cognizant | paloalto NETWORKS

Beyond detection: How AI Is rewriting the rules of security operations

By Shambhulingayya Aralelemath,
Head of Cybersecurity Delivery, Cognizant
A.Shambhulingayya@cognizant.com

The SOC at an inflection point

The security operation center (SOC) has undergone a fundamental transformation over the past few years. What began as modest log-monitoring rooms, focused on known threat signatures and basic alert triage, gradually matured as threats grew more sophisticated, into cyber defense capabilities built not just to watch, but to actively hunt, investigate and contain. This progression represented genuine and necessary growth. The industry has come to understand that the SOC evolution did not traight line. It unfolded along two separate tracks, driven by different pressures, swim lanes converging at roughly the same time.

- **Track 1: Uplift the capability.** Security teams building out deeper defensive depth through comprehensive detection for next-gen IT, threat hunting, intelligence-enriched detection, and automation embedded, and doing more with less using a platformization mindset—the cyber defense center (CDC) emerging as the natural expression of that maturation.
- **Track 2: Governance and risk track.** Security leaders being ready to address board and regulators ask not just "how many incidents did you handle?" but "can you demonstrate resilience?" and "what is our exposure if a key supplier is compromised?" Hence, CDCs evolved to take on risk management and governance alongside detection and response—becoming the operational home for both..

A cyber defense center and a risk operation center are not stages that follow one another in sequence. They emerged from different pressures, and the real breakthrough happens when they meet.

What a modern risk operation center (ROC) represents is the convergence of both tracks, when deep defensive capability meets strategic risk governance. It is the AI layer that finally makes this convergence operationally practical. With it, the defining question of this model—not just "are we being attacked?" but "what could go wrong in our specific environment, is it relevant to us and are we ahead of it?"—becomes something that can be answered continuously, at machine speed. Closing this gap requires more than better tooling. It requires rethinking security operations from first principles.

The fault lines in today's security model

Across organizations of varying maturity and industry, the same structural fault lines appear repeatedly. They are not sector specific. They are the predictable consequence of applying an older model to a threat environment it was never designed for.

The economics of visibility remain broken. Legacy SIEM platforms priced on data volume force organizations to quietly choose which parts of their environment they can afford to monitor—creating blind spots that adversaries are well practiced at exploiting.

Security teams are spending time on traditional way of investigation. Analysts burning 75% of their capacity manually reconstructing what happened is not the work of a mature security function. It is the symptom of a workflow architecture that has not kept pace with the environment it is trying to protect.

Detection logic has not kept pace with adversary behavior. Rule-based systems are only as good as the rules written for them. Modern adversaries probe and adapt. A static detection model is, by definition, always a step behind.

Regulatory expectations have outgrown the architecture. Frameworks like DORA, NIS2, and the SEC's cybersecurity disclosure rules demand continuous, auditable evidence of operational resilience—not periodic reporting. Most legacy architectures were not built with that cadence in mind.

A holistic-integrated model: The Cognizant approach

When we began rethinking what modern security operations should look like, the first assumption we challenged was that detection is the primary objective. Detection is necessary, but a security function that detects well and responds slowly—or cannot distinguish which threats are materially relevant to its specific environment—remains incomplete.

The model we have built is centered on the fusion of five interconnected capabilities: collection, detection, response, intelligence, and risk-based vulnerability and exploitable mitigation. What makes it distinctive is not any single layer but the continuous correlation across all five—connecting what is happening right now with what is known about attacker behavior, what exposures exist and what the business impact would be.

Collection: Full visibility across endpoints, cloud, network, identity and applications—without the cost constraints that force teams to choose what they can afford to see

Detection: AI- and ML-identifying anomalous patterns across unified data—surfacing threats and vulnerabilities that no predefined rule would have anticipated

Response: Acting on detections with speed and precision, compressing the interval between detection and containment from hours to seconds

Intelligence: Continuously enriching every decision with real-world threat knowledge contextualized to the organization's specific environment and risk profile

Risk operations: Vulnerability management and exploitable risk prioritization and remediation based on active threat intelligence, not severity scores alone—because a vulnerability being actively weaponized in the wild is a different priority entirely

This fusion is what allows the question to shift from "something has happened" to "here is what it means, here is our exposure and here is what we are already doing about it." We have operationalized this through the Neuro® Cybersecurity suite, spanning autonomous SOC and ROC operations, cloud security, secure access, endpoint protection and a growing security for AI practice—addressing risks around model integrity, prompt injection and agent security that are arriving faster than most programs have planned for.

From assisted to autonomous—and proved on ourselves

The progression toward autonomous security operations is a deliberate journey, not a switch to flip. We guide clients through it carefully—beginning with AI in an assistive role, enriching alerts, grouping signals into coherent incident narratives and surfacing recommendations for analyst review. Even here, the impact is significant: Reducing alert noise by up to 99% fundamentally shifts how analysts spend their time. As governance guardrails are established and confidence in the system's reasoning builds, we progress toward delegated autonomy—where AI agents act within defined policy limits to isolate compromised devices, revoke credentials and contain lateral movement in seconds. In my experience, that speed is often the decisive factor between a contained incident and one that escalates.

I am conscious that claims of this kind carry more weight when grounded in demonstrated practice. At Cognizant, we manage global client's security operations with intelligence threat defence platforms powered by Neuro Cybersecurity. Our strategic platform is built in partnership with Palo Alto Networks: Cortex XSIAM unifying SIEM, SOAR and XDR into a single incident narrative; Prisma Cloud covering cloud-native environments; Unit 42 keeping threat intelligence current; and Prisma AIRS underpinning our security for AI capabilities. The results were measurable: service levels improved by 40%, operational costs reduced by more than 25%, and mean time to detect and respond compressed from days to minutes. Every hard lesson from that deployment—data migration, analyst upskilling, playbook redesign, organizational change—is embedded in how we work with clients today.

The imperative for security leaders

The shift to AI-led security operations is no longer a matter of forward planning. Adversaries have already made this transition. The question is whether the gap closes on the organization's terms or on theirs.

Metric	Legacy SIEM	AI-led autonomous SOC
Detection speed	Days to weeks	Minutes to seconds
Data ingestion	Restricted by cost	Unified and scalable
Manual effort	High (human synthesis)	Reduced by 75%
Alert noise	Overwhelming fatigue	Reduced by up to 99%
Service levels	Underperforming	Improved by 40%

The SOC of the future will not be measured by alert volumes. It will be measured by the confidence it gives the business—that operations continue under pressure, that data is protected and that when something goes wrong, the response is already underway. Building that capability means bringing together the deep defensive posture of the CDC with the risk governance orientation of the ROC and letting AI provide the connective tissue that makes that fusion work at scale. At Cognizant, that is what we are building—for our own enterprise and for the clients we serve.

The rules of security operations are being rewritten. The organizations that move with intention now will help shape what those rules become.

World Headquarters
300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Tel: +1 201 801 0233

European Headquarters
280 Bishopsgate
London
EC2M 4AG
England
Tel: +44 (01) 020 7297 7600

India Corporate office
Siruseri-Software Technology Park of India (STPI)
SDB Block – Ground floor north wing
Plot No H4, SIPCOT IT Park
Chengalpattu District
Chennai 603103, Tamil Nadu
Tel: 1800 208 6999

APAC Headquarters
1 Fusionopolis Link,
Level 5 NEXUS@One-North,
North Tower, Singapore 138542
Phone: + 65 6812 4000

WF 4792200