Three Practical Ways to Accelerate Threat Hunting Using Natural Language Search

Threat hunting begins when analysts notice activity that doesn't align with normal behavior: an unexpected authentication pattern, a service account behaving like a user, lateral movement that doesn't match past incidents.

The challenge is turning those observations into evidence quickly.

Many security operations teams store years of log and event data. Yet, answering investigative questions often depends on advanced query skills that only a few team members have. That slows early investigation and limits how often your team can proactively hunt.

Natural language search removes that barrier. You can describe what you're looking for in plain language, then refine results using guided filters or advanced queries as needed.

New-Scale Fusion, New-Scale SIEM, and the LogRhythm SIEM Platform all provide natural language and flexible search capabilities designed to support threat hunting at different levels of scale and maturity.

How Exabeam Search Supports Threat Hunting

Product	Analyst Outcome
New-Scale Fusion	Combines natural language search, behavioral analytics, dynamic risk scoring, and machine-built timelines. You can ask questions, pivot directly into investigation context, and prioritize activity based on accumulated risk.
New-Scale SIEM	Provides cloud-scale log management and search with natural language input, guided field selection, long-term search, and advanced query support for deep validation.
LogRhythm SIEM	Supports natural language and unstructured search across logs, alarms, and network telemetry with the ability to replay activity and validate suspicious behavior.

Threat Hunting Flow

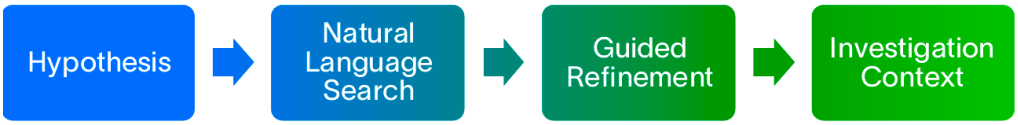

Figure 1.

Move from question to investigation without starting in a query language.

Why Threat Hunting Slows Down

Threat hunting is a proactive discipline. Analysts form a hypothesis, search available data, and adjust based on what they learn.

In practice, that process often stalls early.

New analysts may not know which fields exist or how data is normalized. Experienced analysts may understand the data but lose time translating ideas into structured queries. As a result, many investigative questions go untested, even when you suspect something is wrong.

Natural language search changes how investigations begin. You start with intent instead of syntax. The platform identifies relevant fields, applies normalization, and returns results you can refine immediately.

This approach makes threat hunting more accessible and more repeatable, even as data volumes grow.

Use Cases Supported

- Insider activity and credential misuse
- External threats and lateral movement
- Compliance-driven investigations
- Hypothesis-based threat hunting mapped to MITRE ATT&CK®

Three Ways to Search During Threat Hunts

Threat hunting doesn't follow one single path. You need flexible search options that match where you are in the investigation.

Exabeam Search supports three complementary approaches.

1. Advanced Query Language for Validation and Precision

Advanced queries allow experienced analysts to apply precise logic and conditions to large datasets. They are especially useful when you need to confirm findings, build repeatable searches, or support detection development.

In New-Scale SIEM and LogRhythm SIEM, advanced queries work in tandem with natural language search. You might begin with intent, then refine or formalize searches as the investigation progresses.

Use advanced queries to:

- Apply strict filtering or logic.
- Chain conditions in multiple fields.
- Validate findings before escalation or response.

2. Guided Search for Faster Exploration

Guided search helps you build effective searches without memorizing field names or syntax. As you type, the interface suggests relevant fields, operators, and values based on the data model.

This capability reduces trial and error and shortens time to insight, especially during early investigation.

Guided search is available within New-Scale SIEM and New-Scale Fusion and supports consistent search patterns for teams.

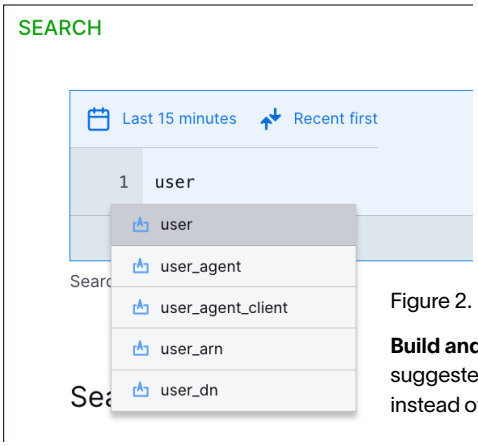

Figure 2.

Build and refine searches using suggested fields and filters instead of memorizing syntax.

3. Assisted Workflows That Reduce Manual Investigation Steps

Investigation Timelines in Search

In New-Scale Fusion, analysts can switch Search results into a timeline view to see activity ordered over time. This view turns filtered Search results into an investigation timeline for users, hosts, or other entities.

Instead of pivoting between tools or rebuilding searches, the timeline view shows how activity unfolded over time. This helps your team understand scope faster and focus effort on riskier activity.

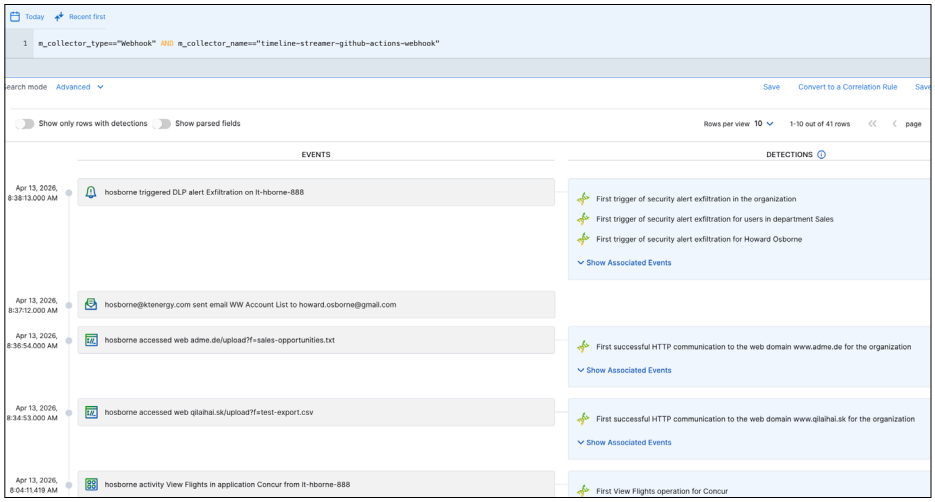

Figure 3.

The Investigation Timeline visualizes Search results as a chronological investigation sequence, helping analysts follow activity patterns and pivots over time.

Natural language search underpins each of the three approaches, giving analysts a consistent starting point for refining,

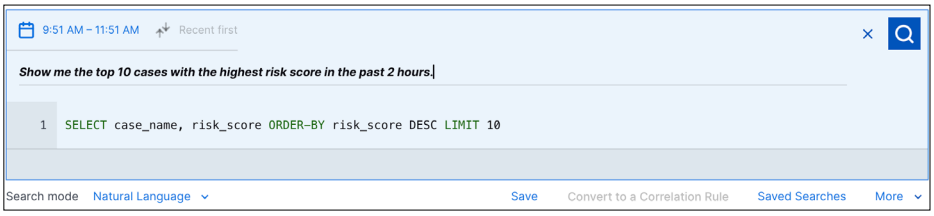

Figure 4.

Describe your search parameters using plain language.

Natural Language Search Removes the Need for Query Syntax

Threat hunting shouldn't depend on writing queries in a single language.

Natural language search lets you submit queries using everyday language. The platform translates intent into structured searches and applies normalization consistently.

This capability helps global teams collaborate and reduces friction when you think and work in languages other than English.

Consistent Results in Multiple Languages

The same investigative intent produces consistent results, even when you submit queries in different languages. This keeps investigations aligned and reduces rework for teams.

Conclusion

Natural language search changes how threat hunting starts. You spend less time translating ideas into syntax and more time testing hypotheses and investigating risk. It also lowers the barrier for less experienced analysts, allowing them to ask meaningful questions and participate in threat hunting and investigations without needing deep knowledge of complex or proprietary query language.

By combining natural language input, guided search, advanced queries, and investigation workflows, Exabeam helps security operations teams hunt threats more often and respond faster when activity escalates.

New-Scale Fusion, New-Scale SIEM, and LogRhythm SIEM each provide flexible search capabilities that fit different environments while supporting consistent threat hunting outcomes.

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 →