GET AHEAD OF THE ATTACKER

AMPLIFY DEFENDER POTENTIAL, BUILD TRUST AND CREATE VALUE

Infosys®
Navigate your next

Brijesh Balakrishnan
Head - CyberSecurity Practice, Infosys

Today's business world is an AI-powered interconnected ecosystem. Boundless business opportunities on one side, and a battleground with AI-powered threat actors on the other. These bad actors work relentlessly 24X7 to break enterprise cyber defenses to exploit vulnerabilities, steal data, and disrupt supply chains eroding the value of enterprises across the globe.

For too long, our defenses have been reactive, relying on security members' expertise, tribal knowledge, and pre-defined SOPs to identify and respond to threats that are increasingly sophisticated and automated. We have been playing a perpetual catch-up game, struggling to keep pace with the speed of adversaries.

This book arrives at a critical juncture. It delves into the transformative power of Cyber AI – the application of artificial intelligence to solve the challenges of cybersecurity and protect AI.

In these chapters, you will explore how cybersecurity services can be transformed into software through AI agents, capable of learning, adapting, and collaborating with the human defender to redefine the future of cyber defense.

With a promise of a paradigm shift, AI agents collaborate with human defenders to build a dynamic and resilient digital immunity for enterprises, constantly learning and evolving in the face of ever-evolving intelligent threats.

The journey into Cyber AI is not without its complexities, AI risks and ethical considerations. This book thoughtfully navigates these nuances, exploring the potential benefits alongside the need to balance the challenges of implementation, Responsible AI, and the ever-present risk of adversarial AI.

Whether you are a seasoned cybersecurity professional, a technology leader grappling with the escalating threat landscape, or simply a curious mind seeking to understand what next in cybersecurity, this book offers invaluable insights to build cyber resilience, build enterprise scale cyber platforms and leverage AI better security outcomes.

Welcome to the future of cybersecurity...

Contents

Why this book?

Introduction

Artificial Intelligence (AI) and Cybersecurity are two important fields that are increasingly intersecting to help enterprises build cyber defense against a constantly evolving threat landscape. This book focuses on providing a blueprint for enterprise for amplifying defender potential through AI.

- **Agentic AI for Hyperautomation**: Agentic AI and Digital defenders enable better automation to reduce human errors and costs. For example, automating vulnerability scanning and patching streamlines processes that frees up analysts for complex investigations.
- **Gen AI-based assistants**: AI assistants analyze data for accurate, data-driven decisions, providing outcomes without human bias. Building the right data sets is crucial.
- **Predictive AI for Threat Analysis**: Continuously learns and adapts to new threats, offering dynamic defense. Monitors data in real-time for immediate response to emerging threats.

The case for "Get Ahead of the Attacker" book

The continued investment in AI, increased sophistication of cyberattacks, and regulatory pressure on enterprises to protect their data has presented an opportunity for AI for Cyber Defense. These trends reflect the increasing reliance on AI to enhance the efficiency and effectiveness of enterprise security, address emerging security threats, and fortify enterprise data resources.

This is a business book for cybersecurity professionals who seek to solve problems using Agentic AI, Generative AI, and Predictive AI. It also serves as a fundamental guide for professionals and students to use AI for Cyber Defense.

In a series of structured chapters, the book describes the building blocks to design cyber defense and scale it for an enterprise. The chapters are progressive and build skills across different domains of security. The book will do the following:

1. Carefully examine the key ideas to use AI in building capabilities to stay ahead of the attacker
2. Give you tools to understand cybersecurity challenges, learn from them and use AI for Cyber Defense
3. Tailor Cyber AI for your enterprise as one size fit all solutions does not work in Cyber AI
4. Details of our recommendations, experiences and share success stories from a wide range of cybersecurity services
5. Guide to design, implement and adopt of enterprise scale Cyber AI

Annotated table of contents

- Foreword (From Brijesh Balakrishnan - Head of CyberSecurity)
- Chapter 1 – Changing Tide of CyberSecurity - Cyber Service as a Software.
- Chapter 2 – Amplifying Defender Potential – Human centricity of Cyber AI
- Chapter 3 – Redrawing the "first line of defense" – AI first Security Operations for Enterprises
- Chapter 4 – Infosys Cyber Next Topaz Fabric for Cyber Resilient Organizations
- Chapter 5 – AI-powered Physical Security
- Chapter 6 – Scaling AI through Platforms
- Chapter 7 – Fly wheel of Innovation for Cyber AI
- Incomplete - End notes, References and Further reading

One notable exception to this book is that you do not have to go through chapter by chapter to use it. See the map below and align the reading order according to your interest.

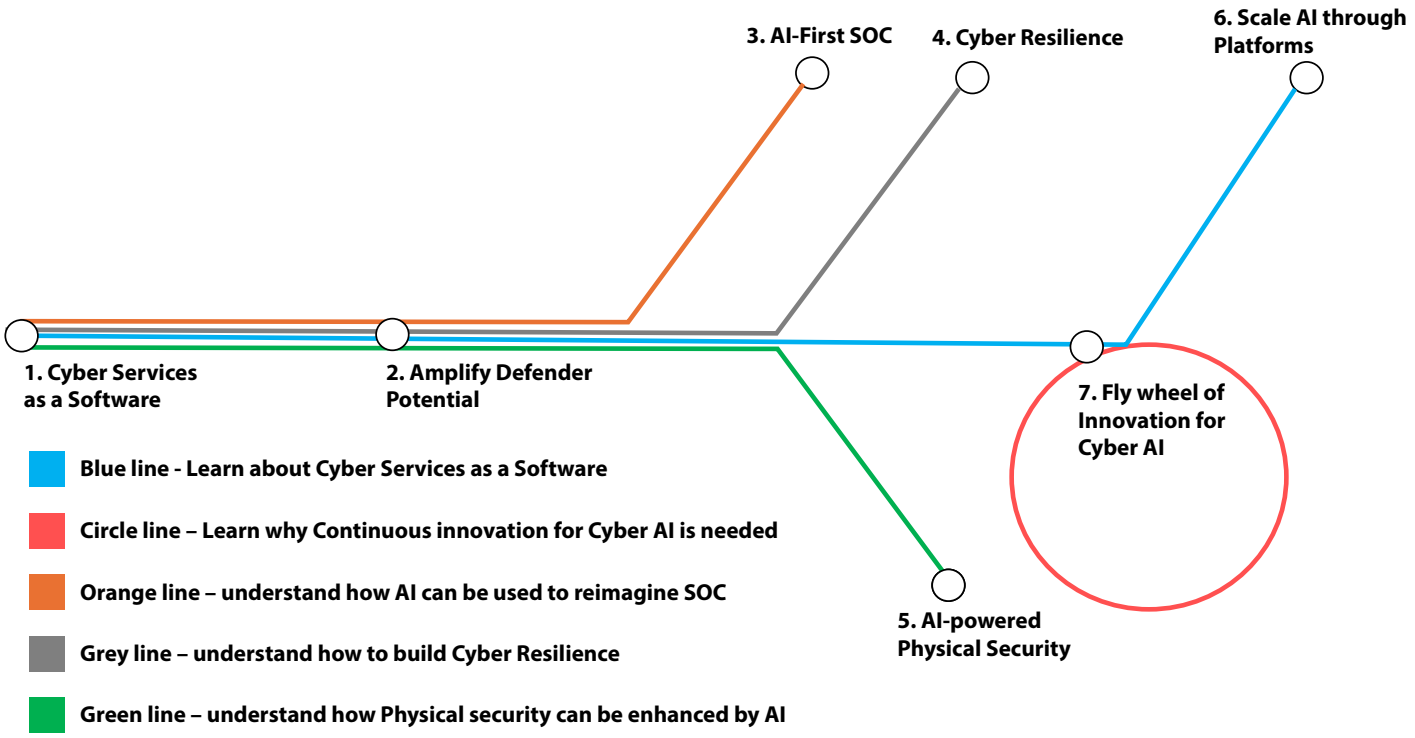
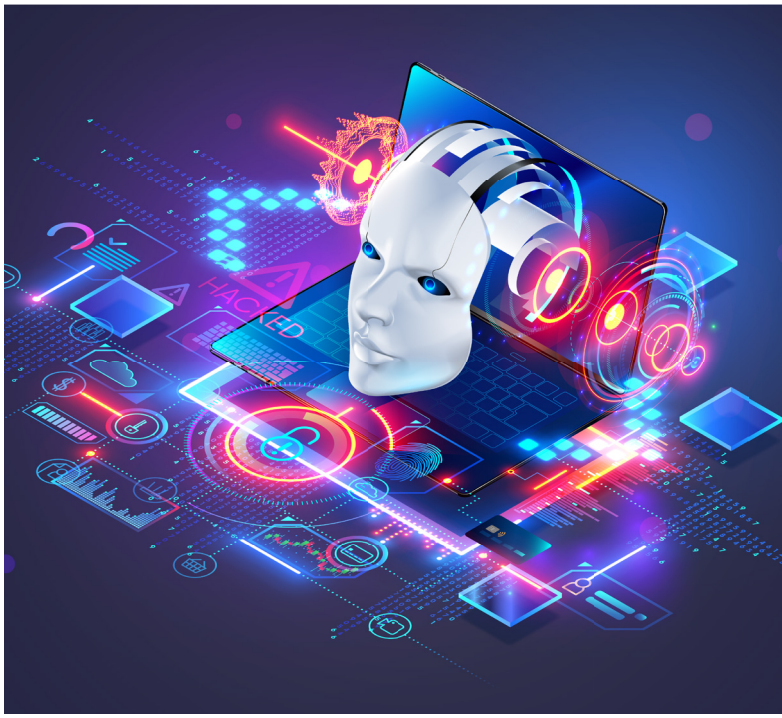


Figure 1 - Reading pathways

1

Cyber Services as a Software – Changing Tide of Cyber Defense

Re-imagining Cyber Defense Services as a Software



Automation of human work has been the norm from the industrial revolution. Artificial intelligence has exponentially scaled automation and replicated human decision making. Agentic AI though in the early days, has the potential to create a network effect to re-define whole categories of work done by skilled cybersecurity professionals.

"Power, to a large extent defines us as individuals and as nations, itself being redefined" - Alvin Toffler in his book, Power Shift[1]. This was his view of the 1990s, where global power was shifted by the collapse of Soviet Union, rise of Asia and the impact of the European Union.

The new wave of AI for Cybersecurity has been transforming Cyber Services-as-a-Software. Enterprises can sell their services or products for cybersecurity but are still responsible for achieving the desired outcome of cyber defense. Services as a software paradigm shift has enabled input as cost of AI Infrastructure and output being prediction, reasoning, and automation provided by the AI to improve cybersecurity posture.

Challenges faced by enterprises in adopting AI for Cyber

Security teams today face AI-powered threat actors, whose attacks are sophisticated, fast and spread over a large attack surface. The teams must navigate data overloads, complex brittle infrastructure and changing regulatory landscape to swiftly respond to cyber threats.

Improving Resilience and recovery while adhering to compliance standards and minimizing business disruption is expensive and skill intensive.

By 2025, cybersecurity services are valued at $ 212 B USD, but the Global cybersecurity spend which includes salaries for security teams has gone up to $ 2 T USD. AI is yet to prove its worth in addressing the skill gap with the industry needed around 4 million professionals in 2023. This skill gap has been growing at 13% year on year making it difficult for enterprises to find security professionals with proficiency or expertise in cyber defense skills that are necessary to function effectively[3].

Digital immunity through Cyber Services as a software

As AI models move into production, even the most advanced standalone AI models struggle to execute multiple steps that require enterprise context and manage dependencies.

Enterprises must start using multi-agent systems which break down complex problems to smaller tasks. These tasks are handed to specialized AI agents. This multi-agent system can offer a modular, scalable, and resilient approach for taking up tasks of a security team.

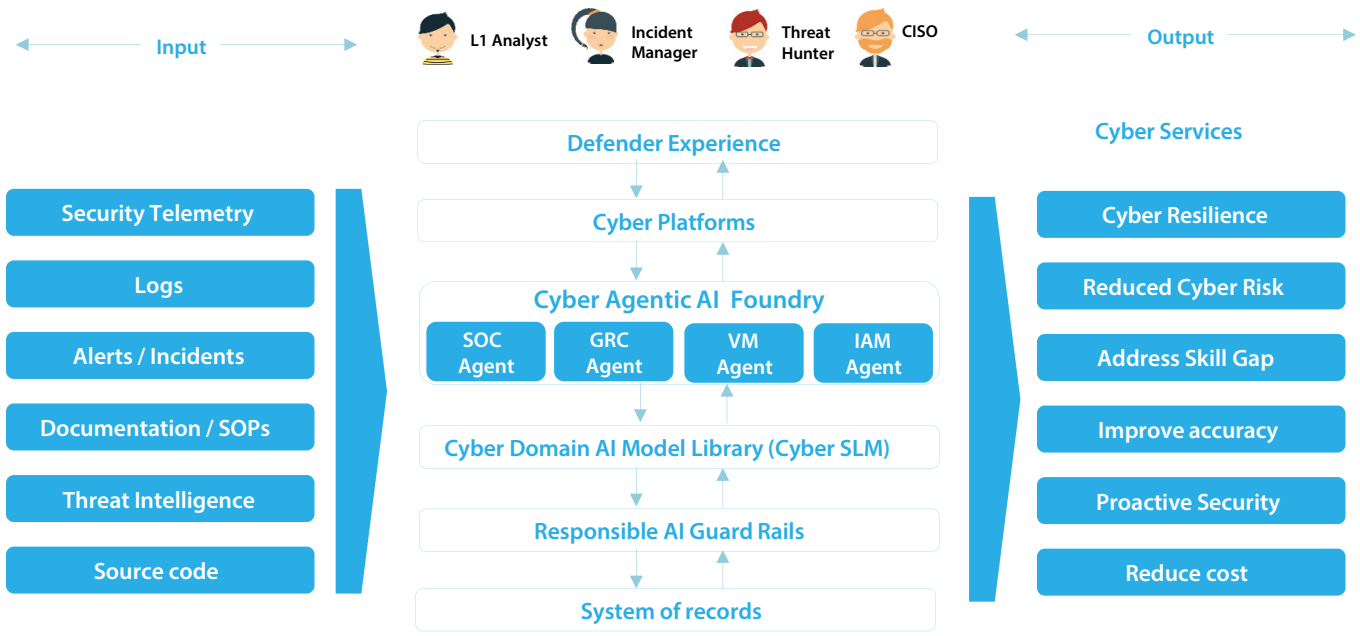


Figure 2 - Digital Immunity with Cyber Services as a Software

For instance, in Security operations, there are enterprise security platform systems and tools which enable security team members to manage alerts and incidents. The system of agents creates a decision engine to orchestrate alerts so that a swarm of agents work like a trained security team.

Shift to Cyber Services as a Software

Cybersecurity has been a never-ending race. Companies are investing in technology, and adding more systems, processes, and modern technologies to support remote work, protect sensitive customer data, and manage data across devices.

Transitioning from cyber services to managed services model powered by AI (Artificial Intelligence) will increase profitability and reduce the risk associated with services. 3 out of 4 of the enterprises are looking at using AI for Cyber defense but still have not moved to production due to the risks they see[4].

Service-as-software brings a 360-degree shift in providing people with process and technology based CyberSecurity Services. In the future Cyber Service-as-a-Software model not only delivers Cyber Services but also constantly evolves the business models of enterprises. Today's enterprises should build a journey map to power their cyber services first, then augment it through agentic AI and move towards holistic software as a service model for tomorrow.

2

Amplifying Defender Potential – Why should AI be human-centric in cybersecurity?

The paradox of Human-centric Cyber AI

Human centricity in AI agents sounds like a paradox. Cyber defense recognizes that people are both the weakest link and the strongest asset in cybersecurity. It is about designing security measures that consider human behavior, psychology, and limitations, rather than relying solely on technology.

Yuri Burda and Harri Edwards, two Open AI researchers, were trying to make LLMs perform basic arithmetic. The models memorized the sums but failed to solve new ones. They came across a surprising result while working on basic arithmetic with Large Language Models (LLMs). By accident, the researchers left the learning process for a longer time only to find this accident enabled the model to add two numbers. This phenomenon is called Grokking in deep learning, highlights a key challenge where traditional statistical intuitions often fail to predict the complex behaviors that can emerge in advanced AI models.

This can result in unfair targeting and raises ethical questions when the security team wants to use AI based User Behavior Analysis to find insider threats within enterprise.

Cost of AI and ethical concerns due to AI

Security AI Agents, while powerful, remain an inert overhead without the active involvement of human security teams. Further, the impact of AI systems in amplifying biases if they are trained on unrepresentative or prejudiced data in cybersecurity could be disastrous.

Gartner, earlier this year, published a report stating that the future of cybersecurity lies with the very people helping businesses to operate and gain revenue, its employees. In fact, the report's number one prediction is that by 2027 at least 50% of CISOs globally will formally adopt a human-centric approach[2].

Designing AI for Cyber Defense should focus on building co-intelligence of security teams with AI. When security teams see AI augmenting their cyber defense and seamlessly integrated into daily workflows rather than replacing their work, they are more likely to adhere to it.

Comprehensive human-centric framework for Cyber AI Adoption

Technical defenses alone cannot fully protect against attacks like phishing or business email compromise. Educated and aware security teams who understand the threats faced in their cyber domains are better placed to recognize AI-powered attacks and effective defense.

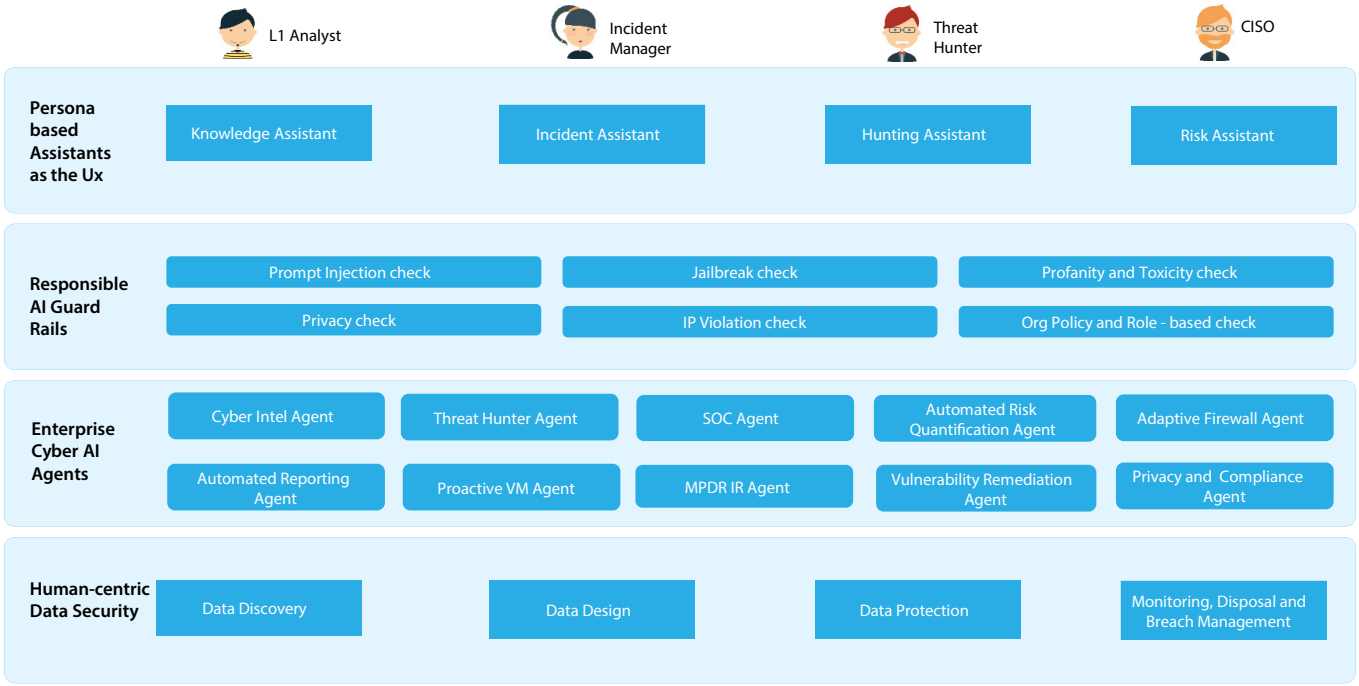


Figure 3 - Human centricity across each layer of Cyber AI

Human centricity across each layer of Cyber AI includes:

- **Personal driven Gen-AI as UX** - Human-centric Gen-AI Assistants can be created only when the intent each security team member can be understood. A Threat hunter would need a hunting assistant, but a CISO would need a more comprehensive risk assistant
- **Responsible AI Guard Rails** - AI for Cyber cannot be unhinged, but with the right guard rails which ensure the data, model and users are protected from multiple threat vectors.
- **Cyber AI Agents** - Infosys Cyber Next Agentic AI Foundry can be leveraged to build Agents or Digital workers for each CyberSecurity service needed by the enterprise.
- **Secure Data** - Critical part of AI is the data used for learning, deployment and decision making. Sensitive data must be identified, designed as per use cases, protected through encryption or obfuscation. Finally, the data should be monitored for breach and disposed after use.

Errors in AI systems are inevitable while defending against Cyber-attacks. Handling the mistakes is harder when the system's decision-making is hidden or black-boxed. Hackers can exploit this black box nature of AI models by building malicious inputs tricking AI to make incorrect cyber decisions or compromise training data so that AI can learn harmful patterns.

Human centricity as the core of Cyber AI

While the enterprise security team is taking a break, cyber agentic AI could look at peta-bytes of security telemetry and take intelligent decisions.

Cyber AI would need 3 key pillars to build trust from the security team:

1. **Predictable outcomes** - Cyber AI must give verifiable results that balance accuracy, precision, and roll back capabilities in AI-based decisions by enabling enterprise security teams to train models on their own security data such as telemetry, SOPs

2. **AI Safety** - Mitigate bias, toxicity, and harmful output by conducting bias, explainability, and robustness assessments, and red teaming to ensure the safety of the AI solutions

3. **Defender in the loop** - AI plays a supporting role to the security analyst, there should be a provision — or where human judgment is required. We need to identify the appropriate balance between the intelligence of the AI model and experience of the cyber defender

The era of Cyber AI has just started, business leaders must begin building Cyber AI use cases as soon as possible rather than waiting on the sidelines. The performance gap between laggards and early adopters will widen quickly. Adoption can improve only when security teams understand the human centricity of AI built to amplify their defender potential.

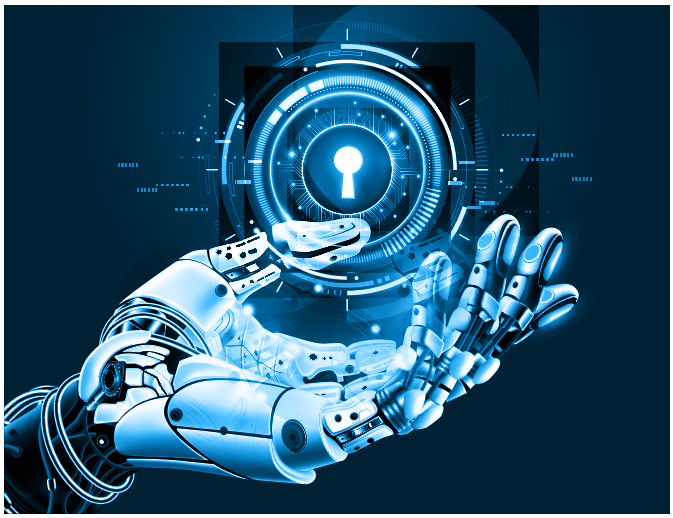
3

Redrawing the "first line of defense" – AI-first Security Operations for Enterprises

How can AI radically transform the enterprise first line of defense

Under the onslaught of AI-powered threats and ransomwares, enterprises struggle to find the right balance between detection and effective response to threats. For enterprise scale cyber defense, it is critical to build, refine and evolve security operations centers (SOC) using AI.

Heather Hoff, an operator in Diabolo Canyon nuclear plan, California, was horrified to see the meltdown of Fukushima nuclear reactor thousands of miles across the Pacific Ocean[1]. The Japanese nuclear reactors were designed to withstand earthquakes, but vulnerable to large tsunamis. The plant was designed based on scientific knowledge collected in the 1960s on historic data indicating a max limit of 3-meter-high tsunami waves. The great East Japan earthquake stuck the Fukushima region created an unprecedent fifteen meters high tsunami wave which destroyed the nuclear reactor.



This example explains the point of how standardized process can create baseline for defense, but still fail in dynamically changing situations such as the modern SOC

Pressing need for AI-powered SOC

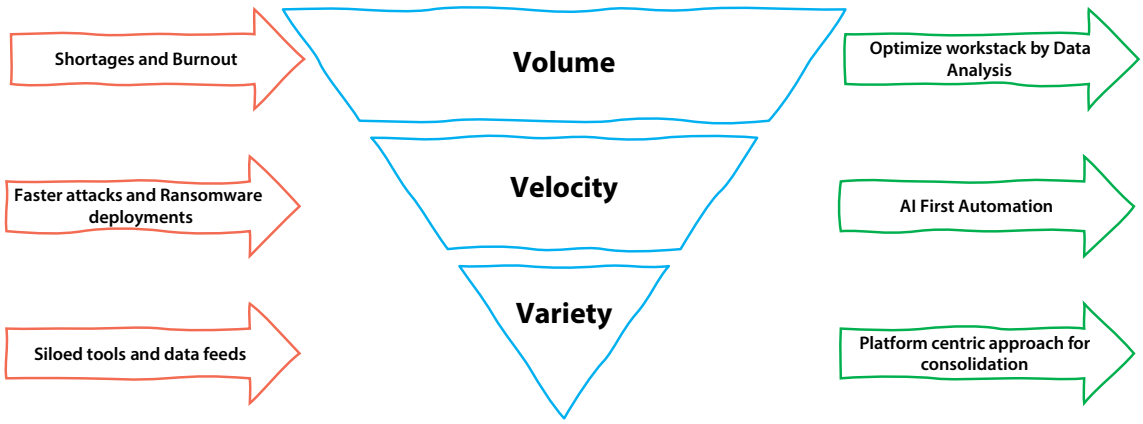


Figure 4 - The 3Vs - Volume, Velocity and Variety driving AI in SOC

- **Volume** – Today's SOC analysts face a complex challenge that contribute to high stress levels and burnout. They are overwhelmed by the high volumes of data they process, often described as finding needles in ever-growing haystacks. As per a study by Ponemon Institute, 65% of SOC Teams suffer burn out[2]. A more exhausted team with a large volume of alerts from disconnected endpoints can lead to inaccurate detection and response.

- **Velocity** – Cybercriminals equipped with Gen AI based weaponry are now deploying ransomware within 24 hrs. which used to take more than 4-5 days. Velocity of comprehension of an attack is critical for an enterprise respond and recovery with minimal impact. The pace of attacks is crucial and as a cascading business impact.

- **Variety** – Too many siloed tools and data feeds results poor threat detection outcomes and delay in incident response. Complex organization structures, such as decentralized operations and independent operations of IT and cybersecurity teams, further widen the gap for the SOC operations. For instance, the Log4j vulnerability created a global impact due to Enterprises and end users alike did not realize how widespread this issue within complex IT landscape[3].

Future of SOC by Agentic AI Foundry

The AI-First SOC[4] is prioritizing organization design change, use cases and AI technology radically changing their security operations.

1. **Assist** – Cyber Assistance for persona of the Security Team
2. **Sustain** – Improved operational efficiency through Agentic AI
3. **Explain** – Nonhuman experts in Cyber defense
4. **Amplify** – Amplifying defender potential
5. **Decode** – Demystifying the unknown-unknown threats

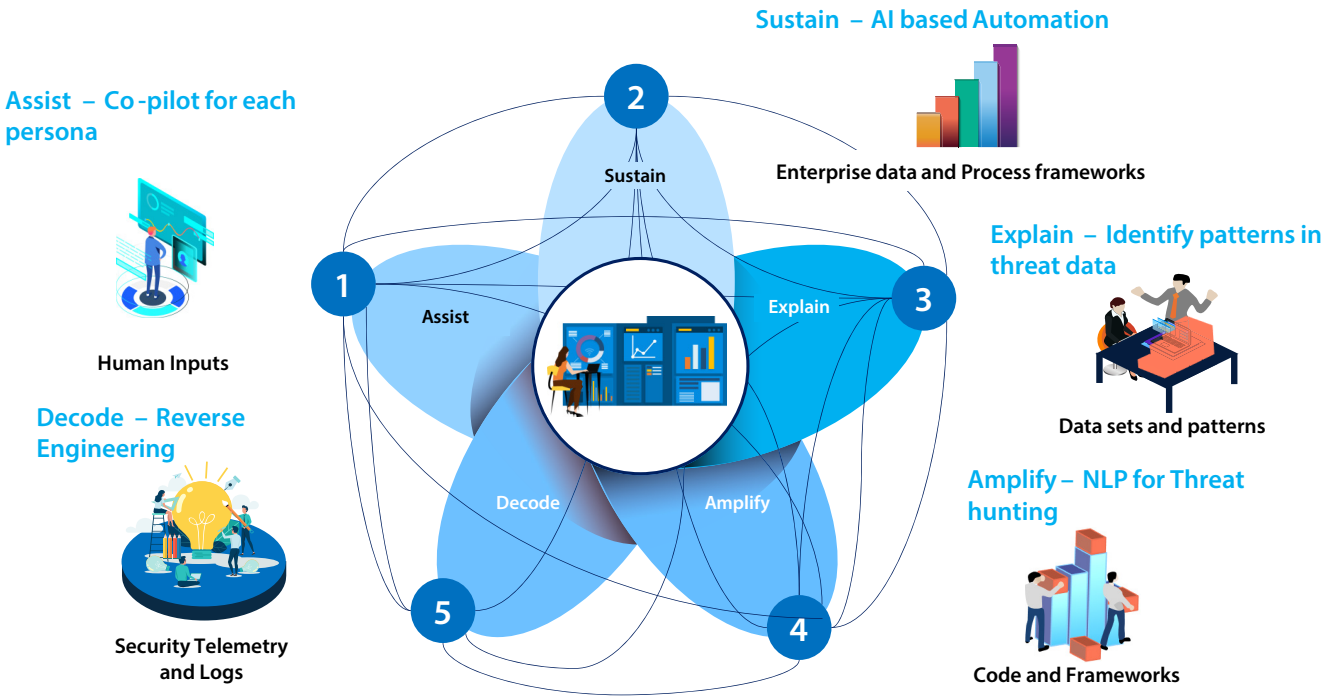


Figure 5 - Value add from AI

Balancing Automation, AI and the Analyst

The future of SOC is one of the biggest issues faced by enterprises today. AI, big data analytics, and advanced automation are enabling algorithms to perform cyber defense tasks that traditionally require human intervention. The opinion on AI is split between AI elimination of security team members or they foresee the augmentation of intelligent threat detection capabilities.

While the future capabilities of AI are unknown, one scenario might be the integration of AI in SOCs moving toward greater automation and even "self-healing" SOC through Agentic AI. Enterprises like IBM have been building agentic AI system which can orchestrate multiple agents to interact and collaborate with each other[5]. This system works across the threat life cycle to solve the low-risk scenarios freeing up bandwidth for the human analyst to focus on high-risk threats.

This future state could include automated remediation of more incidents without human intervention. Ultimately, the SOC must evolve into an AI-powered orchestration layer that spans IT, security, and compliance functions.

4

Infosys Cyber Next Topaz Fabric for Cyber Resilient Organizations

Amplifying Defender Potential through Cyber Next Topaz Fabric

Cyber criminals and attackers use advance AI-powered attacks, therefore we need to defend faster and more effectively using AI. Humankind has always had a fascination for machine intelligence-based defenders in armies fighting our wars. Starting from 1980 Robo Cop to J.A.R.V.I.S (Just A Rather Very Intelligent System) from 2008 Iron man movie, we have seen the AI defenders fighting villains[1] [2].

Agentic AI aims to build autonomous intelligent systems which are capable of planning, reasoning, and executing complex tasks. Agentic AI is ripe for enterprise adoption. For cybersecurity, AI agents which autonomously monitor events, understand the impact, make decisions, and take real world actions have the potential to change the core of enterprise security.

The Agentic AI agents managing cybersecurity threats in real-time, to generative AI agents generating hyper-personalized cyber awareness campaigns, must be human-centric and scaled through an enterprise platform like Cyber Next with the right ethical and security guardrails.

Agentic AI is not only a technical advancement, but a true change in thinking that will have profound effects on how enterprises will equip their security teams. By providing agents to amplify their capability to defend against constant attacks and evolving threats. Infosys has developed Cyber Next Topaz Fabric[3], which offers a collection of over 100+ AI agents that can be designed, built, tested, integrated, and deployed at scale.

Enterprise challenges addressed by adopting Cyber AI Agents

Gen AI models focused on generating text or summarizing interactions. Agentic AI introduces an innovative approach where AI systems interact with IT systems through various tools. Agentic AI is not risk free in a cybersecurity world. Imagine an AI agent that can predict the best course of action in security operations and execute it freeing up bandwidth of security teams.

But at the same time, Agents can work on unstructured workflow patterns across brittle integrations and data siloes without understanding the impact on the risk posture of the enterprise.

Scaling Agentic AI Cyber Next through Infosys Topaz Fabric

As we see the demand increasing with enterprises for AI for CyberSecurity we have designed Cyber Next Topaz Fabric as a catalog of Digital AI Workers. The AI Agent learns to execute the repeatable actions created from the tasks of security team members. For instance, Cyber Next MSSP SOC Agent helps with automate decision-making, streamline workflows, perform alert triage, pick the right automation playbook and incident response.

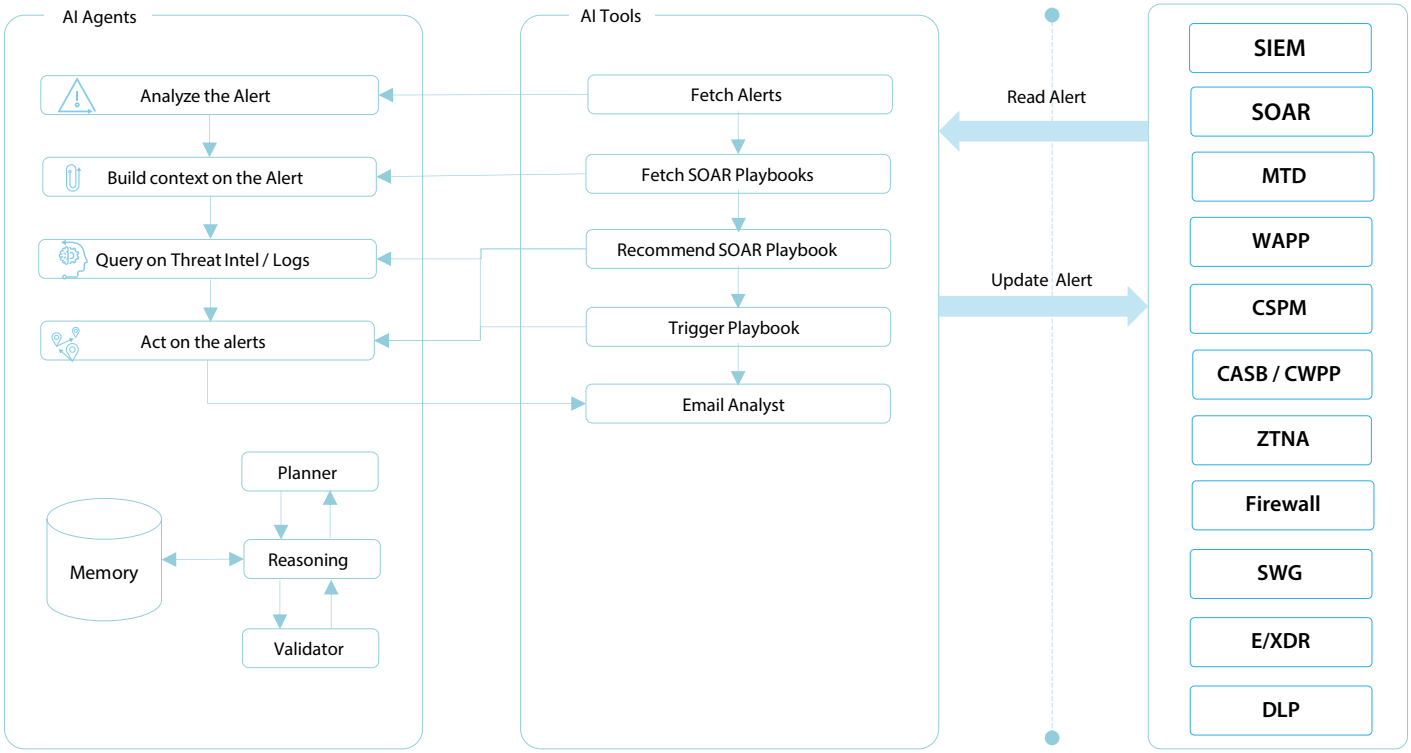


Figure 6 - Inner working of a Cyber AI Agent

Gartner predicts by 2028, 33% of enterprise software applications will include agentic AI, up from less than 1% in 2024, enabling 15% of day-to-day work decisions to be made autonomously[4].

As no one technique is a silver bullet, agentic AI will continue to improve security measures through evolving defense techniques. Enterprises with the first mover advantage on Agentic AI for cybersecurity will become proficient and use it for better business outcomes, improving resilience and reducing the cost of security operations through scalable platforms.

Building Cyber Resilience through Topaz Fabric

Infosys is a pioneer in building Cyber Platforms – Cyber Next[5], building Gen-AI Cyber Advisor and building our own Cyber domain centric Small Language Model (SLM). Agentic AI stage of evolution of Cyber Next as the centralized automation platform to scale and deploy 100+ agents from the Agentic AI Foundry.

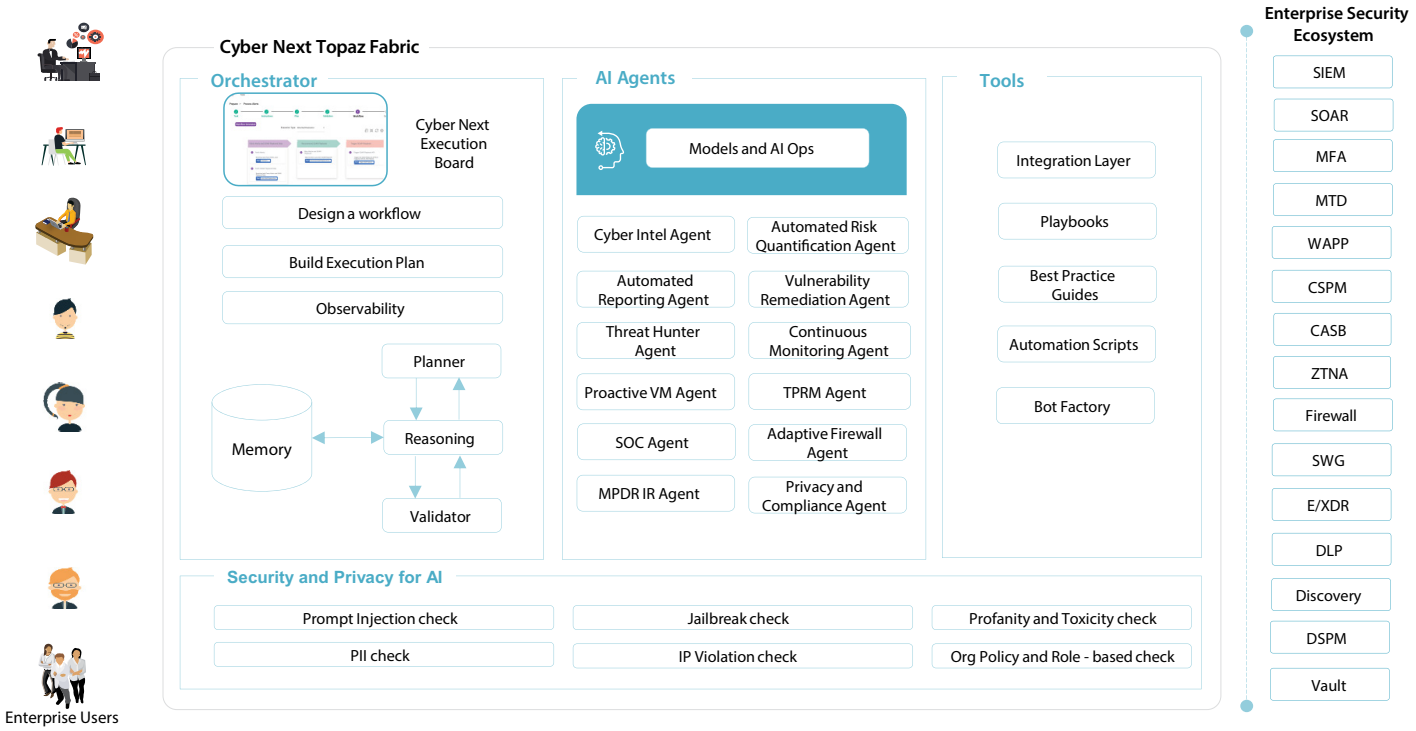


Figure 7 - Enterprise Architecture view of Cyber Next powered by Topaz Fabric

Infosys recommends adoption of Cyber Next powered by Topaz Fabric[4] which aims to align Cyber defenses across automation and AI, two technologies that, when strategically integrated, can revolutionize cyber defense efficiency and effectiveness.

With budgets tightening and security talent difficult to find, a growing number of organizations are taking a close look at Cybersecurity as a Service (CSaaS) – an outsourced model of managing cyber risk on a pay-as-you-go basis. Cyber Next powered by Topaz Fabric is the first step in building AI capabilities to improve the productivity of security teams and scale operations. Enterprises trying to build agentic AI cyber defenders should keep in mind that AI is currently more of an accelerant to existing defense techniques to amplify the defender potential.

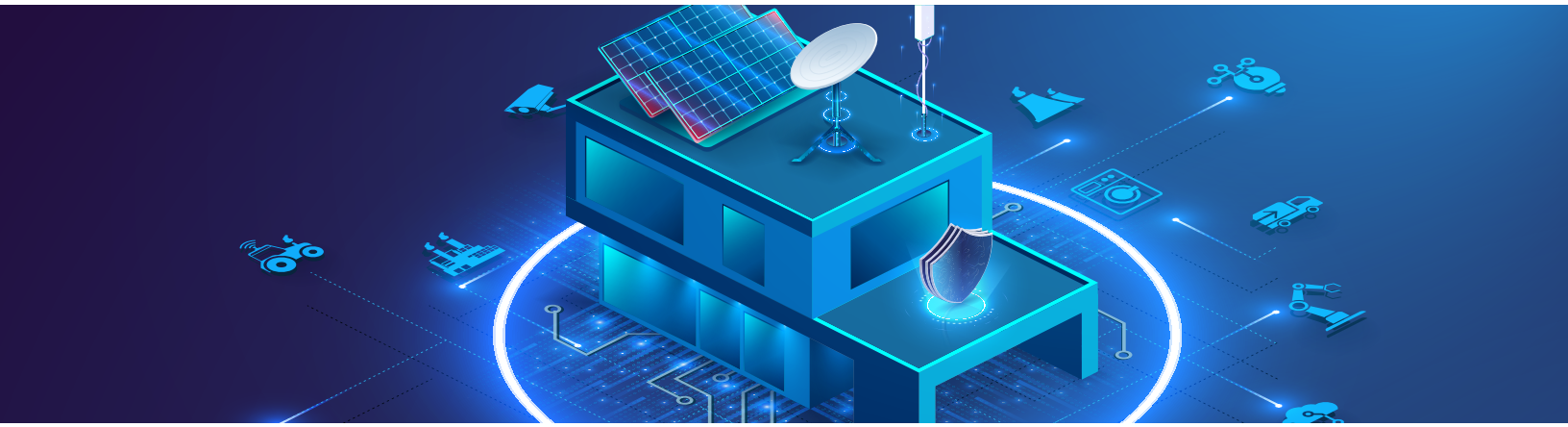
5

Physical Security through AI – Bridging Security Gap

Crossing the virtual barrier and getting into the Physical world

Physical security involves safeguarding assets, facilities, personnel, and information from threats like theft, vandalism, and sabotage through measures such as guards, access controls, and surveillance. It ensures authorized access, business continuity, legal compliance, and protects organizational reputation. This industry is undergoing a major transformation as artificial intelligence (AI) becomes an integral part of surveillance, access control, and threat detection systems. AI-driven security solutions are enhancing the effectiveness of security personnel, improving response times, and reducing operational costs.

In 2001's Minority Report, a science fiction adventure set in 2054, Tom Cruise's John Anderton thwarts iris detection protocols by means of eyeball transplants. Hollywood has long been ahead of the game in both depicting futuristic uses of technology in Physical security[1].



Today, enterprises fight against deepfakes. To defend against these attacks, AI is used to detect subtle alterations made to pictures and videos and employ techniques such as Photoplethysmography (PPG), which measures blood flow per unit of time in an artery to identify AI-generated images or videos[2].

Real world challenges in Security

The primary challenge faced by physical security lies in the fragmented utilization of AI. Analyzing VMS camera feeds, although valuable, offers very limited scope when compared to other sectors harnessing AI for comprehensive data analysis and predictive modeling.

The complexity in using AI for Physical security comes due to the lack of holistic security data aggregation and analysis. The broader application of AI involves amalgamating data from various sources such as guard patrols, incident reports, maintenance logs, compliance documentation, alarm systems, architectural layouts, and asset databases into a unified platform. By harnessing AI algorithms, this aggregated data can be standardized, analyzed, and transformed into actionable insights.

The adoption of Agentic AI must accelerate the interconnections to the real world. The integration of AI into the physical security industry is expected to grow. Market analysts predict that investments in AI-driven security solutions will continue to rise as businesses, government agencies, and critical infrastructure providers seek more efficient ways to protect assets and people.

Zero Trust Physical Security using AI

With attackers now able to replicate a person's voice from just three seconds of audio, and AI face swap video technology becoming increasingly accessible through rising adoption of large language models, stakes are higher than ever. This is especially concerning when attackers can easily build a detailed profile of their target through social media information and exploit potential vulnerabilities.

Identity	• Secure NHI (Non-human identities) and validate authentic users • Least privilege access and analyze human digital, physical and cognitive behavior
Devices	• AI-powered device discovery, threat detection • Agentic AI automated patch governance
Network	• AI based network monitoring and check for machine generated content • Develop a clear response plans for micro segmentation and elimination
Apps	• Continuous Threat Exposure Management for Application security • Clear incident response, communication strategy and legal audits for apps
Data	• Anonymized synthetic for training and fine tuning of AI for Cyber Defense • AI based observability and data governance

Future advancements in AI will also lead to more sophisticated autonomous security solutions, including AI-powered facial recognition gates for seamless access control, smart city surveillance integrations, and advanced threat prediction models that adapt in real time.

Future of physical security in the digital realm...

Enterprises are investing in AI-powered security solutions are not only improving their defenses but also setting the foundation for a future where security is more proactive, adaptive, and intelligent than ever before.

More than 1,400 security experts recently warned the World Economic Forum that technologies like Information and Disinformation through deepfakes which work in the physical realm pose risks which are more catastrophic than inflation, extreme weather, and even war[3].

AI is reshaping the physical security landscape by providing smarter, faster, and more accurate security solutions. From advanced video analytics to predictive threat detection, biometric authentication, and AI-driven robotics, the industry is embracing a new era of security innovation.

6

Scaling AI through a Platform centric approach

Platform-centric Mindset to Get Ahead of the Attacker

Cybersecurity has been a never-ending race. Companies are investing in technology, adding more systems and processes, and leveraging modern technologies to support remote work, protect sensitive customer data, and manage data across devices. Adversaries and threat actors have evolved the cyber-crime marketplace, which affects today's business world.

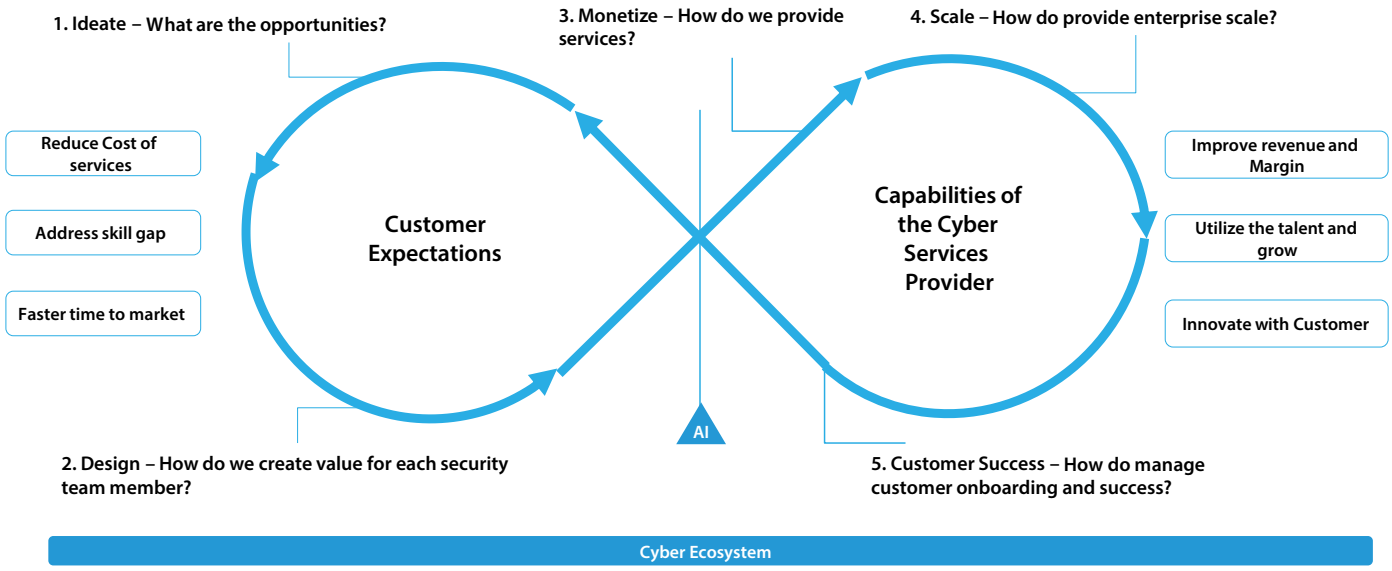


Figure 9 - Platform brings a balance between Enterprise Expectation and Cyber Service Provider capabilities through AI

For instance, as per United Nations, there are crime enterprises like ShadowCrew, which is an international organization with nearly 4000 team members involved in enterprise scale theft of personal information[1].

Enterprises need a unified and integrated suite of security tools and capabilities. This platform approach helps enterprises move away from disconnected point solutions to an interconnected security ecosystem which can provide security posture, detect threats, respond to incidents, and ensure compliance, typically from a centralized platform like Infosys Cyber Next.

While the convergence of information and communication technologies in the 1990s resulted in a short-lived fascination with business models, forces such as deregulation, technological change, globalization, and sustainability have rekindled interest in the concept today.

Challenges faced by our Enterprise customers

The trend of "platformization" continuous to steam roll across the industry, as enterprises need to consider factors such as breadth and depth of integration, alignment to the business needs and economics of training security teams to effectively use this unified platform.

Gartner found out 75% of the enterprises were pursuing a security vendor consolidation and in 2024, launched a Platform consolidation framework to reduce complexity, overlap and blind spots that come from using multiple cybersecurity vendors and tools[2].

In the era of Gen AI-powered threat actors, platforms can cause vendor-lock in, adoption of one platform can cause slowdown in innovation in cutting-edge solutions and cost of integration with their IT landscape.

Cyber Next - Resilience@Core | Platform Driven | AI-powered

1. **Cyber Resilience at core of your enterprise security operations** - Even the most secure enterprises suffer an incident as the attacker needs only one exploitable weakness to breach defenses. Cyber resilience combines cyber security with the ability to detect, respond to and recover from cyber incidents. Infosys believes in providing Cyber Next to build cyber resilience taking in a defense in-depth approach

2. **Scale Managed Services through Platform centric approach** - Unifying multiple solutions into a single platform helps in eliminating the security coverage gaps that naturally occur when multiple point solutions are deployed to solve specific problems. Cyber Next helps with native platform integrations that make each component even stronger and aims to build a 360-degree security posture

3. **AI as a force multiplier** - Cyber Next provided Gen-AI based Cyber Advisor and a Cyber Next Agentic AI Foundry to scale Digital AI Worker across each Cyber Security Domain such as Cloud Security, Identity and Access Management, Vulnerability Management, Data Protection, and Infrastructure Management

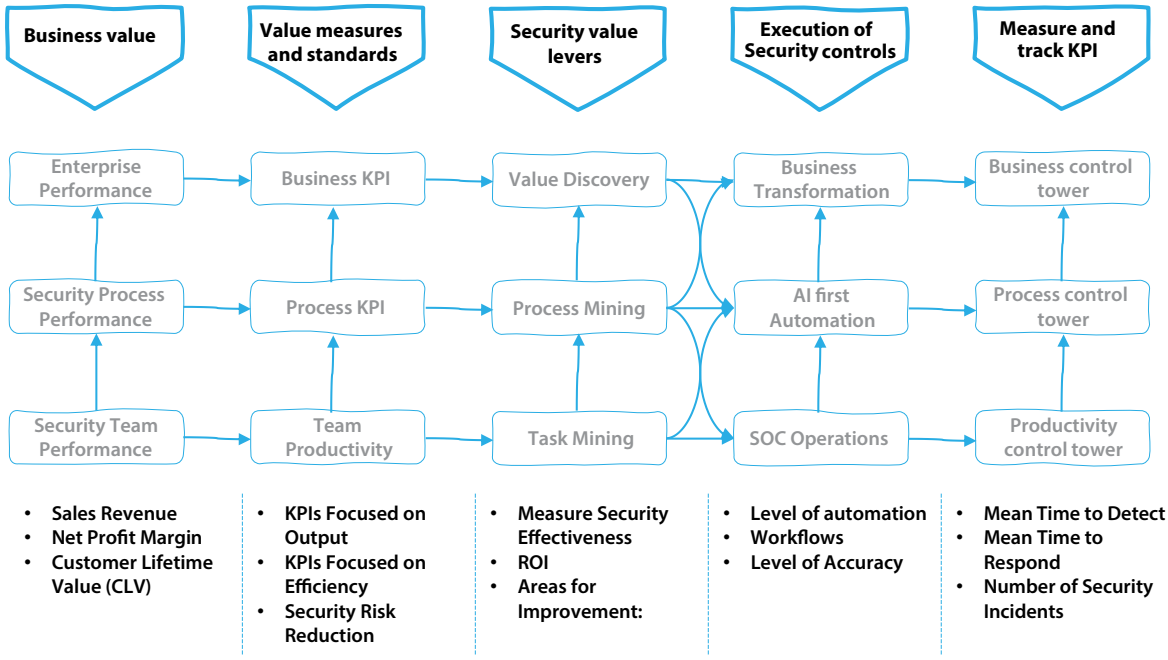


Figure 10 - Business value metrics of Cyber Platform

Enhancing value through a unified Cyber Platform...

Infosys Cyber Next provides a unified cybersecurity solution, eliminating the need for enterprises to invest in multiple security technologies and specialist skills to quickly achieve security maturity. It provides security as-a-service in a single package that combines pre-selected and pre-integrated ready-to-use security technologies that are homegrown or from our partners.

As per Forbes, the cybersecurity market has always been characterized by cycles of consolidation and diversification. In the last decade, McAfee, IBM and Symantec were the Cyber giants who dominated the industry and promised a consolidated cyber platform[3]. After rapid adoption, enterprises found this one-size fit does not work. Post a few years of specialization of cyber domains, we are seeing a second cycle of Cloud and AI platform consolidation through Palo Alto, CrowdStrike, Zscaler and Microsoft.

Platform-centric cybersecurity offerings provide a more effective and efficient way to manage cybersecurity in today's complex threat landscape. By consolidating security functions, unifying data, analytics, and automating security tasks, these platforms help organizations improve their security posture and reduce their risk of cyberattacks.

7

Fly wheel of Innovation for Cyber AI

Network effect of the AI Factory

AI-powered threats are not going to slow down. Rather, they will continue to accelerate and create an endless expansion of the attack surface affecting business outcomes, disrupting operating models, and eroding shareholder value. The good news is, symbiotic relationship between AI and cybersecurity is accelerating, driven by the need for robust defenses against increasingly sophisticated attacks. Gartner has predicted a 15% increase in security spending due to the adoption of AI and Gen-AI[1].

A struggling actor gets a call from a casting agent. The Agent asks the actor to prepare for the role by staying awake for the next 24 hours. The actor agrees reluctantly, and on the day of the shooting, he arrives sleep deprived, tired and watery eyes. After a brief introduction, he walks onto the set for his big moment in the limelight: The cameras roll, and he promptly falls asleep in a prop car — just as he had been instructed. This is hardly the actor's big break. The actor was asked to simulate a situation where risk can threaten safety behind the wheel[2].

There is a shift to use AI for proactive and predictive stance rather than detecting known threats. This fundamental shift in cybersecurity needs the adoption of a fly wheel for continuous innovation where AI can detect AI-Generated attacks and Cyber Defense AI models which must learn and adapt rapidly to new adversarial techniques.

Unseen challenges in the path ahead

As per NVIDIA, ultimate vision is to move from traditional datacenters to AI factories - self-contained, ultra-high-performance computing environments designed to generate AI intelligence at scale. The inputs to these modern factories are electricity and data. The outputs are tokens – the atomic units of prediction, reasoning, and generation that power AI systems. The new unit of productivity is 'tokens per second per watt' – a measure not only of how fast chips are, but of how efficiently intelligence can be produced at enterprise scale[3].

Enterprises will face implementation challenges including privacy, mitigating algorithmic bias, difficulty in protecting AI models from adversarial attacks, managing high initial costs, the need for engineering skills, and compliance to changing AI regulations. Further multimodal AI for cybersecurity would need to work on multiple types of data such as text, video, speech, 3D, and real-time sensors logs.

Many enterprises know they need to adopt AI but lack the internal tooling or expertise to move quickly.

Startups that help them get from "AI strategy" to "AI in production" – whether through observability, orchestration, cost optimization, or governance – can create immediate value.

Reshaping Cyber Defense through Cycles of Creativity

AI for Cyber Defense requires a holistic innovation model, as its dynamic system of multiple agents weave together multiple facets of human experience: ecology, ethics, culture, life, technology, and society. Cyber AI innovation can be visualized through the Krebs Cycle of Creativity (KCC), the sequence of reactions by which organisms generate energy. The KCC is a visual artifact from the work of Neri Oxman from MIT's Media Lab. The KCC focuses on the four modalities of human creativity—Science, Engineering, Design and Art[4].

We can map the KCC to understand how Cyber AI will evolve where the constant movement of use cases from one modality to another. The input for one modality becomes the output for another.

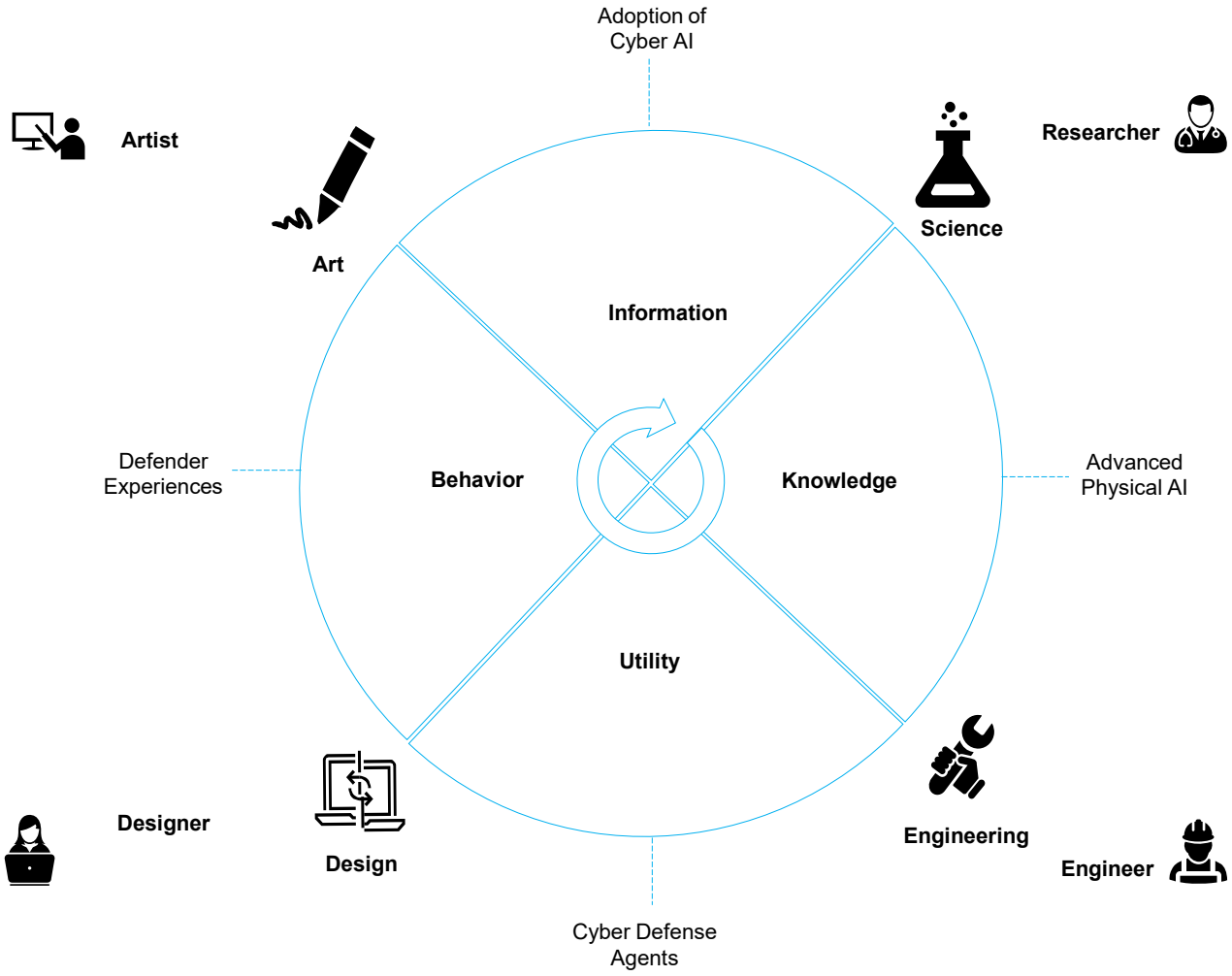


Figure 11 - Applying Krebs Cycle of Creativity to Cyber AI

The flow of information across each modality exerts a major influence on the future of innovation in cybersecurity. For instance, in Cyber AI, science converts information into knowledge for advancement of Physical AI. This needs Engineering capabilities to be designed for effective Cyber Defense Agents. Good Design enables us to create effective Defender Experience. Art takes that context, and influences the security culture, and improves Cyber AI Adoption in the real world.

A peek into the Future…

The rise in test-time computing enables Cyber AI to offer well-reasoned, helpful, and more accurate responses to complex threats. These capabilities will be critical for the detailed, multistep reasoning tasks expected of autonomous agentic AI and physical AI applications. This will boost efficiency and productivity by providing security teams with highly capable AI assistants to build defense against threats at an accelerated speed.

AI tools act as force multiplier in cybersecurity, simplifying complex tasks, providing context-rich insights, and allowing human experts to focus on higher-level strategic analysis and complex threat investigation. Though we have no crystal orb/cystal ball to predict the future, we can map the evolution of Cyber AI use cases across each phase of evolution of AI. This is derived on the keynote by Jensen Huang, NVIDIA CEO in GTC 2025[5].

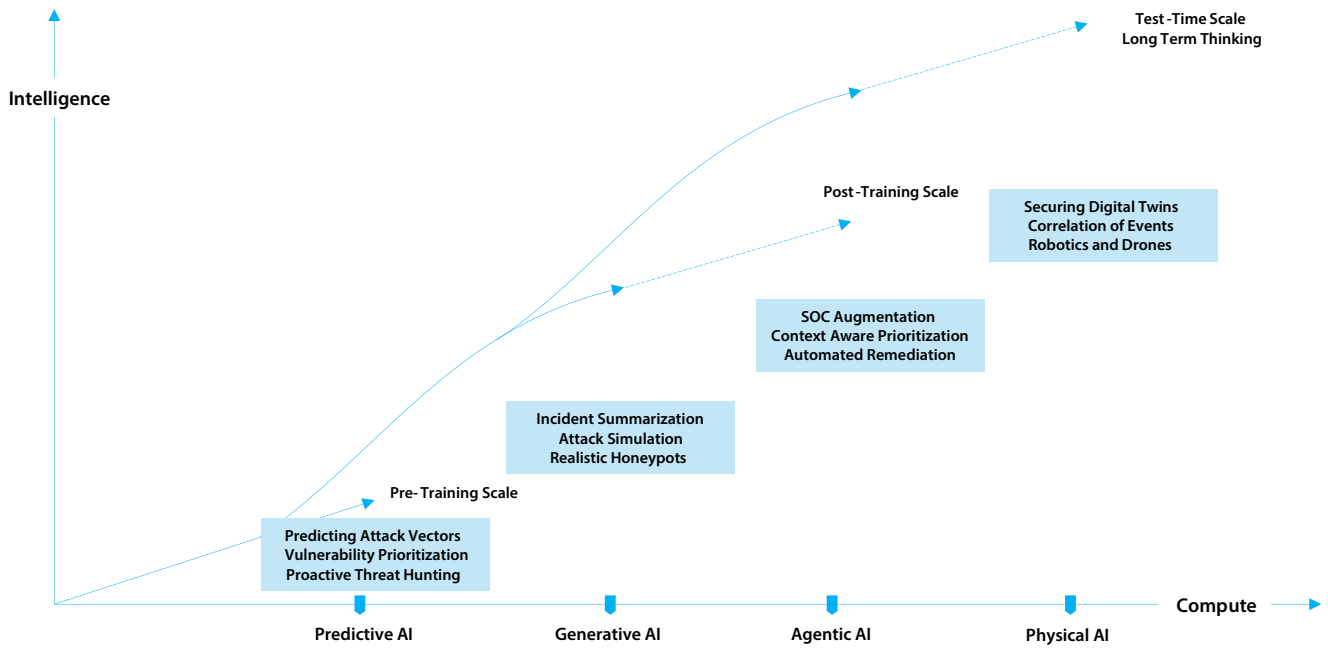


Figure 12 - Future of Cyber AI – Replacement of Traditional AI with AI Factories

The future of Cyber AI is bright with Physical AI based robotic defenders in the real world crossing the virtual environments barrier, enhanced by reinforcement learning, to secure real world assets building value for both enterprises and consumers.

References and Further Reading

Chapter 1

1. Gartner, Stamford Connections, Gartner Forecasts Global Information Security Spending to Grow 15% in 2025, August 28, 2024
2. How the Economy, Skill Gap and Artificial Intelligence are challenging the Global Cyber Security workforce, ISC2, 2023
3. Security And Privacy Concerns Are the Biggest Barriers To Adopting Generative AI, Jeff Pollard with Joseph Blankenship, Zachary Dallas, December 5, 2023

Chapter 2

1. Grokking: Generalization Beyond Overfitting on Small Algorithmic Datasets, Alethea Power, Yuri Burda, Harri Edwards, Igor Babuschkin, Vedant Misra, January 6, 2022
2. Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024, Gartner Security & Risk Management Summit, March 28, 2023

Chapter 3

1. Working in the Diablo Canyon reactor control room turned this mom into a nuclear advocate, Catherine Clifford, June 7, 2022
2. Ponemon Institute and Devo Technology Study Reveals 65% of Cybersecurity Analysts Consider Quitting Due to Burnout, Lack of Visibility, July 29, 2019
3. Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability, Microsoft Threat Intelligence, December 11, 2021
4. How will AI-First SOC Change Cyber Security? Infosys Whitepaper, Karthik Nagarajan, 2024
5. Autonomous Threat Operations Machine (ATOM), IBM, 2025

Chapter 4

1. Robo Cop, Movie, 1987
2. J.A.R.V.I.S., Fictional Marvel Character
3. Infosys Topaz Fabric – A Composable Stack of AI Agents, Services, and Models
4. Intelligent Agents in AI Really Can Work Alone. Here's How., Gartner Report, Tom Coshow, October 1, 2024
5. Infosys Cyber Next – Platform powered Services

Chapter 5

1. Minority Report, Movie, 2001
2. How to secure your business against deepfakes: The role of AI and zero trust, Karthik Nagarajan, Harry Keir Hughes, Kate Bevan, July 10, 2024
3. Global Risks Report 2024, Insight Report, World Economic Forum

Chapter 6

1. Cyber organized crime activities, United Nations Report, Sharing Electronic resources and Laws on Crime
2. Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022, September 13, 2022
3. The Potential Pitfalls of Cybersecurity Platformization, Tony Bradley, August 5, 2024

Chapter 7

1. Gartner Forecasts Global Information Security Spending to Grow 15% in 2025, Gartner, STAMFORD, Conn, August 28, 2024
2. AI Needs Synthetic Data To Build A Real Future, Rowan Curran, September 7, 2022
3. AI Factories Are Redefining Data Centers and Enabling the Next Era of AI, Dion Harris, March 18, 2025
4. Neri Oxman's Krebs Cycle of Creativity, MIT Spectrum, January 2016
5. NVIDIA GTC Keynote, Jensen Huang, NVIDIA CEO, 2025

Figures

About the Author

Karthik Nagarajan is a Senior Industry Principal at Infosys with over 19 years of expertise in Artificial Intelligence, data protection, and customer experience strategy.

Karthik is responsible for Infosys Cyber AI, Cyber Next Platform and Data Protection for enterprise clients.

He holds a Master of Business Administration degree from the Faculty of Management Studies (FMS), Delhi, and a Bachelor of Technology degree in Instrumentation from the Madras Institute of Technology.
https://www.linkedin.com/in/karthikanagarajan/

For more information, contact askus@infosys.com

Infosys®
Navigate your next