Bharati Vidyapeeth (Deemed to be University),
Centre for Distance and Online Education, Pune
School of Online Education

Seminar On
"AI in cybersecurity"

Submitted in Partial Fulfilment of the Requirements for the Award of Degree of

Master of Computer Applications (Online Mode)
2024 – 2025

Submitted by
Akshay Pandurang sadaphule
(PRN: 2345102214)

Faculty Mentor
Dr Mahadev Patil

Abstract

This report explores the integration of Artificial Intelligence (AI) into cybersecurity systems. AI enhances security by enabling intelligent threat detection, and real-time responses to cyber threats. It helps mitigate advanced attacks like phishing and malware by using algorithms capable of learning and adapting. Real-world applications show significant benefits in efficiency and accuracy. However, AI also introduces new risks such abia, adversarial attacks, and future protenstential of AI in cybersecurity.

LATEST TRENDS IN IT
AI IN CYBERSECURITY

Objective of the Seminar

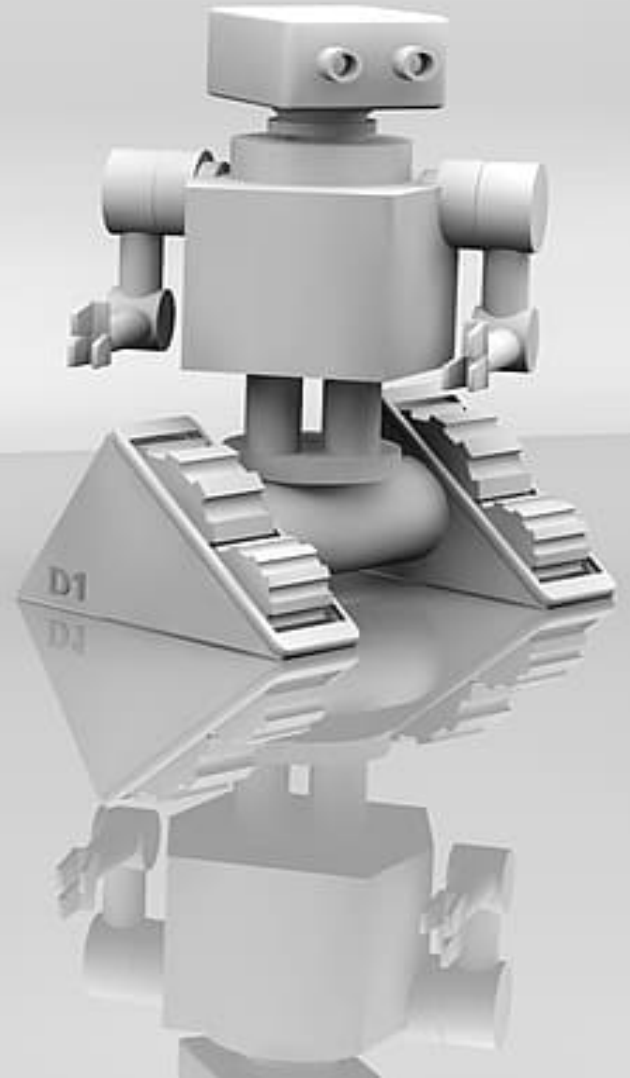
To explore how Artificial Intelligence (AI) is transforming the field of cybersecurity by enhancing threat detection, improving incident response, and enabling predictive security measures.

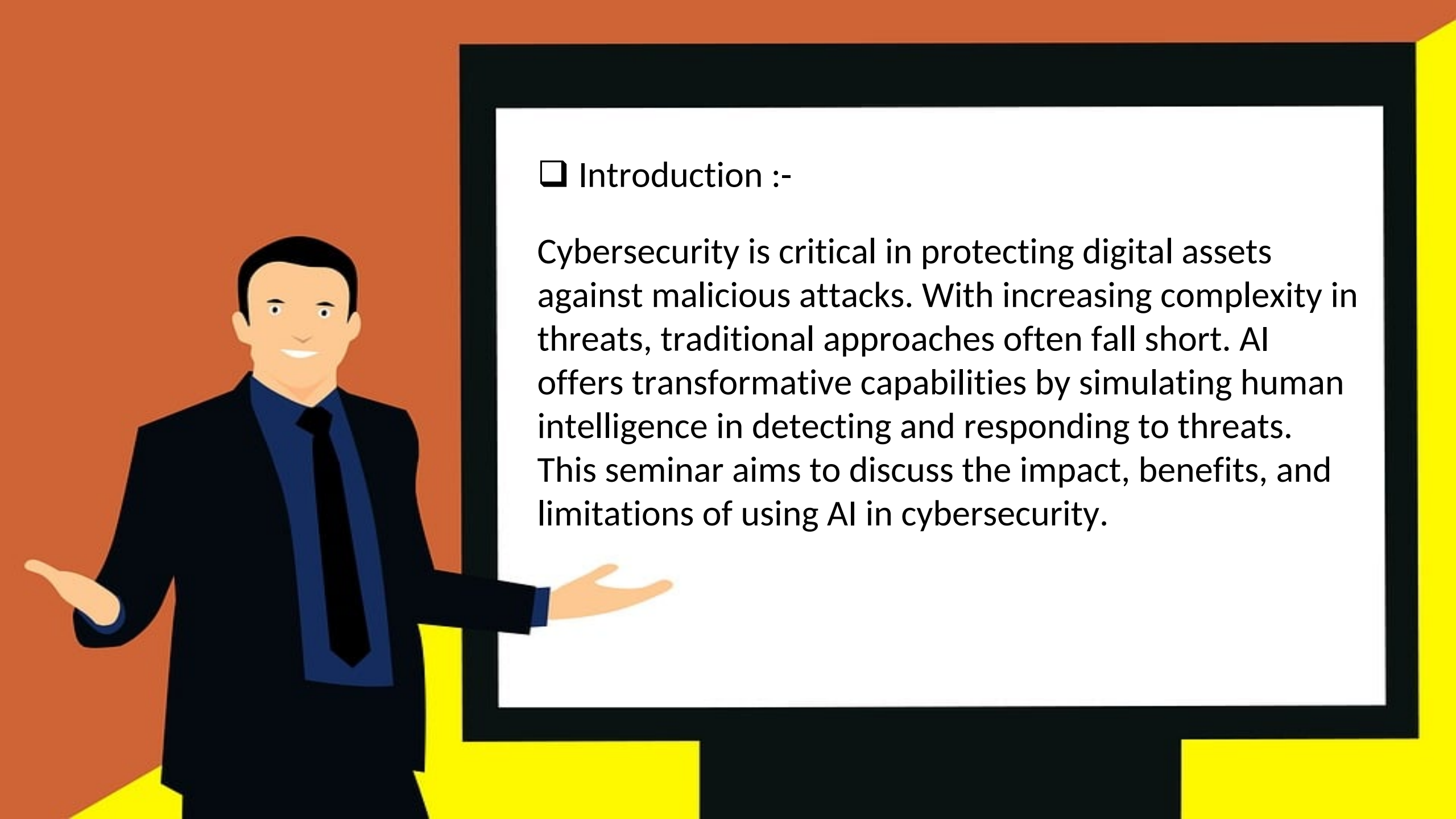
The seminar aims to provide an understanding of AI applications in safeguarding digital infrastructure, while also addressing the associated challenges and ethical concerns.

Scope :-

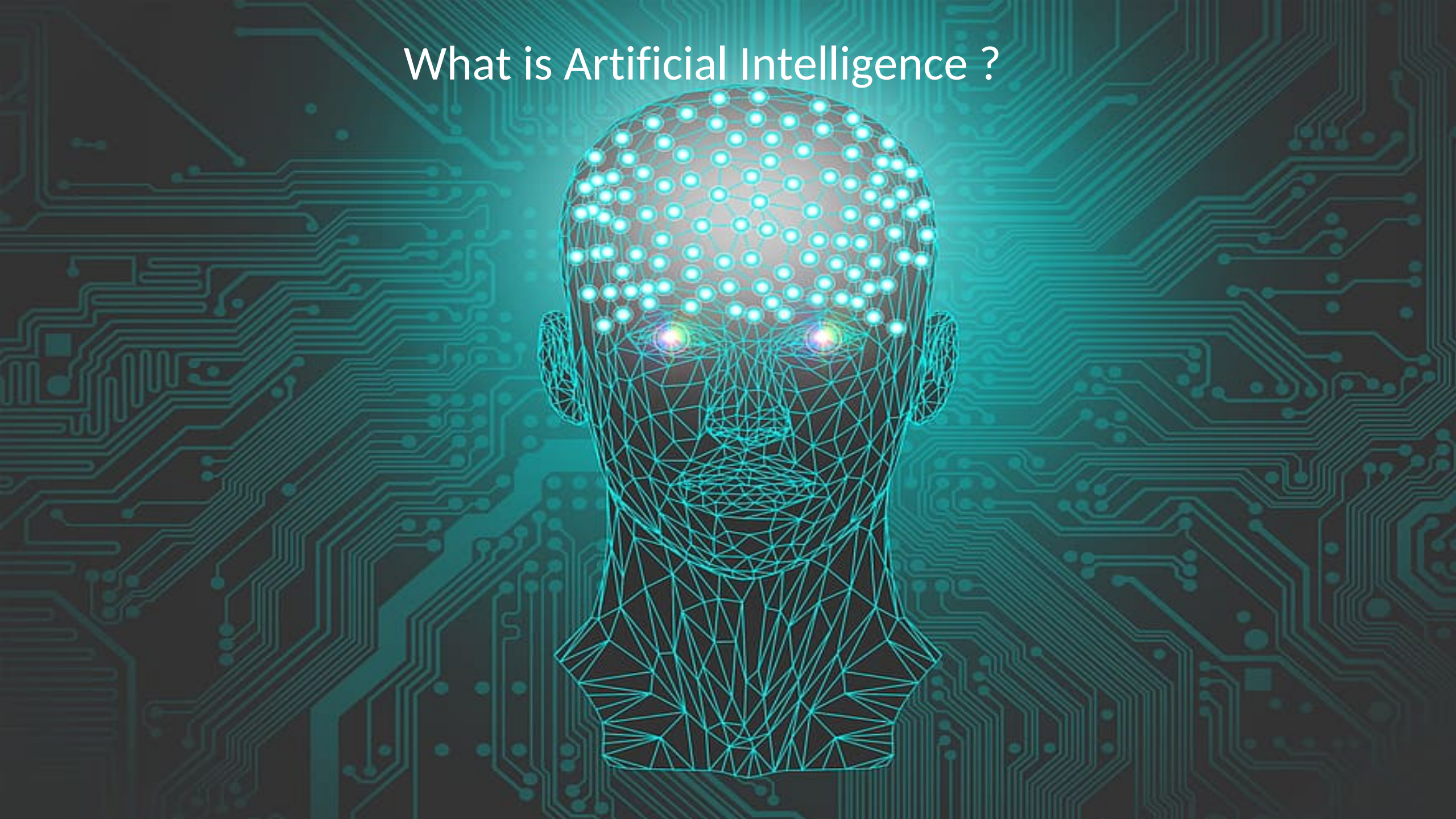
AI in cybersecurity fundamentally enhances security by learning from data to detect subtle threats, predict future attacks for proactive prevention, automate incident response for faster mitigation, improve vulnerability management for a reduced attack surface, analyze user behavior for insider threat detection, enhance security automation workflows, combat social engineering, and enable adaptive authentication.

The core principle is leveraging AI's analytical and learning capabilities to create more dynamic and intelligent security systems




❑ Introduction :-
Cybersecurity is critical in protecting digital assets against malicious attacks. With increasing complexity in threats, traditional approaches often fall short. AI offers transformative capabilities by simulating human intelligence in detecting and responding to threats. This seminar aims to discuss the impact, benefits, and limitations of using AI in cybersecurity.

What is Artificial Intelligence ?



Artificial Intelligence (AI) is a branch of computer science focused on creating systems capable of performing tasks that typically require human intelligence.

What is cyber security?

Cybersecurity

Cybersecurity is the practice of protecting digital systems, networks, and sensitive data from unauthorized access, cyberattacks, and theft.
It ensures the safety, integrity, and availability of information in the digital world.

Literature Review

Past developments in AI and cybersecurity have led to automated threation ad predictive and predictive. Research shows AI's successs scicss in reducing false positives, imprroving improving mably proactive security models. However, studies also highlight te vulnerability systems requirngs to adversarial attacks and requiring caɾreful design ı and monitoring.

Why Cybersecurity is More Important Than Ever ?

- Massive increase in Cyberattacks
- Cost of Data Breaches
- Rise of Ransomware
- Remote Work Vulnerabilities
- Personal Data Exposure
- National Security Risks

Trends in Cybersecurity

Cyber Wars

Ransomware

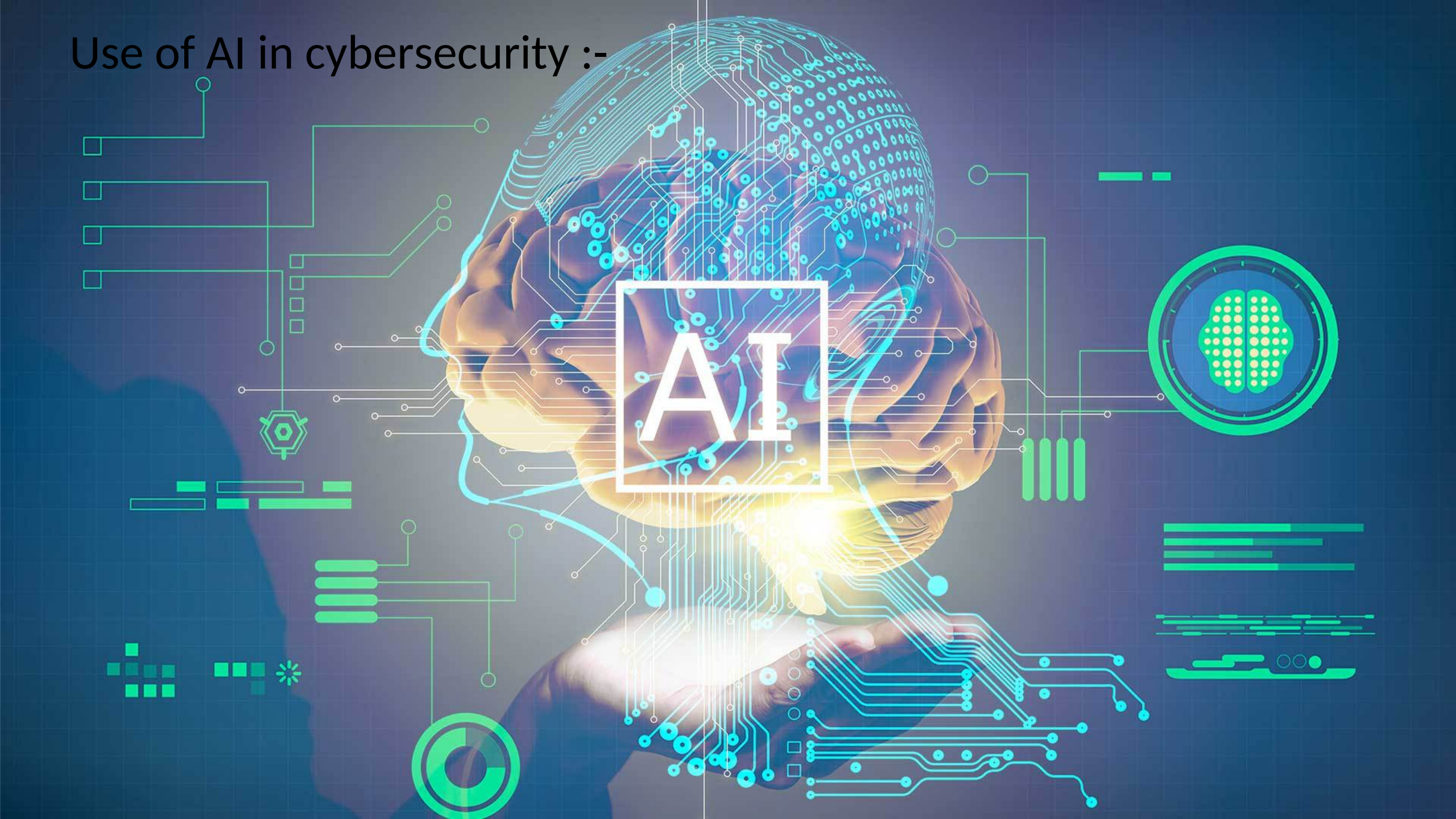
Ransomware

Infostealers

Edge Devices

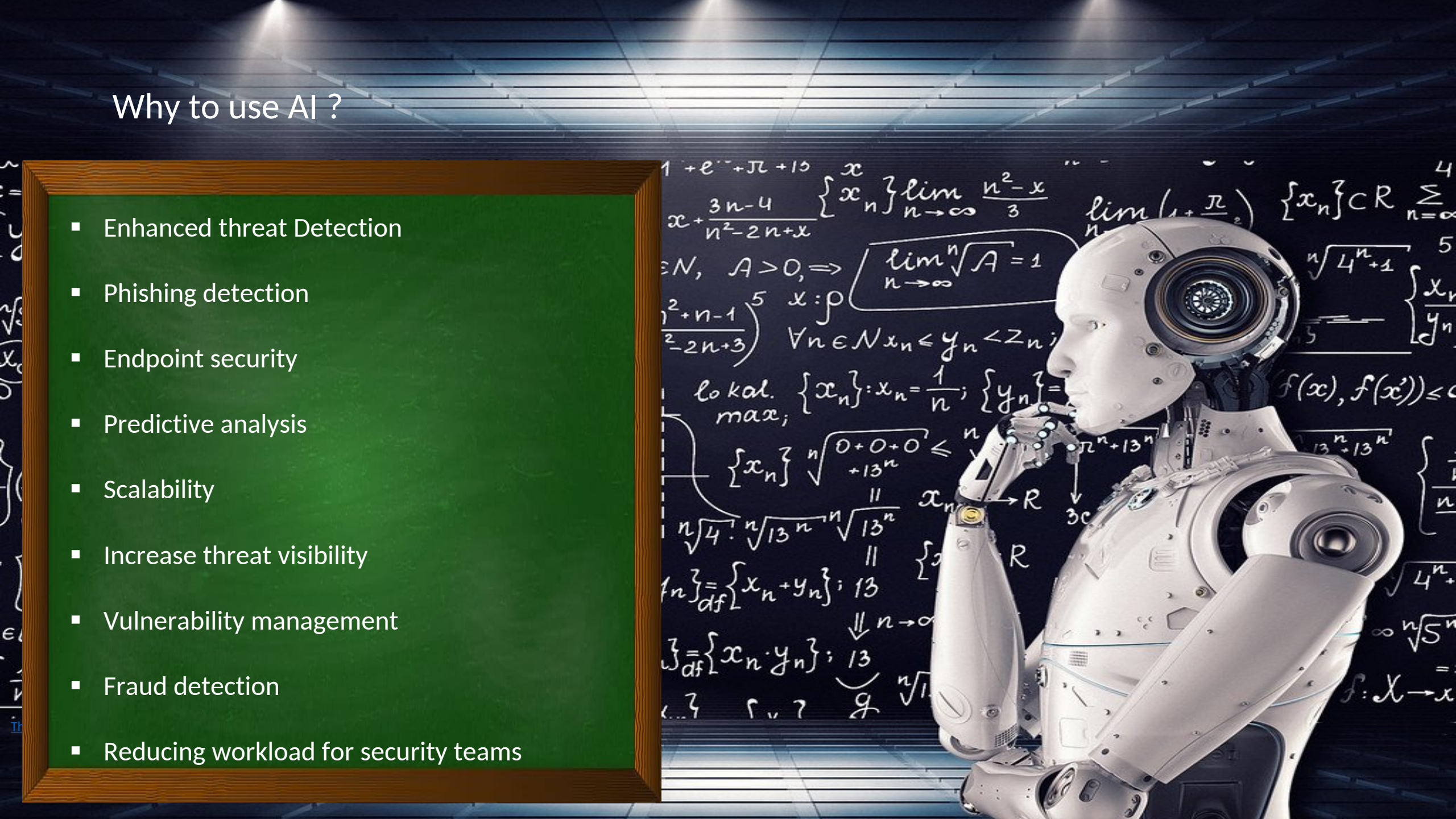
Cloud

Use of AI in cybersecurity :-



Why to use AI ?

- Enhanced threat Detection
- Phishing detection
- Endpoint security
- Predictive analysis
- Scalability
- Increase threat visibility
- Vulnerability management
- Fraud detection
- Reducing workload for security teams



Real world applications

Artificial Intelligence AI in Cybersecurity

Threat Detection

AI analyzes data in real-time to detect anomalies and identify potential cyber threats.

Incident Response

AI automates and speeds up response to incidents, suggesting remediation steps to miligate *damage*

Vulnerability Management

AI identifies weak penits in networks *and systems*, proactively scanning

Predictive Analytics

AI predicts future threats by analyzing historical activities on indentidy attack patterns

Endpoint Protection and Malware Detection

AI detects unsual behavior and flags malicious acti-vtiles on endpoints *liike*

Fraud Detection and Prevention

AI analyzes trans/actions in real-time to detect suspicious activity

Cyber Asset Attack Surface Management (CAASM)

AI tracks *and monitor's-here.* attack threats mySitface

Cloud Security

AI enhances cloud security by offering real-time threat detection and response across cloud environments

Impact of AI in Cybersecurity

- Improved Threat Detection
  - Faster Incident Response
- Predictive Capabilities
  - Enhanced Accuracy
- Advanced Malware Detection
  - Enhanced Cloud Security


Some real-life examples
Basler Zeitu
Vogel Gryff begeist
NRZ
NEUE RUHR ZEITUNG
Neue
DÜSSELDORF
Saarbr
Wie die Saarbrücker
Altersarmut für
Saar-Kommun
in die
WESTDEUTSCHE
junge Welt
Neue Waffen
Ruhr Nachrich
Sorge nach
neuem

Cyber Resilience in the AI Era: Securing the Future of Digital Enterprise

As enterprises embrace AI and cloud-driven transformation, cybersecurity must evolve to counter emerging threats. In this keynote, Jaspreet Singh,Partner and ...Read More

ETCIO
Updated On Apr 8, 2025 at 11:16 AM IST

With rapid AI and cloud adoption, enterprises face evolving cyber threats that demand proactive defense strategies. Jaspreet Singh - Partner and Cyber Advisory Leader, GT, outlines key cybersecurity trends, AI-powered risk management, and zero-trust frameworks to build resilient, secure enterprises. This keynote provides a strategic roadmap for CISOs and digital leaders to navigate cybersecurity challenges and ensure business continuity in a hyper-connected world.

Comparative Analysis

Compared to traditional **rule-based systems**, AI **dynamically adapts** by learning from data. It provides **faster, more accurate threat detection** but introduces **complexity** in terms of model transparency and oversight.

AI AND CYBERSECURITY: A DOUBLE-EDGED SWORD

among the top 25 Most Respected Entities in Sri Lanka for 2023.

This recognition is an accumulated journey of over three decades of dedication, trust, integrity, accountability, transparency and commitment to doing the right thing

that customers and stakeholders have in the company. This honour reaffirms AIA's commitment to putting people and customer centricity at the heart ofeverythingthey do. The company's approach is guided by the belief that insurance should be more

its dedication to delivering excellence, innovation, and value to all lives touched.

Chief Marketing Officer Sasith Bambaradeniya said; "At AIA, our journey to becoming the Most Respected Insurer for 2023 is not just about recogni-

ing what matters most for all Sri Lankans. All ourefforts revolve around creating experiences that resonate with people, educating them about the importance of protection, and empowering them to lead healthier and happier lives."

Numair Cassim Amana Bank PLC was appointed as the President, Varuna Koggalage Seylan Bank as Vice President, Dulan Abeyratne HSBC as Secretary and Jayan Fernando DFCC as Treasurer.

Other members of the committee include Charitha Jayawickrama Sampath Bank Immediate Past President, Ruwani de Silva NDB, Gayan Ranaweera NTB, Jeremy de Zilva PABC, Dhananjaya Day-

Commercial Banks and ized Banks in dealing with new developments and challenges pertinent to the industry. It also supports Internal Audit professionals to enhance comradeship and encourages participation of Banks to share knowledge and industry best practices.

Re-establishing in 2015, the forum has become an integral body that supports and assists Banks with common audit related issues within the industry.

John Keells IT achieves Microsoft Cloud Security Advanced Specialization

John Keells IT, a pioneer in the areas of Digital Transformation, Cloud and Cyber Security Solutions and Platform Technology, has reached yet another significant milestone.

The company has achieved the Microsoft Cloud Security Advanced Specialization, further affirming its stature as a global leader in the ever-critical realm of cloud security.

In this era of accelerated digitization, where safeguarding data and systems is paramount, this accolade is more than an award; it is a testament to John Keells IT unyielding commitment to protecting the digital future of businesses worldwide.

While celebrating this achievement, it's essential to recognize the broader implications. John Keells IT is now the first homegrown Sri Lankan company to be honored with the Microsoft Cloud Security Advanced Specialization. This distinction elevates both the company and the nation onto the global stage, showcasing that Sri Lanka, too, houses enterprises with the expertise and capability to provide world-class security solutions.

John Keells IT proven success in deploying Security Information and Event Management (SIEM) and Defender solutions garnered this esteemed recognition. These are not mere tools; they are fortresses that protect businesses from the relentless onslaught of cyber threats.

For enterprises embarking on the Zero Trust journey, John Keells IT's success implies trust, cutting-edge security solutions that stand at the pinnacle of technological advancement and a partnership with a team relentless in ensuring data and systems are fortified with comprehensive protection. Moreover, John Keells IT's 'Security by design' philosophy orbits around the pursuit of Zero Trust through three fundamental pillars: People, Processes and Technology. Zero Trust with People: access to data and applications is granted on a 'Least Privileged Access' basis. Zero Trust with Processes: aligning all organizational processes because everything undertaken forms a crucial part of the journey. Zero Trust with Technology: harmonizing the technology stack to create an architecture that promotes agility, crucial for quick adaptation when necessary.

Given the mounting reliance on digital systems, vulnerability to cyber threats is on the rise. Proactive measures are vital for protection against risks, and they are equally indispensable for organizations aiming to safeguard their reputation and sensitive data.

John Keells IT's Chief Operating Officer EMEA Territory Nishan Thevathason stated, "I am thrilled to celebrate thelatest recognition received by our Cloud Security team in attaining the Microsoft Cloud Security Advanced Specialization. This recognition is a testament to our unwavering commitment to securing the digital future of businesses. It showcases John Keells IT's 'Security by design' philosophy and our dedication to providing the most cutting-edge and robust security solutions in the realm of cloud security."

Enterprises looking to strengthen their posture on all platforms including multi-cloud and hybrid-cloudcan consult John Keells IT. Through an initial consultation and a comprehensive 360 assessment, John Keells IT's expert cloud team assists enterprises in devising their cloud strategy, architecture, and execution, ensuring their digital environments are secure, efficient, and productive.

The battle for AI security

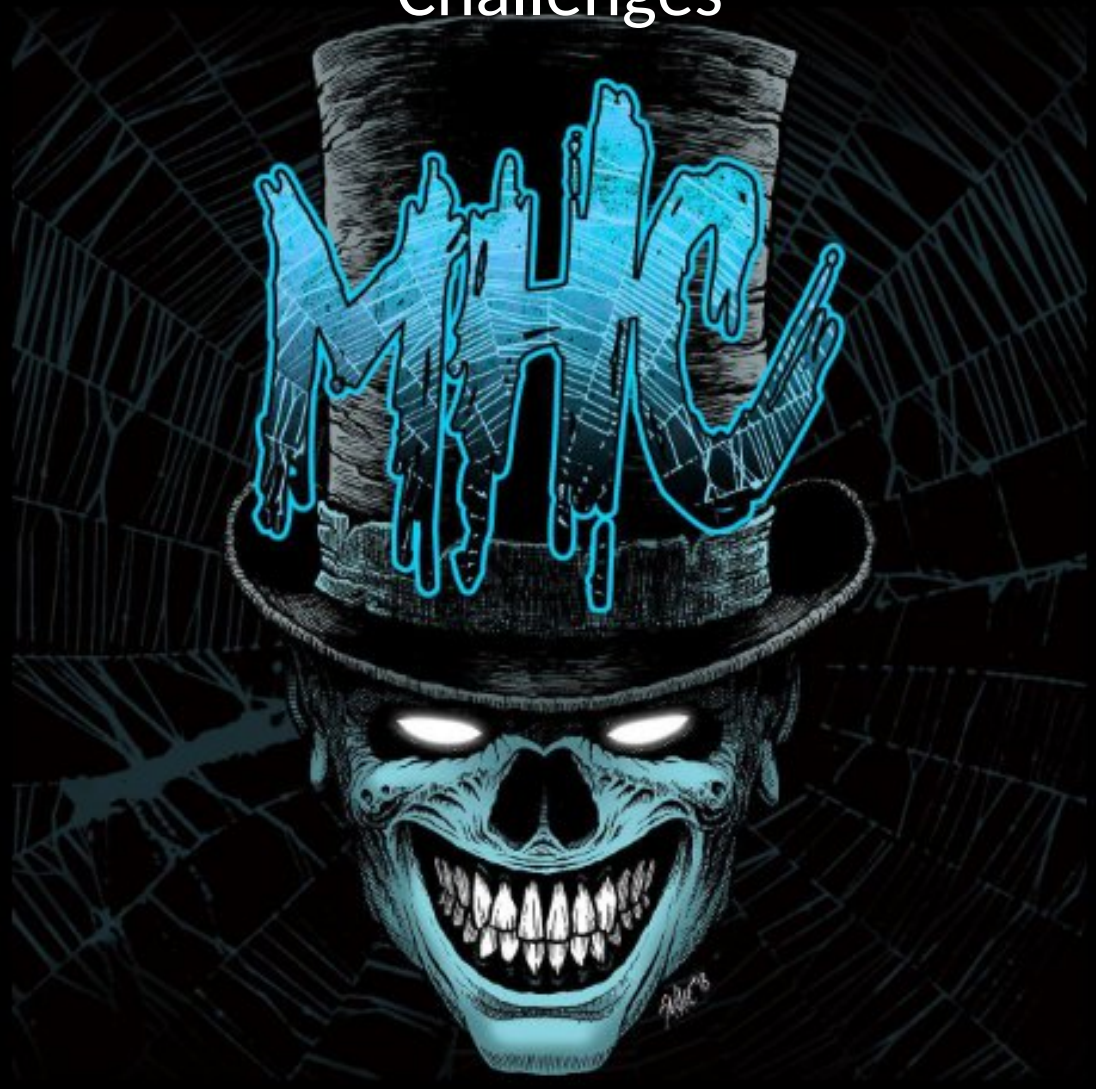
The second episode of Smarter AI Transforming India podcast takes a deep dive into the high-stakes world of security in an AI-driven era.

Brand Connect Initiative • Brand Connect Initiative
Updated On Mar 28, 2025 at 02:55 PM IST

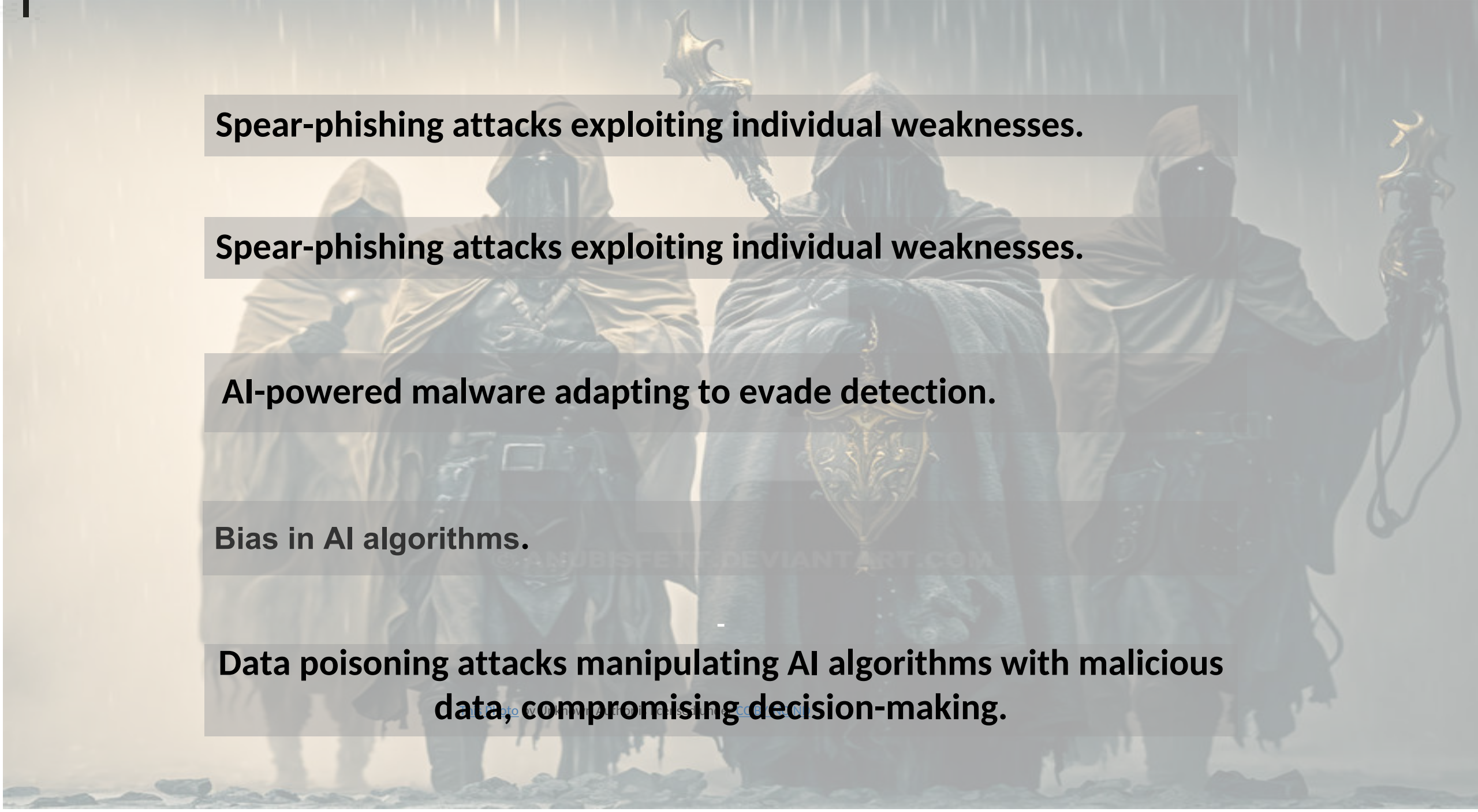
As businesses rapidly adopt AI, securing data, systems, and infrastructure has become more crucial than ever. While AI enhances security, it also introduces new threats, making cybersecurity a top priority for enterprises.

Venkataraghavan SK, Director of Solutions and Services Group (SSG) at Lenovo India, and Manu Dwivedi, Partner & Leader of Cybersecurity and Risk Consulting at PwC India, explored the complexities of AI-driven security in the second episode of the podcast, organised in collaboration with Lenovo, ETCIO, and *The Times of India*'s Times Techies.

Challenges



The dark side of AI



Spear-phishing attacks exploiting individual weaknesses.

Spear-phishing attacks exploiting individual weaknesses.

AI-powered malware adapting to evade detection.

Bias in AI algorithms.

Data poisoning attacks manipulating AI algorithms with malicious data, compromising decision-making.

FINANCIAL EXPRESS
Read to Lead

NEW BATTLEGROUND

Targeted solutions to counter AI risks

Firms seek tools & techniques to detect and prevent attacks

SUDHIR CHOWDHARY

WITH A COMPLEX IT backbone, Mumbai-based Kokilaben Hospital struggled with fragmented security tools, making threat detection and response time-consuming. Managing cyber security across multiple dashboards required hours of manual effort, leaving potential security gaps. By deploying Check Point's AI and ML-powered solutions, the hospital achieved real-time threat intelligence, automated vulnerability detection and a unified security platform. Kokilaben Hospital's security team can now swiftly detect, analyse and remediate threats from a single intuitive dashboard.

Similarly, Alkem Laboratories, operating 24/7 in a highly regulated environment, faced rising cyber threats and an overwhelming volume of phishing attacks, with over 50 daily reports of malicious emails. Here again, Check Point's AI-powered solutions helped the pharmaceutical giant with automated threat prevention, secure remote access, and real-time AI-driven threat intelligence. As a result, phishing reports have dropped from 50+ per day to zero, security management is streamlined, and Alkem's cyber defences are future-proofed.

Sundar Balasubramanian, MD, Check Point Software Technologies, India & South Asia, said, "AI adoption is no longer optional but a competitive necessity. However, enterprises must address critical concerns like security, compliance, and ethical AI usage. AI-driven automation can streamline operations, but without robust safeguards, it can also introduce new vulnerabilities."

Google's decision to buy the cybersecurity firm Wiz for $32 billion comes at a time when AI is bringing new risks and multi-cloud and hybrid are becoming the norm, average. Against this backdrop, organisations are looking for cybersecurity solutions that mitigate AI risks, improve cloud security and span multi-cloud.

The Cisco 2024 AI Readiness Index reveals that only 18% of organisations in India are fully prepared to deploy AI technologies, down from 26% last year, underscoring growing security challenges. Despite 57% of companies investing 10-30% of their IT budgets in AI, many still face infrastructure challenges, data security risks, and governance gaps, hindering their ability to fully leverage AI securely. "With 73% of businesses expecting a cybersecurity incident within the next 12-24 months, the cybersecurity practice leader, Kyndryl India, the increased adoption in AI has led to an expanded attack surface making organisations more vulnerable. While data security gaps persist, and weak governance exposes sensitive information, many firms overlook AI-specific attack vectors, assuming traditional controls suffice. "To close these gaps, businesses must adopt zero-trust AI architectures and chief information security officers must take ownership of AI security, integrating robust governance, continuous monitoring, and least-privilege access to ensure AI remains a business enabler — not a security liability," he added.

Understanding AI security risks gle with effective implementation. "AI security concerns are acknowledged, however, the proactive adoption of security measures is still evolving. Also, most companies today struggle with prioritising what, when, and how to quantify the risk and implement the right security measures, leading to gaps in their AI risk management strategies," said Muthumari S, global head of AI Studio, Brillio.

Interestingly, while companies rush to integrate AI into their systems, many are yet to recognise that AI systems themselves can become targets. "We have reached a place where vulnerabilities, malware, and targeted attacks on AI systems are becoming real con- prepare for the rise of multi-agent AI systems, where attackers can orchestrate multiple AI models to automate complex cyberattacks.

In the process of AI adoption, enterprises must prioritise data privacy, model integrity, and cyber resilience to ensure secure and responsible implementation, feels Puneet Gupta, VP & MD, NetApp India & SAARC. Data poisoning — where malicious inputs compromise AI models, can lead to flawed decision-making, and threats like model theft pose risks to an enterprise's intellectual property. Another risk is that AI-driven automation expands the attack surface, introducing potential vul-

HIDDEN DANGER

- Google's decision to ink a $32 billion deal with Wiz is intended to beef up its cloud security offerings at a time when AI is bringing new risks and multi-cloud & hybrid are the norm
- AI systems require continuous data access, making them vulnerable to data poisoning attacks and privacy risks, especially in AI-driven user analysis

- Cisco 2024 AI Readiness Index reveals that only 18% of firms in India are fully prepared to deploy AI tech, underscoring growing security challenges
- Despite 57% of companies investing 10-30% of their IT budgets in AI, many still face infrastructure challenges, data security risks and governance gaps
- With 73% of businesses expecting a cybersecurity incident in next 1-2 years, the urgency to build cybersecurity expertise is paramount

SAMIR KUMAR MISHRA, DIRECTOR, SECURITY BUSINESS, CISCO INDIA

Indian enterprises recognise AI's transformative potential, but many lack a structured approach to securing its integration. They overlook the security risks that come with it

SUNDAR BALASUBRAMANIAN, MD, CHECK POINT SOFTWARE INDIA

Successful AI adoption isn't just about technology but responsible implementation and use, as well as building resilience against evolving cyber threats

SUNIL SHARMA, VICE-PRESIDENT - SALES, SOPHOS INDIA AND SAARC

Companies need to embed cybersecurity into their AI strategies from day one to minimise risks and unlock its full potential as a force multiplier for innovation & resilience

MUTHUMARI S, GLOBAL HEAD OF AI STUDIO, BRILLIO

Most companies today struggle with prioritising what, when, and how to quantify the risk and implement the right security measures in their operations

AI-driven attacks push firms to strengthen cybersecurity

As GenAI rewrites cyber threat landscape, Indian companies see it as top menace to business

Pratishtha Bagai & Jas Bardia
MUMBAI & BENGALURU

Multi-vector attacks are very sophisticated cyber threats that exploit multiple vulnerabilities simultaneously ISTOCK

With generative artificial intelligence, or GenAI transforming business operations, it is also contributing to escalating cyber threats.

Sophisticated cyberattacks leveraging AI-powered deepfakes, phishing, data manipulation, and malware are on the rise. To combat these complex threats, Indian companies are looking to upgrade their security infrastructure, experts said.

Cybersecurity attacks, which started around the 1980s, have evolved in the past 40-odd years. Earlier, what was only about corrupting standalone devices with viruses, now has the capacity to cripple an organization and even an entire country. "Cyberattacks are currently in the 5th or 6th generation of what is known as multi-vector attacks. These are not only targeting your endpoint devices, but also your networks, data centres, cloud, etc. All of it is happening in parallel, making it much more complex and sophisticated, and difficult to prevent," said Devroop Dhar, co-founder of management consulting firm Primus Partners.

Multi-vector attacks are very sophisticated cyber threats that exploit multiple vulnerabilities simultaneously to breach an organization's defences. A typical example is a distributed denial-of-service (DDoS) attack that combines multiple techniques, such as flooding networks and overwhelming systems, to maximize disruption.

Coupled with other sophisticated technologies such as machine learning, artificial intelligence (AI) can both be a boon or a bane depending on who is using it. Many cyber criminals are using AI technology to intensify their attacks. Firms are using AI to build advanced cybercrime protection systems. "AI is a double-edged sword. It is both a tool for companies to prevent and respond to attacks and also a tool for cyber attackers to increase the intensity of their attacks," Dhar highlighted.

AI: THE NEW WEAPON

COMBINED with other advanced technologies like ML, AI can be both a boon and a bane

A DDoS attack uses flooding of networks and overwhelms systems to maximize disruptions

A sophisticated AI tool used by cyber criminals rampantly to generate attacks is deepfake

FIRMS are now using AI to build advanced cybercrime safety systems to identify unusual patterns

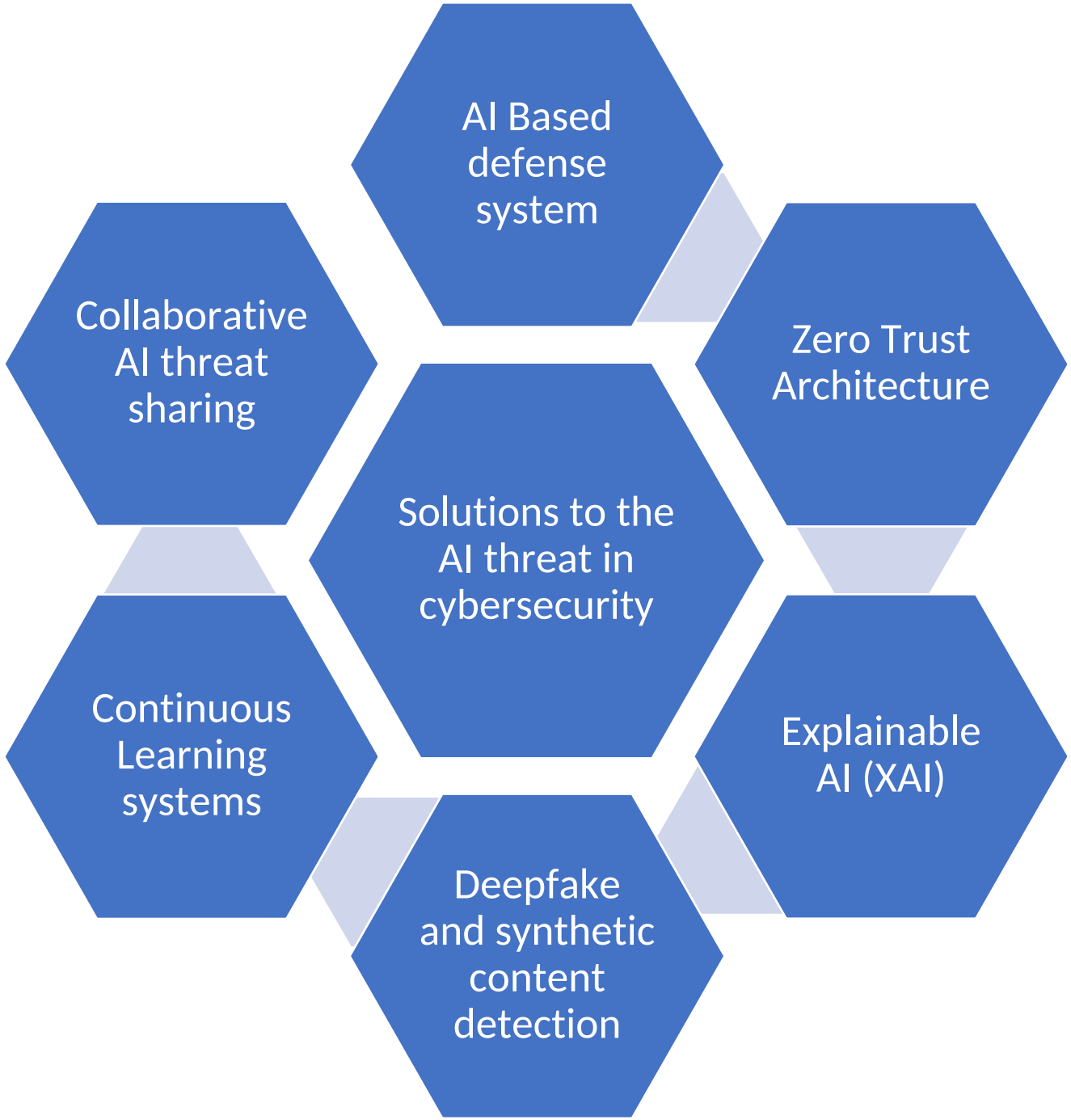
Companies are using AI tools to scan through humongous amounts of data to identify unusual patterns and detect cyber attacks, he added.

As far as cyber criminals are concerned, they are using AI rampantly to generate sophisticated attacks using technologies like deepfake. "Algorithmic attacks were mostly numeric, so attackers would write scripts to go vua millions of combinations of passwords to attack a user id. But now, with AI, the ability to create attacks such as deepfakes, is much higher and to automate them is significantly higher," said Ajay Trehan, chief executive of authentication firm Authbridge that helps firms with identity management. Trehan sees this trend grow further in 2025.

Cybercrime is becoming a concern. In Indian outlook of PwC's Global economic crime survey 2024, it said 33% of senior executives surveyed highlighted cybercrime as one of the biggest problems for businesses. Tata Consultancy Services Ltd, the country's largest software services company, has highlighted cyber threats posed by Gen AI. "GenAI is enhancing operational efficiency, but organizations must equip themselves to counter cyber threats. It is imperative for organizations to harness advancements and implement GenAI-powered threat detection and response systems to stay ahead of the curve," said Ganesa Subramanian Vaikuntam, the global head of cybersecurity at TCS, in the firm's 2025 Cybersecurity Outlook.

jas.bardia@livemint.com

For an extended version of the story go to livemint.com


AI Based defense system
Collaborative AI threat sharing
Zero Trust Architecture
Solutions to the AI threat in cybersecurity
Continuous Learning systems
Explainable AI (XAI)
Deepfake and synthetic content detection

Findings and Discussion

AI improves the speed and accuracy of cybersecurity, Industries benefit through reduced human error, faster response times, and proactive security. Adoption is rising across major sectors, including finance, healthcare, and cloud services.


API
Future Scope

The Future of AI in Cybersecurity

AI-Powered Threat Hunting

Utiliziring machine learning and behavi-oratonnlytice to predict, detect, and neurralze threats before they manitfrest into full-scale attacks.

AI-Driven Security Operations Centeres (SOCs)

Modern SOCs leverage AI for real-tine theat analyisis automared incident titage, and adaptive detense strategies. AI also enhan-ces correlation of data across multiple cou-rces for taster-more acourate hreat res-

AI-Enabled Endpoint Security

Exitpoints are protected using AI models capable of detecting sophis-tmested miawers, rensomwane. and zeno day capisits. AI allows-rai-time-device monitoring, behavioral

Automated Vulnerability Management

Smart deception systems, powered by AI create dly-namic honevoors and trays that adept ba:ed on attac-ker behavior gathering intelligence and delaying or stopping lateral movement within networks.

Additional Related Trends (Broader View)

AI-Augmented Identity & Access Management (IAM)

AI monitersand adepts authentication protectle dunartically: enabling real-time risk, based access controis and detec-ting account takeovers.

Behavioral Biometrics

Continuous AI thentication, based on user behaviors such as toping mytmn, mou-se movement, and foor hacreen inter-action, enhanced with AI.

Autonomous Incident Response

AI systems, capryble of not just detect-ing incidents but initiating real-time cont-tainment. Inrigation, and recovery actions autornatically.

AI-Based Risk Scoring and Fredictive Analytics

Predicting which systems, users, or othird parties pose fre greatest risk based on

Key

- Core
- Extended

Key Challenges in AI Adoption

Adversarial AI

AI systems vulnerable to malicious attacks.

Skills Gap

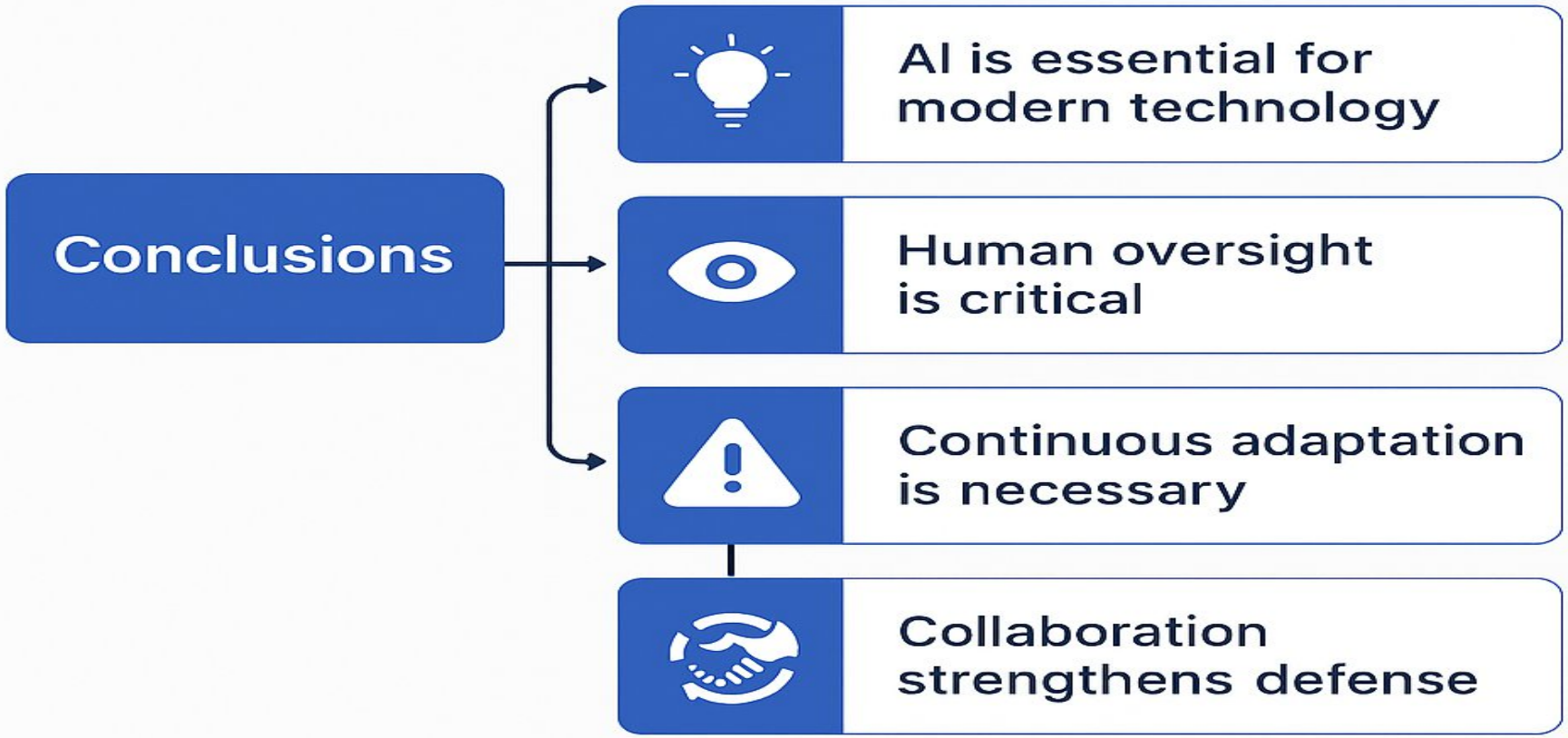
Shortage of professionals with AI expertise

Regulatory Compliance

Meeting new AI laws and ethical standards


Opportunity
Predictive security
Autonomous security systems
Personalized security

Conclusions: AI's Role in Cybersecurity



The integration of AI in cybersecurity represents a paradigm shift in safeguarding digital assets. While challenges like ethical concerns and lack of explainability persist, AI offfers unprecedented potential to enhance security operations.

References

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.

NIST. (n.d.). Cybersecurity *Framework*. National Institute of Standards and Technology. Retrieved from https://www.nist.gov/cyberframev

IBM Security. (n.d.). *How AI is used in cybersecurity*. Retrieved from https://www.ibm.com/security/artificial-intelligence and McKinsey *Company*. (2023). *The state of AI in 2023: Gen*erative AI's breakout year. Retrieved from https://www.mckinsey.com/

Symantec Enterprise Blogs. (n.d.). *How AI and machine leaming enhance cybersecurity*. Retrieved from https://symantec-enterprise-blogs.securit y.com/ Brundage, M., et al. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Retrieved from https://arxiv.*org*/abs/1802.07228


THANK
YOU