HELLO EVERYONE! 👋

MASHREK REZA SIDDIQUE

surrounded with my cherished family ♥

Head of IT

PT. Unilever Oleochemical Indonesia

Career Journey

HOD, IT
(2023 – Ongoing)

Oleochemical business unit of Unilever

Country IT Manager
(2016 – 2023)

CropScience division of Bayer, Germany

IT Manager
(2015 – 2016)

A venture of LAUGFS Group, Sri Lanka

IT In-charge
(2012 – 2015)

Joint venture of Godrej, India and ACI, Bangladesh

Sr. Executive, IT & Projects
(2006 – 2012)

A venture of Orogenic Group, Malaysia

Academic Credentials

- M.Sc. (Information Technology)
- PGD in Supply Chain (ISCEA)
- PGD in Business Communication

Career Vision

Staying focused on customer centricity and ensuring my deliverables create an impact to the Organization ✌

Necessity of cyber readiness for the future of resilience AI

Building trust and security in an AI-driven world

Industry Impact – Case Studies in Cyber Resilience

Finance

159B+ transactions/year processed by AI, streamlining operations and increasing efficiency across financial institutions.

Fraud detection improved 300%, significantly reducing losses and protecting customer assets with advanced machine learning models.
Source: Mastercard 2023

Healthcare

Microsoft Copilot builds AI cyber tools that empower security teams with real-time threat intelligence and automated responses.

Enhances analyst capabilities by supporting faster decision-making and improving accuracy in identifying cyber threats.

Source: PwC 2023 Whitepaper

Telecom

“Salt Typhoon” hack exposes critical AI defense gaps, revealing vulnerabilities in current security infrastructures.

Highlights the urgent need for adaptive AI strategies to fortify telecom networks against sophisticated cyberattacks.

Source: MIT Technology Review 2024

The Urgency of Cyber Readiness in the AI Era

Data Insight

Only 29% of executives feel prepared for AI cyber threats.

Source: PwC Digital Trust Insights 2024

Key Objective

Strengthen cyber readiness for AI resilience.

Critical AI Use

Embedded in finance, healthcare, and telecom sectors.

Innovation fuels risk exposure.

AI and Cybersecurity – A Double-Edged Sword

AI Enhances Defense

Threat detection, automation advancements

New Vulnerabilities

Adversarial attacks, data poisoning risks

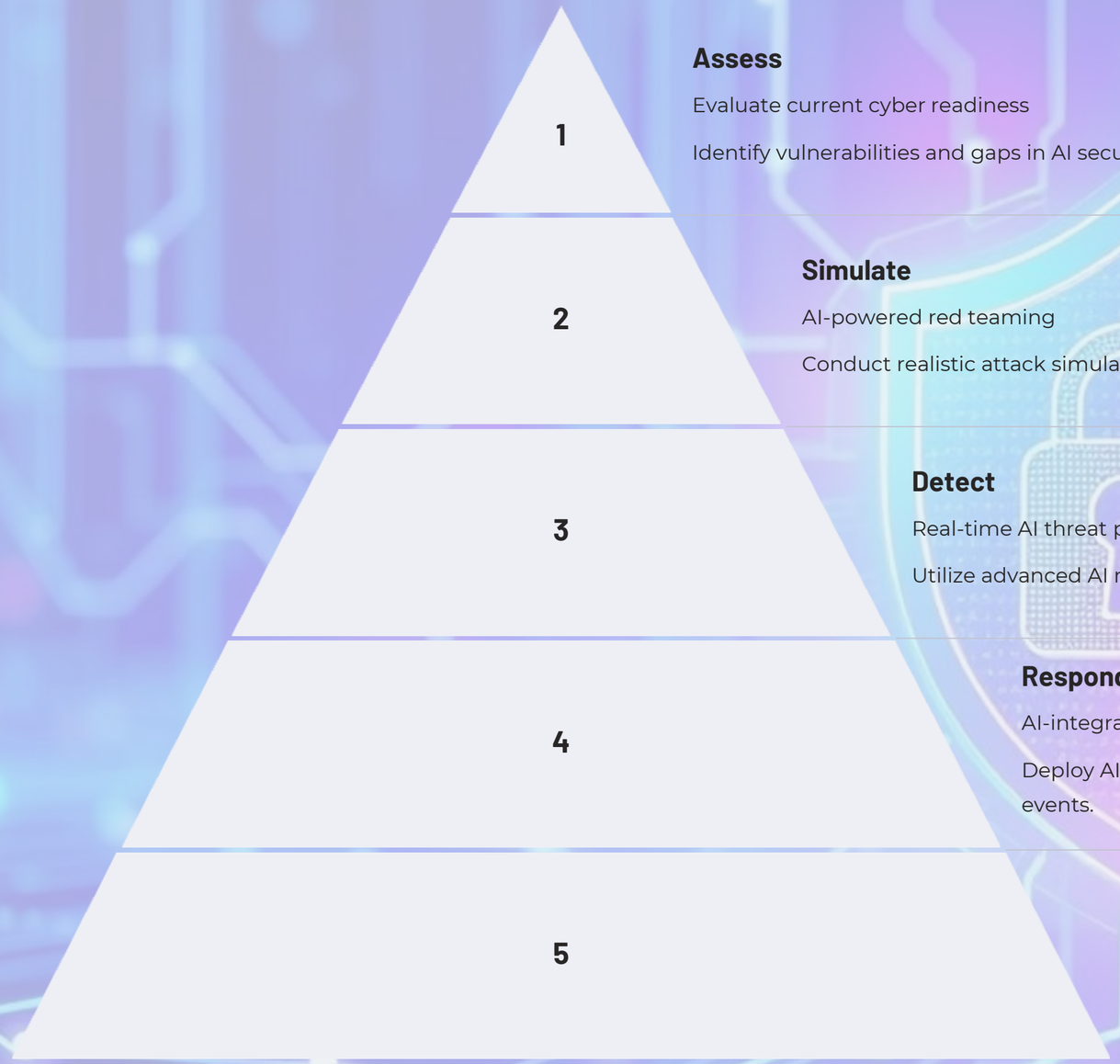
Agentic AI

Self-operating AI creates high-stakes concerns

Deloitte 2024 Insight

27% use agentic AI, only 11% with control protocols

Action Framework for Cyber Resilient AI



Assess

Evaluate current cyber readiness

Identify vulnerabilities and gaps in AI security posture to prioritize mitigation efforts effectively.

Simulate

AI-powered red teaming

Conduct realistic attack simulations using AI to uncover potential weaknesses and improve defense strategies.

Detect

Real-time AI threat platforms

Utilize advanced AI monitoring tools for continuous threat detection to enable rapid identification of cyber incidents.

Respond

AI-integrated incident response

Deploy AI-driven automation and analytics to accelerate response times and minimize impact during cyber events.

Collaborate

Public-private threat intelligence

Foster information sharing across sectors to enhance collective situational awareness and resilience.

Only 7% Indian orgs feel ready; 71% CISOs lack AI-adaptive defenses

Building a Cyber-Ready Future for AI

1

Robust Security

Implement strong protocols around AI and data.

2

Collaboration

Bridge AI developers with cybersecurity experts.

3

Ethical AI

Prioritize ethical development and deployment.

4

Continuous Monitoring

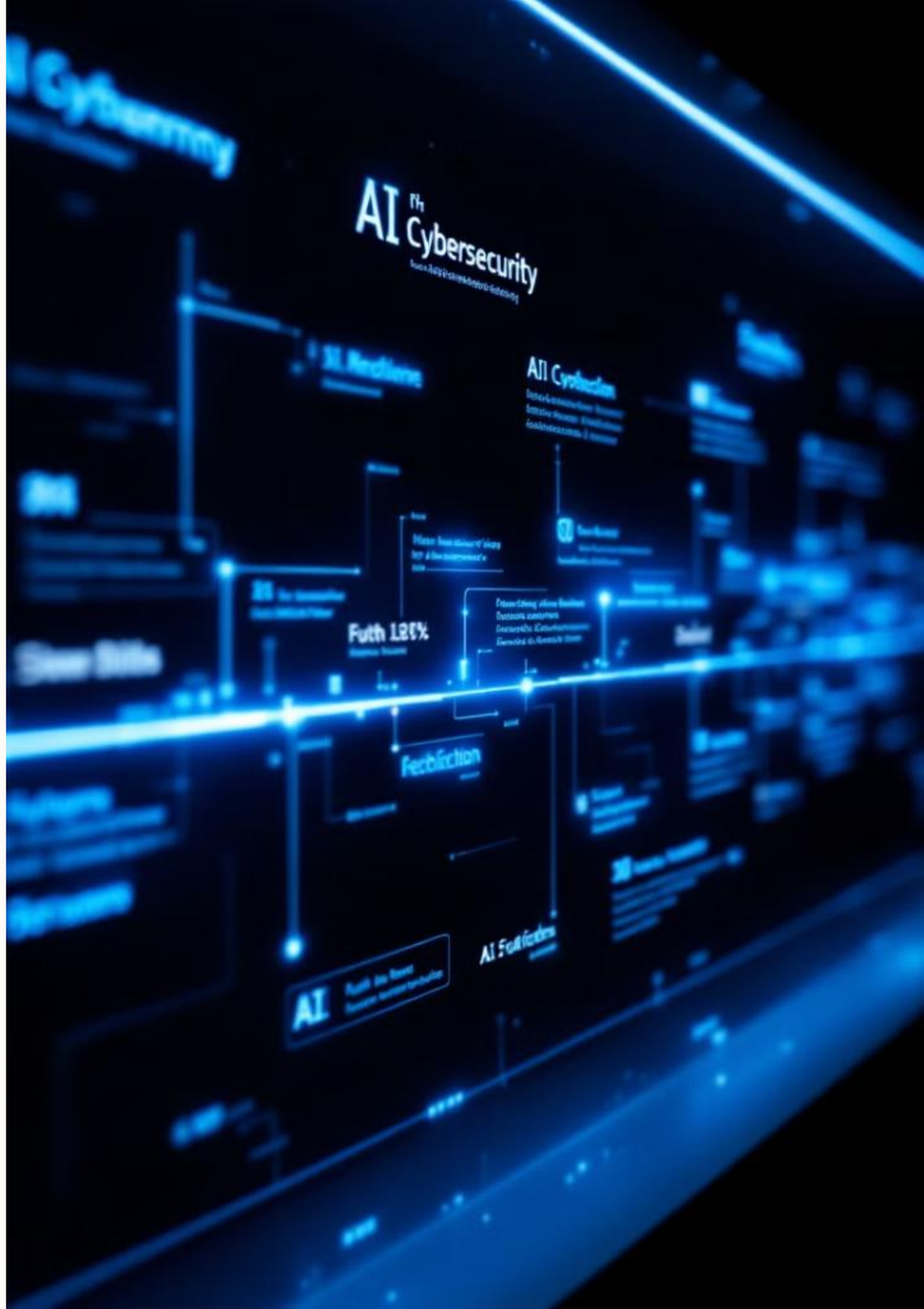
Adapt to new threats through constant vigilance.

5

Proactive Impact

Companies with readiness see 60% less downtime.

Cyber readiness is essential for strong, resilient AI futures.



Conclusion

Securing AI’s Future Together

Invest in Cyber Readiness

Building resilience and trust in AI systems

Implement proactive risk management and continuous monitoring.

Train teams on AI-specific cybersecurity challenges.

Adapt to Emerging Threats

Continuously evolving defenses for AI vulnerabilities

Leverage AI-driven threat intelligence and adaptive controls.

Stay ahead of adversarial tactics and data poisoning risks.

Foster Collaboration

Partnering across sectors to enhance security

Share intelligence with public and private entities to improve response.

Encourage industry standards and regulatory compliance.

By embracing preparedness, flexibility, and cooperation, organizations can confidently navigate the challenges of the AI era.

Together, we can build a secure, trustworthy foundation for AI’s transformative future.