CYBER DEFENSE MAGAZINE

eMAGAZINE

MARCH 2026

# FROM CONTROLS TO CREDIBILITY

*From Controls To Credibility: Cybersecurity Leadership In AI-Augmented Environments*

*Entropy as Infrastructure: The Missing Layer in Post-Quantum Security*

*The Hidden Security Debt That Kills Deals After Letter of Intent (LOI)*

*...and much more...*

MORE INSIDE

# From Threat Detection To Decision Intelligence: Rethinking Modern Cyber Defense

**By Tarun Wig, Founder & CEO, Innefu Labs Limited**

## The Illusion of Progress in Cyber Defence

Certainly, cyber defense has achieved an irrefutable advancement over the last ten years. The number of security tools being deployed by organisations, large amounts of telemetry being gathered, and threats are being identified faster than at any previous time. But the offences keep increasing in magnitude and effects.

This contradiction reveals an uncomfortable truth: more data may not have translated into better outcomes. Of course, detection capabilities have improved but coordination often lags. Alerts are received quicker, yet decisions are made slower. The attacks do not defeat security teams, but the **decisions** which they require.

Such visibility versus action gives an indication that cyber defence requires a radical rethink.

## Why Detection Alone No Longer Defines Security Maturity

Cyber defense has evolved in clear phases: perimeter security gave way to detection, detection expanded into continuous monitoring, and monitoring introduced automation. Each step improved visibility. None fully solved decision-making.

Today, many organisations still measure maturity using detection-centric metrics:

- Number of alerts generated
- Breadth of coverage
- Mean time to detect

These metrics are simply misleading. Alert volume does not equal preparedness. Coverage does not guarantee readiness. The actual bottleneck is prioritisation, situation and trust in action. Security teams have more than ever seen, and they usually have a hard time determining what matters versus what does not, and what to act upon next.

## The Real Challenge: Decisions Under Pressure

Inside most Security Operations Centers (SOCs), the challenge is painfully familiar.

- Which alert needs immediate attention?
- Which can safely wait?
- Which requires escalation beyond the SOC?
- Which is simply noise?

These questions are not a one-time set of questions but in most cases are posed with a lot of time pressure. Analysts have to deal with disjointed tools, team-siloed data and team-to-team handoffs. Tiredness will follow, not because there are no threats, but because it's not obvious. In modern cyber defense, the hardest part is no longer detection, it’s making the right decision, fast, with incomplete information.

## What “Decision Intelligence” Means in Cyber Defense

Decision intelligence in cyber defence is not about replacing human judgment, nor is it about fully autonomous security systems. At its core, it’s about augmenting human decision-making with context.

It focuses on:

- Correlating signals across domains rather than treating alerts in isolation

- Enriching technical indicators with operational and business context
- Presenting prioritised options instead of raw notifications

The goal is not to automate responsibility away, but to reduce hesitation and ambiguity, enabling security teams to act with greater confidence.

## From Alerts to Context: The Role of AI and Intelligence

This shift is made possible by AI, when applied thoughtfully.

Behavioural analytics help establish what “normal” looks like across users, systems, and networks. Cross-domain correlation connects signals that would otherwise appear unrelated. Pattern recognition over time reveals intent, not just activity. Context enrichment will provide meaning by considering user roles, criticality of assets, timing and possible effect.

The usefulness of AI in this case is not technical expertise, but the result-based clarity, fewer distractions, better prioritisation, and more confident decisions. AI does not introduce complexity, it consumes complexity so that we do not.

## How Intelligence-led Defence Reduces Operational Friction

When cyber defense becomes decision-centric, the operational impact is tangible. Alert fatigue decreases as noise is filtered out. SOC collaboration improves as teams work from a shared understanding of risk. Dwell time shortens because uncertainty is reduced earlier in the attack lifecycle. Most importantly, security decisions begin to align more closely with business and operational priorities.

This is where intelligence-led defense moves from concept to capability, transforming response from reactive to deliberate.

## Implications for Security Leaders

For CISOs and security leaders, this shift demands a change in mindset. Investment decisions should move beyond accumulating tools toward designing decision workflows. Success metrics should evolve from alert counts to decision latency and response confidence. Training should focus not only on tool proficiency, but on judgment under pressure. Cyber defense leadership today is less about visibility and more about decision readiness.

Cyber defense will always involve uncertainty. Perfect prevention is unrealistic. The real goal is resilience, the capability to make decisions which are sound and fast even where the information is incomplete. The future of cyber defense lies in organisations which consider security as an intelligence capability, that is, an ability not so much to detect threats, but to enable fast, assured actions when most needed.

## About the Author


Tarun Wig is a self-made entrepreneur and business executive with a decade long outstanding track record in building, growing and leading high-performing, startups in India.

He co-founded and is currently involved full-time at Innefu Labs, a research-oriented group using Artificial Intelligence and Machine Learning for National and Cyber Security. Innefu is a developer of niche and innovative security solutions such as the Intelligence Fusion Centre, Open-Source Intelligence, Forensics Analytical Toolkits, as well as Biometric Authentication. The solutions are running across multiple intelligence and critical infrastructure organizations.

Under Tarun's leadership, Innefu has more than 100+ installations across Indian Subcontinent, Middle East and Southeast Asia, the company is today a de-facto leader in developing and deploying AI for National and Cyber Security.

Tarun can be reached online at digital@innefu.com and at the company website https://innefu.com/