**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.

A majority of the breaches involving credential theft or misuse appear as anomalous activity on an endpoint, server, or application. The analysis of every ransomware attack, phishing attempt, and most malware confirms this. With over 90% of breaches involving compromised credentials, the need for behavioral-based detections highlighting normal and abnormal activity, combined with repeatable workflows, are essential cybersecurity capabilities.

Unlike other products in the market, Exabeam Security Investigation can run on top of a third-party legacy SIEM or data lake to deliver advanced capabilities for threat detection, investigation, and response (TDIR). Exabeam Security Investigation compounds the user and entity behavior analytics (UEBA) capabilities of Exabeam Security Analytics with detection content and prescribed workflows to enable outcome-focused TDIR for ransomware, phishing, malware, and compromised and malicious insiders. Security Investigation offers over 1,800 rules including cloud infrastructure security and over 750 behavioral model histograms that automatically baseline normal behavior of users and devices to detect, prioritize, and respond to anomalies based on risk. This eliminates the writing of hundreds of queries and changes the way analysts do their jobs.

To help standardize around best practices, Exabeam Security Investigation includes prescribed workflows (e.g. ransomware, phishing, malware, compromised insiders, malicious insiders) and pre-built content (e.g. MITRE ATT&CK framework) that focus on specific threat types and techniques to achieve more successful TDIR outcomes. With Exabeam Security Investigation, analysts can run their end-to-end TDIR workflows from a single control plane that automates highly manual tasks such as alert triage and 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 security orchestration, automation, and response (SOAR) integrations.

### Key Features

<table>
<thead>
<tr>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collectors</td>
</tr>
<tr>
<td>Log Stream</td>
</tr>
<tr>
<td>Common Information Model (CIM)</td>
</tr>
<tr>
<td>Anomaly Search</td>
</tr>
<tr>
<td>Pre-built Dashboards</td>
</tr>
<tr>
<td>Correlation Rules</td>
</tr>
<tr>
<td>Pre-built Correlation Rules</td>
</tr>
<tr>
<td>Outcomes Navigator</td>
</tr>
<tr>
<td>Service Health and Consumption</td>
</tr>
<tr>
<td>Threat Intelligence Service</td>
</tr>
<tr>
<td>Advanced Analytics</td>
</tr>
<tr>
<td>Alert and Case Management</td>
</tr>
<tr>
<td>Turnkey Playbooks</td>
</tr>
<tr>
<td>Incident Responder</td>
</tr>
<tr>
<td>Dynamic Alert Prioritization</td>
</tr>
<tr>
<td>Context Enrichment</td>
</tr>
<tr>
<td>MITRE ATT&amp;CK® Coverage</td>
</tr>
</tbody>
</table>

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.
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

How it works
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 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.
Anomaly Search

Exabeam Security Investigation features Anomaly Search, a simplified search interface that allows analysts to search for Exabeam-triggered events across their data repository. Anomaly Search offers a drop-down menu for easy query construction against the list of events to determine and declare incidents. Anomaly Search pairs behavior-based TTP detection with known IoCs to enhance an analyst’s threat hunting and correlation rule testing across a variety of different objects such as sessions, rules, users, assets, MITRE TTPs, anomaly identification, and use cases. Moreover, there’s no learning curve, meaning analysts aren’t required to learn a proprietary query language.
Pre-built Dashboards
Print, export, or view dashboard data with pre-built anomaly and case management dashboards.

The Exabeam dashboard provides powerful visualizations for anomalies and cases. View anomalies by use case, count, or rule name with the Anomalies Dashboard. Case Management Overview dashboard shows open cases and performance metrics including severity and incident types for a summary of your team's ability to resolve, respond, and close incidents.

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 Security Investigation 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 Security Investigation 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.
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.

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.

exabeam.com | 07
**Advanced Analytics**

Advanced Analytics offers UEBA with over 1,800 rules, including cloud infrastructure security, and over 750 behavioral model histograms that automatically baseline normal behavior of users and devices 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 activities get 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 like workstation versus server, service account versus user, identifies personal email addresses, and more.
- Extensive rule mapping enables analysts to do behavior-based threat hunting on abnormal TTPs and use Outcomes Navigator to map your current coverage by log sources.
- Bringing in existing SIEM, XDR, and logs from other data lakes or resources like CASB, SaaS event APIs, and Web gateways adds depth, helps establish normal, and creates correlation potential to see end-to-end attack event strings.
Alert and Case Management

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.

Alert and Case Management helps 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.
Turnkey Playbooks

Turnkey Playbooks automate repeated workflows for investigation into compromised credentials, external attacks, or malicious insider use cases. Turnkey playbooks use Exabeam automation to offer pre-built playbooks that work without requiring configuration or investment in additional third-party products, so analysts can respond to common security scenarios such as phishing with a single product.

Incident Responder

Incident Responder is an option that allows analysts to orchestrate and automate repeated workflows with APIs to 65 different vendors and 100 products with 576 response actions, from semi to fully-automated activity. With Incident Responder, analysts can automate gathering key pieces of information about incidents via integrations with popular security and IT infrastructure, and run response playbooks to programatically perform investigation, containment, or mitigation. Responding to threats faster means organizations better utilize their existing processes and tools, and drastically improve analyst productivity.

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.

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.

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 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

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.