AI and Cyber Security: A New Era

Scaling Cybersecurity with Generative AI and Agentic AI

Eshaan Salwan

The Evolving Threat Landscape

Cybercriminals are using AI

Attacks are becoming faster, more sophisticated, and highly personalized. Phishing attacks account for 80% of all attacks, with an estimate of $17,000 being lost every minute.

The Scale Problem

The sheer volume of data, transactions, and alerts is overwhelming.

The Talent Gap

A global shortage of cybersecurity professionals makes it difficult to staff and scale Security Operations. ISC2 study suggests a total of 10.2 million professionals are required, while current workforce is 4.8 million.

Malware

Polymorphic malware (changes its code signature automatically) can evade traditional antivirus. 40% of global cyber incidents in 2024 involved new malware (400,000+ new types).

AI-Driven Fraud Detection: From Reactive to Predictive

Machine Learning for Anomaly Detection:

Analyse transactions in real-time, detecting subtle deviations from normal behaviour.

Generative AI for Threat Modelling

Generative AI creates realistic, synthetic datasets that mimic new fraud patterns, allowing models to be trained on emerging threats without using real customer data.

Agentic AI for Case Prioritization

Autonomous agents can automatically triage alerts, gather context from multiple systems, and present only the most critical, high-risk cases for immediate human review.

Behavioural Biometrics

AI analyses unique user behaviours like typing speed, keystroke patterns, and mouse movements to provide another layer of real-time fraud detection.

Generative AI for Threat Modelling:

Generative AI creates realistic, synthetic datasets that mimic new fraud patterns, allowing models to be trained on emerging threats without using real customer data.

Mitigating the Insider Threat: Behavioural Analytics

User and Entity Behaviour Analytics (UEBA)

AI models establish a dynamic baseline of "normal" behaviour for every employee and entity within the network. 19% of all data breaches are caused by an internal actor.

Gen AI for Contextual Analysis

Agents analyse communication and access patterns to detect subtle changes in an employee's behaviour, such as accessing sensitive files outside their typical role.

Real-time Alerts and Intervention

Proactive warnings are triggered for unusual activities, such as an employee attempting to download a large volume of data.

Data Exfiltration Detection

AI actively monitors for attempts to move or copy data from the network in unauthorized ways.

Compromised Account Identification

The AI can detect if an employee's account has been compromised by identifying behaviour that doesn't align with the user's established patterns.

Modern SOC: A Force Multiplier

Automated Threat Triage

AI filters out low-priority alerts and false positives, dramatically reducing alert fatigue and allowing human analysts to focus on real threats.

Agentic AI as a Co-pilot

AI agents autonomously investigate and enrich incident data, providing analysts with a comprehensive report for rapid decision-making.

Predictive Threat Hunting

AI identifies hidden patterns and potential attack vectors before a breach occurs, enabling proactive defence.

Automated Remediation

In some cases, AI can take automated response actions, such as isolating an infected device or blocking an IP address to contain a threat.

Accelerated Root Cause Analysis

AI can quickly analyse data to determine the root cause of an incident, speeding up the recovery process.

AI in Vulnerability Management

Traditional Security Tests

Static, rule-based scanning often generates a high volume of false positives that overwhelm developers and slow down the development process.

AI-Powered SAST

AI analyses code with a deeper understanding of context, allowing it to more accurately identify and prioritize real vulnerabilities.

Gen AI for Automated Remediation

Generative AI can propose or even write code fixes, reducing the burden on developers and accelerating the remediation process.

Continuous Integration

AI-powered SAST can be integrated directly into CI/CD pipelines to provide continuous scanning and immediate feedback to developers as they write code.

Prioritization of Fixes

AI prioritizes vulnerabilities based on their severity and exploitability, based on the threat landscape, ensuring that developers focus on the most critical issues first.

Financial Institutions: The Scale Advantage

Leveraging Existing Data

Large banks have vast, proprietary datasets of transactions and customer behaviour—the lifeblood of powerful AI models.

Building Custom Models

The scale of resources allows for the creation of custom, institution-specific AI models that are highly accurate and tailored to their unique risk profile.

Agentic AI for Workflow Automation

Multi-agent systems can automate complex, multi-step tasks like regulatory compliance checks and fraud case investigations.

Real-time Risk Assessment

AI can provide a constant, real-time assessment of risk across an entire financial portfolio, from individual accounts to enterprise-wide operations.

The Human-AI Partnership: The Future of Work

AI as a Co-pilot

AI serves as a powerful co-pilot, automating repetitive and data-intensive tasks, thereby empowering human security analysts.

Upskilling the Workforce

The focus shifts to training employees to work alongside AI, enhancing their productivity and strategic capabilities.

The New Human Role

The human role shifts from transactional tasks to strategic advice, creative problem-solving, and relationship management.

Focus on Intuition and Judgment

Humans will focus on the complex, nuanced problems that require intuition, ethical judgment, and a deep understanding of human behaviour.

Reduced Complexity

The AI handles the "heavy lifting," allowing SMEs to focus on their core business while maintaining a strong security posture.

Thank you!
Q&A