CYBER DEFENSE MAGAZINE

eMAGAZINE

JANUARY 2026

THE YEAR AHEAD IN CYBERSECURITY

- ✓ It Is Time to Radically Transform Cyber
- ✓ Building A Cybersecurity Playbook For 2026
- ✓ Why Knowledge Is Power in the New Age of Cyber Threats
- ✓ Defending Against Insider Threats in OT Environments

MUCH MORE INSIDE!

AI-Driven Cyber Threat Monitoring

Next-Gen Defence Against Evolving Attacks

By Tarun Wig, Founder & CEO, Innefu Labs Limited

Cyber defence has now entered an era where speed, scale, and adaptability define success. Enterprise environments nowadays are no longer confined to a clearly defined perimeter. Cloud workloads, SaaS platforms, remote users, APIs, third-party integrations, etc. have expanded the attack surface far beyond what traditional security models were designed to protect.

The attackers have progressed equally fast, not to mention that they have become dangerous. The contemporary threat actors are resilient, automated and highly adaptive and can combine social engineering, credential misuse and living-off-the-land methods to bypass the signature-based protection. The report on the investigations of the data breaches conducted by Verizon Data Breach Investigations Report (DBIR) revealed that most breaches are based on compromised credentials and third-party exposure, which demonstrates how easy attackers are to sneak through the antique protection machinery.

In such an environment, continuous cyber threat monitoring, that too, powered by AI is no longer a nice-to-have capability; it's more of a foundational requirement for enterprise resilience.

Traditional Detection Models Are Falling Behind

Over decades, signature-based detection, i.e. comparing activity to known malware hashes, pattern of attack, or predefined rules, was used by security teams. These means would have been effective in face of threats observed before but has difficulties in combat with:

- Zero-day exploits with no existing signatures
- Credential-based attacks that appear “legitimate” on the surface
- Low-and-slow intrusions designed to evade threshold-based alerts
- Rapidly changing malware variants such as Polymorphic Malware, generated automatically by adversaries

As a result, detection is delayed. Industry studies consistently show that attackers often remain undetected for weeks, sometimes months, before discovery. IBM’s Cost of a Data Breach Report has repeatedly linked longer dwell times with significantly higher breach impact and recovery costs.

Now, this is where AI-driven monitoring changes the equation!

Behavioural Analytics vs. Signature-based Detection

AI-powered cyber threat monitoring simply shifts the focus from *what an attack looks like* to *how systems and users behave*.

Instead of asking whether an activity matches a known threat, behavioural analytics asks a much more powerful question: **“Is this behaviour normal?”**

As machine-learning models learn how users, systems, and networks typically behave, they can flag subtle deviations like:

- Unusual login locations or impossible travel scenarios
- Abnormal data access patterns by privileged users
- Lateral movement that mimics routine administrative activity
- Early-stage ransomware staging before encryption begins

Behaviour-based detections rather than signature-based detections can also be used because they operate even when the attacker uses previously unknown tools and techniques. This allows them to be especially useful in discovering insider threats,compromised credentials and attacks that have been initiated via the supply chain.

SOC Automation and Intelligent Alert Prioritisation

All the challenges mentioned above are persistent and alert fatigue is one of the most significant challenges that Security Operations Centers (SOCs) face. Contemporary businesses are producing millions, even billions of security incidents every day. In the absence of automation, analysts have to go through the alerts by hand, which makes it more likely that the high-impact incidents will be lost in the noise.

AI tackles this issue directly, automating the fundamental operations of the SOC:

- **Event correlation**: Establishing connections between apparently unrelated events between endpoints, networks, clouds, as well as identity systems.
- **Risk scoring:** Alerts can be prioritised according to their severity, confidence and impact to the business.
- **Context enrichment:** Automatically adding asset criticality, threat intelligence, and user context to alerts.

That is, AI can assist SOC teams in responding more accurately and promptly to a smaller number of high-confidence incidents, as it will cut thousands of low-value alerts to a small number of high-confidence incidents.

Artificial Intelligence on a Massive Scale: Human-level Operability.

Human analysts are by no means scalable, yet they cannot be dispensed with. Monitoring systems based on AI are used in a continuous, distributed environment which spans large areas and processes data of:

- Endpoints and servers
- Network traffic and firewalls
- Cloud workloads and SaaS platforms
- Identity systems and access logs
- External threat intelligence sources

This scale allows AI to surface risks that would be impossible to identify manually. More importantly, it enables **near-real-time detection**, dramatically reducing attacker dwell time.

How Modern Attackers are evading Legacy Controls

Today's modern attackers are not relying solely on malware. They are exploiting trust relationships, abusing legitimate tools, and automating reconnaissance at scale. Common evasion tactics include:

- Credential stuffing using breached identity data
- Abuse of remote management and scripting tools
- API-level attacks in cloud environments
- Blending malicious traffic with legitimate business workflows

Since these techniques often appear normal in isolation, they bypass static rules and signatures. Here, AI-driven monitoring excels in this context by detecting **patterns over time**, identifying coordinated behaviours that reveal attacker intent long before any damage occurs.

Looking Ahead: Intelligence-Led Cyber Defence

With the current and ongoing changes in threats, cyber defence has to transition into intelligence based rather than reactive controls. The use of AI-based cyber threat surveillance is a significant move in that direction, one that enhances human capabilities in terms of speed, scale, and constant awareness.

The future SOC will not be determined by the number of alerts that it is receiving, but by how well it is turning data into actions that are timely and of equal confidence. The businesses adopting AI-powered surveillance will be in a better position to repel the threats of tomorrow!

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/