Google Cloud

SANS | Research Program

Product Briefing

Detection and Response with Google SecOps:

Insights from the SANS 2024 Detection and Response Survey

November 2024

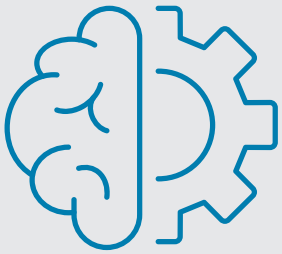
Most of us in cybersecurity spend significant time and energy detecting and preventing attacks on our systems and data. That's a job that requires processing huge amounts of data, fast, and finding and correlating small events that add up to evidence of an attack.

Google SecOps

Google, of course, is known for managing huge amounts of data and using algorithms to highlight the most important matches for your search. As you can imagine, those abilities come in handy when it comes to threat detection and response. Google's SecOps product delivers quick and effective results by grouping alerts into threat-centric cases and then triaging those to show your SOC team the biggest threats first. A low-level alert—for instance, a user mistyping their password several times—becomes a higher-priority case when correlated with other alerts—for instance, if that user then attempts to download malware or send confidential information out of the system.

Each case comes with an AI-generated summary telling you what the threat detection is seeing, along with evidence of what happened, and an assessment of the risk involved (see Figure 1 on the next page). Most importantly, Google's SecOps product delivers an actionable list of next steps to help you understand the problem and make solid decisions about how to remediate it.

Key Findings



Most respondents (65%) use industry threat intelligence platforms as their primary source of threat information.

Many teams (73%) are concerned about the quality and reliability of threat detection rules.

41% of respondents agree that prioritizing response primarily based on the severity of the threat is the most critical to prevent significant harm to an organization.

Google SecOps comes with a wide range of preconfigured rules and playbooks written by its own threat analysis team plus experts from Mandiant. The technology also lets you easily write your own rules and playbooks using the powerful YARA-L syntax. Test and update your rules or Google's, and run them against incoming data or your own historical data to see if there are threats you've missed. Generate your own playbooks quickly and easily, with visualizations to help you confirm the result will do as you intend it to do (see Figure 2). Automation moves things forward, but the humans remain in charge, and are able to make situational decisions.

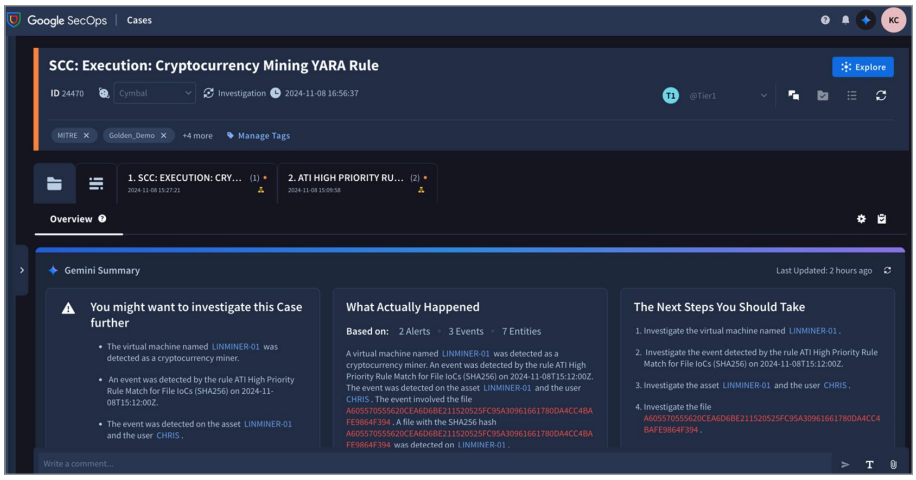


Figure 1. Get the context you need to understand complex threats with AI-generated summaries.

Many SOC teams are already working hard and bringing their skills up to speed. The SANS Detection and Response Survey found that 77% of teams are addressing skill gaps. Google SecOps seeks to make investigations faster and easier rather than creating more work. It integrates smoothly with other products, and allows your analysts to collaborate easily, encouraging skill-sharing and team response to emergent issues while analyzing your organization's data against the wealth of threat intelligence from Google, Mandiant and VirusTotal.

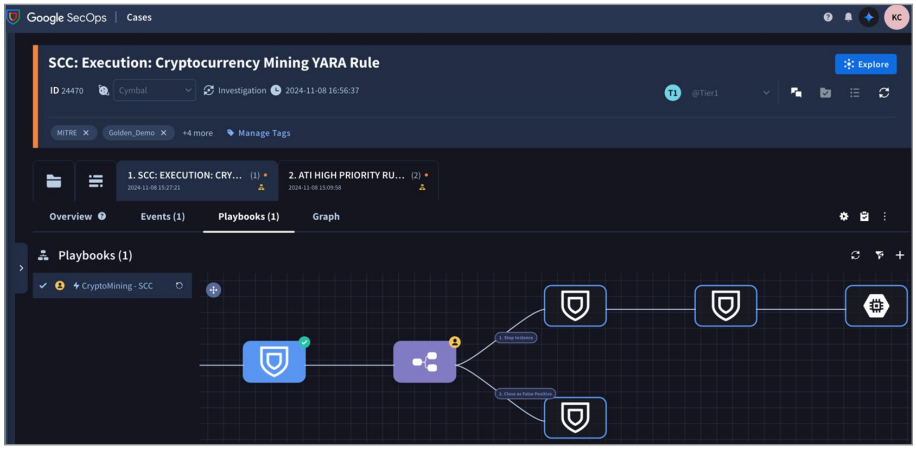


Figure 2. Use generative AI to build playbooks to automate security processes.

You don't have to be the team's coding genius to get good results from Google SecOps. Context-aware natural language queries make it easy for even the less experienced analysts to investigate, learn, and act against threats. Even for the people with more time on the front lines, using plain English instead of learning query language helps make investigations go faster. The data itself is automatically enriched with context and related information as it enters the system, so your queries find that information faster, and it's easier to detect threats from multiple overlapping events.

Google SecOps is ideal for organizations that need to modernize their threat detection and analysis, bringing high-octane cloud processing power to speed and streamline your telemetry, apply constantly-updated threat intelligence to find and triage problems, and use high-quality analysis tools to put your team to work on the highest-risk threats first. It's the ultimate scalable solution, and highly integrated with other Google Cloud products.

If you're not ready to replace your existing SIEM, but want the power Google SecOps brings to the table, that's great too. Deploying SecOps on top of a SIEM helps you eliminate blind spots, get ready to scale when needed, and manage the cost of threat detection and response.

If you're ready to level up your detection and response, visit **cloud.google.com/security/sec-ops**