New-Scale SIEM

Built for the Speed and Scale of Modern Security Operations

Security teams process massive volumes of log data every day. To stay ahead of fast-moving threats, you need a SIEM that scales without slowing investigation or response.

New-Scale SIEM is a cloud-native solution that unifies log data from cloud, on-premises, and hundreds of third-party sources, including AI agent telemetry from leading AI platforms and bring-your-own AI deployments. It normalizes this data to power threat detection, investigation, and response (TDIR) and delivers real-time visibility through a single workbench.

Prebuilt correlation rules, integrated threat intelligence, and AI-driven workflows powered by Exabeam Nova streamline operations. At enterprise scale, New-Scale SIEM processes and analyzes data so your team can detect, investigate, and resolve incidents faster.

Threat Center

Unify Detection, Investigation, and Case Management

Threat Center centralizes your TDIR workflow. It automates evidence collection, tags events, and manages cases in a purpose-built system designed for high-volume ingestion.

- Review events from Exabeam and third-party tools in one place
- Analyze events individually or in correlated groups
- Apply automated triage rules to escalate high-risk activity
- Collaborate across teams with shared case context

By unifying workflows and applying automation at ingestion, Threat Center helps analysts prioritize credible threats and move from detection to resolution faster.

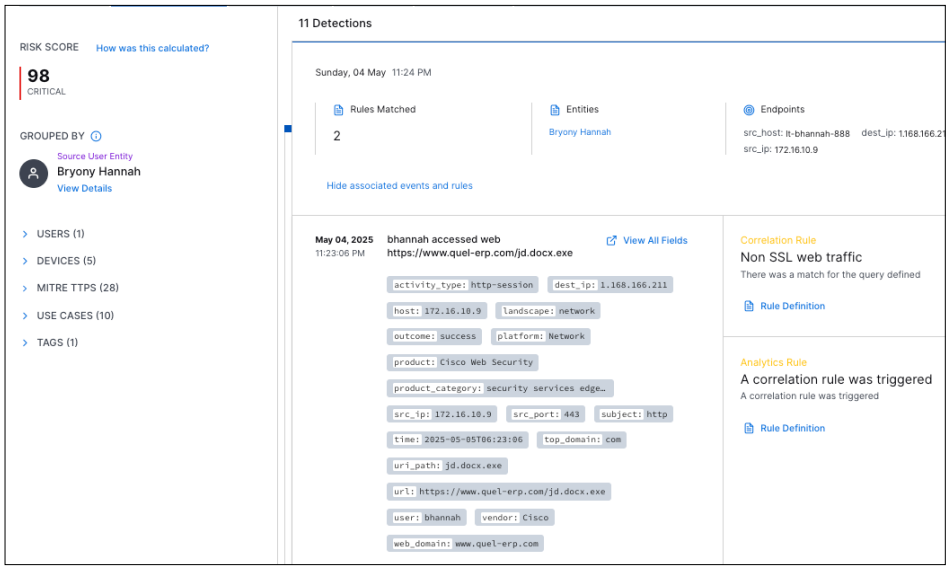

Figure 1.

Threat Center helps analysts prioritize credible threats with a unified view of cases, automated risk scoring, and a purpose-built workflow to accelerate investigation and response.

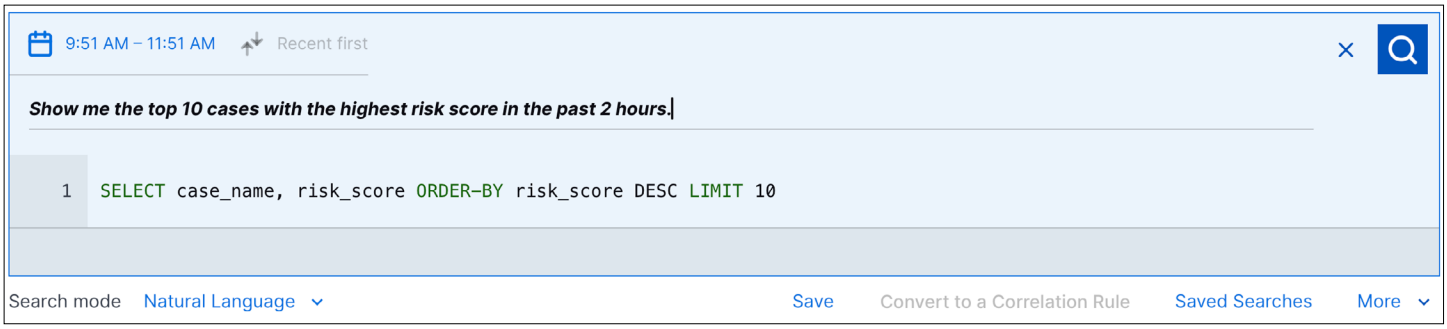

Figure 2.

The Exabeam Nova Search Agent translates natural language questions into precise queries, making advanced threat hunting fast and accessible to analysts of all skill levels.

Exabeam Nova AI Agents for Faster TDIR

Exabeam Nova is a system of purpose-built AI agents embedded in New-Scale SIEM. Each agent automates high-value work, correlates detections, and surfaces contextual evidence to reduce manual effort and speed resolution.

Search Agent

Runs complex searches using natural language. It translates questions into Exabeam Query Language (EQL) mapped to the Common Information Model (CIM), enabling fast, precise threat hunting.

Analyst Assistant Agent

Delivers context-aware answers to case questions. It reduces time spent reviewing raw logs by surfacing relevant insights immediately.

Investigation Agent

Generates case summaries, threat analyses, and recommended next steps. It identifies attack vectors, classifies threats, and highlights priority activity.

Threat Scoring Agent

Analyzes correlated events and applies dynamic risk scoring to prioritize high-value threats. When paired with New-Scale Analytics, it extends risk scoring with behavioral baselines for human and non-human identities.

Visualization Agent

Transforms natural language queries into charts and dashboards. Analysts can visualize trends in logs, detections, and system activity without manual configuration.

Advisor Agent

Provides daily insights on SIEM coverage, MITRE ATT&CK® alignment, and use case adoption. It maps coverage to frameworks including the OWASP Agentic Top 10 and recommends improvements.

Rule Creator Agent

Accelerates detection engineering with AI-assisted rule creation, tuning, and Sigma/YARA conversion. Together, these agents automate evidence gathering, correlate detections, and generate actionable recommendations. The result is faster investigations and more accurate decisions.

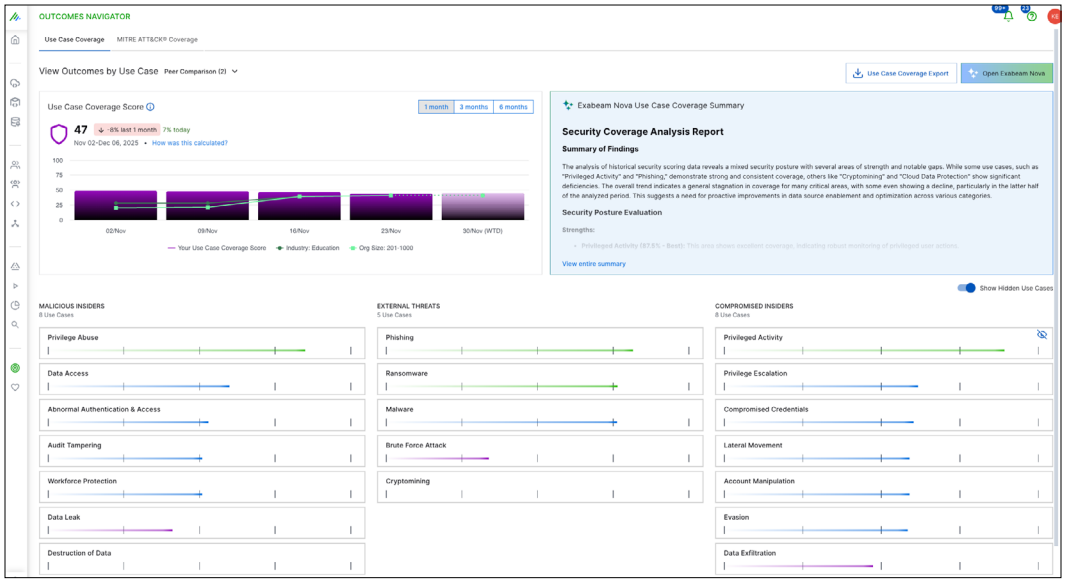

Figure 3.

Outcomes Navigator provides a boardroom-ready view of security coverage, mapping data sources to use cases and the ATT&CK framework to identify gaps and demonstrate program value.

Outcomes Navigator

Prove and Improve Your Security Program

Outcomes Navigator maps log sources to security use cases, ATT&CK, compliance frameworks, and the OWASP Agentic Top 10.

- Identify detection gaps based on current data coverage
- Recommend new log sources to strengthen visibility
- Provide measurable, defensible metrics for leadership
- Align detection coverage with use cases and compliance requirements

Integrated with the Exabeam Nova Advisor Agent, Outcomes Navigator prioritize improvements and track progress. Peer benchmarks and executive-ready reporting enable you to communicate program value and guide investment decisions.

Automation Management

Standardize and Execute Response at Scale

Automation Management reduces manual effort with prebuilt playbooks and a no-code editor.

- Coordinate response actions across tools and teams
- Escalate incidents automatically based on risk
- Notify stakeholders in near-real time
- Extend automation through hundreds of integrations

By standardizing response workflows, automation improves consistency and shortens time to contain threats.

Common Information Model (CIM)

Normalize Data for Faster Detection and Investigation

The Exabeam CIM standardizes how logs are parsed, stored, and analyzed across vendors and sources.

- Normalize disparate data into consistent fields
- Accelerate correlation and detection workflows
- Enable immediate compatibility for new log sources and use cases

CIM creates a shared data structure that simplifies analysis and supports scalable security operations.

Built on New-Scale Fusion

Scalable Foundation for Security Operations

New-Scale SIEM runs on New-Scale Fusion, a cloud-native platform for data collection, analytics, detection, and response.

- Monitor system health, uptime, and data flows in real time
- Optimize ingestion, parsing, and event streams continuously
- Close detection gaps with guided recommendations

Organizations can extend SIEM with New-Scale Analytics to apply behavioral analytics and detect anomalies across human and non-human identities.

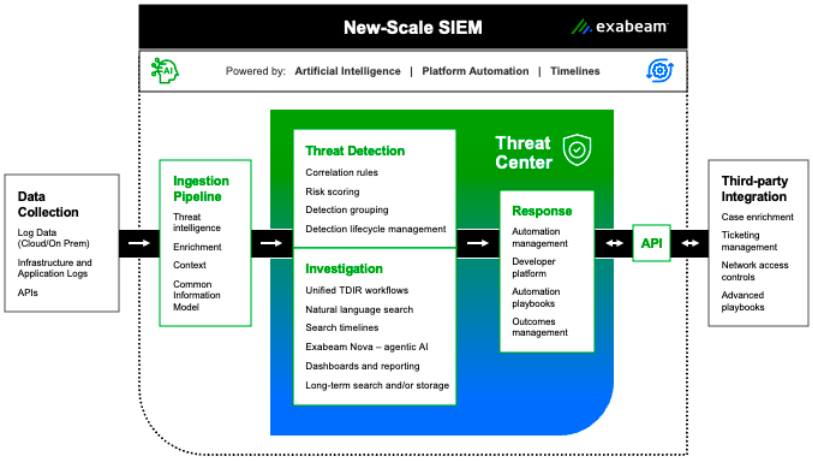

Figure 4.

New-Scale SIEM unifies log collection, detection, investigation, and response in one cloud-native solution.

Key Benefits of New-Scale SIEM

Centralize and Search Logs

Aggregate logs and contextual data in scalable storage with fast, intuitive search.

Normalize Data With CIM

Structure raw logs for faster detection, consistent analysis, and easier onboarding of new sources.

Hunt Threats Proactively

Search for indicators of compromise (IoCs) and correlated events mapped to ATT&CK and security use cases.

Automate Response

Execute coordinated actions through Automation Management playbooks and integrations.

Simplify Integrations

Use OpenAPI Standard (OAS) support to onboard data sources and connect third-party tools.

Support Compliance Reporting

Analyze and export event data for PCI, HIPAA, and other frameworks with built-in dashboards.

Identify and Close Gaps

Use Outcomes Navigator to map coverage to ATT&CK TTPs and the OWASP Agentic Top 10.

Monitor Platform Health

Track system uptime, parser performance, and license usage to maintain availability.

Extend Detection With Behavioral Analytics

Integrate New-Scale Analytics to apply behavioral baselines and identify high-risk anomalies across users, agents, and their interactions.

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR). Learn more at www.exabeam.com.

exabeam

Learn more at
www.exabeam.com →