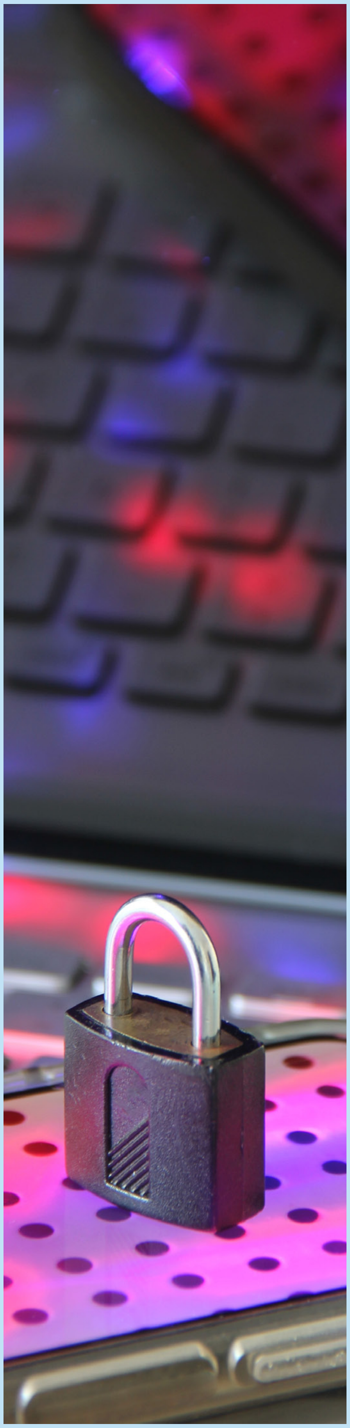
VIEW POINT



LEVERAGING AI FOR REAL-TIME THREAT DETECTION: KEY STRATEGIES REVEALED

Abstract

As AI becomes more deeply embedded in enterprise operations, cyber threats are growing in speed and sophistication. Traditional security tools can no longer keep pace with the rapidly evolving threat actors. Proactive threat detection using AI offers a powerful alternative by enabling businesses to detect anomalies in real-time, automate responses, and reduce manual fatigue. In high-risk sectors, such as finance, where data protection is paramount, these systems ensure compliance and grow customer trust. This article explores essential strategies, such as behavioural analytics, adversarial AI, SOAR, and explainable AI, that modern enterprises can adopt to stay resilient and secure in a developing threat landscape.

Infosys®
Navigate your next

AI: The double-edged sword

In the era of digital living, Artificial Intelligence (AI) has become the breaker. For businesses, wielding this double-edged sword is as much a necessity as it is a call to rethink how they address the challenges posed by a fast-evolving tech environment.

In a recent 2025 AI survey, McKinsey found that 78% of organisations use AI in at least one business function. The same study has also pointed out that businesses are increasingly redesigning their workflows to incorporate proactive threat detection using AI, thereby mitigating the growing risks associated with adopting gen-AI or analytical AI.

Why traditional threat detection no longer holds up

In today's threat landscape, attacks can unfold within minutes. Whether it is financial services data protection, fraud prevention in ecommerce or privacy in healthcare, real-time monitoring and threat detection reduce response time, improving user trust and saving costs. Proactive threat detection using AI is no longer a reactive option but a strategic need for businesses seeking security and growth. These risks span across industries and sectors, and the urgency for intelligent defence is on the rise. Key drivers for this urgency are the several converging trends observed over the last few years.

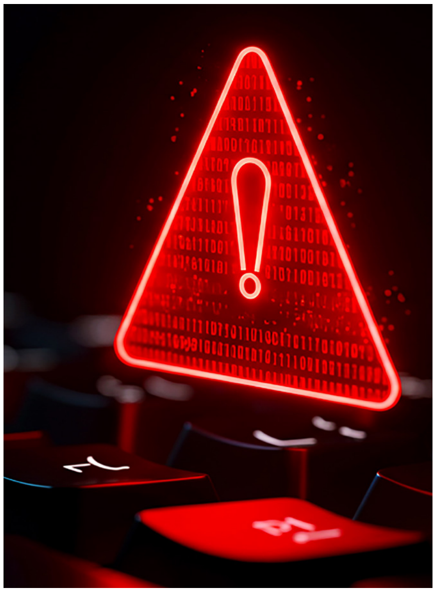
Sophisticated attacks are growing faster than traditional defences can evolve. Signature-based tools or periodic scans fail to detect advanced threats such as zero-day attacks, polymorphic malware, and phishing attacks. A 2024 Human Risk in Cybersecurity survey revealed that 85% of security professionals believe cybersecurity attacks have become more sophisticated.

Alert fatigue is real. Security Operation Centres (SOCs) deal with a massive volume of security alerts. Human teams are forced to prioritise, meaning critical threats get buried under a mountain of false positives and low-priority alerts.

Lag in threat response creates a gap. Manual analysis is slow and allows attackers to access sensitive data. Such delays increase the window of vulnerability, making organisations more susceptible to data loss, high breach costs and operational disruption. Human analysis of volumes of current and historical threat alerts and trends is a time-consuming and futile activity, considering the rate at which attack vectors are growing and transforming to evade detection.

Lack of unified oversight results in poor visibility across domains, severely affecting timely decision-making. The lack of a centralised view across cloud, on-premises, IoT, remote devices, and third-party systems creates blind spots that threat actors can exploit.[3]

AI-to-AI combat is a new reality, where threat actors themselves use generative AI to spike models, steal data, misinform or impersonate. The recent Europol report warns that criminal networks are evolving into sophisticated, technology-driven enterprises that exploit digital platforms to their advantage.

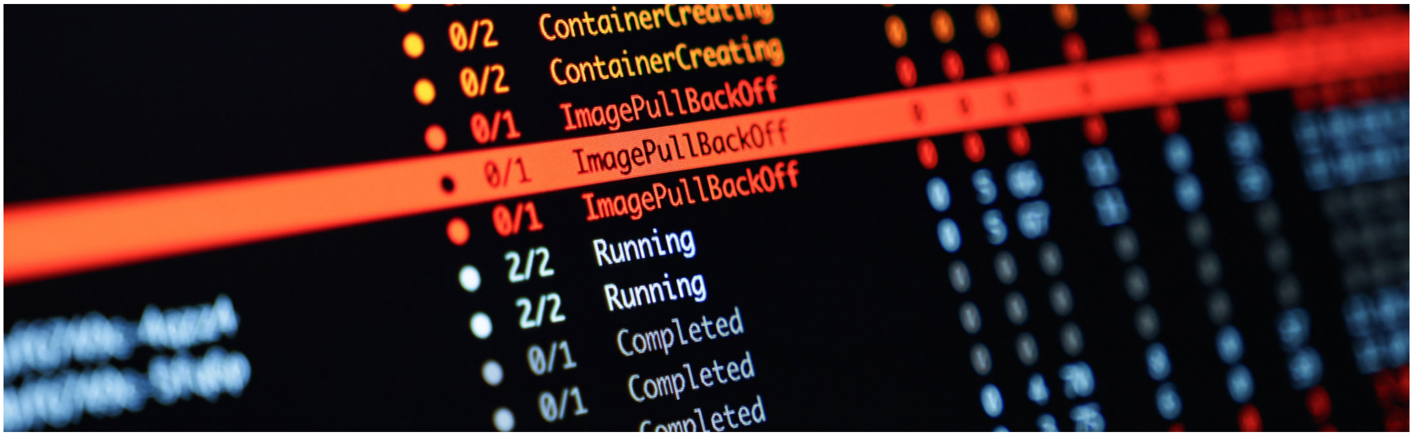


What is AI-powered threat detection?

AI-powered threat detection involves creating, training, deploying, and managing the security aspects of a business with the help of advanced tools, such as Machine Learning (ML).[4] ML can analyse large volumes of data and can quickly assess and alert about threats across embedded processes. It uses data from various functions, including network traffic payloads and patterns, data access logs and activity and user behaviour to train and differentiate between normal and abnormal activity.

On detection of an anomaly, automated processes take further steps such as:

- Preventing access to the network
- Denying data access
- Stopping changes to data or applications
- Creating detailed logs of the anomaly
- Alerting security systems to investigate the threat



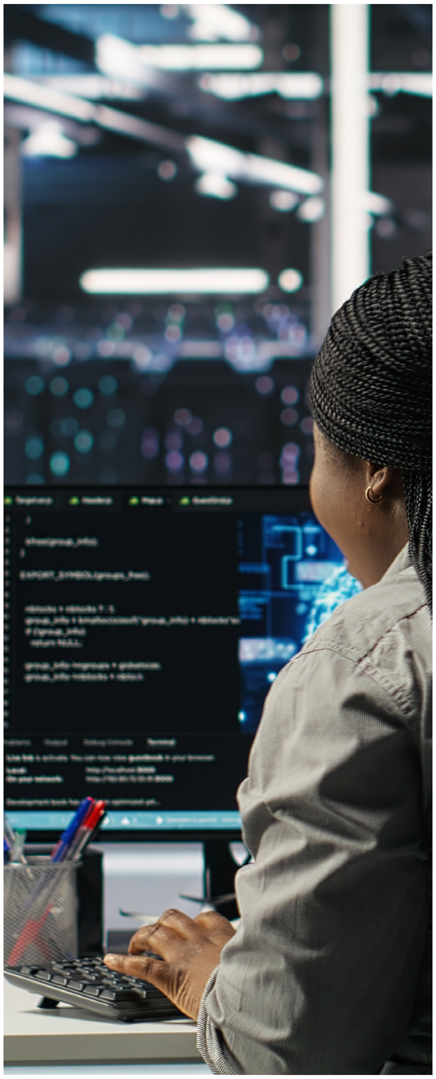
```
0/2   ContainerCreating
0/2   ContainerCreating
0/1   ImagePullBackOff
0/1   ImagePullBackOff
0/1   ImagePullBackOff
2/2   Running
2/2   Running
0/1   Completed
0/1   Completed
      Completed
```

Over time, the AI model becomes smarter, learning from previous logs, new data, and feedback received from human analysts. Particularly in regulated industries, AI helps meet compliance goals related to data protection in the financial services industry. This helps improve its ability to detect threats and respond with greater accuracy and speed than before.

Key strategies for real-time threat detection using AI

As cyber threats continue to evolve in complexity and sophistication, organisations must employ a combination of advanced AI-driven techniques to ensure robust, real-time protection.

Moreover, a recent survey shows that businesses leveraging AI in cybersecurity and threat detection reduced breach costs by 31% in 2024. Below are key strategies that businesses are adopting in 2025:



Behavioural analytics and anomaly detection Modern AI systems leverage behavioural analytics to track User and Entity Behaviour (UEBA) across networks, endpoints, and the cloud. By establishing a baseline of normal activity, AI can flag even subtle deviations such as unusual file transfers, login locations, or irregular network traffic. The emergence of context-aware anomaly detection frameworks further helps reduce false positives while increasing the accuracy of genuine threat alerts.

AI-powered threat hunting

Integrating real-time threat intelligence feeds with AI models enables security platforms to correlate internal threat vectors with global trends and indicators. This helps businesses stay abreast of the latest threat data. AI-enabled threat hunting can be a proactive approach to identify new attack vectors and loopholes in complex systems. Training AI-driven security solutions on this data helps instantly flag emerging malware, phishing tactics or zero-day exploits.

Continuous model training with human-in-the-loop

Proactive threat detection with AI is a dynamic process. To maintain efficiency, retrain AI-powered detection systems with new threat data and analyst feedback. Moreover, human-in-the-loop processes ensure that AI models do not deviate, thereby maintaining oversight and high detection accuracy.

Real-time automated response and orchestration

Empowering Security Orchestration, Automation, and Response (SOAR) platforms with AI enables automatic alerts and responses, such as blocking access. Recent advancements allow these systems to automate complex threat detection across endpoints, including cloud, remote devices, and IoT, reducing the gap between threat and response.

Adversarial AI and continuous red teaming

Real-time threat detection also requires continuous monitoring of the health of threat detection systems by deploying adversarial AI and red teaming. By simulating sophisticated attack scenarios, businesses can test the effectiveness of their defences, identify any weaknesses and fix the loopholes.

Together, these strategies empower enterprises to keep pace with the shifting threat landscape and to predict, detect, and respond to threats in real-time, neutralising potential damage.

Facing the challenges

With the benefits come the challenges of implementing AI-driven real-time threat detection systems. It is like letting out a genie from a bottle who might do your bidding, and yet, it has a mischievous side to it. Some of the challenges while dealing with AI are:

Data privacy

AI requires data to train, and often, this data is sensitive to the business, as it can contain personal information that can be traced back to users. This creates issues of data privacy. As global regulations become stricter for cybersecurity, safeguarding such data and adhering to these regulations is a must. Businesses must prioritise secure data retention and protection to maintain user trust.

Bias

AI Algorithms are as good as the data used to train them. Bias in the training data can mislead the AI into giving skewed responses and making discriminatory decisions. Professionals must carefully train AI on data that is fair and free from bias. This will eliminate potential discrimination and, consequently, prevent poor decisions.

Ethics

AI threat detection gives access to very sensitive information. If it falls into the wrong hands, it can damage the organisation's reputation. At the same time, data from threat detection systems must be used solely for the intended purpose. Using analytics and data to find the weaknesses of competitors and exploiting them is unethical.

Explainability

Explainability in AI refers to the transparency required to understand how AI works and how it uses information to make these decisions. Explainability is vital to building trust.

What to consider before adopting AI threat detection

Choosing the right AI system requires a thoughtful evaluation of its real-world performance, compatibility, and long-term value. Here are key considerations:

System performance and adaptability

In addition to concerns about cost versus value, an AI-enabled threat detection platform should offer real-time detection and be capable of learning from new patterns over time. Look for scalable solutions that adapt as threat volumes and types evolve.

Threat coverage

Start by identifying the kinds of threats most relevant to your business, such as malware, phishing, insider risks, or behavioural anomalies. Then, assess whether the AI system is equipped to detect and respond to them effectively.

Accuracy

The entire operation is worthwhile if the results are accurate. High detection rates are useless if they yield false positives most of the time. The system must be thoroughly tested before deployment. Moreover, models must be fine-tuned regularly to avoid model drift.

Scalability and integration

The primary goal is to enhance threat detection without disrupting the current system. New threat detection systems can work with old ones through middleware or APIs. Hybrid threat detection is more accurate and precise, and quickly adapts to new situations. Scalability ensures they remain relevant as the threat environment evolves and business requirements expand.

Automation

The goal of introducing AI in threat detection is not only to provide real-time alerts about anomalies but also to handle autonomous responses and reduce manual workload.

Compliance

AI should support compliance and regulatory adherence. Human oversight of the AI system can help in regular compliance and support business continuity.

End note

AI is changing the way businesses protect themselves. As threats grow more sophisticated and fast-moving, security needs to be just as innovative and responsive. Real-time, AI-driven threat detection is becoming a business essential. Those who take the lead now will be better placed to manage risk, build trust, and adapt to a rapidly evolving future. In today's digital world, staying secure is not only about defence, but also about being prepared, being responsible, and looking forward to the future.

Infosys®
Navigate your next

For more information, contact infosysbpm@infosys.com