Digital-trust. Assured.

Infosys® | CyberSecurity

INFOSYS PLAYBOOK: AI-FIRST CYBERSECURITY FOR ENTERPRISES

Abstract

This playbook focuses on amplifying human potential through enhanced cyber role specialization, improved decision-making, and accelerated productivity by implementing AI-First cybersecurity design, scale, and controls.

Contents

Figures

Introduction - AI as an enabler of Cyber Defense

Cybersecurity has been a never-ending race. Companies are investing in technology and adding more systems and processes to support remote work, protect sensitive customer data, and manage data across devices. These systems, processes, and technologies help in adding better value and improving insights. However, these advanced technologies also empower the threat actors to build sophisticated cyber-crime, affecting today's business world. Artificial Inteligence (AI) has surfaced as the latest market trend, serving to strengthen initiatives in both cyber defense and cyber-crime realms. While at one hand, AI can be used to increase profitability and reduce the risk associated with organized crime; on the other hand AI-driven operations are susceptible to various types of cybercrimes including botnets, Distributed Denial of Service attacks (DDoS), credit card frauds, malware, spam, and phishing attacks.

AI is an essential tool to fight and protect against cyber threats. Forbes estimates 3 out of 4 enterprises across the globe have prioritized AI and machine learning in their IT budgets for cyber defense. This trend is driven by increasing volume of data across enterprises, which needs to be discovered, analyzed, and secured from cyber threats.

Generative AI (Gen-AI), the latest version of AI again serves as a business enabler, as well as a disruptor. It can create and spread large amount of false information, endangering both national and global security. Alternatively, it can also be used to detect and monitor misinformation. It has brought new problems by empowering users to deploy cyber-attacks and malicious content without traditional coding skills. As per the research by Darktrace, social engineering attacks have increased by 135% post the widespread usage of ChatGPT[1]. For instance, WormGPT built on open source LLM GPT-J and trained malware related data can create scam emails in multiple languages. The rapid rise in cybercrime due to AI makes it difficult for enterprises to combat sophisticated cyber-attacks.

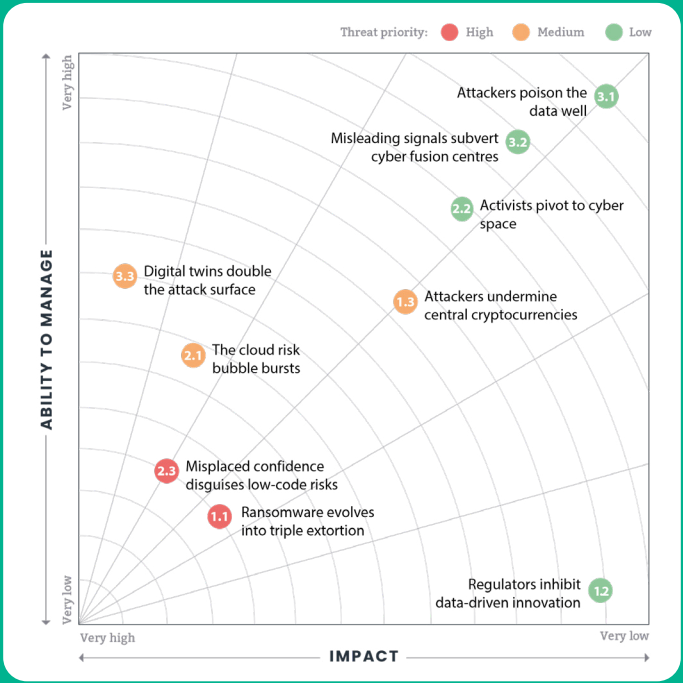


Figure 1- High Impact Attacks - Threat Landscape

Due to shortfall of automated defenses, enterprises are experiencing high impact attacks. They require assistance in automating processes to increase visibility, productivity, network communications and detection time.

Reference: Derived from ISF Threat model

This playbook defines Infosys' AI-First Cybersecurity strategy for its enterprise customers. It illustrates design principles, reference architecture and outcome-based implementation approach for enterprises aiming to take proactive steps by active adoption of AI for Cyber Defense.

Mega trends driving the industry – What should today's enterprises look out for?

AI for Cybersecurity can help enterprises take a proactive, forward-looking mindset to address and mitigate the disruptions in the future. We can expect three major cybersecurity trends that cuts across multiple industries and domains posing serious challenges to enterprises.

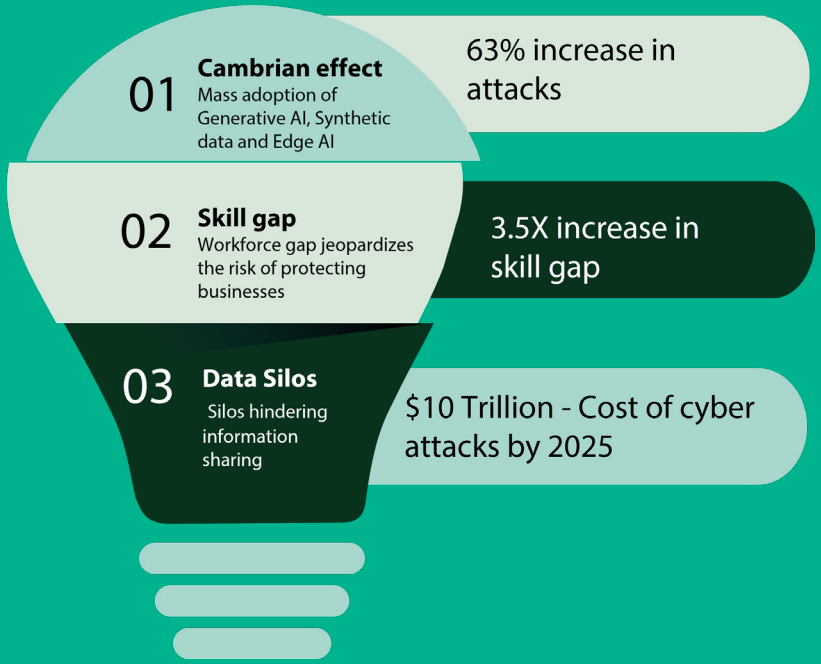


Figure 2 - Mega trends driving the industry

1. **The Cambrian effect of AI-powered cyber-attacks** - Generative AI, synthetic data and edge AI have been adopted universally and are at the peak of inflated expectations as per Gartner Hype Cycle. This increases the effectiveness of threat actors. An increased adoption of co-pilots has shifted the power of Gen-AI to end users. There are multiple concerns and misuse of Gen-AI around social engineering like creating realistic phishing emails, scaling malicious chatbots and upskilling less experienced hackers to become more effective with their attacks. 63% of the CFOs in large organizations anticipate a rise in cyber threats[2].
2. **Skill gap outpacing cybersecurity** - Improving resilience and recovery skills while adhering to cyber and privacy regulations is costly and intricate. The gaps in cybersecurity workforce puts the business at risk when it comes to safeguarding against potential threats. Adoption of AI can fill the increasing cybersecurity skill gap which has multiplied by 3.5 times in 8 years[3].

3. **Data silos within organizations** - According to a McKinsey survey, it is estimated that by 2025, cyber-attacks will cost the world over $10 trillion (about $31,000 per person in the US)[3]. Security teams and enterprises face numerous challenges including sophisticated cyber-attacks, increasing attack areas, data overload and complex infrastructure which weaken their ability to protect data, control user access and swiftly respond to cyber threats.

Beyond the Horizon: AI for Cyber Defense – Infosys design principles, reference architecture and outcome driven approach

Digital disruption is inevitable and prompts swift technology-driven changes. Despite enterprises making large-scale investments in cybersecurity, the most successful security system is still under progress. The dynamic nature of attacks, industrialization of cyber-crime and emergence of new threat vectors require enterprises to build proactive guardrails, which are beyond the horizon of cyber defense capabilities. Enterprises should embrace AI as an enabler to learn, build operational efficiency and create business value.

To ensure effective next gen AI is implemented in the cybersecurity strategy, companies need to invest in models that can draw insights from business' data rather than investing in security teams which work in isolation. Based on insights gained from our customers, Infosys advocates three design principles for adoption of AI in cyber defense:

1. **Secure by Design** - AI investments must prioritize holistic enterprise security as the guiding principle. The development, deployment, and usage of AI for Cybersecurity should actively involve all the AI stakeholders, including security team members, SOC (Security Operations Center) analysts, threat hunters, privacy experts, users, developers, vendors, and business leaders. A robust AI for cyber defense should be inclusive, welcoming inputs from individuals with varying skills and roles, security vendors, and the open-source community. This promotes healthy competition among solution providers and makes the technology more user friendly, resulting in widespread adoption across the enterprise.

2. **Secure by Scale** - AI implementations for security should be adaptable for scaling, whether up or down, based on its usage. Enterprises should create an environment that would enable the growth of cloud, analytics, IoT and other related technologies to support AI models. They should also enable development for better security experiences, operating models, and responsible AI.
3. **Secure the Future** - A new AI investment for security should keep up with rapid technological developments. Establishing a robust governing principle ensures that future AI developments are transparent and inter-connected throughout the enterprise. Additionally, like any other AI platform, the applied AI use cases should be built on a modular platform, thereby enabling developers to re-structure the models and provide training for emerging threats and new actors.

The three pillars for security, their associated principles, and a strong cyber defense platform can ensure that AI is suitably applied for cybersecurity. Powered by **Infosys Cyber Next platform** and partner products, Infosysintends to ensure the AI developments are agile, and ready to accommodate future technology upgrades within each domain of cybersecurity such as Identity and Access, Application Vulnerability, Infrastructure, Data, Cloud, Governance Risk & Compliance and Managed Services. This high-level logical view is composed of blocks that can be built using a phased strategy aligned with Infosys LIVE enterprise strategy.

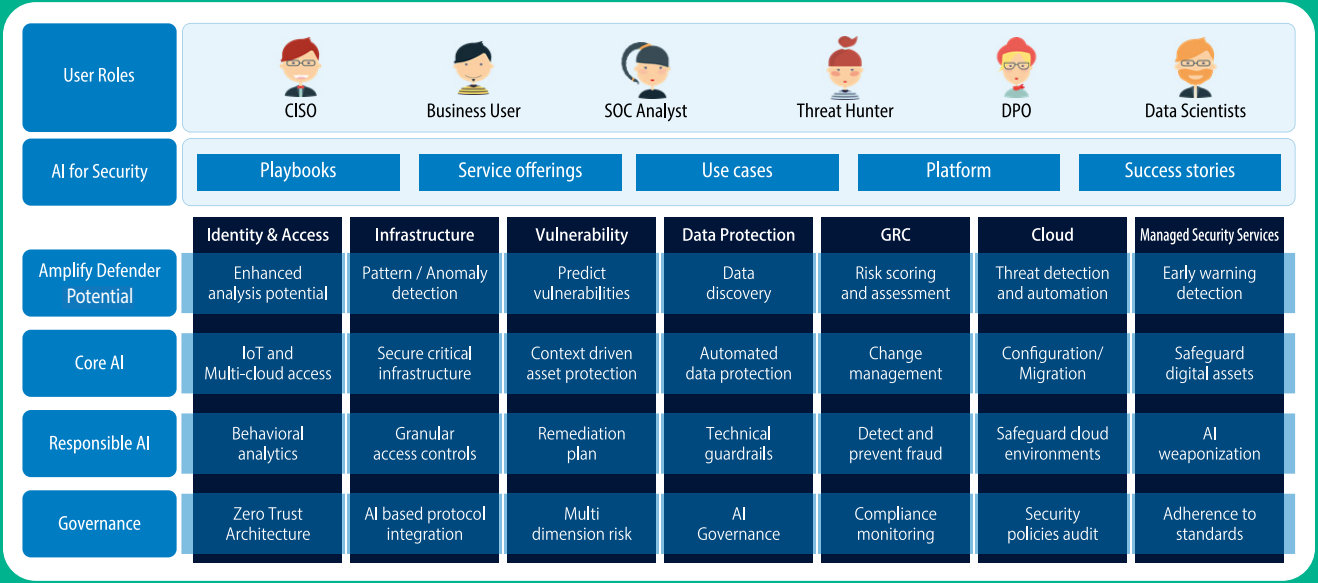


Figure 3 - Reference Architecture : AI for Cybersecurity

The design principles and reference architecture should lead to outcome-based approaches:

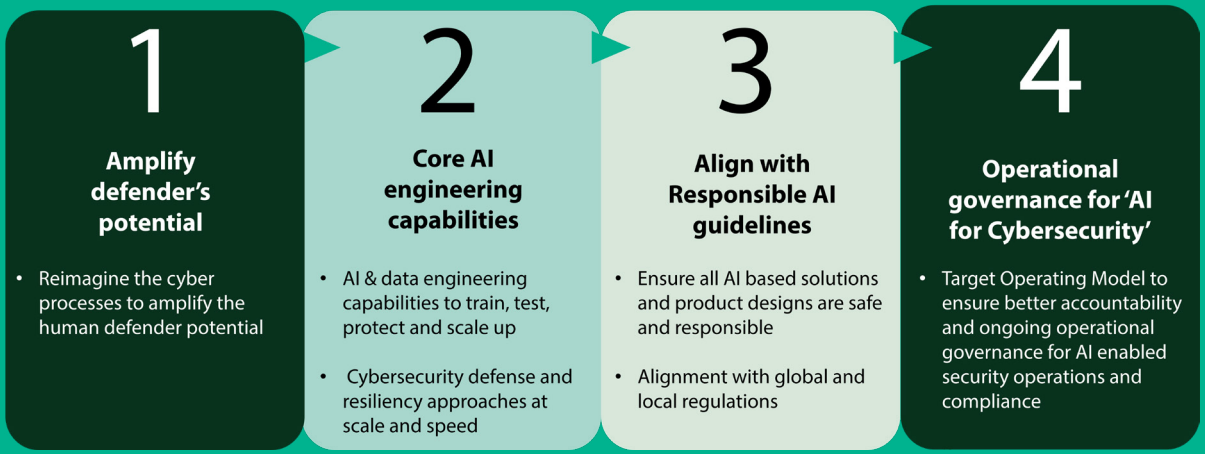


Figure 4 - Outcomes for AI for Cybersecurity

1. **Amplifying defender's potential** – Our focus would be to build AI assistant for each persona of the security team - analyst, employee, partner, threat hunter, SOC analyst or a CISO.

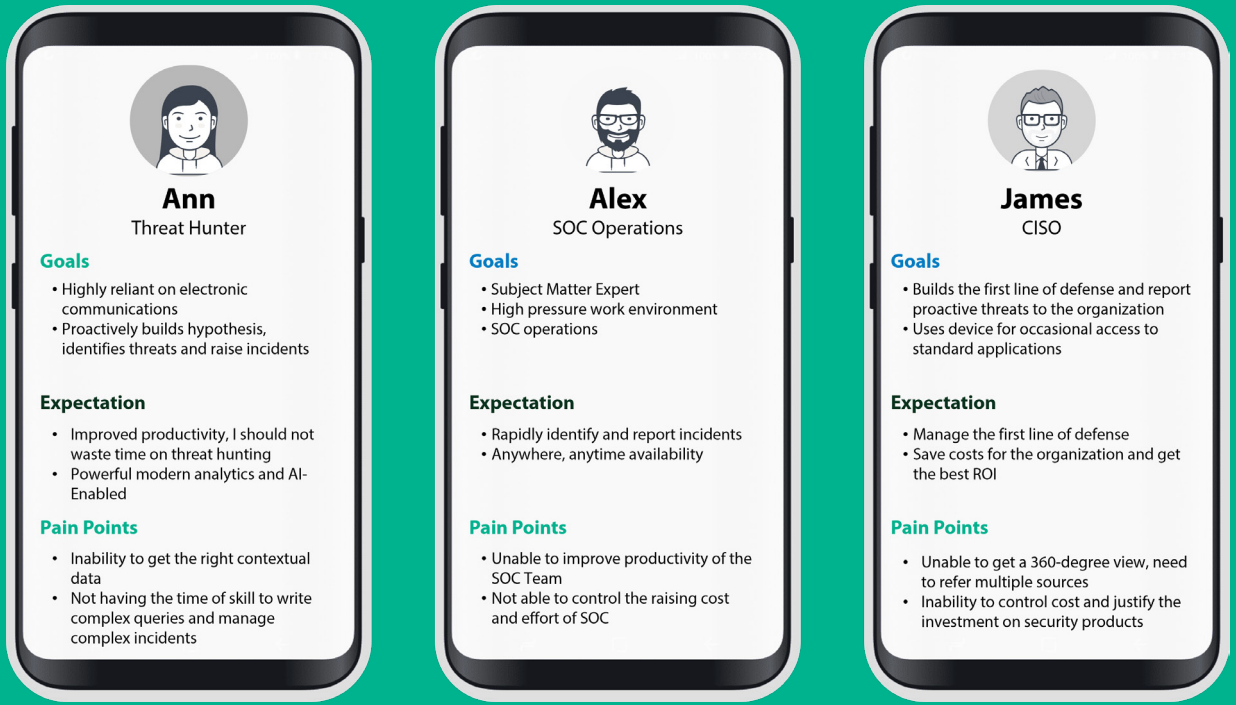


Figure 5 - Personas from Security Team

2. **Strengthen Core AI engineering capabilities** – Enterprises can strengthen their core AI for security engineering capabilities by building Gen AI models, security data for training models and automation capabilities of their ML Operations pipeline through our use case repositories and playbooks. Further there should be focus on building a connected security of AI ecosystem for partner OEM products.

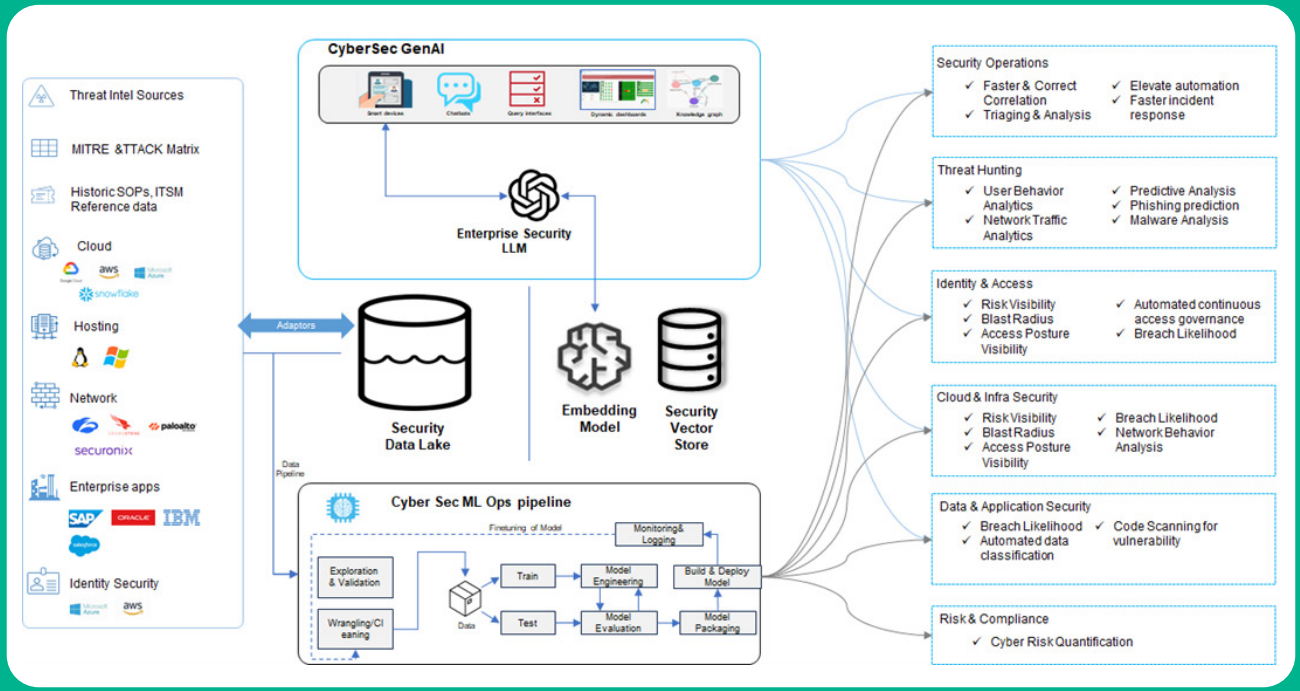


Figure 6 - AI core and technical architecture

3. **Align with Responsible AI guidelines** - Enterprise AI outcomes for security should align with the Responsible AI guidelines. To be responsible by design, there should be focus on building the right protection, privacy checks and bias controls on the data used for AI. Further, in the development cycle, there must be detailed audit of AI models. This will help enterprises address privacy and ethical issues early, thereby strengthening confidence among end consumers, stakeholders, and employees.
4. **Operationalize Governance** - Target Operating Model to ensure better accountability and ongoing operational governance on the right security metrics.

Implementation Model – What should enterprises consider while implementing AI for Cyber

For Cyber AI initiatives to succeed, enterprises must offer compelling value proposition across the enterprise. It needs alignment of cross functional teams to define, track and attain the shared goal. Effective AI for Cyber programs should be a continuous security program focusing on answering the following questions:

1. How can AI enable the enterprise to balance innovation and security risk?
2. What is the outcome-driven approach to showcase cybersecurity priorities and investments?
3. Which part of the organization should be involved?

Recognizing and planning for this reality is critical for program success. The AI-First security program should not only be reactive, agile, and responsive to frequent, unexpected changes in the business, technology, and operating environments; but also drive continuous improvement in the security controls for effectiveness and efficiency. Infosys recommends a 5-step implementation model as follows:

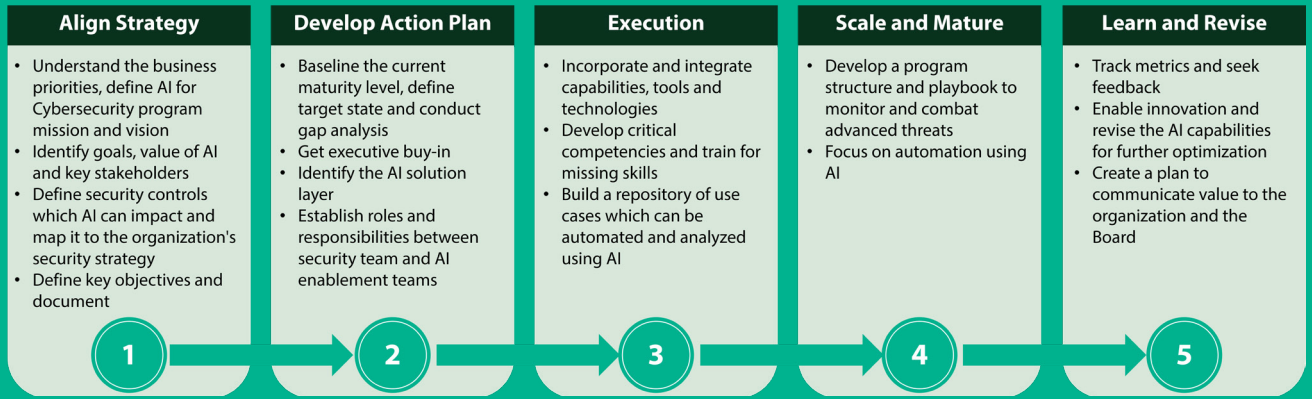


Figure 7 - Implementation Model

Step 1: Align Strategy – The enterprise should focus on analyzing the business priorities. They should define the mission and vision for the 'AI for Cybersecurity' program. This step helps to find the direction of the program in terms of the goals, values and impact of AI on the enterprise and key stakeholders, and the required security controls. These key goals should be documented and shared across the organization.

Step 2: Develop Action Plan – Assess current maturity level and set a target state for the enterprise. Gain executive acceptance for AI investments. Post this, enterprise can build, buy, partner, or invest in AI solutions. Integrating AI insights and automation into security operations is critical for successful AI deployments. AI adopters are currently using a blend of "off-the-shelf solutions and custom-built tools". An early AI adoption would have a higher level of customized development. This customization delivers higher value but can also increase cost to enterprises, which needs to be factored in the security- operations budget. The decision to build or buy AI for security depends on specific enterprise circumstances. Factors such as the purpose of AI, compatibility, customization, IP ownership, time constraint, vendor evaluation, cost, and ownership of data should be carefully weighed to make an informed decision. Each approach has its own pros and cons, and the decision should align with the organization's goals, technical capabilities, and strategic goals.

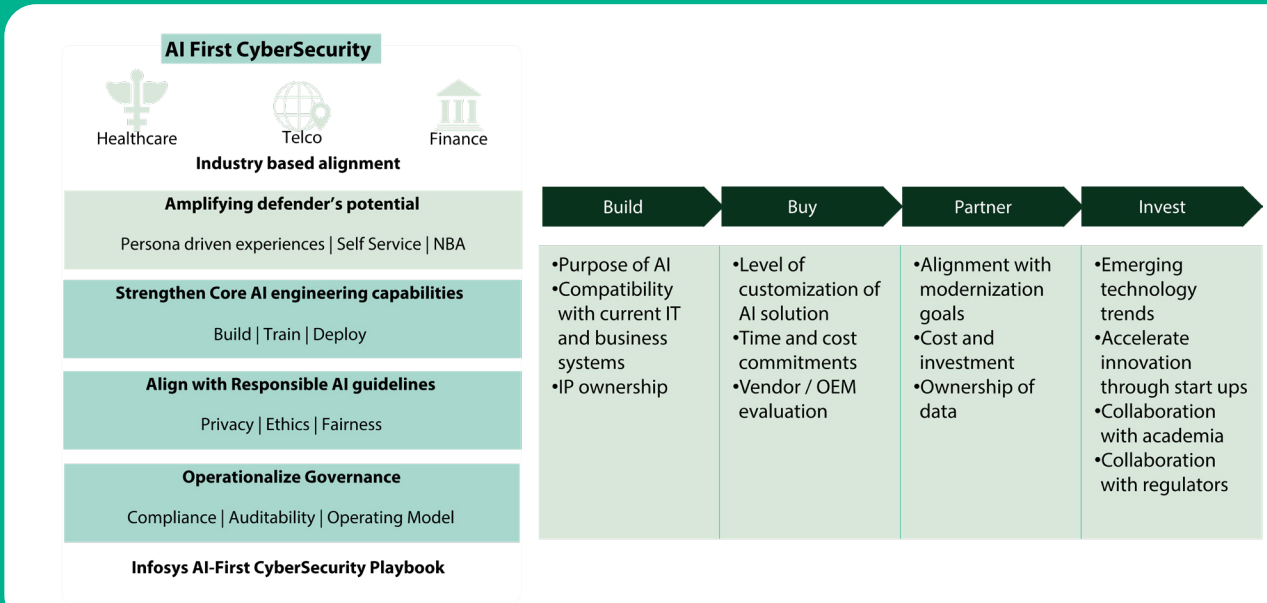


Figure 8 - Build, Buy, Partner or Invest in AI

Step 3: Execution – In the process of implementing AI, it is important to grasp its value, build competencies and fill the skillgap. Broadly, enterprises have three layers of AI capabilities based on the value added to the Cyber Defense capabilities.

1. AI for Automation - Automating security tasks like vulnerability scanning and patching using AI can cut cost and errors. It lets human analysts to focus on more complex investigations and decisions, thereby enhancing overall cyber hygiene.

2. AI for improving the accuracy of security controls - AI assistants can take more accurate decisions based on data and can analyze vast amounts of data from logs, network traffic, user behavior, and threat intelligence feeds. Risk scoring by Gen-AI assistants for privacy impact assessment is more accurate without human subjectivity. It is critical for an enterprise to build the right data set for their Gen-AI platforms and products.

3. AI for predicating risk – AI systems can continuously learn and adapt to new threats and attack methods, offering a dynamic defense against evolving threats. They can continuously monitor and analyze data in real-time, enabling immediate response to emerging threats, reducing the impact of successful attacks.

Step 4: Scale and Mature – This is a critical step in building scale and developing the AI based security offerings. Enterprises should focus on creating accelerators, playbooks, and scalable teams to build and execute the cybersecurity roadmap. This enables enterprises to scale their AI powered defense processes and keep a control over their security budgets..

Step 5: Learn and Revise – The final step focuses on crafting an actionable AI-First Cyber Defense roadmap by tracking metrics and seeking feedback. The critical aspect of the plan is to communicate clear ownership across cross-functional teams within the enterprise. The executive reporting framework and processes must be followed to achieve the business KPIs (Key Performance Indicators). The following map showcases recommended functions and their roles in the program. Enterprises need a clear vision outlining program goals and necessary building blocks for successful execution. This vision should be understandable by specialists from cross-functional teams, who can offer guidance and support.

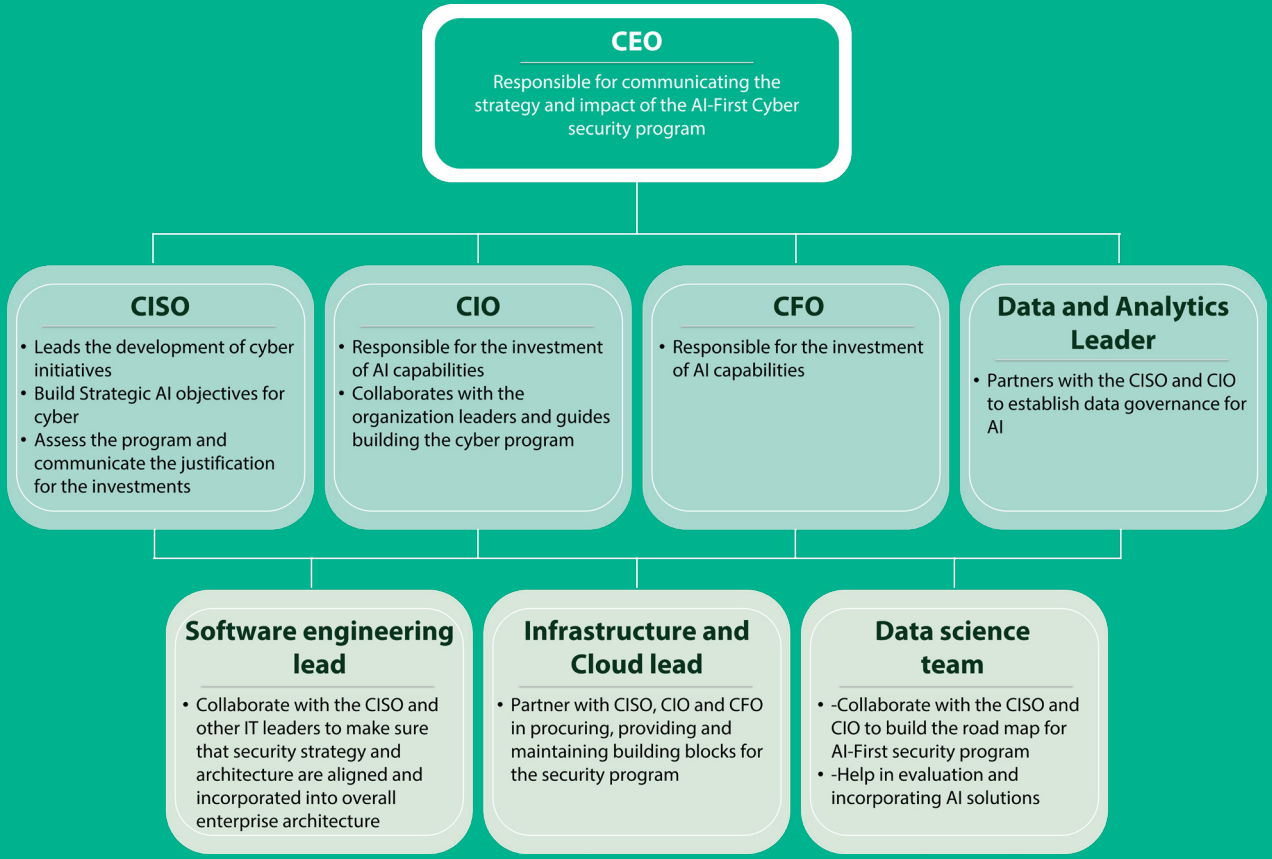


Figure 9 - Stakeholder Map

Way forward and next steps

Digital disruption is unavoidable and will lead to rapid technology-driven changes. As enterprises make large-scale investments in cybersecurity, the most successful security system is one which is work-in-progress. As per Gartner, 75% of the employees will get, change, or create technology outside IT's visibility[4]. The industrialization of cyber-crime, dynamic nature of attacks, and emergence of new threat vectors demand enterprises to set up a proactive approach beyond the horizon of cyber defense capabilities. Enterprises should embrace AI as the enabler to learn, build operational efficiency and balance business value while protecting from cyber threats.

Each enterprise has a different level of AI maturity and cybersecurity capability. The AI-First cybersecurity program should be a continuous learning program and can be applied to any enterprise based on their level of maturity. This can be achieved by following the below steps :

A. Automation – Enterprises should collaborate with experts to detect, examine, and quantify the advantages of AI for cyber defense. To begin, organizations can automate complex, time intensive and redundant activities, which can enhance efficiency and reduce errors. AI can also be utilized to identify sensitive data and assets to protect and automate assessments.

B. Baseline – Baseline standards for AI enabling the enterprise to build scalable security automation processes, which can reduce cost and give higher visibility of threat landscape. There is a need to create building blocks for AI and data which can be utilized for training and deployment of self-learning algorithms, LLM and AI products.

C. Community – This is a mature stage, where enterprises can build a center of excellence that houses experts who can build skill and scale to accelerate AI adoption. This phase focusses on building the right talent for AI and security, ML pipelines and best practices.

The continued investment in digitization, increased sophisticated cyber-attacks, and regulatory pressure on enterprises to protect their data has posed a need for AI for yber defense. A report from McKinsey estimates around 2Tn will be invested in technology to make cybersecurity providers more competitive. Automated IT delivery was a novel idea 20 years ago, but today every enterprise uses automated DevOps pipeline for delivery. Likewise, we are at a starting point of AI for cybersecurity where we will see more tools, standards and communities evolving to enable the same.

How can Infosys help?

Infosys Cybersecurity practice can help organizations strengthen their security and risk posture by carving out an AI-First security approach. We can help enterprises Re-Imagine, Re-Architect and Renew their entire cyber strategy with a focus on building AI capabilities.

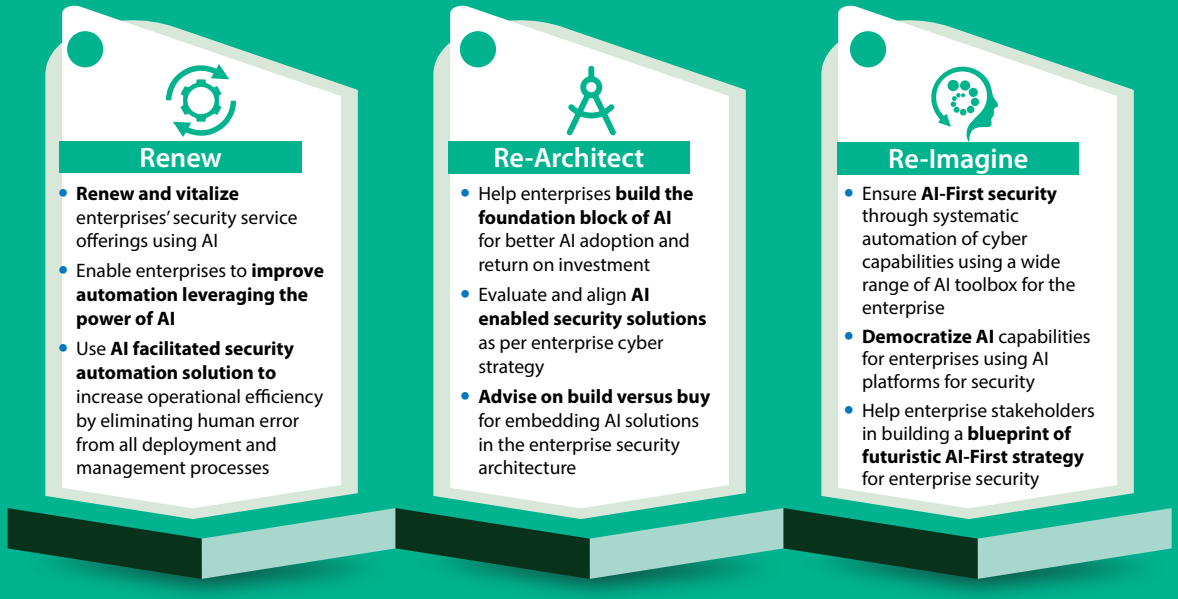
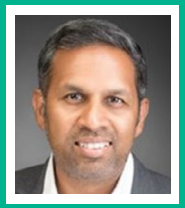


Figure 10 – Infosys 3R strategy for AI-First Approach

Authors



Karthik Nagarajan

Practice Manager and Senior Industry Principal

Karthik heads Infosys Data Protection and Privacy services. He has 17+ years of experience in product design and consulting services, with an expertise in AI, data privacy and customer experience strategy.

Nitin Bajpai

Principal Consultant

Nitin is an experienced and accomplished Information Security Professional with 18+ years of experience, spanning all facets of Information Technology and Security. His proficiency includes design & implementation of Identity Security solutions, Cloud and Digital Workplace Security, Zero Trust Enterprise Architecture, Emerging Technologies and Security Advisory.

References and further reading

1. Gartner Research, How to Build a Robust, Defensible Security Program That Enables Business Growth and Agility, Tom Scholtz, 23 February 2022
2. AI and automation for cybersecurity – IBM Security
3. Gartner Research, What's New in Artificial Intelligence from the 2023 Gartner Hype Cycle, Lori Perri, 17 August 2023
4. McKinsey, New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers, Bharath Aiyer, Jeffrey Caso, Peter Russell, 27 October 2022
5. Gartner Research, IT Roadmap for Cybersecurity, 2023
6. Information Security Forum, Establishing a Business-Focused Security Assurance Program, March 2019
7. Forbes, 76% Of Enterprises Prioritize AI & Machine Learning In 2021 IT Budgets, Louis Columbus, 17 January 2017
8. FT.com, Why CFOs must collaborate across teams to overcome cyber threats, 2023
9. BlackBerry Global Research, ChatGPT May Already Be Used in Nation State Cyberattacks, Say IT Decision Makers, 02 February 2023
10. Cyber Next – Platform Powered Services, Infosys
11. Cybersecurity Jobs Report: 3.5 million Unfilled Positions In 2025, Steve Morgan, 14 April 2023
12. https://darktrace.com/blog/tackling-the-soft-underbelly-of-cyber-security-email-compromise
13. 76% Of Enterprises Prioritize AI & Machine Learning In 2021 IT Budgets (forbes.com)

For more information, contact askus@infosys.com

Infosys®
Navigate your next