Five Questions to Evaluate Your AI Security Operations Strategy

A Practical Framework for Assessing Readiness, Risk, and Next Steps

As a security leader, you're likely moving quickly to apply AI across security operations. At the same time, you may be weighing new risks connected to data use, automation, and AI-driven attacks.

Few teams can say they're fully prepared. The gap is rarely intent. More often, it comes down to visibility, control, and how quickly you can act on what AI surfaces.

New-Scale Fusion runs on Google Cloud, giving you cloud-scale storage, compute, and global availability while keeping control over where your data lives.

These five questions help you assess where you stand today and where your next investments will deliver the most value.

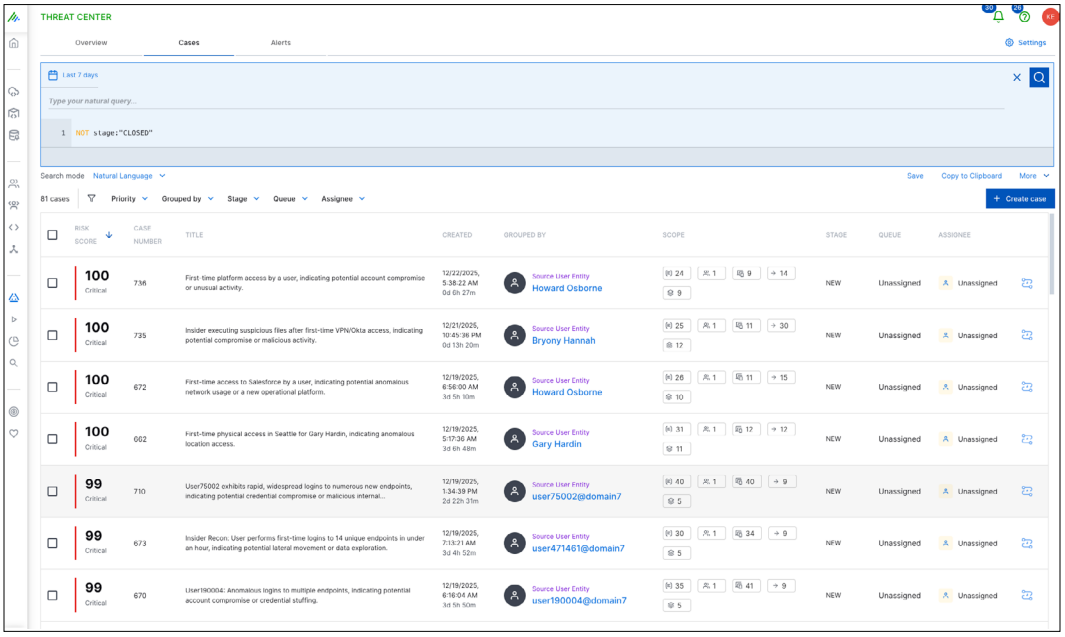

Figure 1.

New-Scale Fusion includes Threat Center, a single workbench for detection, investigation, and response.

1. How Does AI Show Up in Your Security Operations Today?

AI is not new to security operations. Exabeam has applied behavioral analytics and automation for more than a decade. What has changed is the scale security teams are expected to manage.

New-Scale Fusion brings together New-Scale SIEM and New-Scale Analytics in a single, cloud-native platform built on Google Cloud. It uses machine-learned detections, dynamic risk scoring, and automation throughout threat detection, investigation, and response (TDIR).

As you evaluate your environment, ask yourself:

- Where does AI already reduce manual analysis and noise for your team?
- Which detections improve when behavior, context, and risk are evaluated together?
- How consistently do investigations follow the same steps and logic, regardless of who works the case?
- Which metrics define success, such as time to detect, time to respond, or analyst workload?

Outcome focus: When AI is working well, you see fewer false positives, faster investigations, and more time spent on real risk.

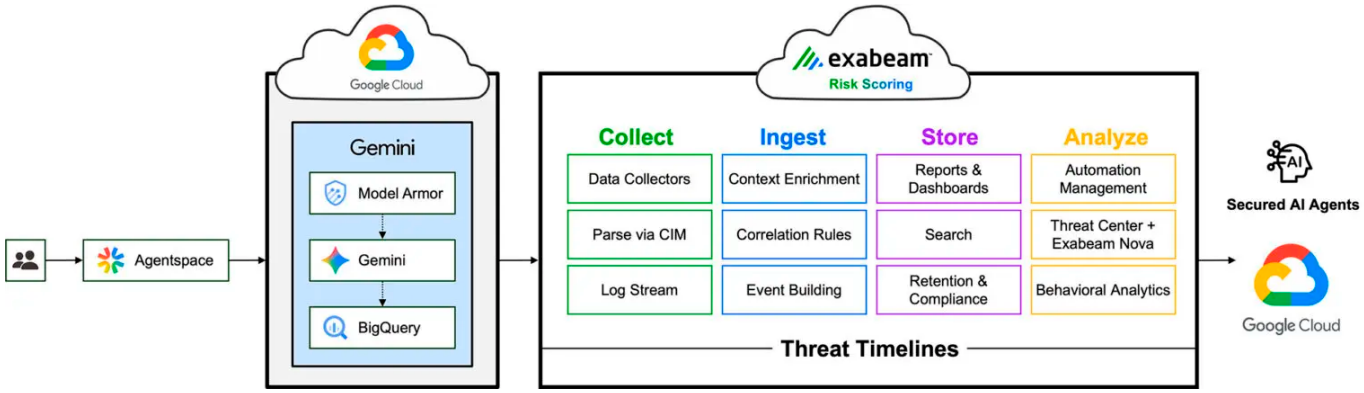

Figure 2.

New-Scale Fusion runs on Google Cloud to collect, analyze, and act on security data at scale.

2. How Does AI Change Your Data Handling and Privacy Requirements?

AI increases the value of your security data. It also raises the stakes for how that data is handled, stored, and governed. Where your platform runs matters just as much as what it analyzes.

You need visibility into how data is ingested, stored, analyzed, and shared, especially when AI is involved. This includes logs related to users, service accounts, and AI agents.

With New-Scale Fusion on Google Cloud, you control where your data is stored and how long it is retained while applying behavioral analytics and automation at scale. This foundation supports regional residency, tenant isolation, and consistent performance as data volumes grow.

As you review your posture, consider whether:

- Sensitive data stays governed according to your policies and obligations.
- Access controls and auditability extend into AI-driven workflows.
- Data usage remains transparent for internal teams and trusted partners.

Outcome focus: You can use AI without expanding risk or eroding trust.

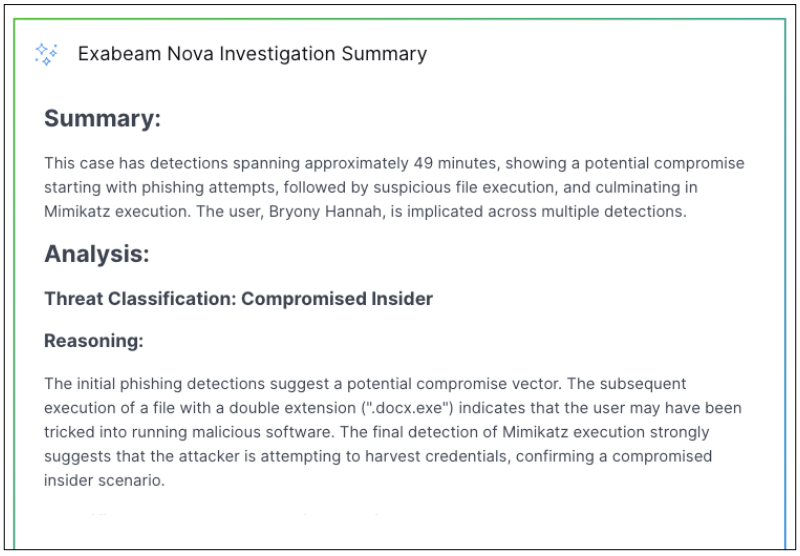

Figure 3.

Exabeam Nova summarizes activity, explains risk, and classifies threats so investigations progress faster.

3. Which AI Use Cases Deliver Value Now, and What Comes Next?

Near-Term Impact

Today, AI helps reduce friction in day-to-day security operations:

- Faster onboarding of data sources through normalized parsing and a Common Information Model (CIM)
- Natural-language search and summarization that reduce time spent writing queries
- Threat explanations that clarify why an alert matters and what to do next
- Guided investigations that reduce guesswork and missed steps

These capabilities shorten investigation cycles and reduce analyst fatigue.

Medium-Term Progress

As AI capabilities mature, you can expect:

- Insights to surface automatically instead of waiting on dashboards
- Risk to be prioritized based on behavior, not static rules
- Investigations to begin with signals that already include context

Exabeam Nova plays a central role here. Embedded in Threat Center, it automates evidence collection, correlates detections, and recommends next steps during investigations. Running on Google Cloud allows these capabilities to scale as your environment grows, without tradeoffs between data retention, performance, and cost.

Outcome focus: You spend less time chasing alerts and more time reducing real risk.

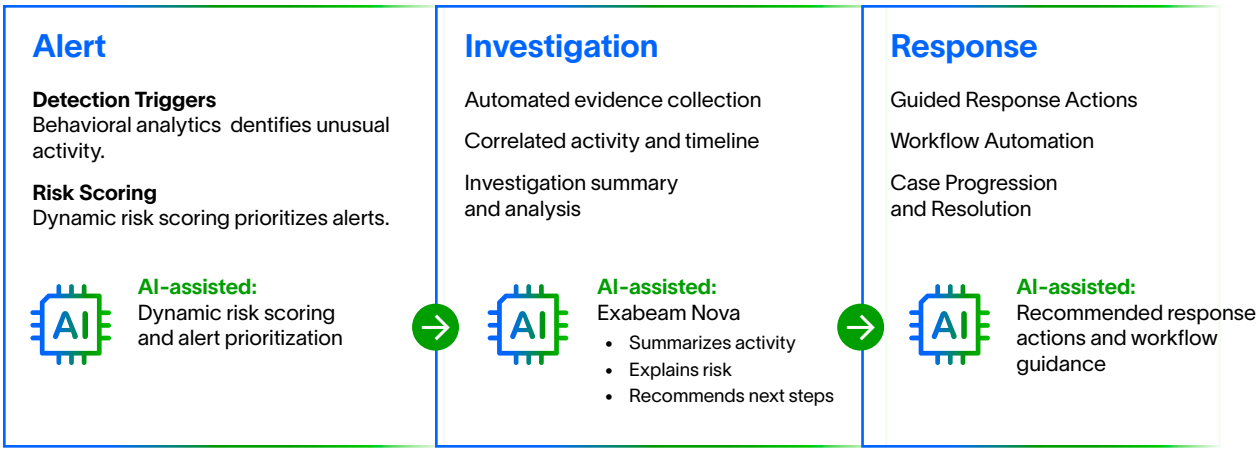

Figure 4.

AI-assisted workflows guide alerts through investigation and response, reducing manual effort and keeping teams focused on genuine risk.

4. How Are You Enabling Your Team to Work Alongside AI?

AI doesn't replace people. It changes how your team spends its time.

When repetitive tasks are automated, analysts can focus on judgment, validation, and response. That shift requires enablement, not just technology.

Strong programs make sure:

- Analysts understand how AI reaches conclusions.
- Investigations remain explainable and reviewable.
- Teams trust automation enough to act on it.

New-Scale Fusion standardizes workflows so investigations follow a shared process, regardless of experience level. Exabeam Nova reinforces that consistency by guiding each step. Because these workflows run on Google Cloud, your team gets consistent performance without managing infrastructure.

Outcome focus: Your analysts resolve incidents faster and spend more time on meaningful work.

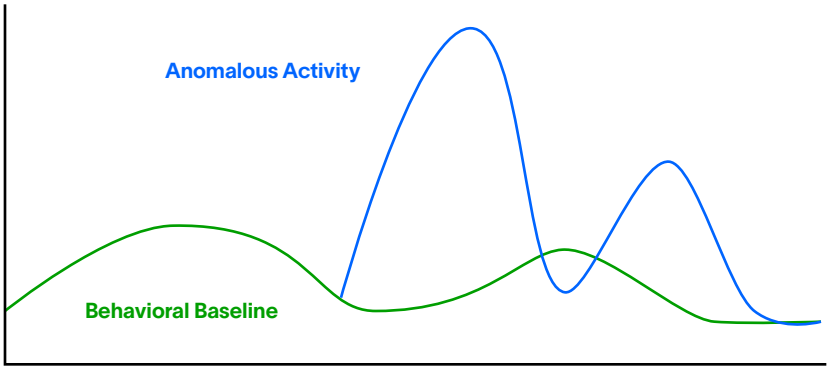

Figure 5.

Behavioral analytics establishes a baseline of normal activity and surfaces meaningful deviations that indicate risk.

5. Are You Prepared for AI-Driven Attacks?

Threat actors already use AI to increase scale and complexity. You should expect that trend to continue.

Common AI-driven attack patterns include:

- Highly targeted phishing and social engineering
- Rapidly changing malware variants
- Infrastructure designed to evade static controls

Behavioral analytics is one of the most effective ways to detect these attacks. By evaluating how users, entities, and agents behave over time, New-Scale Analytics helps you identify risk even when tactics change.

Detecting these patterns requires analyzing large volumes of behavior over time. New-Scale Analytics delivers that capability at scale on Google Cloud.

Outcome focus: You detect intent and abnormal behavior before damage spreads.

Build an AI-Driven Security Operations Program

Exabeam helps you apply AI where it produces measurable outcomes.

New-Scale Fusion unifies data collection, behavioral analytics, and response workflows in a cloud-native platform built on Google Cloud. This foundation gives you the scale to retain and analyze more data while maintaining control over where that data lives.

Exabeam Nova works throughout investigations to automate evidence collection, correlate related activity, and recommend next steps. By reducing manual work and standardizing how investigations progress, your team can move faster and stay focused on real risk.

Together, Exabeam and Google Cloud help you:

- Shorten investigation and response cycles.
- Improve detection quality through behavioral context.
- Scale security operations without adding operational overhead.

To see how this approach works in practice, request a demo.

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).

exabeam

Learn more at
www.exabeam.com →