Goodbye, SOAR/SecOps? Hello, CIAO!

Artificial intelligence (AI) is transforming cybersecurity from a semireactive organization to a more proactive force

Government agencies are aware, sometimes painfully, that AI has radically changed the cybersecurity playing field. AI-powered attacks are rapidly growing in volume and sophistication. Attackers are leveraging AI to generate highly convincing social engineering messages, identify and exploit vulnerabilities, evade existing protections, and create new tools that evolve and improve over time. AI democratization has enabled novice script-kiddies with expert capability, dramatically expanding the size of the threat landscape.

As agencies advance a zero-trust (ZT) strategy, they often focus their efforts on microsegmentation and identity, credential, and access management (ICAM). However, "assume breach" is also a core principle of ZT. Agencies may overlook the implications of this principle, including the increased volume of alerts produced by a zero-trust framework and architecture (ZTF/ZTA). To align with ZT, agencies need the operational capability—and more so, the operational excellence—to proactively address vulnerabilities and handle greater load.

Introduced not even a decade ago, security orchestration automation response (SOAR) and security operations (SecOps) technologies were supposed to help cybersecurity teams detect threats and automate responses. But in this rapidly escalating cyber warfare, these SOAR and SecOps technologies can feel more like stopgap measures than sustainable solutions, the technology equivalent of bringing a knife to a gunfight. One leading analyst firm has gone as far as to declare that SOAR is now obsolete.[1]

Not everyone agrees with that assessment, but one thing is certain. We can no longer rely on humans alone to handle the growing pace and sophistication of cyber threats. No matter how capable our human resources may be, technology is required for speed of analysis and rapid response.

Why modern government is important

Government agencies in the US must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

[1] "Is SOAR Obsolete? Here's Why Security Engineers And AI Make The Difference," Daryl Lim, Forbes, January 22, 2025.

The missing link

Legacy SOAR and SecOps solutions may fail to meet expectations because they lack a key ingredient: the capability to collect and analyze a mountain of threat intelligence. These solutions were designed primarily to be reactive—in large part, they're designed to respond when attacked. But in a world where AI is rapidly escalating the volume and sophistication of attacks, federal agencies can't wait to be attacked or to triage minutia to understand the motives and tactics of an attacker.

Cyber intelligence automation orchestration (CIAO) is designed to address this challenge. CIAO elevates SOAR/SecOps technologies to the next level by adding enhanced and near-real-time threat intelligence aggregation. CIAO technologies continuously ingest and analyze data from a wide variety of external sources and correlate that data with data from internal systems to understand threat and provide an effective defense.

More importantly, CIAO doesn't just continuously and proactively monitor the attack surface, it also helps to remediate vulnerabilities and misconfigurations before attackers can exploit them. It doesn't just gather security information event management (SIEM) data, it helps to improve security incident response with applied human and agentic playbooks.

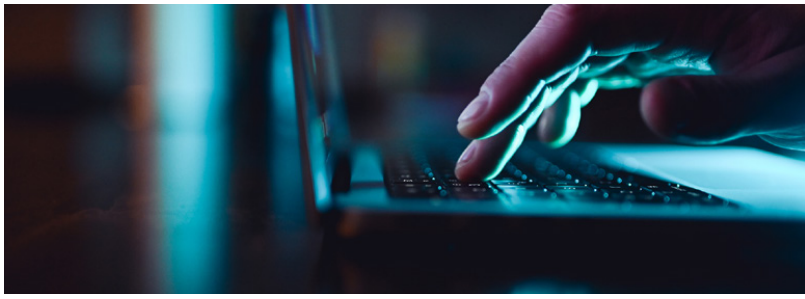
CIAO services can provide tailored insights into threat risk specific to an agency's technology stack. When an attack does occur, CIAO can help to identify, prioritize, and assign resources to a threat more quickly. It can provide actionable insights and enrichment on the nature of the attack, including who the attacker is, their capabilities, the potential impact of the attack, and the steps to address it. By arming cybersecurity teams with this information, CIAO can help cyber professionals to make better decisions faster, and to execute on those decisions quickly.

Leveraging the power of agentic AI

AI may be a potent weapon in the hands of attackers, but it is equally powerful for defenders. CIAO isn't an AI-powered intrusion detection system—AI fighting AI. But its enhanced capabilities are enabled by a combination of AI technologies, including AI agents. AI agents are often described as a paradigm shift in AI. They move AI from passive information retrieval to proactive execution and even decision-making. They possess higher levels of autonomy and intelligence, enabling them to optimize their actions in response to situational changes.[2] AI agentic systems are evolving rapidly, moving from simple "taskers" designed to automate single functions to "orchestrators" where multiple AI agents interact to achieve complex tasks at scale.

This is no incremental improvement. AI agentic systems are more revolution than evolution. Agentic AI is poised to radically transform security operations centers (SOCs) in the same way the cloud transformed SOCs from perimeter defense-centric organizations designed to protect on-premise servers. Some go even further, arguing that agentic AI could upend the entire software-as-a-service (SaaS) model.[3]

Given the rapid pace at which these systems are evolving, it's not unreasonable for some to believe they're not yet real or at least not yet fully baked, as if we're talking about flying cars. But they are very real and very much here today—and need to be taken advantage of. At a recent Wall Street Journal CIO Network Summit, 61 percent of attendees said they're currently experimenting with AI agents.[4]



[2] "The Rise of AI Agents and the Evolution of Innovation in AgentLayer," Medium, March 3, 2024.
[3] "Creating value with AI agents," David Muir, et al., KPMG, March 2025.
[4] AI Agents Are Everywhere…and Nowhere," Belle Lin, *The Wall Street Journal*, February 12, 2025.

Humanoid resources: not a technology but a transformation

Leading solutions such as the ServiceNow AI Platform are already incorporating agentic features. However, CIAO isn't a single technology but a combination of technologies and processes inside an operating model reimagined to take advantage of them. **It's an organizational transformation from human resources using technology to "humanoid resources" partnering with technology.** It's designed to empower people—to extend and enhance the capabilities of cyber professionals by providing real-time intelligence and automating or simplifying tasks, allowing them to focus on critical issues without being bogged down by distractions or manual processes. It's designed to promote collaboration and help reduce bureaucratic hurdles, focusing on and enabling governance, risk, and compliance (GRC).

The benefits for stakeholders are clear:

- **Chief information officers:** CIAO helps improve regulatory compliance, with greater transparency and increased accountability. It can also help focus resources and budgets on the most critical cyber needs.
- **Security officers and division/branch chiefs:** CIAO provides proactive solutions and progress reports while reducing manual effort.
- **System owners:** CIAO helps consolidate vulnerability and misconfiguration notifications, approve actions efficiently, and reduce response time.
- **System administrators:** CIAO offers a unified view, helping to prioritize tasks effectively and enhance knowledge.

How KPMG can help

KPMG LLP (KPMG) has developed a host of CIAO services designed to help transform your SOAR/SecOps capabilities into a modern, agile force capable of proactively addressing today's increased cyber threats.

We offer a CIAO solution built on the ServiceNow AI Platform designed specifically for federal agencies, customized to meet each agency's specific needs. It leverages the ServiceNow management, instrumentation, and discovery (MID) server to integrate with dozens of leading SIEM systems or connect directly to SIEM systems provisioned in the cloud. It's designed to minimize firewall rule changes. It takes advantage of powerful ServiceNow AI Platform features, including its organization data, discovery and configuration data, and cyber service catalog features. It also leverages email communications designed to minimize fatigue and advanced real-time collaboration through team messaging.

Our CIAO solution was developed and is continuously improved using agile methodologies to help keep pace with the evolving threat landscape and agency needs. It can be implemented as an independent service or bundled with other KPMG cybersecurity solutions including our cyber managed services. Resources can be engaged in a variety of ways (on-site, off-site, or hybrid) to suit your agency's needs, with minimal management effort required.

Why KPMG

KPMG has worked with federal, state, and local governments for more than a century. We have over 1,500 dedicated cybersecurity professionals worldwide, and have been recognized by Forrester, IDC, and ALM Intelligence as a leading global organization of professional services for cybersecurity.[5, 6, 7]

We're a multidisciplinary organization with business, technology, data and AI, risk, audit, and change management professionals working together as one team. We combine our cybersecurity acumen, government operations experience, cross-sector and cross-disciplinary skills, and alliances with leading technology providers to deliver solutions to address your organization's most pressing needs.

Because each organization is unique, we take a collaborative, client-centric approach. We'll work closely with you to understand your specific needs and tailor our solutions to meet them. We see our role as a trusted adviser, drawing upon our multidisciplinary skills and experiences to foster an exchange of ideas that challenge assumptions and spark innovation.

KPMG is a leading ServiceNow alliance partner. Our cyber professionals hold multiple ServiceNow certifications, including Certified System Administrator, Certified Application Developer, and Certified Implementation Specialist for Security Operations. We have experience integrating ServiceNow with multiple leading security systems, including Splunk, Tanium, Microsoft, Tenable, Qualys, Rapid7, HackerOne, Palo Alto Networks, Prisma, Expanse, Analyst1, VirusTotal, and Pwned.

[5] Source: ALM Intelligence Pacesetter Research, April 2022.
[6] Source: "IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment", October 2023.
[7] Source: "The Forrester Wave, Cyber Risk Quantification," Q3, 2023.

Contacts

Tyler A. Carlin
Federal Cyber & Tech Risk
Offering Lead
KPMG LLP
240-306-5097
tcarlin@kpmg.com

Dan Gruber
Specialist Managing Director,
Federal Advisory
KPMG LLP
571-512-0046
dgruber@kpmg.com

read.kpmg.us/modgov

KPMG

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**