Department of Administrative Services

Transforming State Cybersecurity Operations

Contact: State Chief Information Officer
Katrina Flory
Ohio Department of Administrative Services
Katrina.Flory@DAS.Ohio.gov

Category: Cybersecurity

Project Dates: 1/1/2025 – 4/30/2026

State: Ohio

Agency: Department of Administrative Services

EXECUTIVE SUMMARY

The Ohio Department of Administrative Services (DAS) modernized statewide cybersecurity by implementing an Agentic Security Operations Center (SOC) powered by Google SecOps and Gemini AI, enabling rapid, coordinated defense across 26 cabinet agencies and numerous boards and commissions. This transformation allows Ohio to identify and respond to malware, ransomware, identity compromise, and data-exfiltration attempts before they can disrupt government services.

By moving from manual investigative workflows to an artificial intelligence (AI)-driven security ecosystem, Ohio automates triage, correlation, and enrichment, allowing analysts to make informed decisions within minutes. Natural-language queries, automated summaries, and scalable playbooks significantly reduce workload while improving response quality.

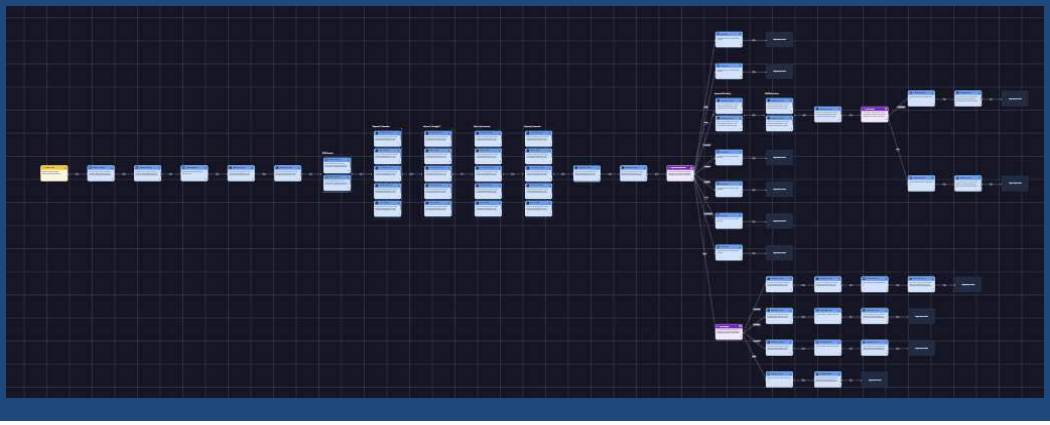
A key innovation is Ohio's centralized agency information security officer (AISO) model, which provides a dedicated point of contact for monitoring and risk response to each state agency. This structure creates a unified enterprise security fabric while still addressing agency-specific needs.

Ohio's disciplined governance ensures stable, rapid implementation of new capabilities, while its partnership with Google drives platform enhancements that position the state as a national leader in AI-enabled cyber defense. These advancements deliver measurable improvements in speed, automation, and resilience, offering a scalable model other states can readily adopt.

Hundreds of curated detections assist DAS SOC analysts. Over 50 custom rules have been created to address specific needs within Ohio's environment.

Many actions no longer require DAS SOC analysts to take action, freeing them up for value-adding activities. Tickets and emails are automatically sent to affected parties for well-defined processes.

Over one hundred playbooks are in use. These playbooks take a trigger, perform analysis, and then take clearly defined actions based on low-code drag and drop actions.



IDEA

What Problem or Opportunity Does the Project Address?

The DAS SOC faced a critical inflection point characterized by a lean team managing a massive surge in threat volumes alongside rigid budget constraints. Prior to this initiative, the DAS SOC relied on manual, labor-intensive workflows for threat detection and investigation. This environment created a substantial risk of analyst fatigue and, more critically, increased the likelihood of missing high-priority security incidents that could potentially disrupt essential state services for millions of Ohioans.

Why Does It Matter?

Modernizing security operations was a necessity for ensuring the continuity of government operations. The platform's integrated tools and intelligence plugins enable broad, multi-disciplinary security expertise. It is a strategic imperative to maintain the state's security posture against increasingly sophisticated, machine-speed attacks across disparate technologies. Automating routine tasks was an absolute operational necessity. By reducing manual workload, the state frees analysts to focus on high-value investigations instead of routine triage. Automated summaries and recommendations accelerate onboarding for entry-level analysts, enabling agencies to mitigate risk faster and more effectively.

What Makes It Different?

This project represents a shift toward an "Agentic SOC." Unlike traditional models that rely on static rules, this implementation leverages Gemini AI to automate the entire threat lifecycle—from detection and containment to active threat hunting and remediation. Furthermore, the project is strengthened by Ohio's unique organizational model: dedicated AISOs are centrally employed by DAS, creating a tightly woven system of centralized communication and distributed management. This enables seamless collaboration and standardized security protocols across the statewide enterprise while still accommodating individual agency needs.

What Makes It Universal?

This project delivers a scalable, repeatable model for transforming how states safeguard their digital ecosystems reflecting NASCIO's top CIO priorities, including Cybersecurity and Risk Management, AI, and Budget and Cost Control. State governments continue to face the challenge of optimizing limited resources while operating in complex, decentralized environments. This initiative tackles those long-standing issues by creating a blueprint for threat visibility across diverse agencies, enabling earlier detection and faster response. By integrating AI-driven analysis, it lowers the technical barrier for entry-level analysts and accelerates decision-making, empowering teams despite workforce shortages. Additionally, the project stabilizes cost structures in an era of rapidly expanding data volumes, ensuring predictable long-term fiscal management. Taken together, these outcomes demonstrate innovation, measurable impact, and strong alignment with the strategic priorities that guide state CIOs nationwide.

IMPLEMENTATION

What Was the Roadmap and Who Was Involved?

The project was executed by the core DAS SOC team in close partnership with Google and its implementation partner, Citrino which provided critical support for deployment, operationalization, and ongoing knowledge transfer to ensure the state team achieved full proficiency in the new capabilities. To ensure long-term financial sustainability, the state negotiated a three-year agreement featuring predictable, ingest-based billing — providing budget certainty while seamlessly accommodating data growth. Continuous collaboration with Google ensures that platform updates are strategically prioritized and aligned with the state's operational objectives.

Agency Collaboration

Recognizing that enterprise security requires total stakeholder buy-in, the DAS SOC team initiated a comprehensive engagement strategy. This included workshops and town hall meetings designed to educate agency partners on the capabilities of the new SecOps platform. These collaborative forums allowed agencies to request tailored reporting and facilitated the precise tuning of detection rules based on agency-specific application data, effectively minimizing false positives and ensuring the system was relevant to each department's unique mission.

The DAS Office of Information Security and Privacy's Security Incident Response Team (SIRT) and AISOs take feedback and input from the security tools and agencies to deliver high-value continuous improvements.

The tools and regular software updates continually enhance capabilities, such as mitigations for zero-day attacks. The agencies provide pointed feedback to reduce false positives and improve alerting for the entire enterprise.

How Did You Do It?

The implementation utilized a robust defense-in-depth architecture. Google SecOps was configured to aggregate telemetry from across the state's technology stack — including firewalls, intrusion detection system, intrusion prevention system, application logs, and endpoint detection — into a single, unified enterprise view. The DAS SOC team engineered custom playbooks to automate data correlation, analysis, and contextual enrichment. Once centralized, AI algorithms provide immediate context to every alert, including severity weighting and actionable remediation recommendations. Analysts from the SIRT or agency partners can then review this comprehensive data to apply human oversight, compressing an hours-long investigative process down to mere minutes.

IMPACT

What Did the Project Make Better?

The integration of Gemini AI has revolutionized the daily experience of the DAS SOC analyst. Features such as automated phishing detection, case summarization, and natural-language query generation have democratized security expertise. Analysts who previously required specialized coding skills to hunt for threats can now use simple English queries to interrogate vast datasets. This shift has enabled the team to pivot from reactive maintenance to proactive threat hunting and the investigation of complex, high-risk security events. The timeline from identification to mitigation has been dramatically compressed.

How Do We Know?

The success of the "Agentic SOC" is demonstrated by significant quantitative improvements across key operational performance indicators:

Performance Metric	Operational Result	Strategic Impact
Operational Efficiency	66.94% speed improvement - reduced average handling time by 4.86 hours per ticket	Analysts complete workflows **3× faster** due to improved triage and automation
Process Simplification	Closed over 250,000 cases via SOAR automation	Drastically reduced manual processing and eliminated repetitive review workloads
Responsiveness (MTTR)	Mean Time to Resolution improved by ~15% year-over-year (4.95 days down to 4.23 days)	Jan–Apr 2026 consistently outperformed 2025, despite significantly higher ticket volumes
Operational Stability	Maintained improved close times across mean, median, and P95 metrics	Absorbed a 35–70% increase in monthly volume during Q1 2026 through systemic efficiency
Financial and Capacity Impact	Enhanced throughput, increased automation, and minimized idle time	Strengthened security posture while successfully containing operational costs

What Now?

DAS is committed to the continuous evolution of its security capabilities to counter machine-speed, AI-driven attacks. Experienced analysts leverage low-code, drag-and-drop interfaces to rapidly architect new playbooks, maximizing operational capacity. The state is also investing in the future of the cybersecurity workforce through innovative talent development programs, such as partnerships with local technical career centers. By utilizing AI-assisted workflows, the state can rapidly upskill entry-level talent, ensuring a sustainable pipeline of security professionals equipped to defend the state's digital infrastructure for years to come.

CONCLUSION

Continuous vigilance and innovation is protecting the State of Ohio. In today's relentless threat landscape, absolute prevention is impossible, making rapid, automated response essential to shielding Ohioans' sensitive data.

By transitioning to an AI-powered "Agentic SOC," Ohio has already saved thousands of investigative hours. Because cybersecurity is a team sport, Ohio's centralized enterprise fabric and strategic partnerships allow the state to stand strong against sophisticated adversaries. The state remains dedicated to defending our critical infrastructure while ensuring that vital government systems remain resilient, secure, and available to Ohioans whenever they need them.