



EXECUTIVE PERSPECTIVE

AGENTIC SOC SUMMIT: THE NEW STANDARD FOR AUTONOMOUS DEFENSE

The SOC Is Broken. And Adversaries Know It.

Adversaries are outpacing traditional defenses, using AI to exploit blind spots, target unmanaged edge devices, and move faster than humans can respond.

The data is clear: The average eCrime breakout time dropped from 62 minutes to just 29 minutes in 2025. The fastest observed was only 27 seconds. At that speed, any delay from manual investigation, fragmented data, or missed connections becomes exposure.

Frontier AI models accelerate this shift, collapsing the window between discovery and attack from weeks to minutes, and in some cases in near real time.

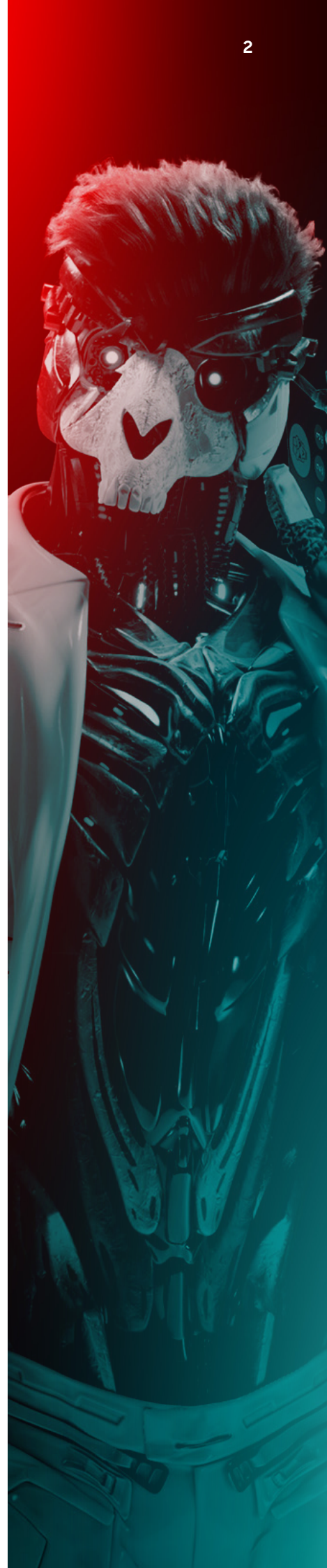
This is no longer just a security operations problem. It is an existential business resilience issue, and it requires executive ownership now.

Organizations will not survive this shift by adding more tools or more people. They will survive by adopting a new model: the **agentic SOC**, where humans and AI operate as a coordinated system to stop breaches at machine speed.

In 2025, 82% of detections were malware-free, as adversaries increasingly exploited trusted identities, legitimate tools, and authorized access paths to evade traditional defenses.¹

This is the inflection point: the move from tools that simply detect problems to a system that resolves them. Humans no longer chase the work. They direct it, with the right data, the right context, and AI agents executing in lockstep.

¹ [CrowdStrike 2026 Global Threat Report](#)



AI Demands a New SOC Model



Operationalize the agentic SOC

The agentic SOC is a practical evolution, not a rip-and-replace. Organizations can move from fragmented, manual workflows to unified, AI-driven operations through a phased approach — unifying data, operationalizing intelligence, and orchestrating response.



Separate trusted security AI from generic AI

Not all AI is built for security. High-performing agents are trained on real adversary behavior, validated against expert decisions, and operate within clear guardrails — delivering measurable, explainable outcomes at scale.



Secure AI investments

AI is rapidly expanding the attack surface. To realize its value, organizations must treat AI as critical infrastructure — with full visibility, governance, and human accountability — ensuring it strengthens the business instead of introducing unmanaged risk.

Act Now or Fall Behind

Traditional SOC models can't keep up with AI-accelerated adversaries. They're overwhelmed by alerts, noise, and manual effort — forcing humans to investigate in hours while adversaries execute in seconds.

As exploitation windows continue to shrink, CrowdStrike observed a 42% increase in zero-day vulnerabilities exploited prior to public disclosure in 2025, further compressing the time organizations have to detect, prioritize, and respond.²

The agentic SOC is the operating model built for this moment: operating continuously, at machine speed, and under human control. When fraud must be contained before a transaction executes, or lateral movement stopped before a production line goes down, speed and control can't be a trade-off.

The organizations that operationalize this shift right now will be the ones that outpace adversaries, establish security operations that scale, and build a compounding advantage over those still running legacy models.

Explore how security leaders are preparing for the transition to AI-driven, autonomous defense.

Watch the Agentic SOC Summit on demand —→

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: <https://www.crowdstrike.com/>

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Instagram](#)

Start a free trial today: <https://www.crowdstrike.com/trial>