# Google Cloud plans agentic AI to transform security operations



Google Cloud has announced detailed plans to integrate agentic artificial intelligence (AI) into its security operations, aiming to streamline routine tasks and enhance efficiency within security teams. This development is part of Google's broader vision to evolve security operations centres (SOCs) by introducing intelligent AI agents capable of independently identifying, reasoning through, and dynamically executing complex security tasks while maintaining ongoing collaboration with human analysts.

Unlike traditional assistive AI, which supports humans without autonomous operation, agentic AI is designed to function more independently within security workflows. Google Cloud’s newly developed AI agents, as part of its Gemini in Security suite, embody this shift towards more autonomous and collaborative AI functionality.

One of the key innovations includes the alert triage agent in Google Security Operations, which is built to perform dynamic investigations on alerts and provide conclusive verdicts. This agent uses context-aware analysis to gather supporting information, compiling detailed audit logs that explain its evidence, reasoning, and decisions. It aims to reduce the repetitive workload commonly faced by Tier 1 and Tier 2 security analysts who deal with the high volume of alerts generated each day. Google Cloud plans to make this agent available in preview to selected customers by the second quarter of 2025.

Complementing this is the malware analysis agent in Google Threat Intelligence, scheduled for preview release alongside the alert triage agent in Q2 2025. This AI is designed to reverse engineer potentially malicious files by examining suspicious code, running deobfuscation scripts, and producing summaries with decisive conclusions about file safety.

The overarching concept involves multiple specialised AI agents working collectively within a SOC environment, alongside human analysts, to automate and orchestrate varied security workflows. Google Cloud projects that this agentic SOC framework could yield significant operational efficiencies by freeing security professionals to focus on more complex threats and strategic concerns.

Key SOC functions targeted for automation or orchestration include data management, alert triage, threat investigation and response, threat research and hunting, malware analysis, exposure management, and detection engineering. The company supports this initiative with its extensive security data, AI research capabilities, and integrated technology infrastructure, enabling the development of agents that perform human-like planning and reasoning to produce consistent, high-quality security outcomes.

A notable technical feature is the introduction of interoperability protocols such as Agent2Agent (A2A) for communication between agents developed by different parties, and the model context protocol (MCP) for standardised interaction between AI systems and security applications. Google Cloud is also open-sourcing MCP servers for its Unified Security platform, facilitating customers’ ability to build custom workflows that integrate Google Cloud and other security products. This open ecosystem approach intends to encourage collaboration among diverse agents and products.

Grant Steiner, Principal Cyber-Intelligence Analyst at Emerson, highlighted the practical benefits: "We see an immediate opportunity to use MCP with Gemini to connect with our array of custom and commercial tools. It can help us make ad-hoc execution of data gathering, data enrichment, and communication easier for our analysts as they use the Google Security Operations platform."

Google Cloud has additionally launched SecOps Labs, a programme providing customers early access to AI pilot projects within Google Security Operations and a platform to offer feedback. Initial pilots include autonomous conversion of threat intelligence reports into detection rules, automated creation of playbooks based on incident history, and updating data parsers via natural language commands. SecOps Labs offers a trial space for teams to test and refine these AI capabilities and contribute to shaping future Google Security Operations technologies.

Hector Peña, Senior Information Security Director at Apex Fintech Solutions, reflected on current customer experiences with Gemini, telling SecurityBrief Australia: "No longer do we have our analysts having to write regular expressions that could take anywhere from 30 minutes to an hour. Gemini can do it within a matter of seconds."

This development marks a step towards increasingly automated and intelligent security operations environments, combining human expertise with advanced AI to address the growing complexities of cybersecurity workloads.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.itpro.com/security/live/rsac-conference-2025-live-all-the-latest-news-and-updates> - This article discusses the integration of agentic AI into security operations, highlighting Google's efforts to evolve security operations centers (SOCs) by introducing intelligent AI agents capable of independently identifying, reasoning through, and dynamically executing complex security tasks while maintaining ongoing collaboration with human analysts.
2. <https://www.securityweek.com/google-cloud-unveils-new-ai-powered-security-capabilities/> - This source details Google's announcement of new AI-powered security features, including the Gemini suite, which embodies the shift towards more autonomous and collaborative AI functionality within security workflows.
3. <https://datatechvibe.com/news/google-cloud-launches-ai-powered-security-operations-to-india/> - This article covers the launch of Google's AI-powered Security Operations in India, emphasizing the introduction of intelligent AI agents capable of independently identifying, reasoning through, and dynamically executing complex security tasks while collaborating with human analysts.
4. <https://europeantech.news/google-cloud-uses-generative-ai-to-boost-security-operations/> - This piece highlights Google's use of generative AI to enhance security operations, focusing on the development of AI agents that perform dynamic investigations on alerts and provide conclusive verdicts, thereby reducing the repetitive workload of security analysts.
5. <https://cloud.google.com/blog/products/identity-security/introducing-google-security-operations-intel-driven-ai-powered-secops-at-rsa> - This blog post introduces Google Security Operations, detailing the integration of AI agents designed to function more independently within security workflows, marking a significant shift towards autonomous and collaborative AI functionality.
6. <https://www.expresscomputer.in/amp/news/google-cloud-brings-ai-powered-security-operations-to-india/112261/> - This article discusses the launch of Google's AI-powered Security Operations in India, highlighting the introduction of intelligent AI agents capable of independently identifying, reasoning through, and dynamically executing complex security tasks while collaborating with human analysts.
7. <https://news.google.com/rss/articles/CBMiqgFBVV95cUxPTXVIZ3hZeGJPc2ZRTklYYk5uX01VOHNWS090dXc5UFVVaUljSGY3Y0N1NnMzamE0R05lTEhtbVBqQW1KdndlbHBtcHk5QTlqYVBiYlcwbXVwdWp3dVdReURPSVNHTUJFcHI0cE1BWTVEcXJBRGdqaUpkenlqRnlDU0JkanJPTm1yS09aclBNQ3RDcnpnQ3NHa3hvSG9wcDV2RmRVN3hkbjRWUQ?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data