Exabeam SIEM

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

Security information and event management (SIEM) plays a central role in security operations monitoring, alerting, threat detection, and compliance management. As data volumes, exposure points, third-party alerts, and the cost of talent and storage have multiplied, the speed of SIEM innovation has not kept up.

Every sensor, detection product, or feed required to enable security use cases in a SIEM solution drives the collection of more data, often into terabytes per day. As the window of opportunity to detect and investigate attacks decreases, defenders are left vulnerable if they don't know what to look for. Unfortunately, most SIEM products can't meet this requirement; customers deserve a better approach.

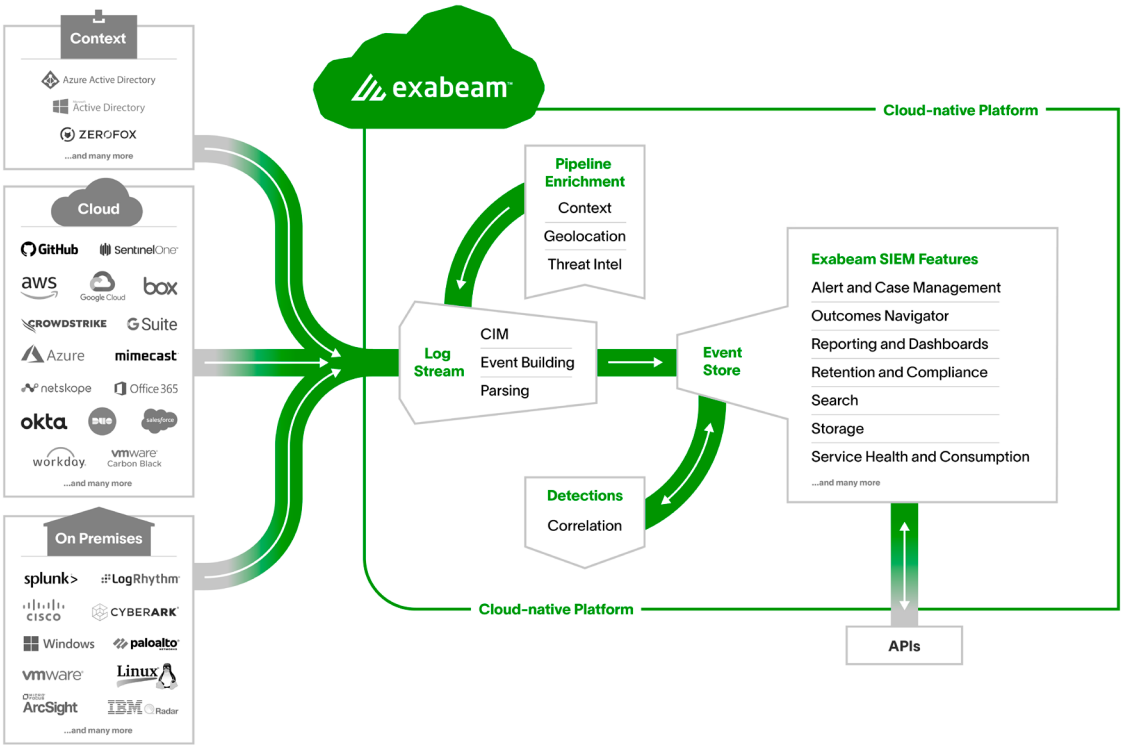
Welcome to New-Scale SIEM™ from Exabeam. New-Scale SIEM is a breakthrough combination of threat detection, investigation, and response (TDIR) capabilities security operations need in products they will want to use. Exabeam SIEM delivers limitless scale to ingest, parse, store, search, and report on petabytes of data — from everywhere.

Pre-built with integrations from 549 security products, with the ability to onboard new log sources in minutes, Exabeam SIEM delivers new speed, processing at more than one million events per second (EPS), and efficiencies to improve their effectiveness. Exabeam SIEM includes everything in Exabeam Security Log Management, plus more than 120 pre-built Correlation Rules, a Correlation Rule builder, and Alert and Case Management. Integrated threat intelligence improves the fidelity of detections, adding deeper context to rules and promoting more accurate and efficient threat management.

Key Features

- Collectors
- Log Stream
- Common Information Model (CIM)
- Search
- Dashboards
- Correlation Rules
- Pre-built Correlation Rules
- Outcomes Navigator
- Threat Intelligence Service
- Service Health and Consumption
- Context Enrichment
- Alert and Case Management
- ATT&CK Coverage

How it works



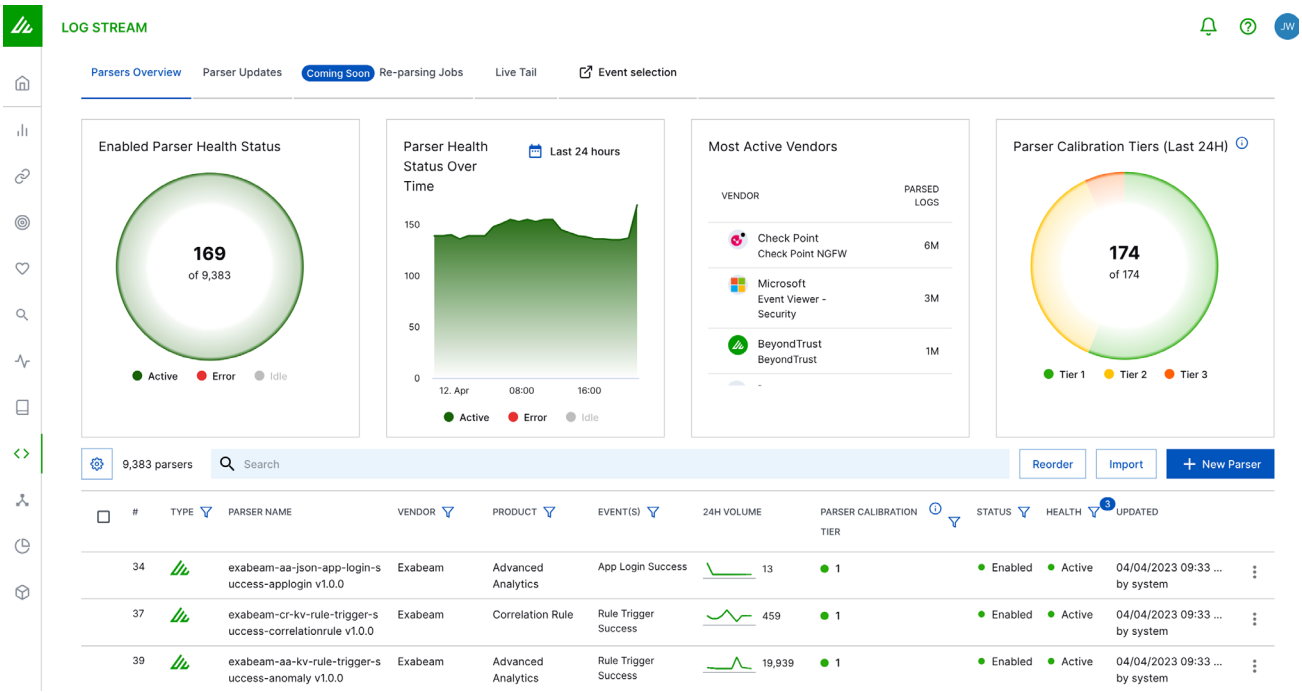
Key Features

Collectors

The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service at scale from on-premises, cloud, and context sources. The platform collects logs and events from 471 products under 56 categories, from more than 250 different vendors, through a variety of transport methods including APIs, collectors, syslog, and log aggregators. To meet the increasing need for cloud security and cloud data collection, Exabeam supports 30+ cloud-delivered security products, 10+ SaaS productivity applications, and 20+ cloud infrastructure products from the three leading cloud infrastructure providers. For context, the platform supports the collection of threat intelligence feeds, geolocation data, user, and asset details.

Inbound Data Source Categories for Log Ingestion Include:

- Authentication and Access Management
- Applications Security and Monitoring
- Cloud Access Security Broker (CASB)
- Cloud Security and Infrastructure (CWP)
- Data Loss Prevention (DLP)
- Database Activity Monitoring (DAM)
- Email Security and Management
- Endpoint Security (EPP/EDR)
- Firewalls (WAF, SWG, Proxy)
- Forensics and Malware Analysis
- Information Technology Service Management (ITSM)
- IoT/OT Security
- Network Access, Analysis, and Monitoring (NDR, IDS, IPS)
- Physical Access and Monitoring
- Privileged Access Management (PAM)
- Risk Management Software
- Security Analytics
- Security Information and Event Management (SIEM)
- Threat Intelligence Platforms
- Utilities/Others
- VPN, ZTNA Servers
- Vulnerability Management (VM)
- Web Security and Monitoring (CWP)



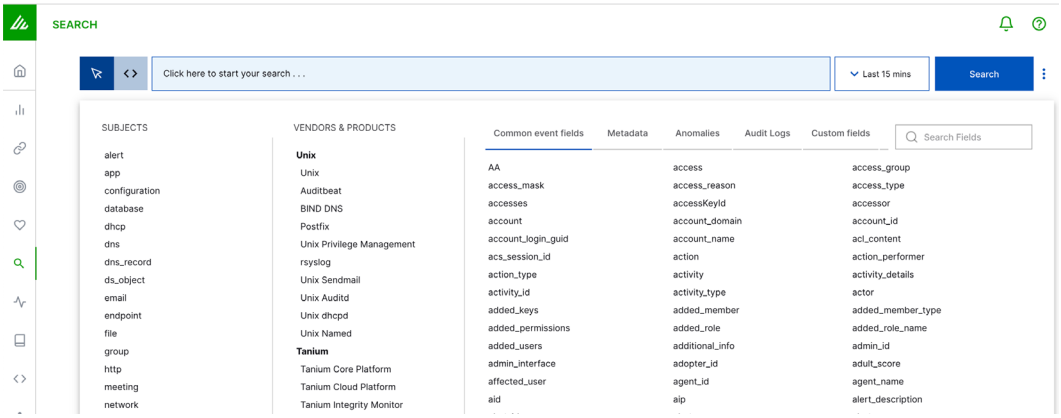
Log Stream

Log Stream delivers rapid log ingestion processing at a sustained rate of more than 1M EPS. A central console enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. As it is ingested, data is parsed using more than 9,000 pre-built log parsers, and enriched using three context collectors from open-source and commercial threat intelligence feeds. Enriched, parsed data is available as security-relevant events for faster performance in search, correlations, and dashboards.

Live Tail provides self-service, real-time monitoring of parser performance, and visibility into the data pipeline, allowing organizations the ability to take immediate action to improve the quality of data ingestion.

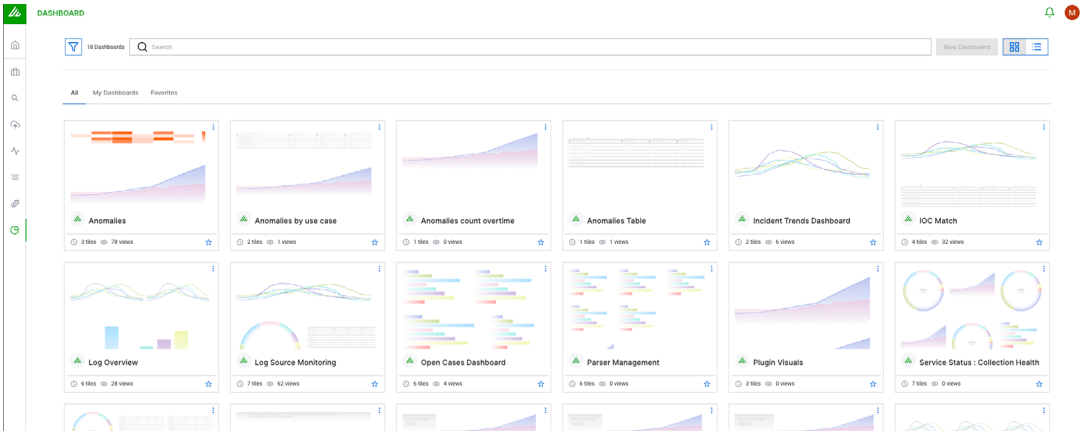
Common Information Model (CIM)

Exabeam built a common information model (CIM) that provides a schema to simplify the normalization, categorization, and transformation of raw log data into actionable events in support of security use cases. The CIM defines the 10 most important fields and 76 subjects used by security experts and specifies them as core, detection, or informational, and includes 395 activity types and two outcomes (specified as success or fail). This process allows organizations to more quickly detect and respond to threats, visualize and report on data, and supports lightning-fast search performance. A robust CIM also establishes a standard process for customers and partners to efficiently create and modify log parsers that are easier to maintain and less prone to misconfiguration.



Search

Search offers a simplified search experience with faster query and instant results over petabytes and years of data; search hot and cold data at the same speed. Search is a single interface that allows analysts to search for events, alerts, strings, or IoCs. The time savings is particularly valuable, as investigations usually entail multiple queries and require that search terms be refined over multiple iterations to obtain the desired results. Moreover, there's no learning curve, meaning analysts aren't required to learn a proprietary query language. Search delivers a query-builder wizard to point and click from a list of intelligent fields to help build effective search queries quickly and easily.

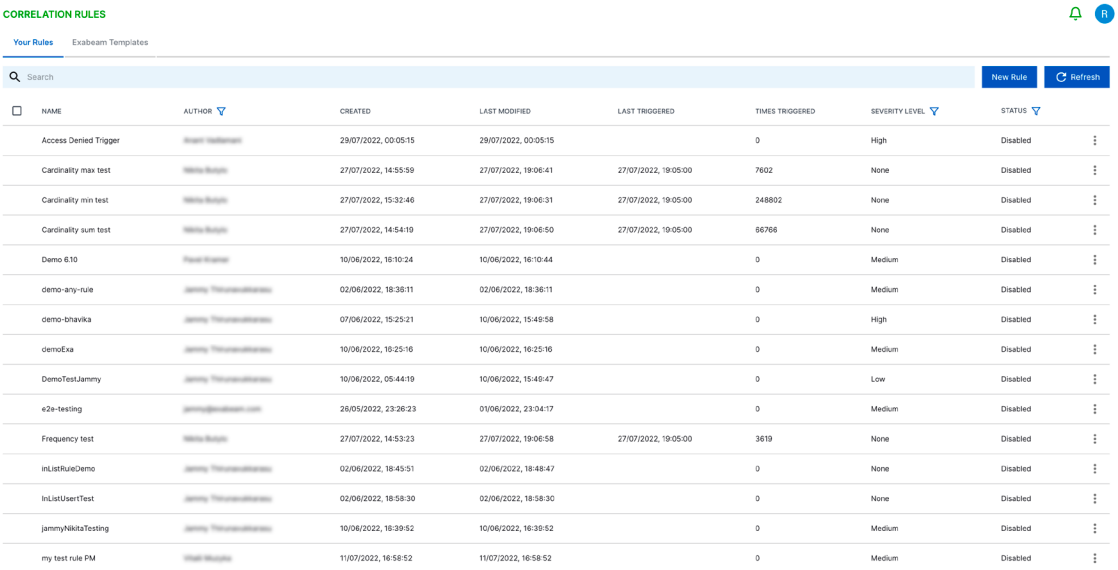


Dashboards

Print, export, or view security event data with 14 pre-built customized reports, or build your own dashboards with 14 different chart types.

The Dashboards app is fully integrated within Exabeam SIEM, allowing you to quickly create powerful visualizations from your parsed log data.

Choose from a variety of options, including bar charts, column charts, line graphs, area charts, pie charts, donut charts, bubble charts, funnels, single values, sankey maps, word clouds, heat maps, tables, and coverage maps. Customize your visualizations to highlight the metrics that matter most for your business needs.



Correlation Rules

Correlation rules define conditions that function as triggers by comparing incoming events with predefined relationships between entities to identify and escalate anomalies. Write, test, publish, and monitor custom correlation rules for your most critical business assets. Define higher priority entities, or add specific Threat Intelligence Service-sourced conditions and assign specific MITRE ATT&CK® tactics, techniques, and procedures (TTPs).

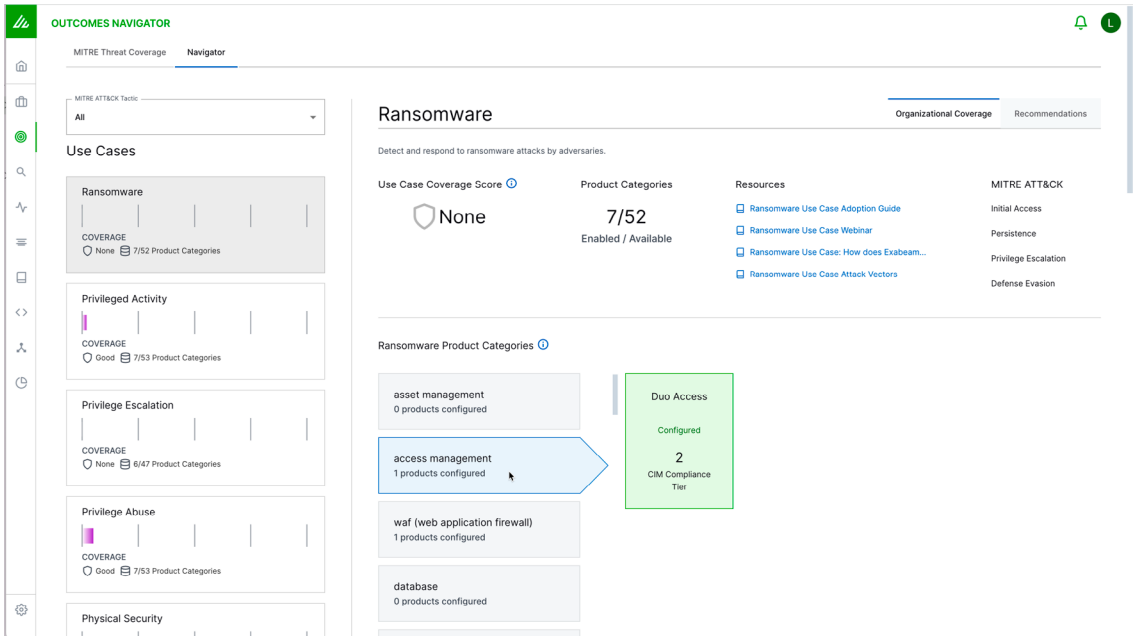
Properly designed Correlation Rules enable enterprises to surface a broad range of abnormal behavior and events.

Correlation Rules builder provides analysts with an easy application to create custom correlation rules suited to their organization's security and use case requirements.

Correlation Rules monitors for well-known threats, identifies compliance violations, and detects signature-based threats using context from the Exabeam Threat Intelligence Service or other third-party threat intelligence.

Pre-built Correlation Rules

Exabeam SIEM offers more than 120 pre-built, fact-based correlation rules and models matching some of the most common use cases of malware and compromised credentials.

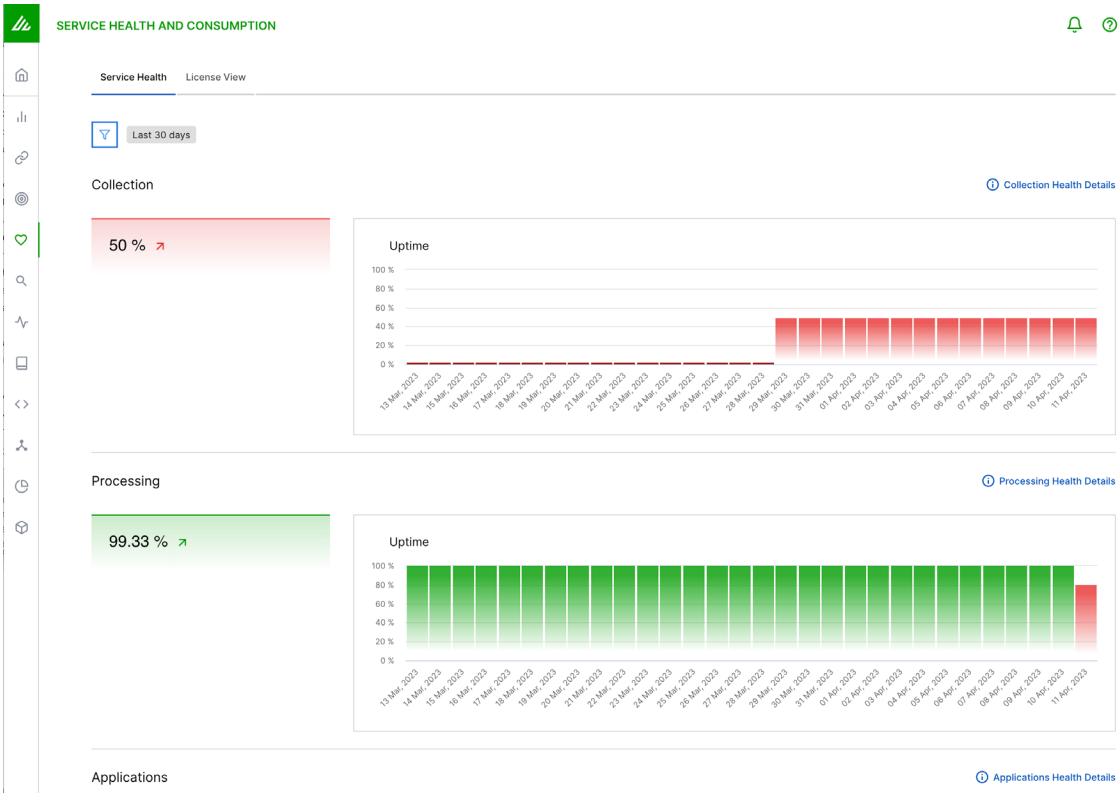


Outcomes Navigator

Outcomes Navigator maps the security log feeds that come into the Event Store against the most common security use cases and suggests ways to improve coverage. It examines the completeness of the logs parsed and the Dashboards and Correlation Rules associated with those use cases, identifies gaps in log parsing or sources, and suggests ways to improve coverage. Outcomes Navigator supports measurable, continuous improvement by recommending information, event stream, and parsing configuration changes needed to close any gaps.

Threat Intelligence Service

Available in all Exabeam products at no additional cost, the Exabeam Threat Intelligence Service ingests multiple commercial and open-source threat intelligence feeds, then aggregates, scrubs, and ranks them, using proprietary machine learning algorithms to produce highly accurate IoCs. It adds context enrichment such as file, domain, IP, URL reputation, and TOR endpoints to events from multiple external threat intel services and feeds. The threat intelligence data is refreshed every 24 hours.

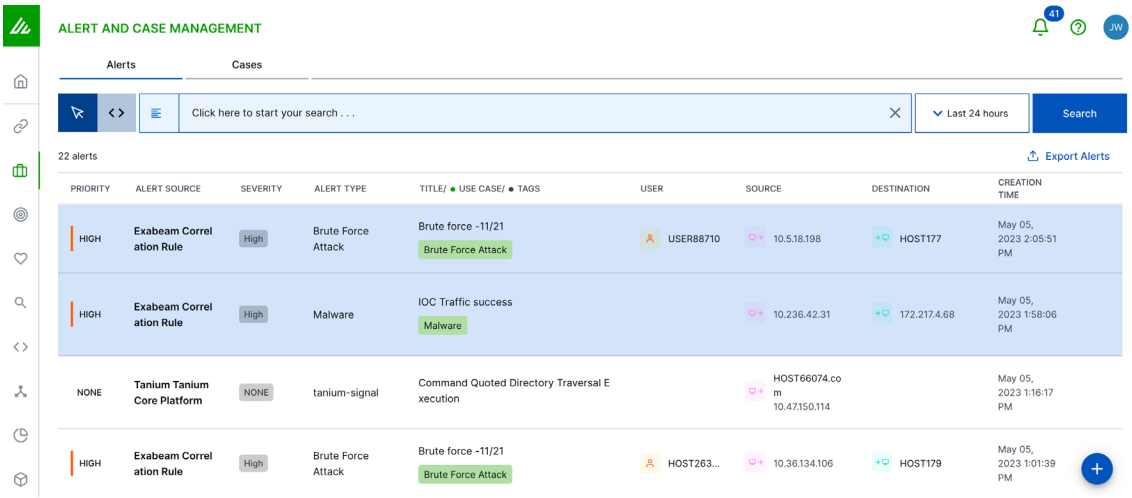


Service Health and Consumption

Visualize the health of every service and application, as well as data consumption, while monitoring your connections and sources. Service Health and Consumption provides dashboards showing uptime and health of all your log parsers, applications, data flow and connections, as well as your total license volume consumptions to help with long-term storage and capacity planning.

Context Enrichment

Context enrichment provides powerful benefits across several areas of the platform. Exabeam supports enrichment using three methods: threat intelligence, geolocation, and user-host-IP mapping. Armed with the most up-to-date IoCs, our threat intelligence service adds enrichments such as file, domain, IP, URL reputation, and TOR endpoint identification to prioritize or update existing correlations and behavioral models. Geolocation enrichment provides location-based context not often present in logs. Outside of authentication sources, user information is rarely present in logs. Exabeam enrichment adds user details and relationships to event logs, which is critical to building correlation rules and dashboards to detect and report on potentially suspicious activity.



Alert and Case Management

A defining feature separating a SIEM solution from a security data lake is the ability to sort alerts by severity, and combine them into cases and incidents to be worked through to resolution by your analysts. Alert and Case Management centralizes events and alerts from Exabeam or third-party products, letting an analyst review them individually or at volume. Analysts can set conditions to automate the alert triage workflow and escalate events and alerts into incidents. Alert and Case Management enables analyst teams to add tags, ATT&CK labels, screenshots, attachments, and events to incidents, and then collaborate across groups and time zones.

ATT&CK Coverage

The Exabeam Security Operations Platform uses the ATT&CK framework as a critical lens to help improve the visibility of your security posture. Support for ATT&CK spans all 14 categories, including 193 techniques and 401 sub-techniques in the ATT&CK framework.

Exabeam Customer Success Services

At Exabeam, customer success means more than just deploying and maintaining software. For us, it means helping you achieve your desired business goals and security outcomes. To that end, Exabeam Customer Success provides around-the-clock access to an experienced team of support professionals with the technical expertise to ensure your Exabeam environment is running optimally.

Exabeam Support

Exabeam offers three levels of support options which include operational assessments, reporting, and ongoing adoption tuning services.

Standard Support

Standard Support is is available through the Exabeam Community. You get access to the support portal, self-help Knowledge Base, documentation, webinars, videos, and guidance on deploying Exabeam products. The Exabeam Community also provides customers a forum to directly interact with each other and is included as part of the Exabeam annual subscription license.

Premier Support

Premier Support provides all of the benefits of our Standard Support offering plus a point of contact for support escalation for faster, more personalized response and resolution. You'll also get monthly performance reports to ensure your team is maximizing system performance and a bi-annual security coverage assessment.

Premier Plus Support

Premier Plus Support is our highest level of support and provides all of the benefits of Premier Support, plus a named Customer Success Manager (CSM) and a Technical Account Manager (TAM) who provide a tailored customer adoption experience post deployment. The TAM works with you to ensure execution on defined operational outcomes to achieve your security goals.

Exabeam Customer Success Management

Customer Success Managers (CSMs) are your strategic partners to help you achieve your business goals with Exabeam. CSMs will:

- **Guide and advocate for customers** throughout the Exabeam customer journey
- **Coordinate and align resources** to meet customer needs
- **Collaborate with the Technical Adoption Manager** (TAM) to share best practices to maximize the value-add from Exabeam

Exabeam Customer Success: delivering around-the-clock access to an experienced team of support professionals with the technical expertise to ensure your Exabeam environment is running optimally.

Exabeam Professional Services

Exabeam Professional Services provide a well-defined framework of fixed delivery packages or customized services to accelerate deployment, integration, and platform management while maximizing your success. Exabeam Professional Services are designed to allow you to accelerate your deployment and time to value.

Exabeam Professional Services include Deployment Services and Staff Augmentation Services.

- **Deployment Services** support the implementation and roll out of the Exabeam Security Operations Platform
- **Staff Augmentation Services** extend your reach and supplement your resources with experienced Dedicated and/or Partial Resident Engineers

Exabeam Education

To maximize your Exabeam investment, our Education team has created a series of classes to get you up and running as quickly and efficiently as possible. Whether you are a security analyst, engineer, or just interested in understanding more about the functionality of Exabeam, we have training for you in a variety of modalities: eLearning, Virtual Instructor-led, and Onsite.

About Exabeam

Exabeam is a global cybersecurity leader that created New-Scale SIEM™ for advancing security operations. We help organizations detect threats, defend against cyberattacks, and defeat adversaries. The powerful combination of our cloud-scale security log management, behavioral analytics, and automated investigation experience results in an unprecedented advantage over 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.