Exabeam SIEM

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

The SIEM plays a central role in security operations monitoring, alerting, threat detection, and managing compliance. As data volumes, exposure points, third-party alerts, and the cost of talent and storage have all 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 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.

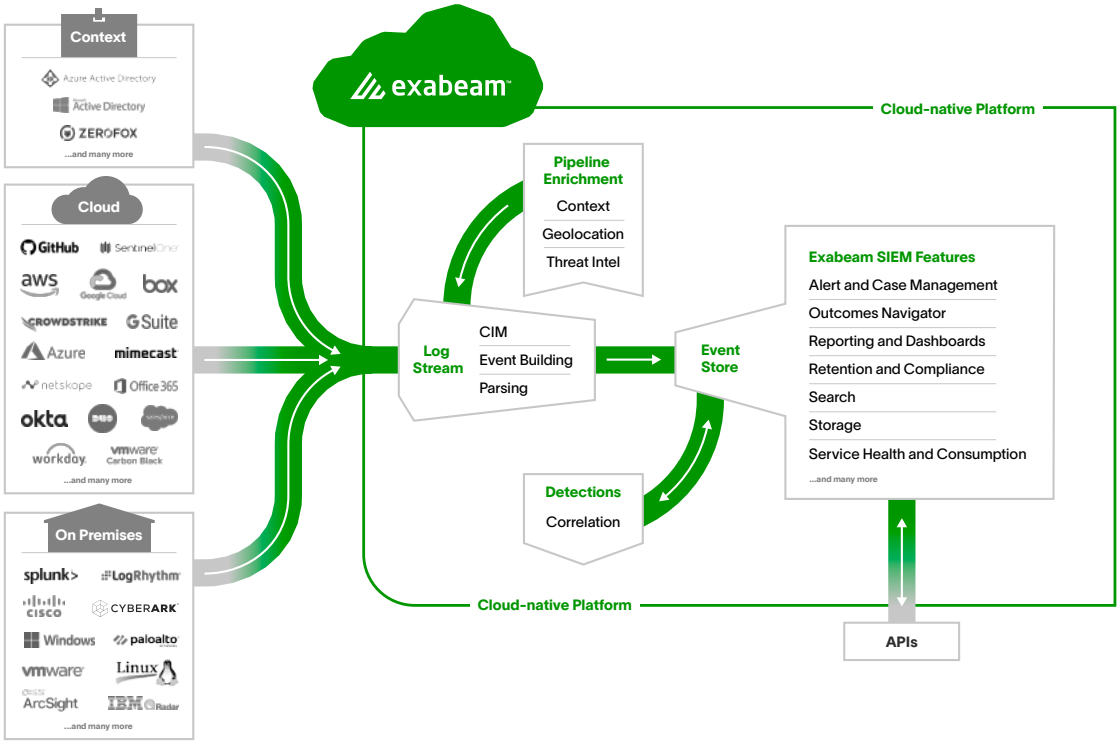
Welcome to New-Scale SIEM™ from Exabeam. New-Scale SIEM is a breakthrough combination of threat detection, investigation, and response (TDIR) capabilities security operations need in products they will want to use. Exabeam SIEM delivers limitless scale to ingest, parse, store, search, and report on petabytes 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 analysts new speed, processing at over one million EPS, and efficiencies to improve their effectiveness. Exabeam SIEM includes everything in Exabeam Security Log Management, plus over 100 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
- Reporting and Dashboards
- Correlation Rules
- Pre-built Correlation Rules
- Outcomes Navigator
- Threat Intelligence Service
- Service Health and Consumption
- Context Enrichment
- Alert and Case Management
- MITRE ATT&CK Coverage

How it works



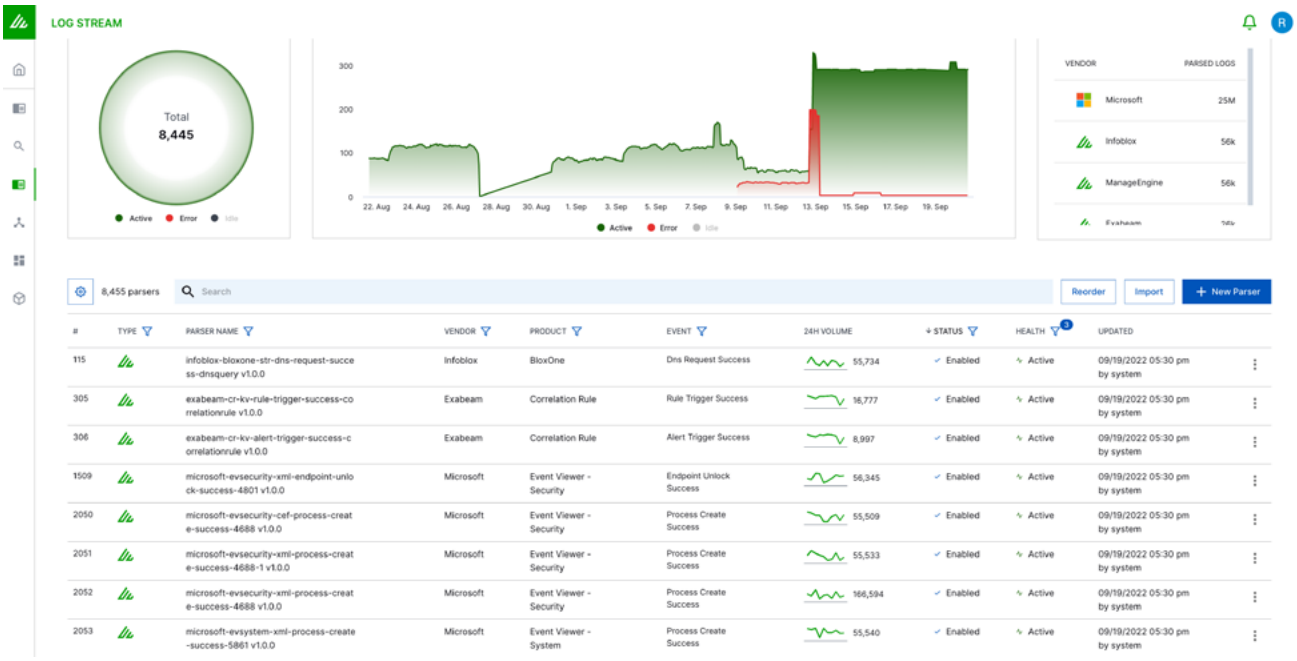
Key Features

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 provides collection from 200+ on-premises products, through a variety of transport methods including APIs, collectors, syslog, and log aggregators such as SIEM or log management products. 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
- Data Loss Prevention (DLP)
- Database Activity Monitoring (DAM)
- Email Security and Management
- Endpoint Security (EPP/EDR)
- Firewalls
- Forensics and Malware Analysis
- Information Technology Service Management (ITSM)
- IoT/OT Security
- Network Access, Analysis, and Monitoring
- Physical Access and Monitoring
- Privileged Access Management (PAM)
- Security Analytics
- Security Information and Event Management (SIEM)
- Threat Intelligence Platform
- Utilities/Others
- VPN Servers
- Vulnerability Management (VM)
- Web Security and Monitoring



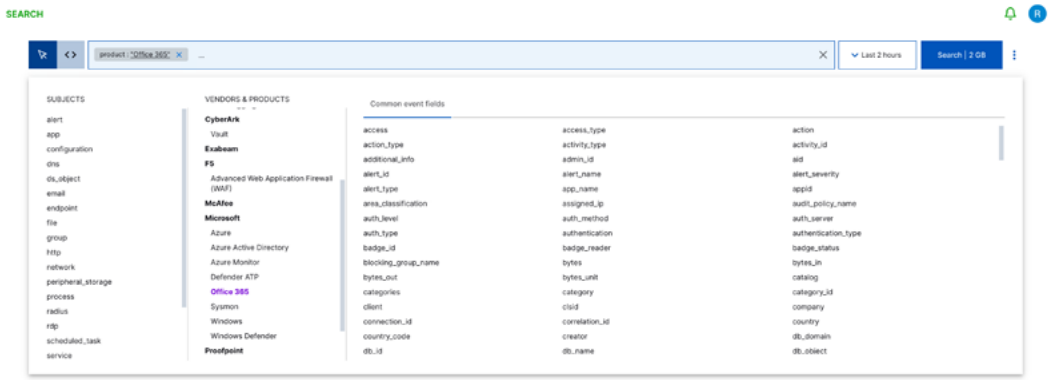
Log Stream

Delivers rapid log ingestion processing at a sustained rate of over 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 7,937 pre-built log parsers, and enriched using 3 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.

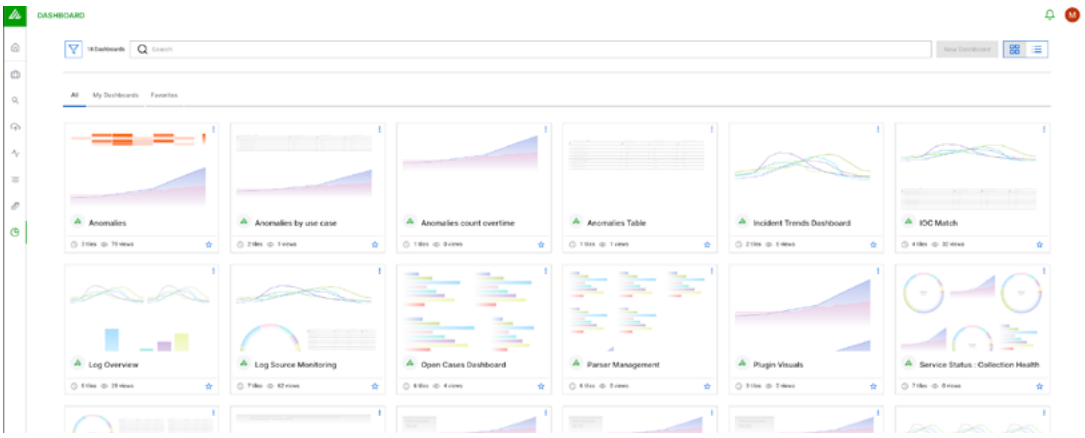


Search

A simplified search experience with faster query and instant results over PB-scale and/or years of data — search hot and cold data at the same speed.

Search is an essential feature of Exabeam SIEM. Search is a single interface that allows analysts to search for events, logs, or Indicators of Compromise (IoC). 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. Analysts no longer have to wait hours to get search results from NAS or other offline storage. Search across real-time or historical data is no longer a barrier. SOC teams do not have to import and wait for historical data to be restored and processed.

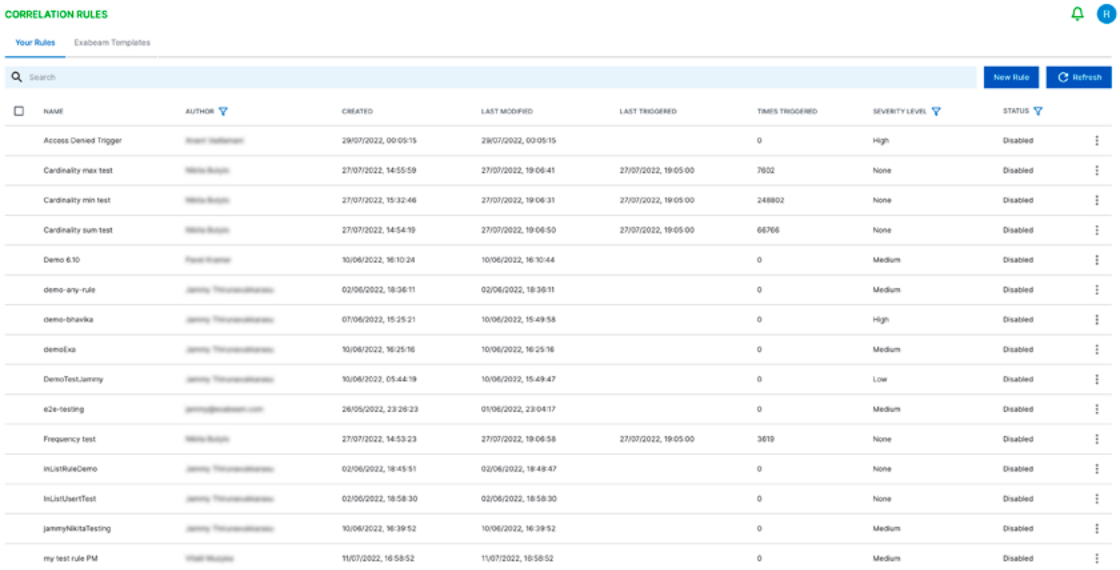
Moreover, there's no learning curve, meaning analysts aren't required to learn a proprietary query language. Search delivers a query builder wizard to point and click from a list of intelligent fields to help build effective search queries quickly and easily.



Reporting and Dashboards

Print, export, or view dashboard data with pre-built compliance reports, and customize reports and dashboards with 14 different chart types.

Build a dashboard in a minute from 14 different pre-built chart types as if you were using a leading BI tool. The Exabeam dashboard app is fully integrated within Exabeam SIEM, allowing you to create powerful visualizations from your parsed log data quickly. Customers can choose one or more visuals to meet their business needs. These include bar chart, column chart, line graph, area chart, pie chart, donut chart, bubble chart, funnel, single value, sankey map, word cloud, heat map, table, and a Coverage Map.



Correlation Rules

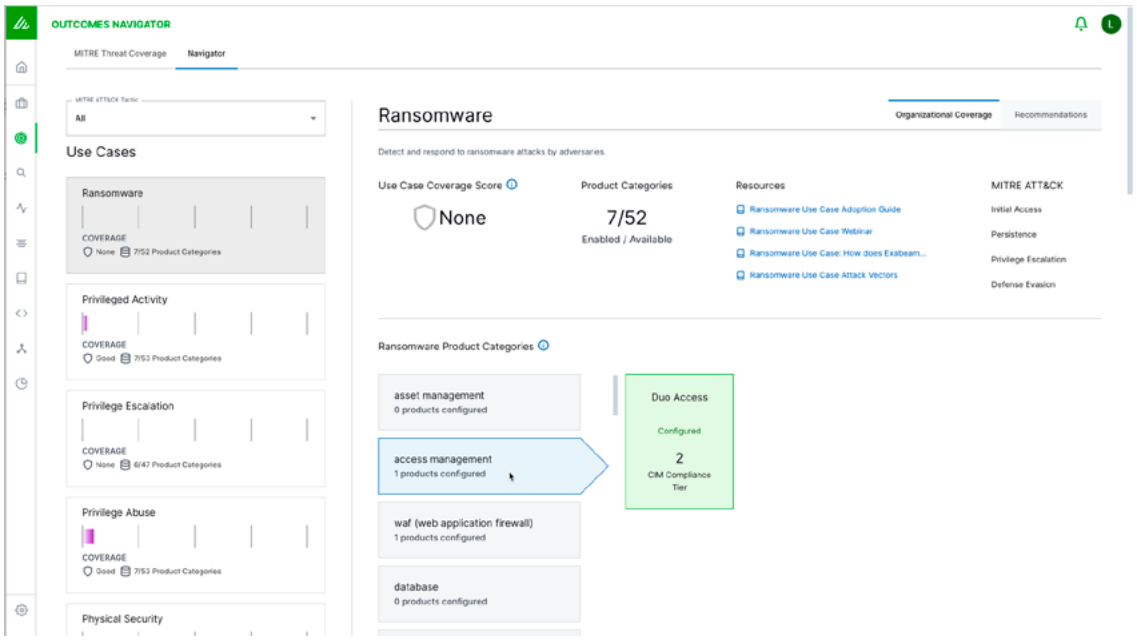
Correlation rules define conditions that function as triggers by comparing incoming events with predefined relationships between entities to identify and escalate anomalies. Write, test, publish, and monitor custom correlation rules for your most critical business entities and assets, including defining higher criticality for events that correspond to Threat Intelligence Service-sourced activity.

Properly designed correlation rules enable enterprises to surface a broad range of abnormal behavior and events. Correlation builder provides analysts with an easy application to create custom correlation rules suited to their organization's security and use case requirements.

Correlation rules monitor for well-known threats, identify compliance violations, and detect signature-based threats using context from the Exabeam Threat Intelligence Service or other third-party threat intelligence.

Pre-built Correlation Rules

Exabeam SIEM offers over 100 pre-built correlation rules and models matching some of the most common use cases of malware and compromised credentials.

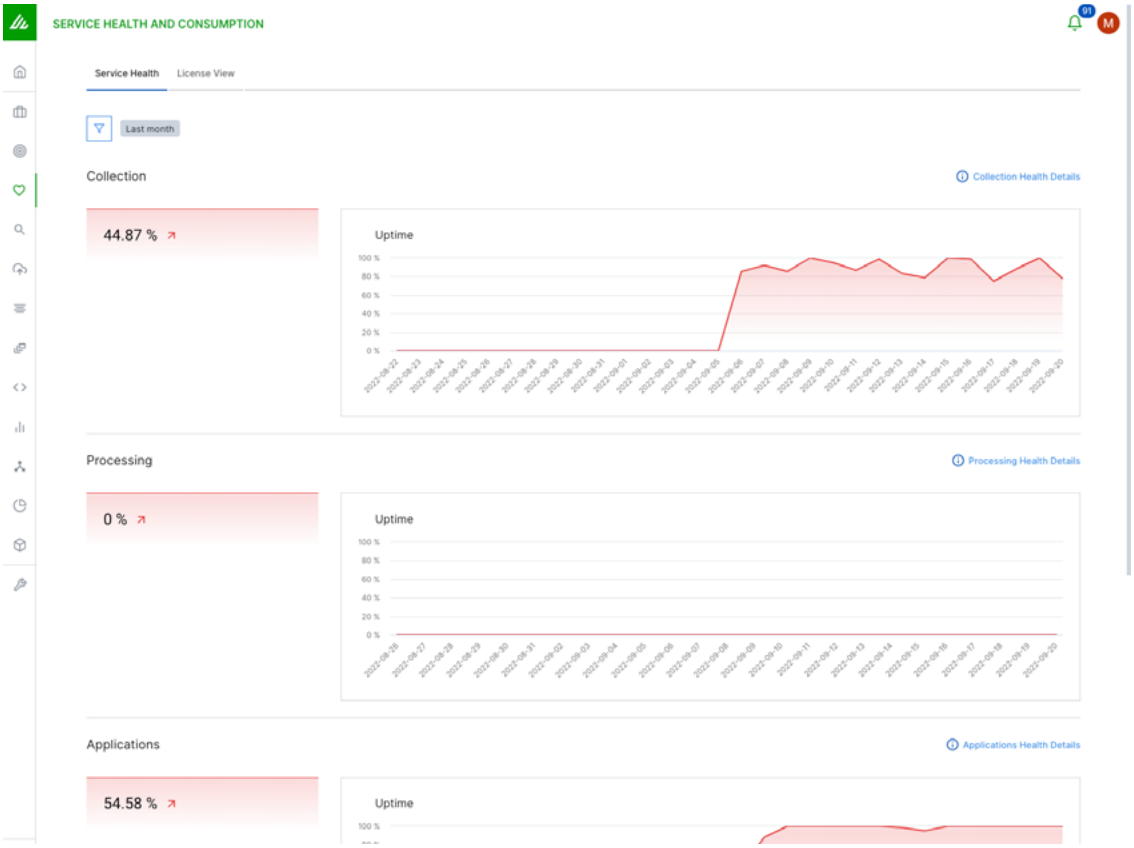


Outcomes Navigator

Outcomes Navigator maps the feeds that come into our SIEM against the most common security use cases and suggests ways to improve coverage. Outcomes Navigator supports measurable, continuous improvement focusing on outcomes by recommending information, event stream, and parsing configuration changes 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 a highly accurate, up-to-date stream of 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.



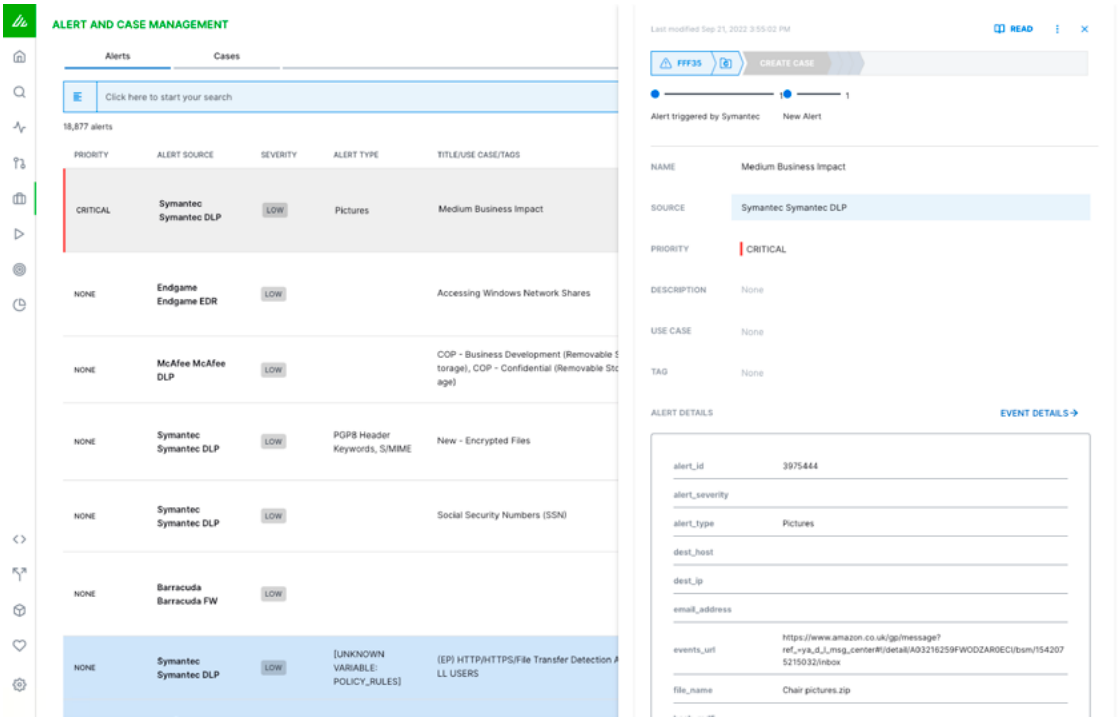
Service Health and Consumption

Visualize your service health for 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.

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 often not present in logs. Outside of authentication sources, user information is rarely present in logs. Exabeam's User-host-IP mapping enrichment adds user details to logs which is critical to building behavioral models for detecting anomalous activity.



Alert and Case Management

A defining feature separating a SIEM 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 sourced from Exabeam 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. Case Management helps analyst teams add tags and events to incidents, collaborate across groups and timezones, and offers customizable, outcome-driven steps for analysts to guide them through to mitigation or resolution.

MITRE ATT&CK Coverage

The Exabeam Security Operations Platform uses the MITRE ATT&CK® framework as a critical lens to help improve the visibility of your security posture. Support for MITRE ATT&CK spans all 14 categories, including 101 techniques and 180 sub-techniques in the MITRE 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 Services

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

Standard Support

Standard Support 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

Exabeam Education provides remote and hands-on courses to up-level your security analysts or engineers with instructor-led training or self-paced online classes. Your team will learn to maximize the features and functionalities of Exabeam products to get the most value out of the platform. Our Education team is constantly working to create new courseware for all learning types.

Classes include topics like:

- Administering Advanced Analytics
- Introducing Common Information Model
- Fundamentals of Log Stream
- Introducing Search
- Behavioral Analytics and Investigation in the Exabeam Security Operations Platform
- Security Search and Dashboards in the Exabeam Security Operations Platform

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now →

CYBERSEER

Official MSSP Partner - **To request more information, please visit:** https://www.cyberseer.net/technologies/**exabeam/**

Book a call | info@cyberseer.net