehensive Threat Detection, Investigation and Response (TDIR) for Successful Outcomes

Automation

Exabeam automates manual and repetitive tasks

Based on a Ponemon research study, SOC teams spend 12% of their time on detection, 36% on triage, 26% on investigation, and 26% on response.

Yet most cybersecurity vendors provide security analytics that only automates the Detection and Response parts of the workflow.

Exabeam automates everything that the SOC needs from detection to triage to investigation and response.

- Automation helps improve security teams' productivity at every phase of their workflow, not just response.
- Automation assists with detection, triage, and investigation where analysts spend 74% of their time.
- With automation, even junior analysts can make decisions. Advanced hunters can still query raw logs.

Use Cases

Use case-based content for successful outcomes

Industry analysts such as Gartner and Forrester have recognized the need for pre-built content as part of a successful security strategy.

Exabeam allows security teams to achieve repeatable outcomes and improve their defense against **compromised insiders, malicious insiders**, and **external threats**, as well as meet **compliance** requirements.

Exabeam offers:

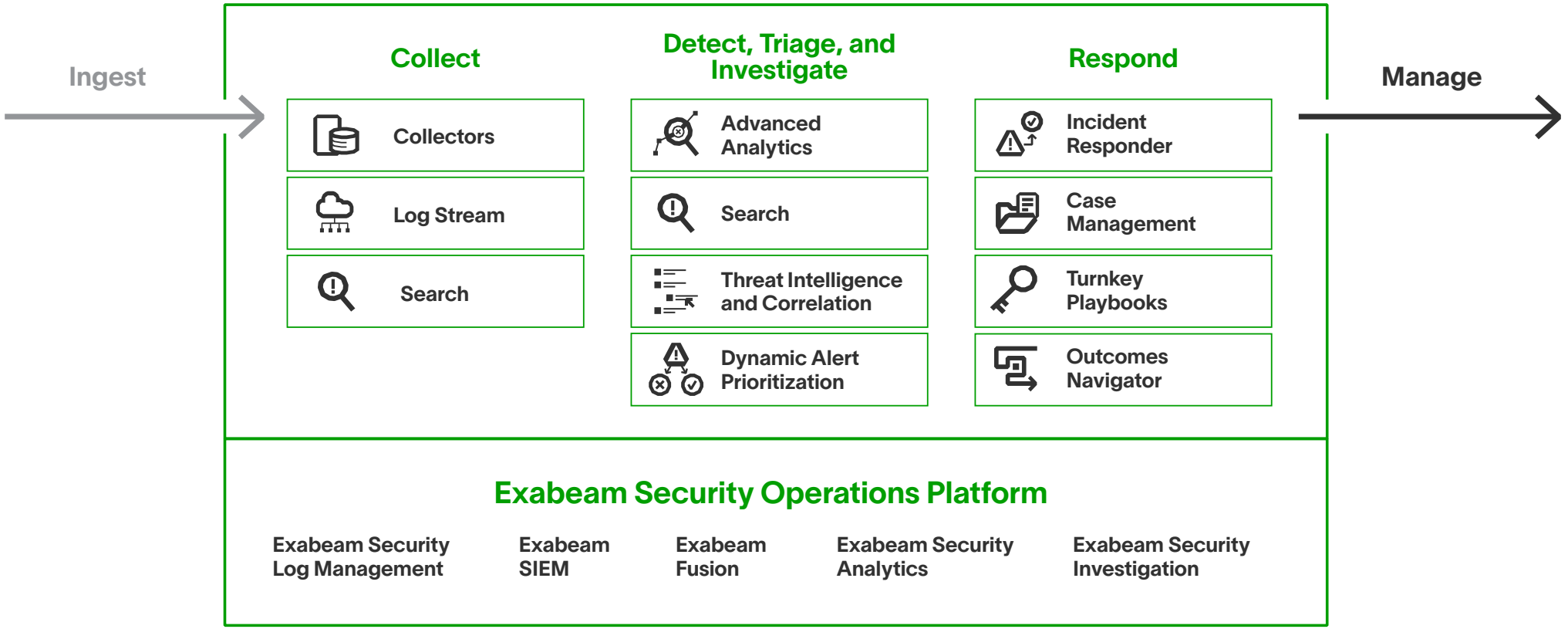
- Automatic threat intelligence enrichment with pre-built correlation rules
- Use case content and features for each stage of the analyst workflow, not just detection
- Outcomes Navigator to show current MITRE coverage and recommend potential new log sources

SOC STEPS	TIME SPENT	EXABEAM SOLUTION	VALUE
Collection		Collectors	• Common Information Model (CIM) • Collection from 200+ on-premises products, 34 cloud-delivered security products, 11 SaaS productivity applications, and 21 cloud infrastructure products • 7,937 log parsers • Log Stream
Detection	12%	User and Entity Behavior Analytics (UEBA)	• 750+ behavior-based detection models • 1,800+ fact-based correlation rules • MITRE mapping
Triage	36%	Alert Prioritization	• Dynamic Alert Prioritization • Correlation Rule Builder • Threat intelligence enrichment
Investigation	26%	Automated Incident Timeline Creation	• Prebuilt incident timelines for all entities • Outcomes Navigator
Response	26%	Security Orchestration, Automation, and Response (SOAR)	• Turnkey Playbooks • Automated incident workflows for 65 vendors, 100 products, and 567 operations • Case management with incident checklists

Advancing Security Operations

Modular and cloud-native platform to augment or replace a legacy SIEM.

The Exabeam Security Operations Platform is modular and delivered as a cloud-native solution or through a managed security service provider (MSSP). Whether you replace a legacy product with a New-Scale SIEM, or complement an ineffective SIEM solution by adding the industry's most powerful UEBA and automation to it, the Exabeam Security Operations Platform can help you achieve security operations success.



exabeam

Why Exabeam

Successfully used by customers across the globe

> **Directly mapping common security use cases to response workflows is critical for SecOps success."**

Marc Crudgington

CISO, SVP Information Security

WOODFOREST NATIONAL BANK

> **We've strengthened our processes with workflows that have helped our team become far more effective as a result of the Exabeam partnership. Our team members can now ask the critical questions connecting security to business function."**

Lindbergh Caldeira

Cyber Security Operations Manager

SA Power Networks

> **Technologically advanced companies like Exabeam allow us to better understand the truly anomalous user behavior that matters to our business. The value is in being able to maximize our efficiency at analyzing events that could pose a threat to our clients' businesses."**

Jorge Castañeda

Corporate General Manager

SecureSoft
Powerful Intuitive Cybersecurity

> **We put Exabeam to the test by giving them an aircraft log. They were able to turn it around in 48 hours. That was a significant use case for us, it had significant savings attached to it. Exabeam was able to resolve logs for us within hours, as opposed to months or years. We deployed Exabeam as our SIEM and we haven't looked back."**

Deborah Wheeler

CISO

DELTA

Analysts and Recognition

Recognized for leadership and innovation

Select Awards and Recognition

Gartner

2022 Gartner® Magic Quadrant™

Leader

Our vision to build a cloud platform that improves threat detection, incident investigation, and response for security ops and insider threat teams is making a real-world impact. Gartner agreed and named Exabeam a Leader in the 2022 Magic Quadrant for SIEM.

For more information, visit www.exabeam.com

exabeam

For more information and to learn about our products, visit www.exabeam.com