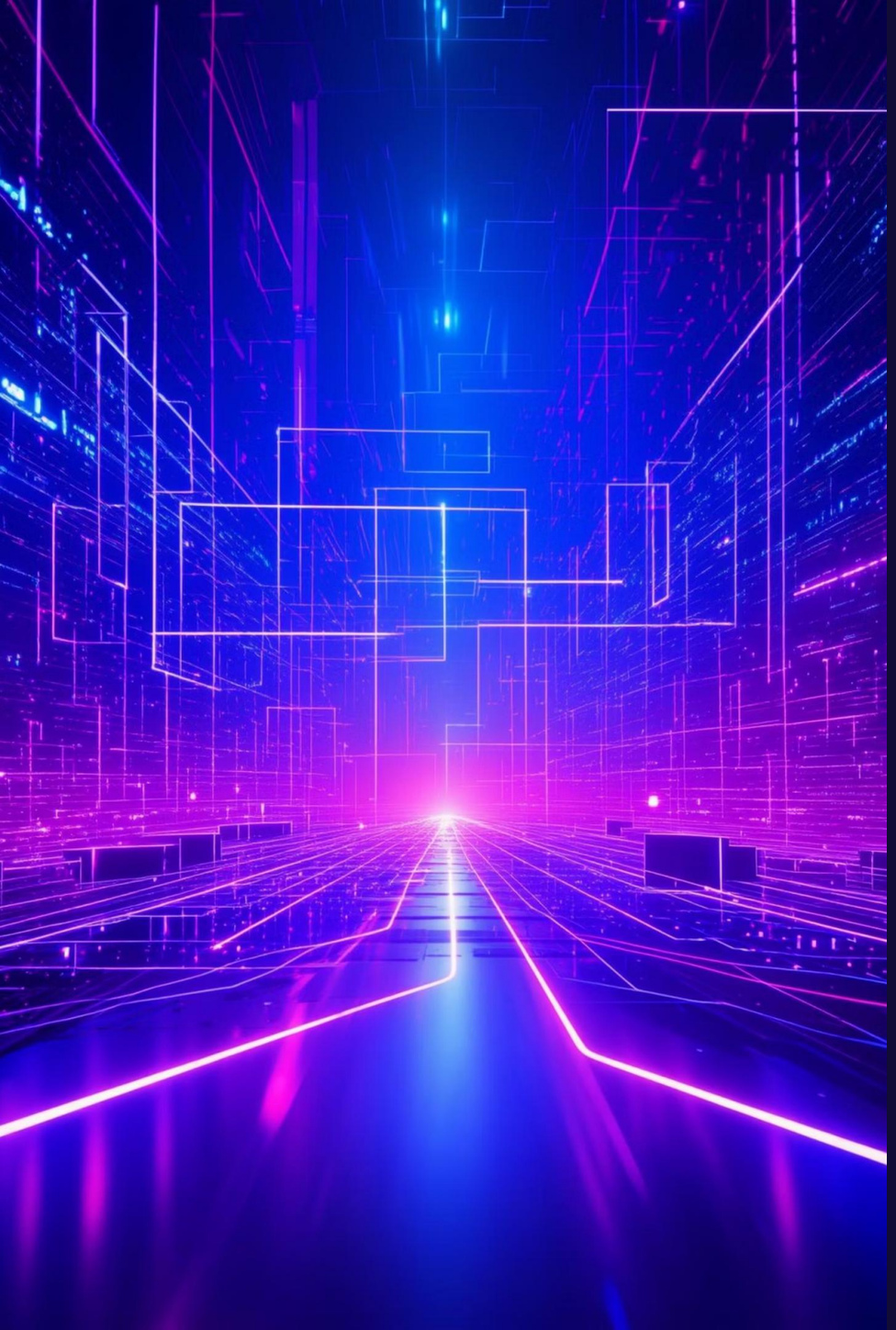
Data, AI and Cybersecurity

The Power Trio Reshaping Digital Defence

Samrat Seal
Head of Transformation and Governance
Cyber and AI, Kmart Group, Australia



Journey Ahead

Convergence of Data, AI and Cyber

How these three domains are increasingly intertwined to create new defence paradigms

Data as the Core Foundation

The critical role of quality data in building effective AI-driven cybersecurity systems

AI for Proactive Defence

Moving beyond reactive security with predictive capabilities and threat intelligence

Challenges and Risks

Navigating the double-edged sword of AI in cybersecurity contexts

The Future Landscape

Emerging trends and strategic considerations for organizations

The Convergence of Data, AI and Cybersecurity

1. Evolving Digital Landscape
2. Sophisticated Threat Actors
3. Exponential Data Growth
4. AI as a Transformative Force
5. Constant Vigilance: Detecting, Analyzing, and Responding to Cyber Threats

AI and data are revolutionizing cybersecurity, creating new capabilities and challenges.

Data as the Core Foundation for AI-Driven Cybersecurity

10TB

Daily Data*

Average volume of security data processed daily by enterprise SOCs

89%

Faster Detection*

Improvement in threat detection speed with AI-powered data analysis

60%

Cost Reduction*

Decrease in incident response costs with AI-augmented analysis

The Data-AI Symbiosis

High-quality, diverse data is the essential fuel that powers effective AI systems in cybersecurity. Organizations must cultivate comprehensive datasets that encompass:

- Historical threat intelligence and incident data
- Network traffic patterns and anomalies
- User behavior analytics across systems
- Global threat feeds and signature databases

Without robust data foundations, even the most sophisticated AI algorithms will fail to deliver meaningful security insights.

**Sources: IBM Security Intelligence Report 2023, Gartner Cybersecurity Trends Report 2023, Ponemon Institute Cost of a Data Breach Study 2022, Microsoft Digital Defence Report 2023.*

AI for Proactive and Predictive Cyber Defence

Traditional Reactive Defence

Security teams respond after threats are detected, resulting in potential damage and longer remediation times

Enhanced Detection Capabilities

AI systems analyze behavioral patterns, identifying subtle anomalies that signature-based tools miss

Predictive Defence Posture

AI forecasts potential attack vectors by analyzing threat intelligence and network behavior, enabling preemptive action

Case Study: A major financial institution implemented an AI-driven security platform that reduced their average threat detection time from 11 hours to just 9 minutes, while decreasing false positives by 73% compared to traditional SIEM solutions.

Source: Deloitte Cyber Intelligence Center Report 2023

By shifting from reactive to predictive defence strategies, organizations can identify and mitigate potential threats before they materialize into actual breaches.

Challenges and Risks of AI in Cybersecurity

The Double-Edged Sword

As security teams leverage AI for Defence, threat actors are simultaneously weaponizing these same technologies. This adversarial dynamic creates significant challenges:

AI-Powered Attacks

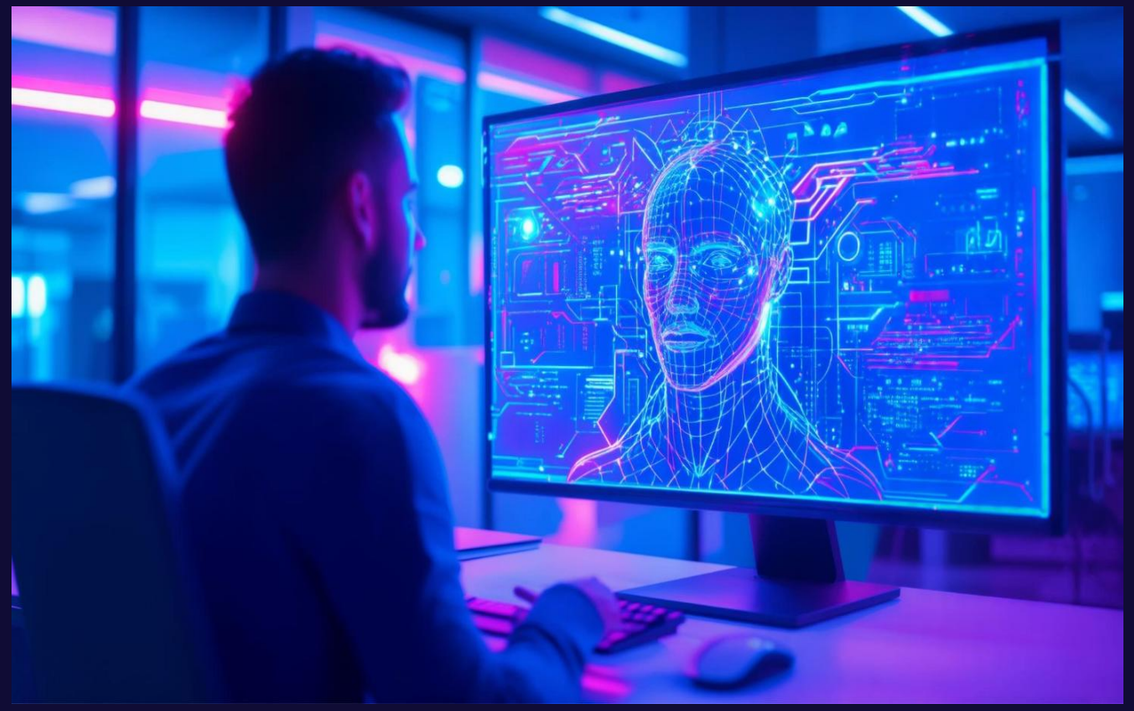
Deepfakes for social engineering, automated vulnerability discovery, and intelligent malware that evades detection by learning security patterns

Data Privacy Concerns

AI systems require vast amounts of sensitive data, creating tension between security efficacy and privacy regulations like GDPR and CCPA

Algorithmic Limitations

Bias in training data can create blind spots, while over-reliance on AI without human oversight risks catastrophic failures



Mitigation Strategies

1. **Implement ethical AI guidelines**

   Establish clear principles and protocols to ensure AI-powered cybersecurity tools are designed and deployed responsibly, with safeguards against bias and misuse.

2. **Maintain human oversight**

   Keep human experts in the loop to provide strategic direction and make critical decisions, rather than fully automating cybersecurity processes.

3. **Conduct regular AI audits**

   Continuously monitor the performance, accuracy and impact of AI systems to identify any issues or unintended consequences early on.

4. **Practice adversarial testing**

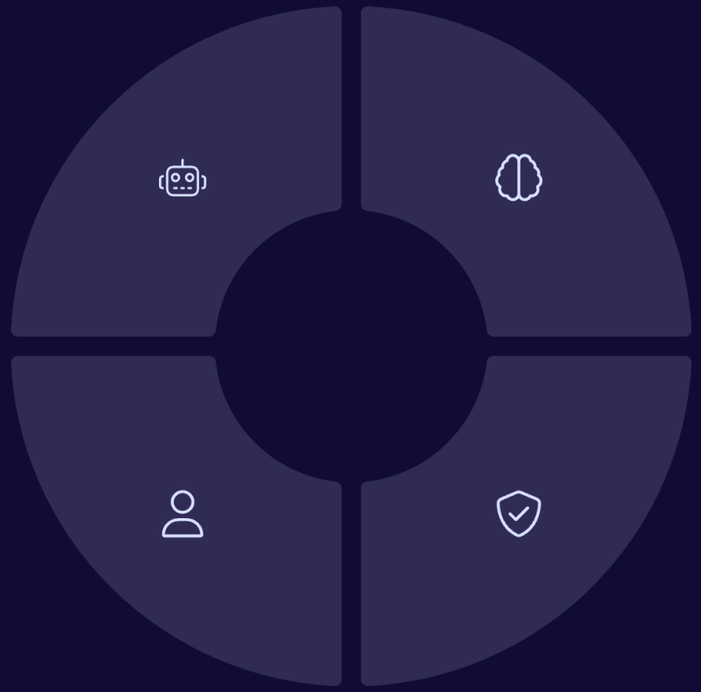
   Proactively challenge AI-driven Defences with simulated cyber attacks to uncover vulnerabilities and strengthen resilience against evolving threats.

Future of Cybersecurity with Data and AI

As we look toward the horizon, the integration of AI and data will fundamentally transform cybersecurity operations.

Autonomous Security

Self-healing systems that can detect, contain, and remediate threats without human intervention, particularly for common attack patterns



Cognitive Security

AI systems that understand context and intent, moving beyond pattern recognition to true comprehension of attacker behaviors

Human-AI Teaming

Evolved security operations where human analysts and AI systems form intuitive partnerships, each complementing the other's strengths

Zero-Trust Architecture

AI-powered continuous authentication and authorization based on behavioral biometrics and contextual risk analysis

> The most effective cybersecurity strategy will not be human-only or AI-only, but a thoughtful integration where each enhances the capabilities of the other in a continuous learning ecosystem.

By embracing this convergence while addressing its challenges, organizations can build resilient security postures capable of adapting to tomorrow's threats.

Thank You

Connect with me
2samrat@gmail.com
www.linkedin.com/in/samratseal

Disclaimer:

The views, opinions, and content presented herein are solely my own and do not represent or reflect those of my employer. This presentation is based entirely on my personal knowledge, professional experience, and independent research.