Machine-Speed Cyber Warfare Forces Shift Beyond Human-in-the-Loop Security Models

AI-enabled cyber threats are compressing attack timelines from hours to seconds, forcing defense organizations to rethink human-driven security models.

SILVER SPRING, MD, UNITED STATES, May 18, 2026 /EINPresswire.com/ -- Cybersecurity operations built around human analysis are no longer keeping pace with the speed and scale of modern attacks as artificial intelligence enables adversaries to automate reconnaissance, planning, and execution in seconds rather than hours or days.

> The entire cybersecurity landscape so far has been built around identification, mapping out attack vectors, and then responding with a human in the loop. It's a very slow process."
>
> *Craig Opie, co-founder and CTO of Holocron Security*

That transition from human-paced defense to machine-speed conflict is redefining cybersecurity strategy within defense and critical infrastructure sectors because response times anchored to human decision-making cannot match automated attack cycles.

These were among the insights from a recent BizTechReports vidcast interview with Craig Opie, co-founder and CTO of Holocron Security, who described how organizations are beginning to operate under a widening assumption that response must occur at machine speed or risk becoming operationally ineffective.

Security operations centers, he stated, face a structural imbalance between alert volume and available expertise, with organizations processing hundreds to thousands of alerts daily while remaining understaffed and overwhelmed. Automation has improved prioritization and triage, but most environments still rely on human validation as a gating function for response, introducing delays that attackers increasingly exploit by blending malicious activity into alert noise.

"The entire cybersecurity landscape so far has been built around identification, mapping out attack vectors, and then responding with a human in the loop," Opie said. "It's a very slow process."

That latency becomes consequential because the nature of attacks has changed from discrete

events into continuous, adaptive processes driven by AI systems. AI-enabled attack systems compress the timeline of cyber operations by collapsing reconnaissance, planning, and execution into a continuous loop that operates without human intervention.

AI-driven cyber operations are forcing security organizations to rethink defense models built around human response times.

FROM DETECTION TO EXECUTION AT MACHINE SPEED

Attackers now deploy systems that evaluate environments, identify relationships between assets, and dynamically execute attack paths based on real-time conditions rather than predefined sequences.

“They can map out the networks, assess the scope, plan the attack, and implement all within seconds,” Opie said.

Traditional defensive workflows introduce delays at each stage of triage, escalation, and validation, which creates exploitable gaps when adversaries operate at machine speed. That mismatch between machine-speed attacks and human-paced response erodes the core assumption behind perimeter security, which depends on detecting and containing threats before they move across increasingly distributed systems.

THE END OF PERIMETER ASSUMPTIONS

As a result, organizations are moving away from perimeter-based security models because distributed cloud architectures, expanding identity surfaces, and deeply embedded supply chain dependencies have eliminated clearly defined network boundaries and introduced access points that cannot be fully controlled.

Gartner has identified this trend toward decentralized, interconnected environments as a primary reason traditional perimeter defenses are no longer sufficient. The erosion of boundary control is changing how organizations treat intrusion.

“It’s not a question of if they’re going to get into your systems,” Opie said. “They’re already in.”

This recognition reflects the reality that hybrid cloud environments and interconnected systems expand the attack surface beyond what perimeter defenses can reliably protect, requiring a focus on limiting adversary movement within systems rather than preventing entry altogether.

Containing adversary movement within these environments depends on response times that human-driven processes cannot consistently achieve. People often introduce delays that are structurally incompatible with machine-speed attacks because analysis, correlation, and response cannot be compressed to match automated execution cycles.

“When security teams continue to rely on processes measured in minutes or hours, while adversarial systems operate in seconds, it creates persistent exposure, even in well-resourced environments,” Opie explained.

That gap cannot be closed through incremental improvements to existing workflows. Marginal automation strategies, such as alert prioritization and workflow optimization, do not resolve this gap because they retain human approval as a prerequisite for action.

READ ON HERE.

Lane Cooper
BTR/MCC
+1 4156466592
email us here