

November 2024

# GenAI-powered Cybersecurity Vendor Landscape

The report provides a comprehensive overview of the Generative AI powered cybersecurity market landscape, exploring tools and vendors essential to automate tasks, address new threats, and bridge skill-gap.

AIM Research is the world's premier AI and data science market research firm and advisory council, specializing in delivering transformative insights into modern markets.

[aimresearch.co](https://aimresearch.co)

**CONFIDENTIAL AND PROPRIETARY:** This document is the result of research carried out by **AIMResearch**. Permission may be required from AIMResearch for the reproduction of the information in this report. Reasonable efforts have been made to source and present data that is believed to be reliable but makes no representations or warranty, express or implied, as to their accuracy or completeness or correctness. All rights reserved with the aforementioned parties.

© 2024 **AIM Media House LLC** and/or its affiliates. All rights reserved. Images or text from this publication may not be reproduced or distributed in any form without prior written permission from Analytics India Magazine. The information contained in this publication has been obtained from sources believed to be reliable. Analytics India Magazine disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This publication consists of the opinions of Analytics India Magazine and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

# Table of Contents

---

Executive Summary 04

---

Key Research Findings 05

---

Introduction to GenAI-powered Cybersecurity 06

- Evolving Landscape of Cybersecurity
  - Generative AI in Cybersecurity
- 

Deep Dive into GenAI-powered Cybersecurity 09

- Current State of Cybersecurity
  - GenAI-powered Cybersecurity Over Conventional Solutions
  - Need for GenAI-powered Cybersecurity Solutions
  - Key Applications
- 

Vendor Landscape of GenAI-powered Cybersecurity Tools and Platforms 15

---

AIM Research's PeMa Quadrant Methodology 18

---

PeMa Quadrant for GenAI-powered SOC Analyst Platforms 22

---

Vendor Profiles 24

---

# Executive Summary

The landscape of cybersecurity is undergoing a transformative shift with the integration of Generative AI (GenAI) technologies. This report explores the current state of GenAI-powered cybersecurity solutions, highlighting key vendors, their offerings, and the implications for organizations navigating an increasingly complex threat environment.

**AIM Research defines GenAI-powered cybersecurity as the integration of generative artificial intelligence technologies into cybersecurity solutions to enhance the detection, triage, and response capabilities against cyber threats.** By leveraging large language models (LLMs), automation architecture, and advanced machine learning techniques, these solutions empower security teams to improve their overall security posture.

The report begins by outlining the fundamental concepts necessary for understanding the GenAI-powered cybersecurity market. It then identifies the relevant tools and vendors in the space. Finally, the report ranks these vendors on AIM Research's Penetration and Maturity (PeMa) Quadrant matrix.

Vendors are expanding their product lines to include a variety of GenAI-powered solutions such as AI agents, copilots and context-aware AI assistants, integrated security platforms with automation and analytics capabilities, and simulation and training platforms. These advancements aim to improve threat detection, automate security processes, and provide actionable insights for security teams.

# Key Research Findings

## Rise in Adoption

All major cybersecurity solution providers have either launched new GenAI security tools or integrated GenAI capabilities into their existing suite of solutions

## Driving Factors

Skill-gap, burnout crisis, need for automating repetitive and complex tasks, and increased threats drive the adoption GenAI-powered tools

## Diverse Product Offerings

Vendors are broadening their offerings with GenAI-powered AI agents, copilots, context-aware AI assistants, automation and analytics security platforms, and training simulators

## Key Features Offered

Intelligent summarization, querying in natural language, conversational functions in multiple languages, proactive security, alert prioritization, decision ready analysis, guided recommendations, and automation

## Availability of New Features

Vendors offering GenAI-powered features are transitioning from private preview for select partners to public preview in 2024, with some already generally available

## Growth Plans

Vendors have moved beyond providing intelligent summarizations and are now focusing on proactive security and risk prioritization. We can expect them to enhance functionalities in autonomous threat detection and recommendations, while also providing clarity on how the systems reach specific conclusions

# Introduction to GenAI-powered Cybersecurity

# Evolving Landscape of Cybersecurity

The evolution of AI technology in cybersecurity has transitioned from traditional machine learning methods to sophisticated AI-native and Generative AI solutions that enhance predictive capabilities and automate complex tasks. As cyber threats continue to evolve, integrating these advanced technologies will be crucial for organizations seeking to fortify their defenses and respond effectively to an increasingly complex threat landscape.

In 2016 and 2017, we saw how IBM's Watson distinguished itself by utilizing natural language processing to analyze vast amounts of unstructured data, which allowed it to provide cognitive insights and augment human analysts' capabilities. This approach marked a significant advancement in how AI could be applied within cybersecurity operations, particularly in handling the increasing complexity and volume of security threats.

Since then organizations and cybersecurity companies have continued to invest in developing AI and advanced machine learning capabilities. AI was leveraged to predict zero-day vulnerabilities and advancing beyond traditional signature-based systems and positioning the technology as key to improved cyber defense capabilities.

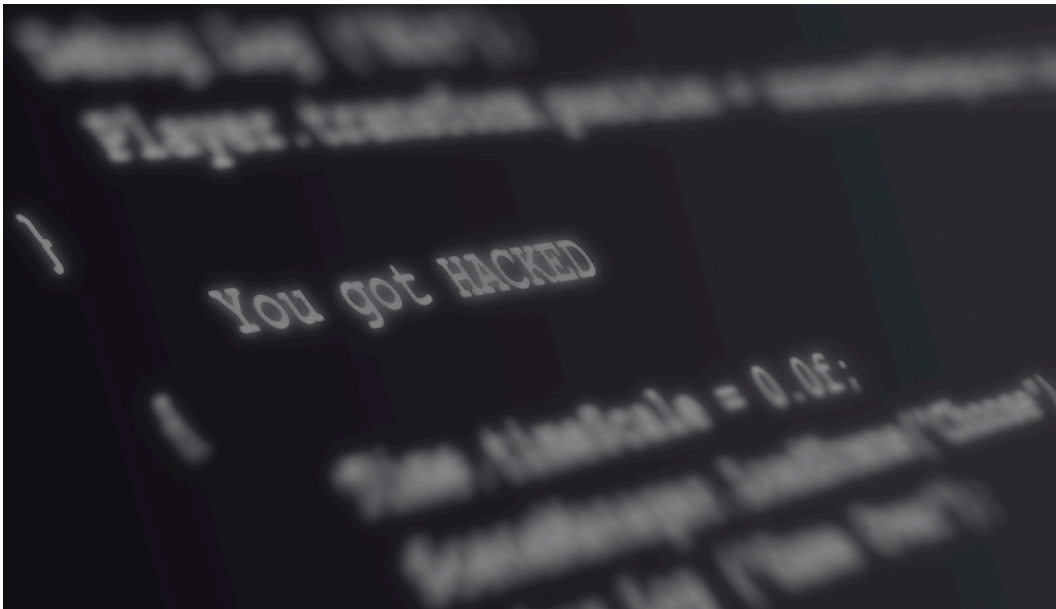
With the maturation of AI technologies, all major Cybersecurity solution providers have added AI capability layer to their existing cybersecurity solutions and/or planning for an AI-native architecture based product from the start. With the emergence of GenAI, we are now noticing a rise in the integration of Generative AI-specific capabilities into cybersecurity tools.

Initially, the vendors rolled out GenAI integrated solutions in a private preview, but we are now seeing many of these becoming generally available.

# Generative AI in Cybersecurity

GenAI offers potential for automating routine tasks, providing remediation guidance, and enhancing threat detection. While GenAI offers substantial benefits for cybersecurity, it also poses risks, as bad actors can exploit these technologies to launch more sophisticated attacks.

This dual-use nature of GenAI highlights the need for organizations to balance innovation with robust security practices, ensuring that while they harness the benefits of generative technologies, they also mitigate associated risks.



“84% of the executives plan to prioritize generative AI cybersecurity solutions over conventional ones, according to IBM Institute for Business Value.”



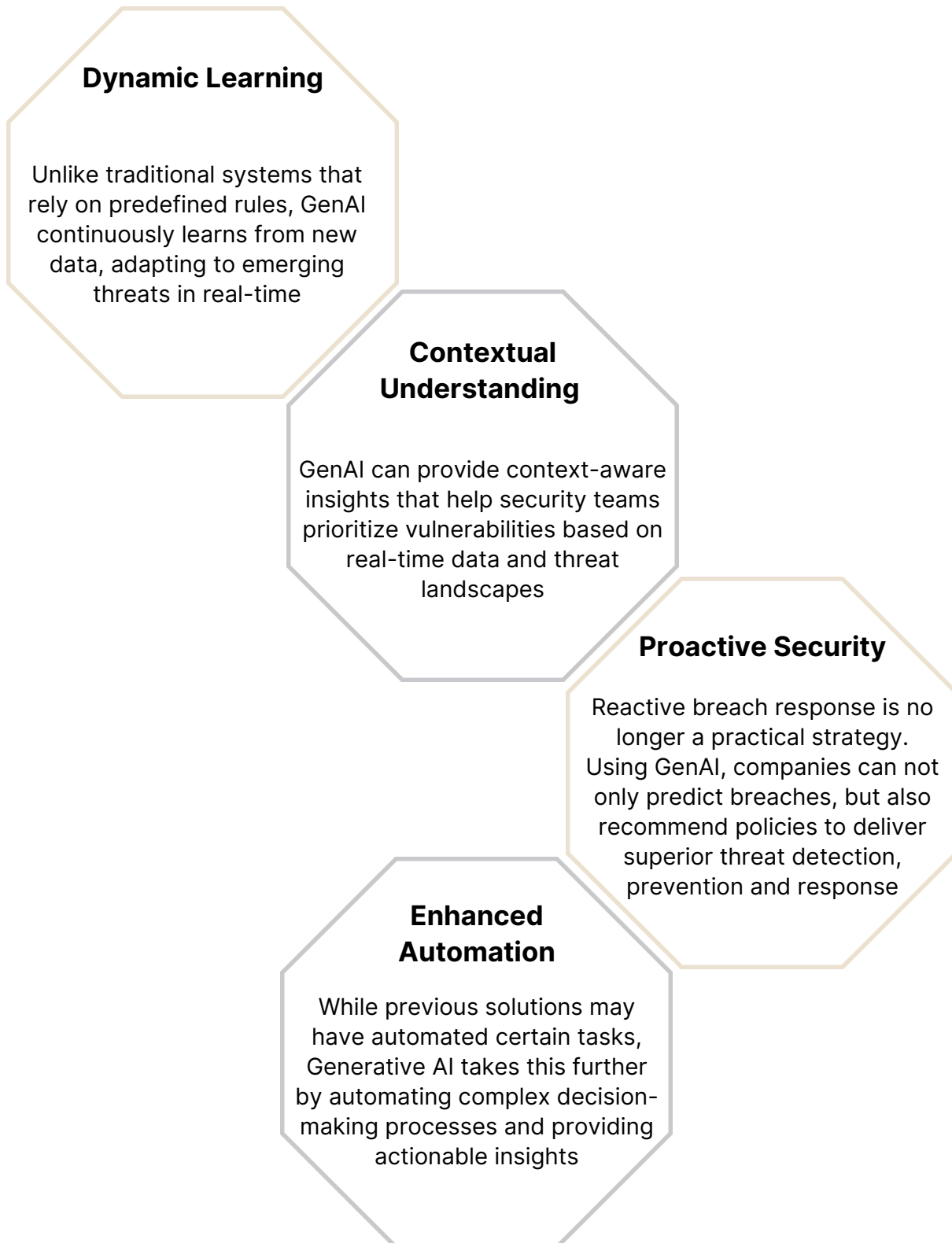
# Deep Dive

Understanding the need for GenAI-powered Cybersecurity Solutions



*Since the launch of IBM Watson for cybersecurity in 2016 to the rise of AI-native cybersecurity platforms, the industry has focused on creating solutions to address the persistent cybersecurity skills gap, as well as challenges related to automation and emerging threats.*

# GenAI-powered Cybersecurity Over Conventional Solutions



# Need for GenAI-powered Cybersecurity Solutions (1/2)

## 1. Supplementing Understaffed Security Teams and Bridging the Skill Gap

According to [ISC2 survey](#),

- **Increase in Demand and Workforce Gap:** In 2023, there were roughly four million cybersecurity professionals needed in the workforce, a 12.6% increase from the previous year.
  - **Skill Gap:** 92% of professionals polled reported having cybersecurity skills gaps within their organizations.
- 

## 2. Enhanced Threat Detection and Response

Generative AI is significantly improving threat detection capabilities by analyzing normal behavior patterns to identify anomalies indicative of potential threats. Recent advancements include:

- **Malware Simulation:** GenAI can generate simulations of malware to understand its behavior and identify new threats, allowing organizations to proactively defend against emerging risks.
  - **Real-Time Anomaly Detection:** By leveraging large datasets, GenAI can quickly detect deviations from established baselines, enabling faster responses to potential incidents.
- 

## 3. Predictive Threat Intelligence

Organizations are increasingly using GenAI for predictive analytics to foresee potential security events. Key advancements include:

- **Data Ingestion for Forecasting:** GenAI can process vast amounts of data to create a frame of reference for future security events, enhancing predictive threat intelligence and vulnerability management.
- **Automated Vulnerability Management:** GenAI can predict vulnerabilities in applications and recommend or automate patches based on historical data, streamlining the vulnerability management process.

# Need for GenAI-powered Cybersecurity Solutions (2/2)

## 4. Automation of Security Operations

The automation capabilities of GenAI are revolutionizing cybersecurity operations:

- **Incident Response Automation:** GenAI can automate incident response workflows by providing security analysts with strategies based on successful tactics from past incidents, thereby speeding up response times.
  - **Security Patch Automation:** Using neural networks, GenAI can scan codebases for vulnerabilities and either apply or suggest appropriate patches through NLP and ML algorithms.
- 

## 5. Phishing Prevention

Advancements in phishing prevention technologies are noteworthy:

- **Language Pattern Analysis:** GenAI can analyze language patterns in emails to create models that detect and filter out phishing attempts more effectively than traditional methods.
  - **Malicious URL Detection:** The technology can also analyze URLs for malicious content, enhancing overall email security.
- 

## 6. Context-Aware AI Assistants

Recent innovations include the development of context-aware AI assistants that help organizations navigate complex security environments.

---

## 7. Compliance Automation

As regulatory requirements evolve, GenAI tools are being developed to ensure compliance:

- **Automated Compliance Monitoring:** AI will be able to regularly scan systems to ensure they meet all regulatory requirements, thus reducing the burden on compliance teams.

# Key Applications of GenAI-powered Cybersecurity Tools

Upon analyzing the key vendors that currently offer Generative AI-powered cybersecurity solutions, we observe the following areas where the solutions are focused.



### Security Operations

Augment Security analysts and automate repetitive and complex operations



### Endpoint Security

Improve protection of endpoints and devices



### Cloud Security

Address the unique security challenges of cloud environments



### Application Security

Identify and mitigate vulnerabilities in applications



### Identity and Access Management (IAM)

Enable robust identity verification and access control



### Network Security

Enhance threat detection and response in network environments



### Service and Help Desk

Make it easier to look up technical information and isolate the root cause of user complaints

# Vendor Landscape

In this section, we dive into the categorization of tools, platforms, and the vendors offering them.

# GenAI-powered Cybersecurity Tool Categories

1

## AI Agents

AI Agents are autonomous/semi-autonomous systems that utilize Generative AI to monitor networks, analyze threats, and respond to incidents with minimal human intervention.

Example: Dropzone AI replicates the techniques of elite analysts and autonomously investigates every alert.

---

2

## Copilots and AI Assistants

Copilot enables IT teams to identify the root causes of issues, assist in triaging end user problems, reduce escalations, enhance their knowledge through interactive questionnaires, and drive cost savings by freeing up resources in compute, network, security, and application teams that support end users.

---

3

## GenAI-integrated Cybersecurity and Analytics Platforms

Security platforms that incorporate Generative AI for comprehensive cybersecurity across various layers (cloud, endpoints, networks, etc.).

In GenAI-powered cybersecurity, security tools are built/integrated with advanced analytics and automation capabilities, utilizing AI to enhance threat detection, response, and prediction within a single framework.

---

4

## Attack Simulation and Training Platforms

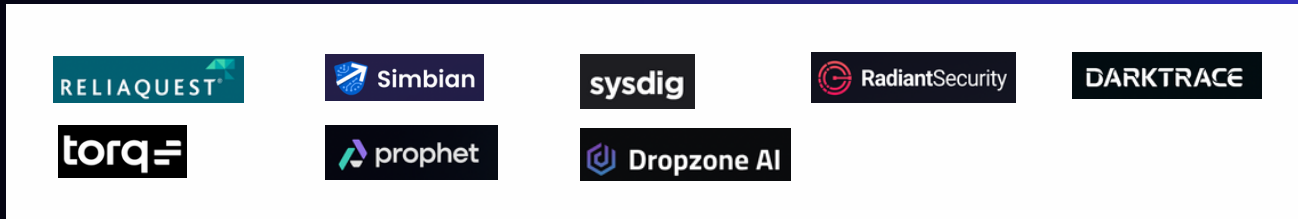
Generative AI to simulate potential vulnerabilities and test the organization's security posture, helping teams prepare for actual incidents by understanding how attackers might exploit their systems.



# GenAI-powered Cybersecurity Vendors Landscape

## AI Agents

Autonomous/Semi-Autonomous Systems to Monitor, Analyze Threats, and Respond to Incidents



## Copilots and AI Assistants\*

Advanced AI Assistants for Real-time Guidance, Actionable Insights, and Security Querying



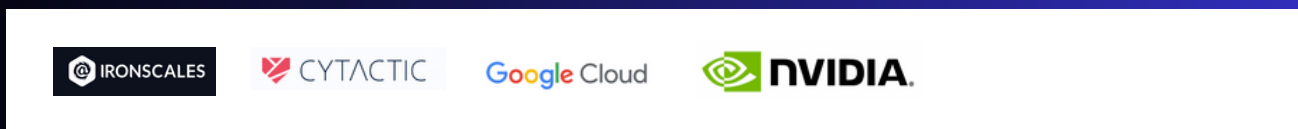
## Integrated Security, Automation, and Analytics Platforms

Platforms that incorporate GenAI for comprehensive cybersecurity across various layers (cloud, endpoints, networks, etc.)



## Attack Simulation and Training Platforms

GenAI-based systems to simulate potential vulnerabilities and test the organization's security posture



\*While some vendors launched advanced AI assistants as new products, others introduced them as features accessible through the user interface of their existing cybersecurity products

```
Invite {
message1;

Invite2 {
message1, message2;
```

```
new Invite();
msg1();
<br>;
```

```
= new Invite();
>msg1();
>msg2();
```

```
2345678;
mp(is_int($x));
```

```
2345.6789;
mp(is_int($x));
```

```
rtotime("December");
il(($d1-time()), $d2);
There are " $d2 " days
```

```
filter_var($int, FILTER_VALIDATE_INT);
{"Integer is valid";
{
{"Integer is not valid";
```

```
'f1.0';
```

```
website = "";
```

```
() {
```

# AIM Research's PeMa Quadrant Methodology

# The Quadrants

The AIM Research's Penetration and Maturity (PeMa) Quadrant uniquely combines two critical dimensions:

- **Penetration** - measuring the extent of market adoption and reach
- **Maturity** - assessing the offerings and technological advancement

## Seasoned Vendors

With **strong technical capabilities**, these vendors have made an impact in the market. However, they still must strive to keep pace with our Leaders if they wish to excel even further!

## Leaders

These vendors are highly sought-after on the market, with a **long track record of expanding reach and success in multiple sectors worldwide**. Their teams boast unparalleled experience and skillset when it comes to providing comprehensive services using cutting edge technology that's always at the forefront.

## Challengers

At first glance, Challengers may appear to be at a disadvantage when competing with larger players. However, their smaller size and scope of solutions equip them with an advantage that rivals can't compete against - **superior delivery capabilities and specialized, cost-effective solutions**.

## Growth Vendors

Among the top contenders in their industry, these **vendors have seen remarkable revenue expansion**. While they still trail behind the market leaders with regards to maturity, it's clear that impressive progress has been made.

# Assessment (1/2)

For the PeMa Quadrant assessment, we have exclusively considered vendors that provide GenAI-powered SOC Analyst Platforms.

## GenAI-powered SOC Analyst Platforms

**Definition:** AI-powered cybersecurity tools that serve as virtual SOC analysts or augment SOC analyst teams in investigating attacks. These tools utilize technologies such as LLMs, automation architecture, and advanced analytics to improve threat detection, triage alerts, and streamline incident response.

**Function:** Focus on supporting SOC analysts in monitoring, detecting, and responding to security incidents.

**Features:** Use generative AI to simulate human-like decision-making, analyze security event data, prioritize alerts, and reduce noise for efficient incident handling.



# Assessment (2/2)

The following parameters are considered for analyzing vendors offering GenAI-powered SOC Analyst Platforms:

- 
- 1 Company growth**  
Employee count and growth

---

  - 2 Launch date of GenAI-powered Cybersecurity Platform**  
The longer the platform has been tested/run in the market, the lower the model inaccuracies become

---

  - 3 Ease of use and integration**  
To understand how easily the platform integrates with existing tools to ensure a seamless workflow for cybersecurity

---

  - 4 How long has the company been offering Cybersecurity solutions?**  
Experience in the Cybersecurity market (considering non-GenAI markets as well) contributes to the company's expertise and understanding of the field

---

  - 5 Recent activity** (based on press releases)  
Company's recent alliances, R&D, and marketing activity

---

  - 6 Unique Selling Point (USP)**  
Key features, AI and automation capabilities, and differentiators

---

  - 7 Customer confidence**  
Known clients and testimonials
-



# PeMa Quadrant for GenAI-powered SOC Analyst Platforms

# PeMa Quadrant

## GenAI-powered SOC Analyst Platforms 2024



Copyright © 2024 AIM Media House LLC. All rights reserved.



# Vendor Profiles

Detailed profiles of the vendors offering GenAI-powered platforms to augment capabilities of SOC Analyst Teams





# Swimlane

Founded year: 2014

Headquarters: Denver, Colorado, USA

Employee count: 253



[Website](#)



[LinkedIn](#)

## GenAI-powered Cybersecurity Solutions

### Product:

- [Swimlane Turbine](#)

### Product Brief:

- Swimlane Turbine is an AI-enhanced security automation platform. It is the triple threat of automation, low-code and artificial intelligence teams need to solve their most challenging SecOps problems.
- Hero AI is the ultimate SecOps companion, available within the Turbine platform. Security analysts can rely on Hero AI to quickly and seamlessly understand even the most intricate cases, alerts, and intelligence.

### Key Features:

**Save 10 Minutes per AI Prompt**

**Generates Complex Python Scripts in Seconds**


**Enterprises Achieve 240% ROI in Year One**

### Differentiator:

- Turbine Platform’s AI-augmented reporting, enables one-click preparation of stakeholder-ready after-action reports.
- AI-enhanced features including case summarization, recommended actions, AI-augmented reporting, crafted prompts, text-to-code and schema inference tools help SOC teams increase their productivity by 20%, above and beyond automation alone.
- The platform features a low-code playbook building studio, enabling users to create automations using natural language and drag-and-drop functionality.
- Swimlane’s proprietary LLM keeps organization’s data always private and secure.

# Glossary

GenAI	Generative AI
GenAI-powered Tools	Tools incorporated with Large Language Models or Generative AI capabilities
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
MTTD	Mean Time To Detect
MTTR	Mean Time To Remediate
MTTC	Mean Time To Contain
IAM	Identity and Access Management
CVEs	Common Vulnerabilities and Exposures



**AIM India**

1st Floor, Sakti Statesman, Marathahalli – Sarjapur  
Outer Ring Rd, Green Glen Layout, Bellandur,  
Bengaluru – 560103

**AIM Americas**

2955, 1603 Capitol Avenue, Suite 413A,  
Cheyenne, WY, Laramie, USA, 82001

[www.aimresearch.co](http://www.aimresearch.co)

[info@aimresearch.co](mailto:info@aimresearch.co)

**AIM** | RESEARCH