Exabeam SIEM

AI-powered, cloud-native SIEM for fast, modern search, dashboarding, and coordinated response from a single workbench

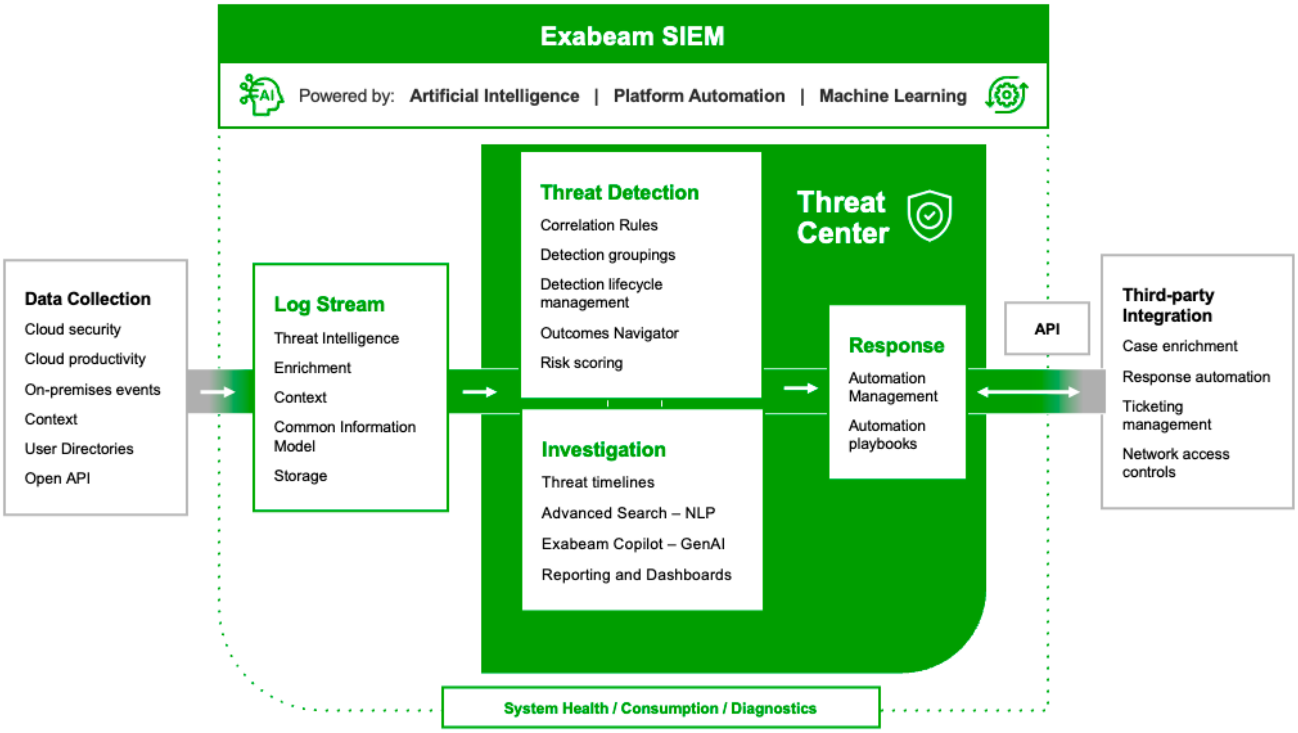
Logging data within an IT environment is a critical component of every enterprise security strategy. Every sensor, detection product, or feed required to support security use cases in a SIEM system drives the collection of more data, often into terabytes per day. With growing volumes of data and limited time to detect, investigate, and respond to threats, log collection, correlation building, investigation, and response need to be simple and efficient.

Cloud-native security log management, pre-built and customizable correlation, and case management

Exabeam SIEM is a cloud-native solution that aggregates cloud, on-premises, and third-party party log data, then normalizes it for better threat detection, investigation, and response (TDIR). Exabeam SIEM gives you a massively scalable view of your environments in real time.

Exabeam SIEM combines security log management with TDIR capabilities, providing a centralized workbench for investigation and response. It also offers more than 180 pre-built correlation rules, integrated threat intelligence feeds for improved event context and detection, and powerful dashboarding capabilities. The solution equips analysts with unparalleled speed, consistently processing over 2 million events per second (EPS).

Threat Center is integrated into Exabeam SIEM to facilitate TDIR. Threat Center improves analyst productivity with automated evidence collection, event tagging, notes, and a ticketing system specifically designed for security. For organizations in need of extended storage time, Exabeam SIEM is designed to easily scale, offering expanded cloud storage capabilities like long-term search, long-term storage, and dashboard visualizations to accommodate those requirements. Threat Center features Exabeam Copilot, a generative AI capability that accelerates the training of security analysts, facilitates risk communication with detailed threat explanations, and deepens threat understanding through a security-centric large language model (LLM). Through natural language processing (NLP), analysts and engineers can effortlessly create complex search queries in almost any language, bypassing the need for advanced programming knowledge. Exabeam Copilot uplevels security expertise for faster, more precise TDIR.



Exabeam SIEM

Powered by: **Artificial Intelligence** | **Platform Automation** | **Machine Learning**

Data Collection
- Cloud security
- Cloud productivity
- On-premises events
- Context
- User Directories
- Open API

Log Stream
- Threat Intelligence
- Enrichment
- Context
- Common Information Model
- Storage

Threat Center

Threat Detection
- Correlation Rules
- Detection groupings
- Detection lifecycle management
- Outcomes Navigator
- Risk scoring

Investigation
- Threat timelines
- Advanced Search – NLP
- Exabeam Copilot – GenAI
- Reporting and Dashboards

Response
- Automation Management
- Automation playbooks

API

Third-party Integration
- Case enrichment
- Response automation
- Ticketing management
- Network access controls

System Health / Consumption / Diagnostics

Intelligent data ingestion using a Common Information Model (CIM)

An average enterprise security stack consists of at least 45 security solutions, each having its own logs and structures. Typically, different sources have different styles of storing and sending log information; it's important to normalize this data before it can be ingested and analyzed. Exabeam built a CIM to provide a foundational way to parse, store, and view security information from any vendor. Our CIM supports a standard process to create new log parsers which adhere to this model, are easier to maintain, and are less prone to errors and misconfiguration. This standardization also defines extensibility to future-proof new log sources and use cases.

Faster, more accurate TDIR

Security operations teams must coordinate responses, assign duties, and have a central point for handling event investigation through incident response. A defining feature separating a SIEM solution from a security log management system is the ability to sort alerts by severity and combine them into cases and incidents for analysis and resolution. Threat Center centralizes events and alerts sourced from Exabeam and/or third-party products, enabling analysts to review alerts individually or at volume, or set conditions to automate the alert triage workflow and escalate events and alerts into incidents. Threat Center enables analyst teams to create incidents, see events in chronological order, add tags and events to the incident, collaborate across groups and timezones, and customize outcome-driven steps to guide them through to mitigation or resolution. Threat Center provides multiple teams, queues, and tracking for all incidents as they are investigated to completion.

Built on the Exabeam Security Operations Platform

Bringing a cloud-native experience built to scale with your organization, the Exabeam Security Operations Platform allows you to collect and search log data, leverage behavioral analytics to detect attacks, and automate incident response. Visualize the health of your security log feed for every service, log, and application with dashboards showing uptime, health, and data flows. The Exabeam Security Operations Platform supports measurable, continuous, outcomes-focused security posture improvement by recommending information, event stream, and parsing configuration changes to close any common security use case gaps.

Exabeam SIEM helps security teams:

- **Collect, store, and search security event logs and context for TDIR.** Gain visibility across the entire ecosystem with highly scalable, centralized storage and rapid search, without requiring advanced query skills.
- **Simplify the normalization, categorization, and transformation of raw log data.** A common information model (CIM) supports swift threat detection and response, and establishes a standard process to efficiently create and modify log parsers.
- **Threat hunt.** Search on known indicators of compromise (IoCs) and correlated events mapped to use cases and the MITRE ATT&CK® framework.
- **Coordinate response with Automation Management.** Manage event investigation and notification within clicks of discovery.
- **Report on compliance standards.** Gain and export visibility into events required by common compliance standards like PCI, HIPAA, and many more with pre-built dashboards.
- **Close security gaps.** Outcomes Navigator maps data sources against security use cases and ATT&CK tactics, techniques, and procedures (TTPs), along with associated correlation rules and dashboards.
- **Visualize your service health and data consumption.** Monitor the uptime and health of all your log parsers, applications, data flows, and connections, as well as your total license consumption.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. The company was the first to put AI and machine learning in its products to deliver behavioral analytics on top of security information and event management (SIEM). Today, the Exabeam Security Operations Platform includes cloud-scale security log management and SIEM, powerful behavioral analytics, and automated threat detection, investigation, and response (TDIR). Its cloud-native product portfolio helps organizations detect threats, defend against cyberattacks, and defeat adversaries. Exabeam learns normal behavior and automatically detects risky or suspicious activity so security teams can take action for faster, more complete response and repeatable security outcomes.

exabeam®

Detect
Defend
Defeat™

Get a demo →

Speak with an Expert →

Join a CTF →