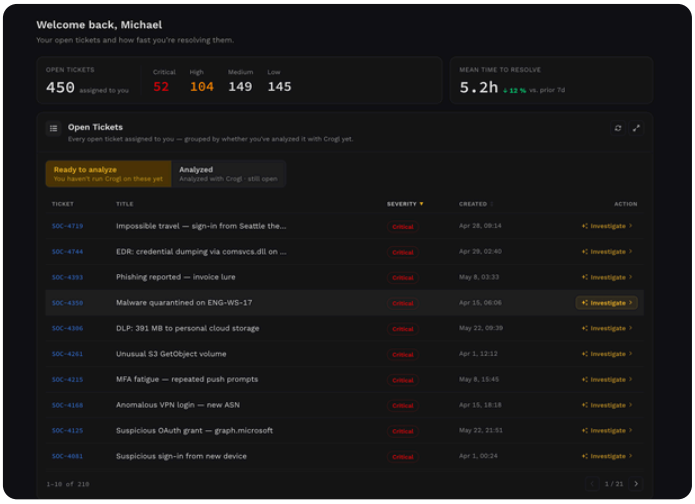
Achieving Outcomes for AI SOC Transformation

Sophisticated security teams are building their own AI SOC capabilities. 95% of AI projects fail because they are not anchored in business value. Security teams require operational capabilities beyond one-shot LLM chats. Security leaders want to manage costs, govern their AI risks and achieve their security objectives. Enterprise operations requires Enterprise grade AI SOC.



Challenges with home grown AI solutions

95%
Generative AI projects fail

AI Sovereignty
required deep engineering experience

Data Normalization
and tool sprawl demands frameworks

Challenge

Zero shot prompting of AI tools create the illusion of speed and ease for security use cases. And an “I can build it myself” inspiration. Hand holding an AI project for a demo demonstrates opportunities, the trouble arises when security engineers try to move to production.

Operationally relevant AI requires uptime, data normalization and most importantly, governance. Teams building their own in-house solutions have to confront consistency, auditability and customization of the solution. Then comes the issues of runaway costs, integrations with tens of tools and boring software engineering issues like secrets management and role based access controls. And these are just the tip of the iceberg. What about maintenance, updates, security testing?

Solution

Crogl adapts to your SOC, working interactively or autonomously to investigate alerts, work tickets, execute threat hunts, check compliance, and elevate human expertise.

Unlike solutions that require months of data engineering work upfront, Crogl works directly with non-normalized security data across your entire environment, eliminating 40% of analyst time currently lost to normalization and context-switching. It queries your SIEM, EDR, cloud platforms, and threat intel feeds in their native languages—SPL, KQL, and beyond—correlating findings automatically so analysts can focus on decision-making rather than data retrieval.

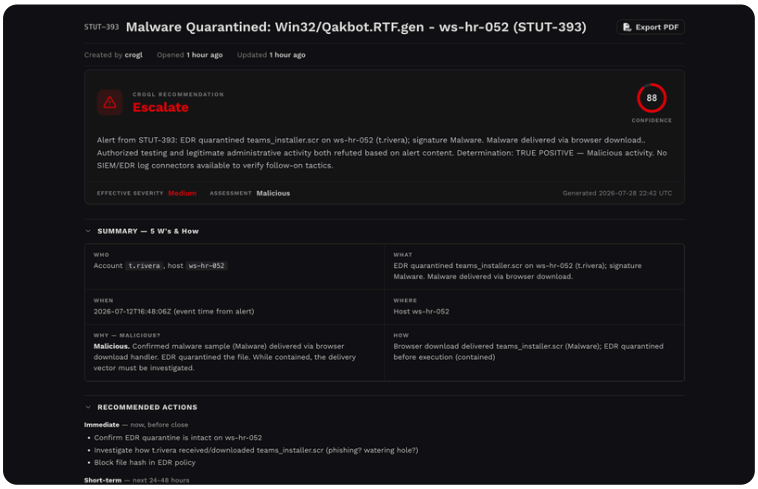
CROGL

AI for Enterprise Security

crogl.com

Why Crogl?

Crogl works directly with your existing security data without requiring normalization, learning your analysts' actual workflows rather than forcing them to adapt to vendor schemas. Every AI decision is fully auditable with complete transparency into reasoning and evidence chains, making it ideal for highly regulated and privacy-constrained data estates. The result: faster MTTR, reduced alert fatigue, and a SOC that scales without adding headcount, all while maintaining complete control and privacy by design.



Customer Outcomes

U.S. Federal Government Agency

100+ TB
Data analyzed per day

100+
SOC analysts supported

3
SIEMs under management

1500+
Alerts investigated per day

Key Capabilities

Alert Triage
Context-aware prioritization and evidence collection

Documentation
Every action logged, explainable, and audit-ready

Investigation
Multi-source evidence mapping, MITRE ATT&CK alignment

Fully Private Deployment
Runs in customer managed cloud, on-prem, or air-gapped environments

> Cyber task orders that took 2 weeks now turn around in days. Crogl handles high-volume exfiltration alerts we couldn't get to before.
>
> Director, SecOps
> *U.S. Federal Government Agency*

50+ Integrations

splunk> Jira tines databricks
servicenow CROWDSTRIKE Cribl + more

Contact us | sales@crogl.com

Join our community | crogl.com/community