Exabeam Fusion

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

Security operations success needs to be redefined, and it starts with security information and event management (SIEM). As IT infrastructure shifts into the cloud, the entire security portfolio needs to scale and follow suit. Traditional SIEM solutions force security operations teams to manage massive amounts of data across billions of events, but they don't show the complete picture of complex and hard-to-detect, credential-based attacks. Whether it's phishing, ransomware, malware, or lateral movement, accessing valid credentials is the adversaries' primary objective. This demands a shift in investment from legacy on-premises detection approaches to a massively scalable, cloud-native platform designed to detect abnormal behavior. Security operations success requires a new approach: New-Scale SIEM.

Exabeam Fusion represents New-Scale SIEM, the industry's most powerful and advanced cloud-native SIEM solution. The combined capabilities of SIEM, user and entity behavior analytics (UEBA), and security orchestration, automation, and response (SOAR) include a cloud-native data lake, rapid data ingestion, hyper-fast query performance, powerful behavioral analytics to uncover weak signals that other tools miss, and automation that changes the way analysts do their jobs. Pre-built integrations with more than 549 third-party security tools, more than 1,800 fact-based correlation rules, and more than 735 behavioral model histograms automatically baseline normal behavior of users and devices to detect, prioritize, and respond to anomalies based on risk. Exabeam enriches events using three methods: threat intelligence, geolocation, and user-host-IP mapping. Exabeam Fusion enables analysts to run their end-to-end TDIR workflows from a single control pane that performs automation of highly manual tasks such as alert triage and prioritization, incident investigations, and response to accelerate investigations, reduce response times, and ensure consistent, repeatable results.

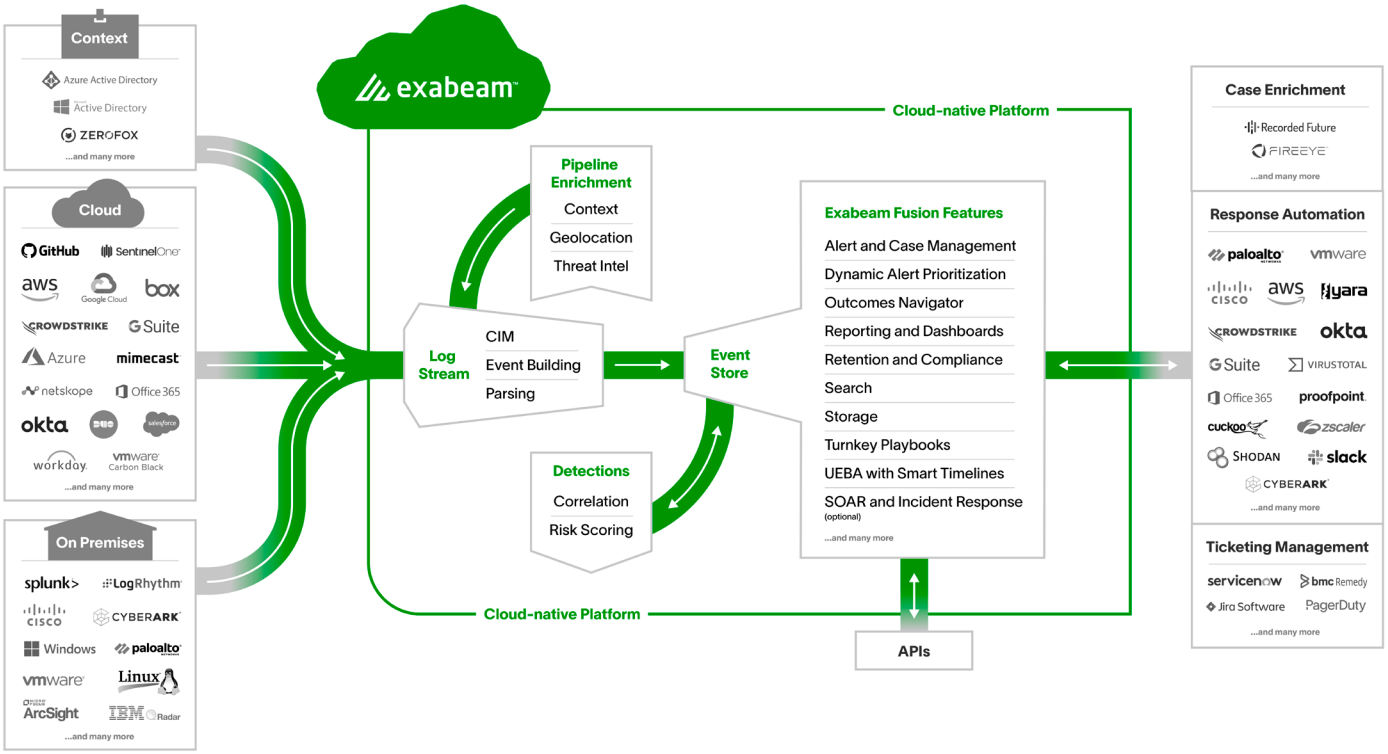
Key Features

- Collectors
- Context Enrichment
- Log Stream
- Common Information Model (CIM)
- Search
- Dashboards
- Correlation Rules
- Pre-built Correlation Rules
- Outcomes Navigator
- Service Health and Consumption
- Threat Intelligence Service
- Advanced Analytics
- Alert Triage and Case Management
- Dynamic Alert Prioritization
- Turnkey Playbooks
- Incident Responder
- ATT&CK® Coverage

Exabeam Fusion capabilities include rapid data ingestion, a cloud-native data lake, hyper-fast query performance, powerful behavioral analytics for next-level insights that other tools miss, and automation that changes the way analysts do their jobs. Security log management leverages a cloud-scale architecture to ingest, parse, store, and search data at lightning speed. Behavioral analytics employ over 1,800 rules, including cloud infrastructure security, with more than 735 behavioral model histograms that automatically baseline normal behavior of users and devices to detect, prioritize, and respond to anomalies based on risk. Smart Timelines™ convey the complete history of an incident and highlight the risk associated with each event.

Automated investigations in Exabeam Fusion reduce highly manual tasks, such as alert triage, with dynamic alert prioritization, incident investigation, and incident response. This boosts analyst productivity and allows security operations to accelerate investigations, reduce response times, and ensure consistent, repeatable results with hundreds of SOAR integrations.

How it works



Key Features

Collectors

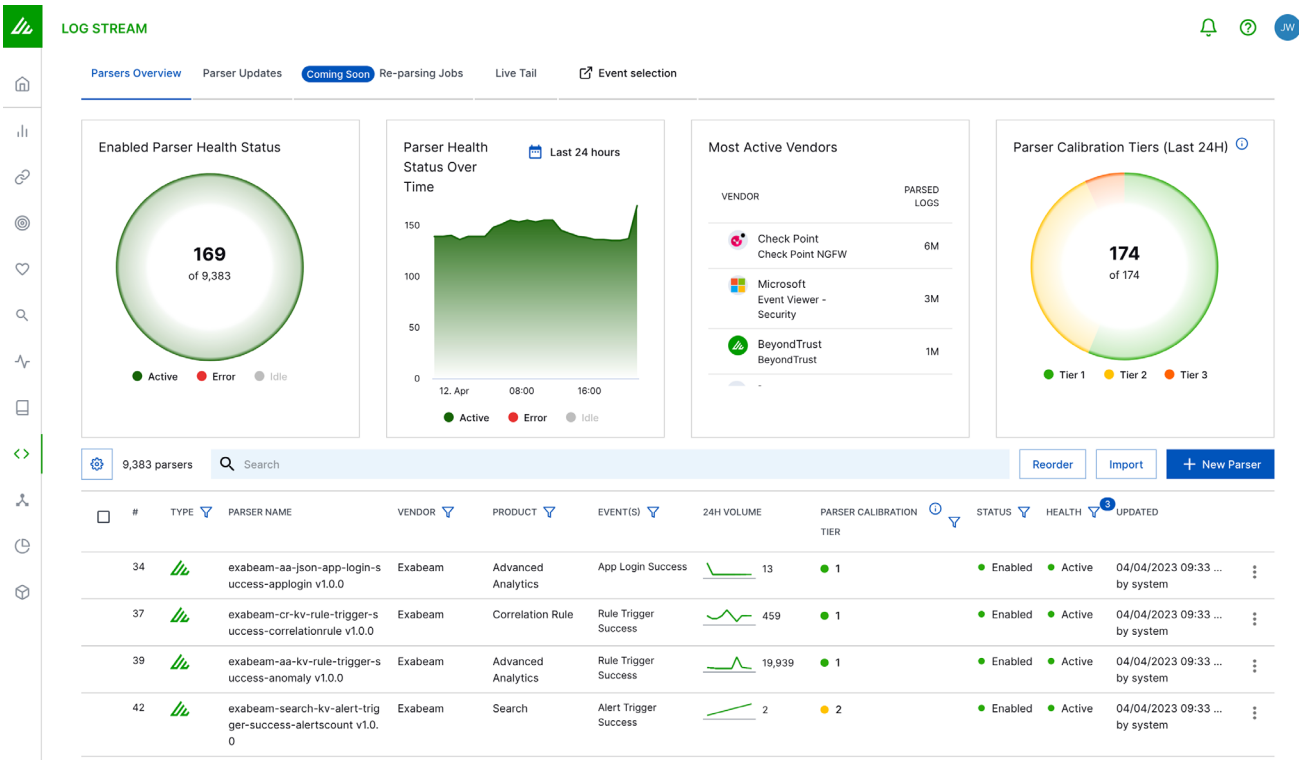
The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service at scale from on-premises, cloud, and context sources. The platform collects logs 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 such as SIEM or log management products. To meet the increasing need for cloud security and cloud data collection, these include 30+ cloud-delivered security products, 10+ SaaS productivity applications, and 20+ cloud infrastructure products. For context enrichment, 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)

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's User-host-IP mapping enrichment adds user details to logs which is critical to building behavioral models for detecting anomalous activity.

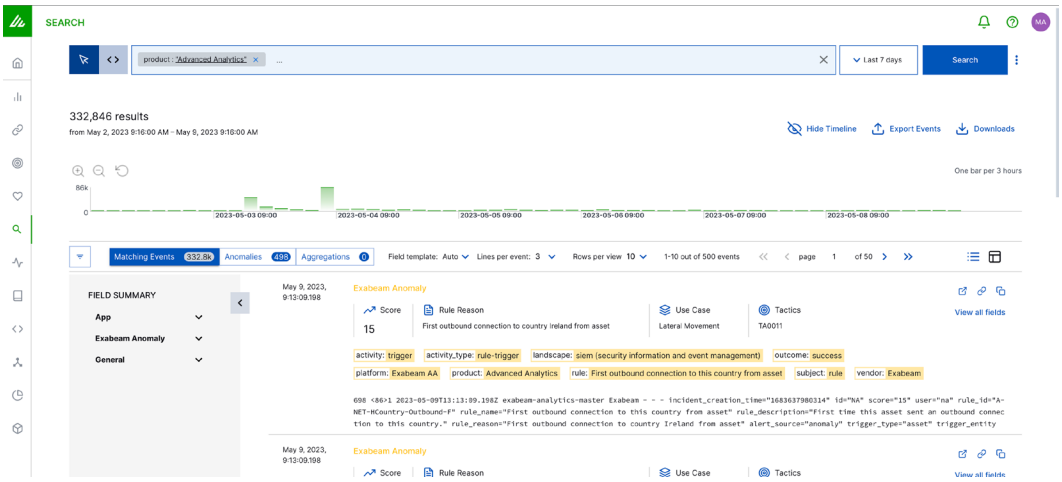


Log Stream

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, edit, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. Upon ingestion, 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. Live Tail provides self-service, real-time monitoring and management of parser performance, and visibility into the data pipeline.

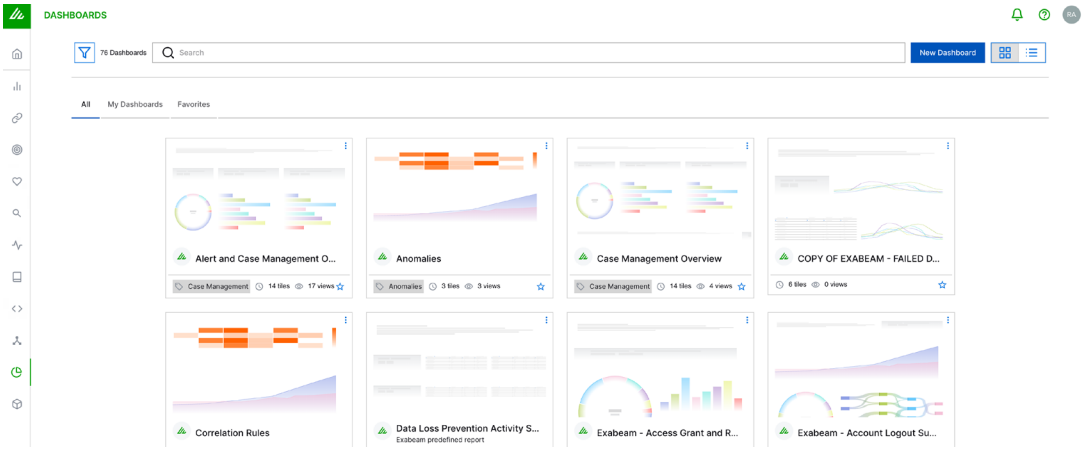
Common Information Model (CIM)

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). 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.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 petabytes and years of data. Search is a single interface that allows analysts to search for events, IoCs, or Exabeam-generated anomalies. 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 15 pre-built dashboards covering most compliance needs, including anomalies, Correlation Rules, and Case Management overview reporting — or create your own dashboards in a minute via 14 different chart types as if you were using a leading BI tool.

The Dashboards app is fully integrated within Exabeam Fusion, 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

Compare incoming events with predefined relationships between entities to identify and escalate events and alerts. Write, test, publish, and monitor your own custom Correlation Rules for your most critical business entities and assets, including defining higher-criticality or specific inclusion of Threat Intelligence Service-sourced conditions, and assign specific MITRE ATT&CK® tactics, techniques, and procedures (TTPs) to custom rules according to your own critical path needs.

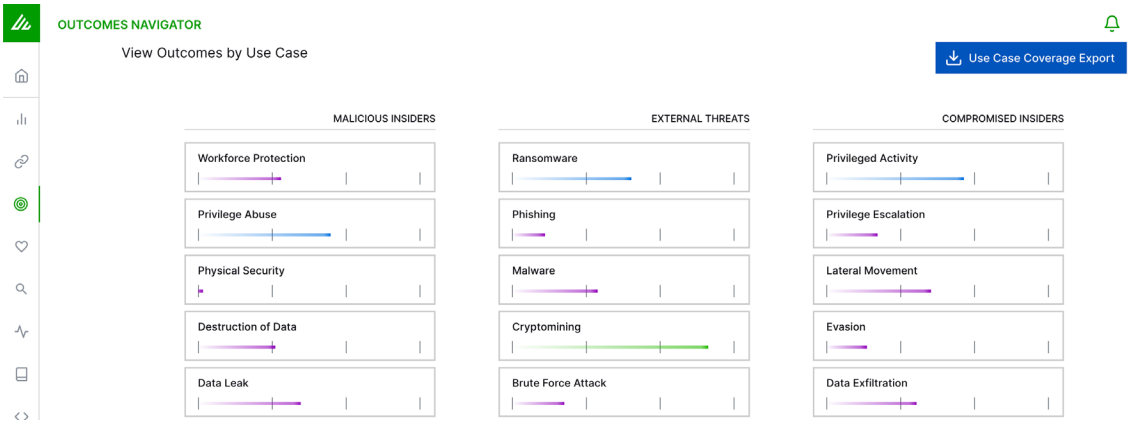
Properly-designed Correlation Rules enable enterprises to surface a broad range of abnormal behavior and events. Correlation Rule builder provides analysts with an easy application to create custom Correlation Rules suited to their organization's security and use case requirements.

Correlation Rules helps analysts 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

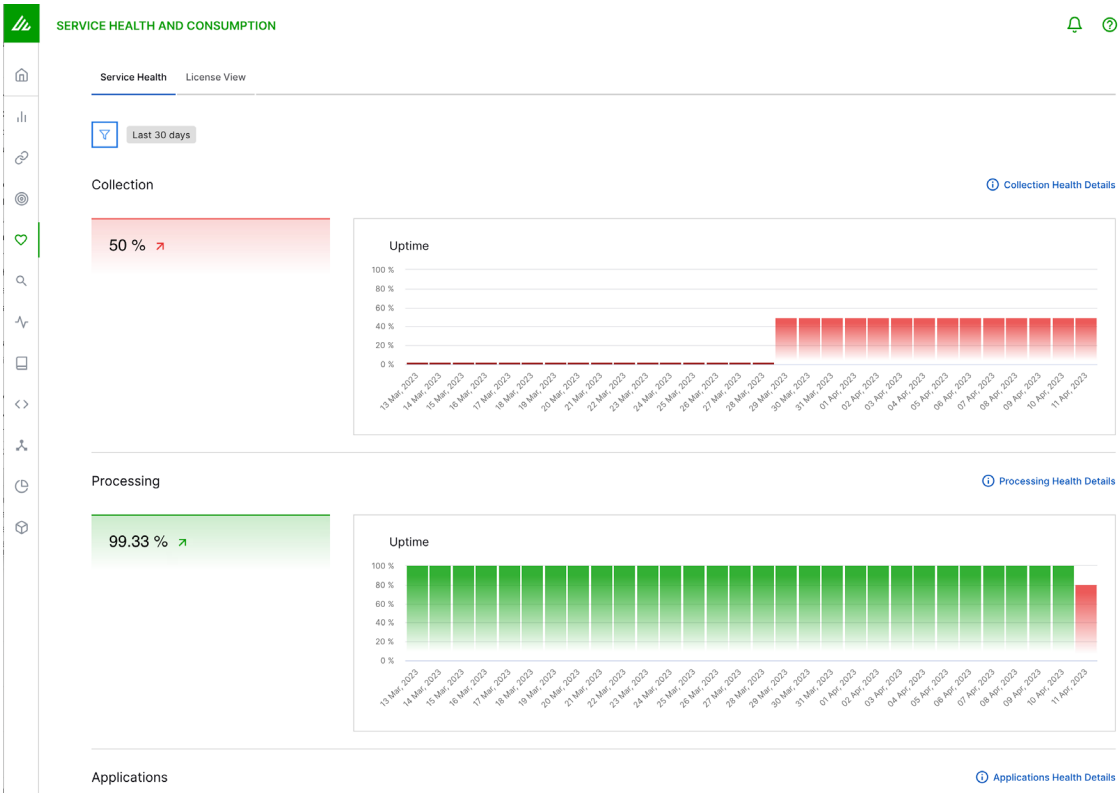
Exabeam Fusion offers more than 120 pre-built fact-based Correlation Rules and models matching some of the most common use cases of malware and compromised credentials. Employ pre-built Correlation Rules, or edit them to fit your own most pressing use cases or notification needs.

All Correlation Rules-triggered events can automatically create an incident for your team to investigate, or even connect via API into an outside IT service management queue.



Outcomes Navigator

Outcomes Navigator maps the security log feeds that come into the Exabeam Event Store against the most common security use cases. Outcomes Navigator examines the completeness of the logs parsed, the Dashboards, Advanced Analytics, 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.

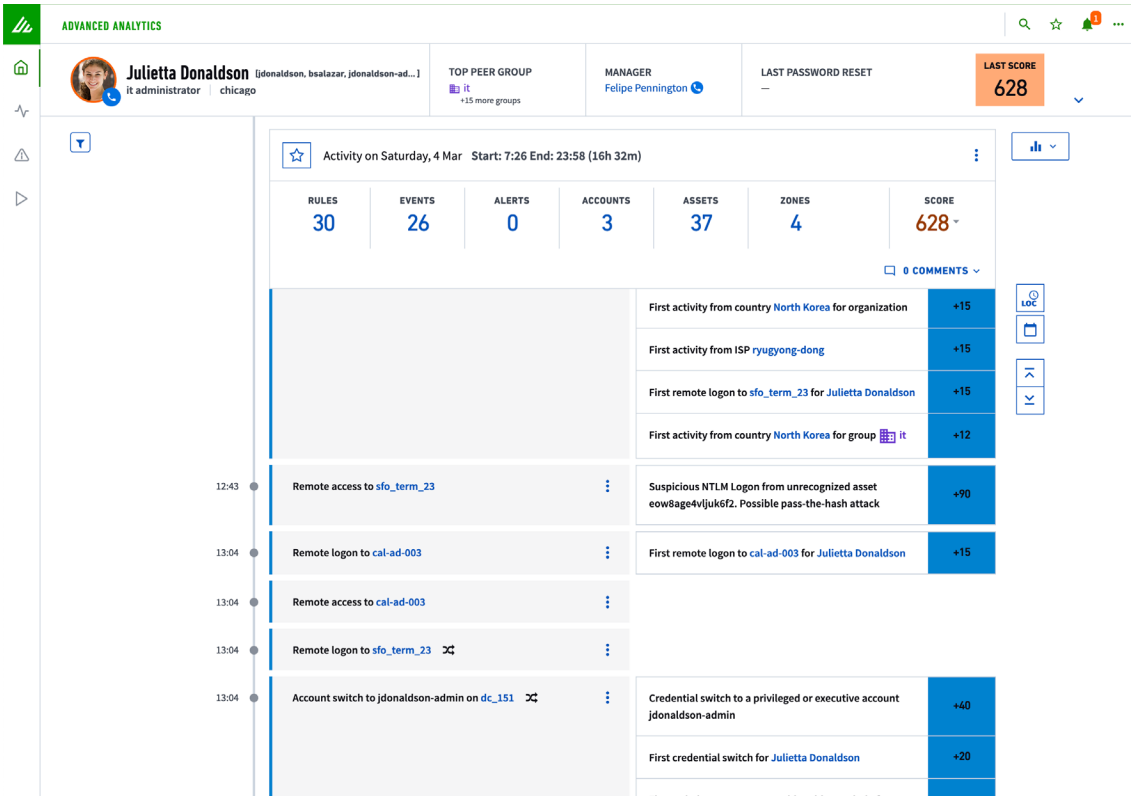


Service Health and Consumption

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.

Threat Intelligence Service

Available 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 stream of IoCs. It offers context enrichment and compares 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.

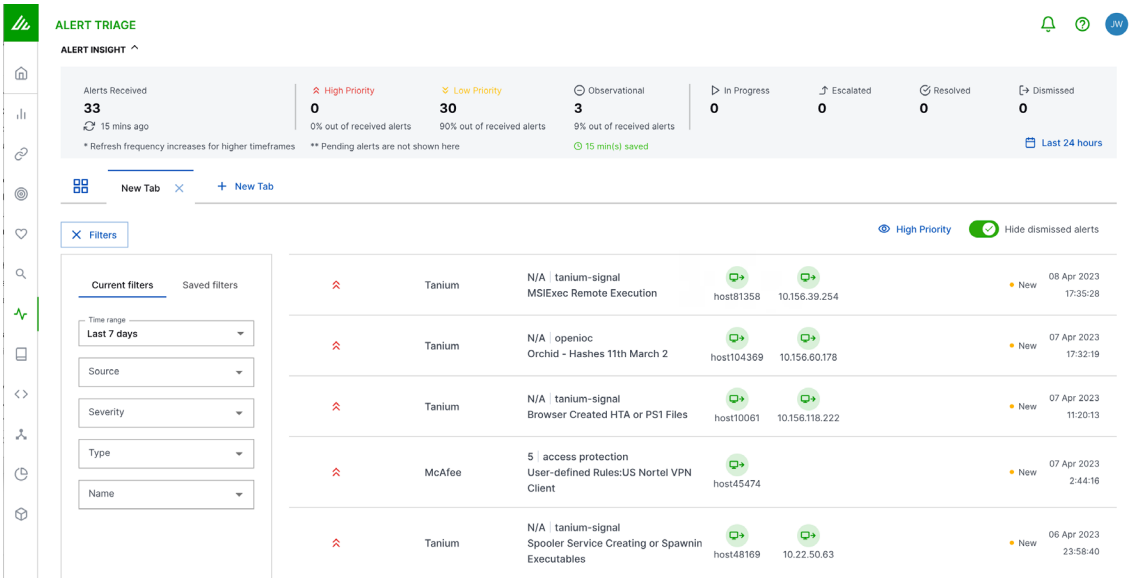


Advanced Analytics

Advanced Analytics offers UEBA with more than 1,800 rules, including cloud threat detection, and more than 735 behavioral models to automatically baseline normal behavior of users and devices with histograms to detect, prioritize and respond to anomalies based on risk. Advanced Analytics automatically visualizes these events in Smart Timelines™ that show full event flows and activities to inform the next right action.

To understand normal and detect anomalies as normal keeps changing, all user and device activity gets baselined. Risk-based prioritization uses machine learning to automatically assign risk scores to all events, prioritizing triage, investigation, and response for key incidents, and automatically visualizing these events within Smart Timelines that show full event flows and activities to inform the next right action. Smart Timelines detect lateral movement by organizing incidents to follow attack activity, credential use, or permission changes within your environment. The results: find and stop the threats other tools miss, uplevel your security team speed and performance, and stay ahead of your adversaries.

- Machine learning classifies entities, such as workstation versus server, and service account versus user, identifies personal email addresses, and more.
- Extensive rule mapping enables analysts to do behavior-based threat hunting on abnormal behavior, IoCs and TTPs.
- Bringing in data from existing SIEM solutions, XDR platforms, and security log resources adds depth, helps establish normal, and creates correlation potential to see end-to-end attack event strings.



Alert Triage and Case Management

Alert Triage categorizes, aggregates, and enriches third-party and Exabeam-generated security alerts, so analysts can confidently and efficiently dismiss or escalate alerts from a single screen.

Case Management allows analyst teams to create incidents, add tags and events to the incident, collaborate across groups and time zones, and offers customizable, outcome-driven steps for analysts to guide them through to mitigation or resolution.

Alert Triage and Case Management help the analyst sort incoming events at volume, making it easy to see the most crucial events that correspond to anomalies or high-value signatures. Analysts can manually or automatically sort events into incidents for focused investigation and/or escalation — or export into other third-party workflow solutions. Auto attribution of alerts to users and assets, nearby anomalies, and user and host context provides additional context for more effective triage and investigations.

Dynamic Alert Prioritization

Dynamic Alert Prioritization applies machine learning to automate third-party alert prioritization by infusing third-party security alerts with context from UEBA to dynamically identify, prioritize, and escalate the alerts which require the most attention. Classifying alerts provides a starting point for the analyst to begin the triage process, focusing time and resources on the alerts of the highest risk to the organization.

Turnkey Playbooks

Automate repeated workflows for investigation into compromised credentials, external attacks, or malicious insider use cases with guided checklists for resolution.

Turnkey Playbooks automation offers pre-built playbooks that work without requiring configuration or investment in additional third-party products, so analysts can respond to common security scenarios within a single UI.

Incident Responder

Incident Responder is an optional add-on to orchestrate and automate repeated workflows to 103 third-party products with 613 response actions, from semi- to fully automated activity. With Incident Responder, analysts can automate gathering key pieces of information about incidents via pre-built integrations with popular security and IT infrastructure, and run response playbooks to programmatically perform investigation, containment, or mitigation. Running response playbooks allows organizations to respond to threats faster and more consistently.

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 the ATT&CK framework spans all 14 categories, including 193 techniques and 401 sub-techniques.

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.

exabeam

Detect
Defend
Defeat™

Learn how at Exabeam.com →