# The New-Scale Security Operations Platform

The AI-driven New-Scale Security Operations Platform: Bring an end to your SIEM nightmares. It's time for faster, easier, and more accurate threat detection, investigation, and response (TDIR).

Organizations face a challenging landscape in security operations, struggling to identify critical threats amid an overwhelming flood of data and disparate tools. Complex, siloed solutions generate low-fidelity alerts, requiring manual analysis with limited success, particularly against credential-based attacks that continue to evade most security information and event management (SIEM) tools. In addition to this, according to Enterprise Strategy Group, 61% of security professionals surveyed claimed that the skills shortage has led to increasing workloads for existing staff.

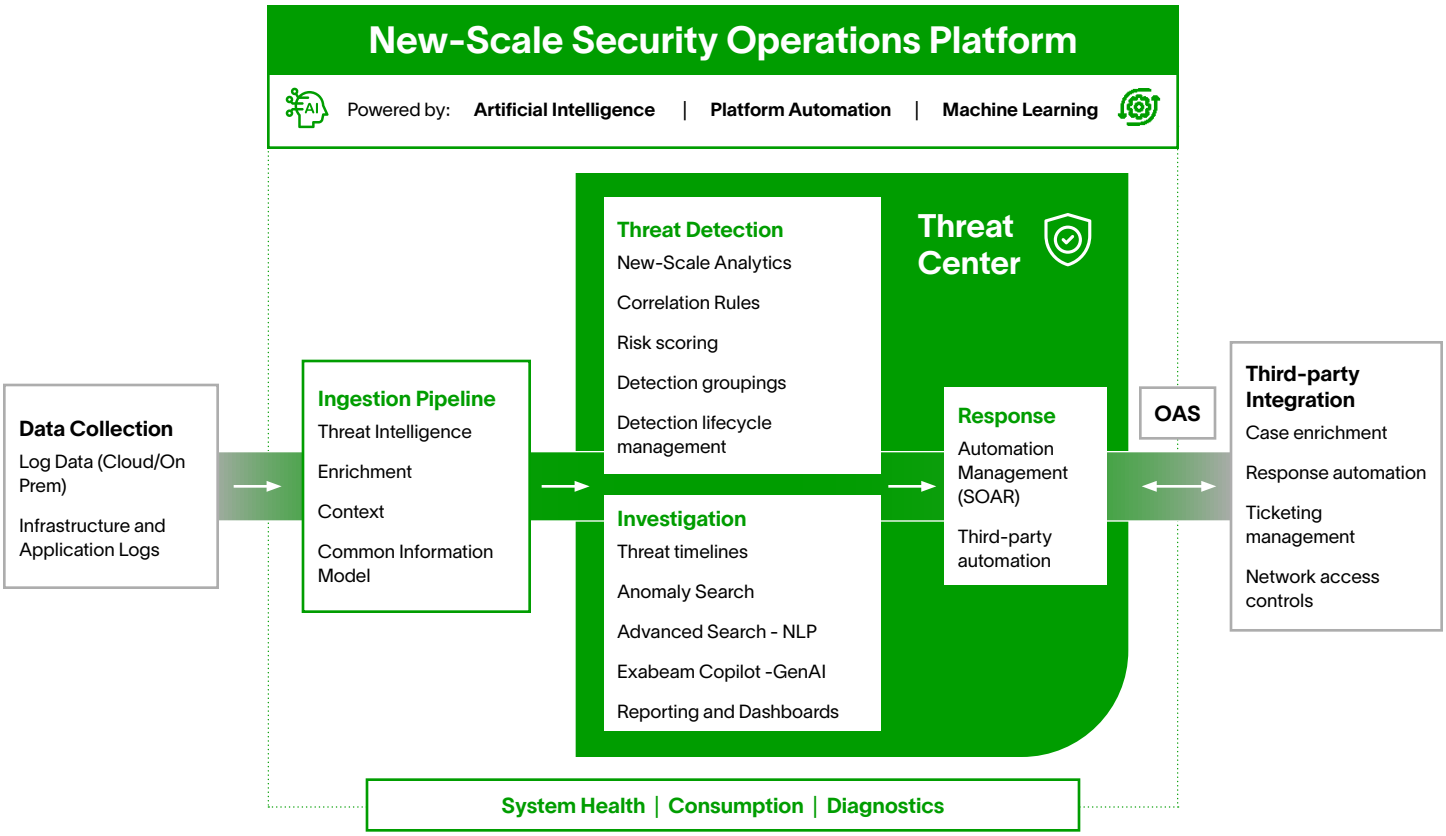
Compounding these challenges, organizations continue to rely on siloed security point products that fail to provide holistic insights. Recognizing this, organizations are consolidating tools and looking for SIEM products with native capabilities for a more integrated and effective approach.

Security operations teams are drowning in noise, desperate to deliver strategic security outcomes while maximizing existing investments. Addressing these challenges requires a shift towards unified platforms, automated analysis, and AI-powered solutions that can detect high-risk threats, enable swift response, and, ultimately, turn these security investments into proactive protection.

## New-Scale Security Operations Platform

The New-Scale Security Operations Platform applies AI and automation to security operations workflows for a holistic approach to combating cyberthreats, delivering the most effective TDIR. AI-driven detections pinpoint high-risk threats by learning normal behavior of users and entities and prioritizing threats with dynamic, multi-layer risk scoring. Automated investigations simplify security operations, correlating disparate data to create threat timelines. Playbooks document workflows and standardize activity to accelerate investigation and response. Visualizations map coverage against the most strategic outcomes and frameworks to bridge data and detection gaps. Exabeam empowers security operations teams to achieve faster, more accurate, and more consistent TDIR.

The New-Scale Security Operations Platform combines SIEM, TDIR, user and entity behavior analytics (UEBA), and security operations center (SOC) automation into a single experience, and is modular enough to allow each SOC persona to work efficiently and independently. The combined capabilities include scalable and dynamic log retention, rapid data ingestion, AI-assisted, lightning-fast query performance, and powerful behavioral analytics




to uncover threats that other tools overlook. More than 500 pre-built rules and behavioral models automatically learn normal user and device behavior to detect, prioritize, and respond to anomalies based on risk. Additionally, Exabeam offers the first security operations platform compatible with the Open API Standard (OAS), setting a new benchmark for openness in SOC automation. By integrating third-party solutions and best-of-breed tools into a unified experience, the New-Scale Security Operations Platform delivers the ultimate flexibility for customers to leverage existing security investments, while also benefiting from Threat Center.

At the heart of the New-Scale Security Operations Platform is Threat Center. Threat Center simplifies security analyst workflows by centralizing threat management, investigative tools, and automation within a single workbench. Threat Center reduces alert fatigue with prioritization, automated evidence collection, and timeline creation, providing every analyst with a consistent view of threats. Correlating disparate alerts allows organizations to mitigate an entire threat at once, not just a portion of it.

Threat Center also features Exabeam Copilot, the generative AI experience of the New-Scale Security Operations Platform. Exabeam Copilot offers an AI assistant that provides on-demand guidance, including threat explanations with suggested next steps. A simplified TDIR workflow combined with AI insights and automation make Threat Center invaluable for delivering faster and more accurate investigation and response.

## Benefits

- **Pinpoint high-risk threats**
- **Fast, more accurate investigation and response**
- **Improve threat coverage**
- **Realize the full potential of your security investments**

## The New-Scale Security Operations Platform Features Overview

| Features | Core | Add-on Options |
|---|---|---|
| **Collectors** | ● | |
| **Context Management** | ● | |
| **New-Scale Analytics** | ● | |
| **Threat Center** | ● | |
| **Exabeam Copilot** | ● | |
| **Outcomes Navigator** | ● | |
| **Threat Intelligence Service** | ● | |
| **Log Stream** | ● | |
| **Search** | Past 30 days | |
| **Pre-built Dashboards** | • Correlation<br>• Noteable events and alerts<br>• Case Management | |
| **Custom Dashboards** | ● | |
| **Detection Management** | ● | |
| **Audit Logging** | ● | |
| **Service Health and Consumption** | ● | |
| **Notifications Service** | ● | |
| **New-Scale API** | ● | |
| **Correlation Rules expansion packs (100)** | | ○ |
| **UEBA expansion packs (100)?** | | ○ |
| **Long-term Search add-on (Sold by TB)** | | ○ |
| **Long-term Storage add-on (Sold by TB) – unlimited duration** | | ○ |
| **API add ons** | | ○ |
| **Threat Center case retention** | | 90+ days |

## Features Descriptions

### New-Scale Analytics

New-Scale Analytics enhances SOC capabilities with multi-layered risk scoring, support for late-arriving event data, and integration with NetMon for network anomaly detection. Together, Automation Management and New-Scale Analytics deliver unparalleled SOC efficiency, advanced threat detection, and unmatched automation flexibility.

### Exabeam Copilot

Exabeam Copilot is the generative AI experience of the New-Scale Security Operations Platform. With Exabeam Copilot, security analysts gain powerful productivity and insights that will make them more efficient and effective in protecting their organization. By automating tasks, translating complex queries, and delivering threat and response insights, Exabeam Copilot helps drive improved TDIR.

### Threat Center

Threat Center simplifies analyst workflows by centralizing threat management, investigative tools and automation in a single workbench to efficiently investigate and respond to threats. Threat Center reduces alert fatigue with prioritization, automated evidence collection, and timeline creation, providing analysts a consistent view of threats.

### Automation Management

Automation Management combines security orchestration, automation, and response (SOAR) with pre-built playbooks and a no-code editor to standardize response efforts, automate repetitive processes, and decrease the time needed to resolve security incidents.

### Open API Standard (OAS)

The Exabeam New-Scale Platform is the first SOC platform to support the Open API Standard (OAS), revolutionizing how security operations integrate third-party tools. OAS compatibility enables rapid onboarding, no-code automation creation, and seamless integration, empowering analysts to automate workflows without engineering support. The new Developer Playbook Designer further simplifies playbook creation through a point-and-click interface.

### Collectors

Extensive data collection capabilities and coverage through a single interface securely configure, manage, and monitor the transport of data into the Exabeam service from on-premises, cloud, and context sources.

### Common Information Model (CIM)

Simplify the normalization, categorization, and transformation of raw log data into actionable events in support of TDIR. The CIM defines the most important fields for TDIR use cases and to help customers get the most value out of data being sent to the Exabeam platform.

### Context Management

Exabeam supports enrichment using threat intelligence, geolocation, and user-host-IP mapping. 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. Context management capabilities can used for ad-hoc lookup in searches, detection management, and dashboards.

### Dashboards

View, print, or export security event data with pre-built customized reports that map to compliance requirements, or build your own dashboards with 14 chart types. Dashboards can also be used as effective investigation tools, allowing the analyst to automate and run numerous searches simultaneously.

### Log Stream

Rapid log ingestion processing at a sustained rate of more than 2M 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. Live Tail provides self-service, real-time monitoring and management of parser performance, and visibility into the data pipeline.

### Outcomes Navigator

Maps the security log feeds that come into the New-Scale Security Operations Platform against the most common security use cases and ATT&CK framework to identify gaps and improve coverage.

## Features (cont.)

### Search

A simplified search experience, enhanced with natural language processing (NLP). Query on real-time and historical data in the same interface with blazing speed. Easily pivot from results to creating correlation rules or dashboards for visualization.

### Service Health and Consumption

Service Health and Consumption provides dashboards showing the 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. You can visualize the health and data consumption of every service and application while monitoring your connections and sources.

### Threat Intelligence Service

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 indicators of compromise (IoCs).

### Notifications Service

Notifications Service gives customers flexibility to receive notifications through the communication channel of their choosing. The Notifications service supports email, Teams, and Slack to notify users of critical alerts and threats.

## Optional Add-ons

### Correlation Rules expansion:

Sold in packs of 100 additional rules.

### Long-term Search:

For those that require more than a 30-day Search functionality, Long-term Search includes 12 months of log retention, including Correlation Rules and Dashboards, for the duration of the Search retention period, sold by TB.

### Long-term Storage:

Includes 10+ years of log archiving for compliance. Logs retrievable for use with Search, sold by TB.

### Threat Center case extensions:

Sold in 90-day increments.

## About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam™

**Learn more at**
**www.exabeam.com →**

Without limitation, the Exabeam and LogRhythm names and logos, related product, service, and feature names, and related slogans are service marks, trademarks, or registered marks of Exabeam (or its affiliates) in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.

2024 Exabeam, LLC. All rights reserved.