What Comes Next for Your AI Cybersecurity Strategy?

Evaluate your strategy and potential next steps with five key questions

Security leaders worldwide are eagerly exploring AI—especially generative AI (GenAI)— use cases within their environments while also worrying about its implications for organizational cybersecurity.

Today, no security leader can confidently claim they can mitigate AI-related threats and risks. To understand your weak points and where to strengthen your position, here are five questions to answer about how your organization handles this cutting-edge technology. As you answer, consider an emerging challenge: how you will secure the AI you build yourself. The GenAI-powered agents and automations that organizations are now deploying create a new class of digital insiders that require a new security approach.

1. How are we currently using AI in our security operations?

While headlines make AI feel like a recent phenomenon, it has been around for decades. Exabeam has employed AI for user and entity behavior analytics (UEBA) and automated the threat detection, investigation, and response (TDIR) workflow for over ten years. The UEBA and TDIR features in the Exabeam Security Operations Platform also use AI to increase detection accuracy and security operations center (SOC) productivity.

Maximize the impact of your security operations by:

- Evaluating how your current solutions leverage AI
- Learning how and where you can further employ AI within your solutions
- Exploring how to use AI to combine and augment your existing solutions
- Defining your KPIs, such as mean time to detect and repair

2. What impact does AI have on our data handling and privacy policies?

While AI helps you use your existing data in new ways, it creates new implications for handling and protecting data. AI—especially GenAI—will have a significant impact on your sensitive data handling and storage. The consequences of improper data use can lead to legal action or fines.

Ensure that:

- Sensitive data is segregated from your GenAI models so they do not use private or customer data for training.
- You and your partners are accessing and using the data in ways that maintain customer trust and ensure regulatory compliance.

3. What are the near- and medium-term AI use cases for our security?

AI will impact your teams in the near and medium term. In the near term, AI can help your teams streamline and automate processes across security operations.

In the medium term, advanced natural language processing (NLP) will enable your security analysts to use conventional language instead of code to retrieve logs and take action. Instead of analyzing dashboards, AI will automatically surface those insights.

Ensure that:

- Your teams understand how intelligent data tagging and parsing of security data works along a common information model (CIM). These capabilities will ingest new data and context.
- Having a transition plan to move your SOC analysts away from query language codes and toward NLP searches to construct complex search queries.
- Your teams are prepared to use threat explainers and conversational SOC assistants. These features will help your team increase its speed, effectiveness, and cybersecurity knowledge.
- Your security strategy accounts for the digital workforce you build on Google Cloud. Exabeam can ingest security signals from agents created with Vertex AI and Agent Builder, and from platforms like Google Cloud Agentspace. By baselining agent behavior, your SOC can detect compromises and ensure your AI innovations are deployed securely.

4. How are we training and supporting our SOC team to employ AI?

AI will not replace your SOC personnel. Humans will always have to review AI output. Instead, it will simplify and automate manual and repetitive tasks to help your team do more faster. It will undoubtedly impact how security engineers, analysts, managers, threat hunters, and security leaders work.

Ensure that:

- Every member of your SOC team knows how to maximize the effectiveness of AI in your tools and processes.
- All team members have the training and skills required to leverage these AI benefits.

5. How do we adapt our cybersecurity strategy to counter AI-driven threats?

While AI will help you significantly scale your security operations, threat actors already use AI to launch larger, more complex, and harder-to-detect attacks.

Expect and prepare for more:

- Targeted social engineering and phishing attacks against your users.
- Polymorphic attacks that constantly change code to evade your detection.
- Domain-generating algorithms that create command-and-control servers to install malware on your users' devices.

Build an AI-driven SOC

Exabeam and Google Cloud can help you answer these questions and build an AI-driven SOC function for your organization.

Built on Google Cloud's technology, Exabeam provides the industry's most complete, AI-driven security operations platform for TDIR in security log management, behavioral analytics, and automation. These solutions help security teams detect, defend, and defeat complex threats.

Exabeam uses AI-driven automation to improve the analyst experience by controlling more data sources at higher volumes. This control increases the fidelity of detections and provides faster views of data flow and parser health. These capabilities are further enhanced by Exabeam Nova, an autonomous AI agent embedded in Threat Center that goes beyond simple assistance to proactively investigate threats, correlate detections, and recommend or initiate response actions. Importantly, Exabeam Nova's behavioral analytics capabilities also extend to the AI agents your organization builds, allowing it to monitor them as non-human entities and detect anomalous activity. By automating complex investigative workflows and providing high-fidelity insights, Exabeam Nova enables SOC teams to simplify investigations, improve internal risk communications, and accelerate threat resolution.

Together, Exabeam and Google Cloud create a cloud-native, AI-powered portfolio of security solutions that provide customers with cloud-scale storage and TDIR. To see how your security team can use this portfolio to detect, defend, and defeat complex threats, request a demo.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

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.

2025 Exabeam, LLC. All rights reserved.