The AI-Powered SOC

Capgemini

Find and deploy secure, repeatable, and efficient AI use cases

Modern SOCs need a new approach

The world of cybersecurity is experiencing a seismic shift. Distributed IT environments, AI-powered threats, and a continued flood of false positives leave security analysts and SOC leaders moving from incident to incident with little room to focus on the big picture.

SOC teams are adding more security tools, but they often aren't helping cut through the noise to prevent and respond to growing threats. Instead, the modern SOC needs a new approach entirely; one that focuses on secure-by-design AI use cases, carefully chosen to improve security posture while minimizing complexity and analyst burden.

Combine AI, automation, and human intelligence

The key to AI security success is finding a way to combine AI expertise with automation and prompt libraries that support consistent outputs.

By applying AI agents alongside traditional automation and human intelligence, you can avoid overspending while tackling all SOC workloads efficiently and securely. AI supports high-judgment tasks and effectively synthesizes and summarizes unstructured data, while automation rapidly delivers deterministic outputs.

The AI-Powered SOC from Capgemini

Capgemini works with partners around the world to deliver a comprehensive AI-Powered SOC service. Combining the AI agents and security solutions you're already paying for with Capgemini's cybersecurity expertise and prompt and automation libraries, SOCs can find and deploy the right AI use cases to improve security and efficiency.

AI-Powered SOC support services

Capgemini delivers a full suite of SecOps services designed to help you get maximum value from your existing AI agents and security solutions, including:

- Unified Security Operations Platform and AI Operations
- An AI agent gallery, including agents specialized to tackle specific categories of alerts
- AI natural language threat hunting and threat intelligence capabilities
- An AI-powered playbook library and knowledge management for advanced correlation
- Back-end investigation and incident creation using ITSM tools

Together, these solutions help you **transform and modernize** your **SOC** by making the most of cutting-edge technologies from leading cybersecurity partners, **enhance cyber team capabilities** by upskilling and augmenting teams with AI tools, and **accelerate deployment** with low-risk technology transitions and delivery models that align with broader business objectives.

The Capgemini difference

Capgemini is a top-tier partner with all major cybersecurity vendors, including Microsoft, CrowdStrike, Tanium, Palo Alto Networks, Devo, Swimlane, and many others. This makes us ideally placed to help SOCs scale up and meet growing threats head-on.

We maintain a collaborative operating model with our partners and customers, developing joint offers, co-authoring research and thought leadership, and conducting capability research to help all cybersecurity functions access the latest innovations.

Our cybersecurity clients traditionally achieve:

20% reduced average incident detection time

25% lower average alert investigation time

30% decrease in average incident resolution time

70% fewer incidents being reopened

80% less false positives on average

43% increase in incident response accuracy

Capgemini has been recognized as a leader in the ISG Provider Lens™ Cybersecurity – Services and Solutions report for five years consecutively and has also been named a leader in Avasant's Cybersecurity Services 2025 RadarView™ report.

Capgemini services in action

Major global enterprise

We expanded threat monitoring to this organization's growing AI agent ecosystem while reducing the amount of benign true positives its team had to investigate.

Using the organization's existing OpenAI infrastructure, we deployed SIEM detection rules to create a 'Benign True Positive Researcher' agent, and integrated a 24/7 SOC model with OpenAI agents, helping the company:

- Boost analyst productivity by **20%**
- Reduce human interventions from **1,200 to just three**

Capgemini internal SOC transformation

As our customers began to need evolved SOC capabilities and more resilience, we transformed our own SOC model to ensure we could meet their needs.

We created a single global platform that delivers increased levels of automation, continuous improvement capabilities, and enriched alerts. Consolidating our SOCs from 15 to seven, and creating deep, product-led partnerships with leading organizations like Microsoft, Devo, Crowdstrike, and Databricks, we:

- Deliver centralized and regionalized security models from our Global Delivery Center
- Standardized SOPs to deliver consistent value
- Developed a Unified Threat Management library and SOAR automation and integration resources
- Enabled threat intelligence collaboration across **Capgemini** and **our partners**

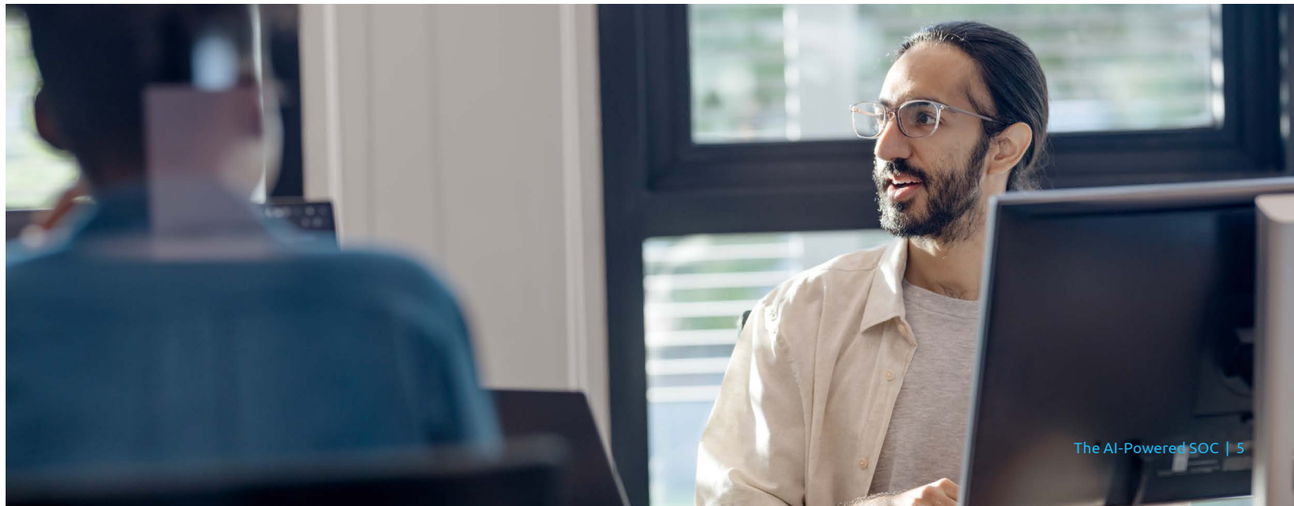
Start your AI-Powered SOC journey

Identify the right AI use cases in your SOC, deploy repeatable, effective agents, and keep pace with fast-changing cyber threats.

Identify and implement the right AI use cases

Deploy AI across SOC use cases to:

- Create **repeatable, efficient processes** with a new operating model
- Enable **observability and monitorability** for agent security
- **Accelerate threat detection** and monitoring
- **Save valuable resources** with smarter investigation and response



For more details, contact:

cybersecurity.in @capgemini.com

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real.
www.capgemini.com

GIS_04.06.26_SC

Capgemini