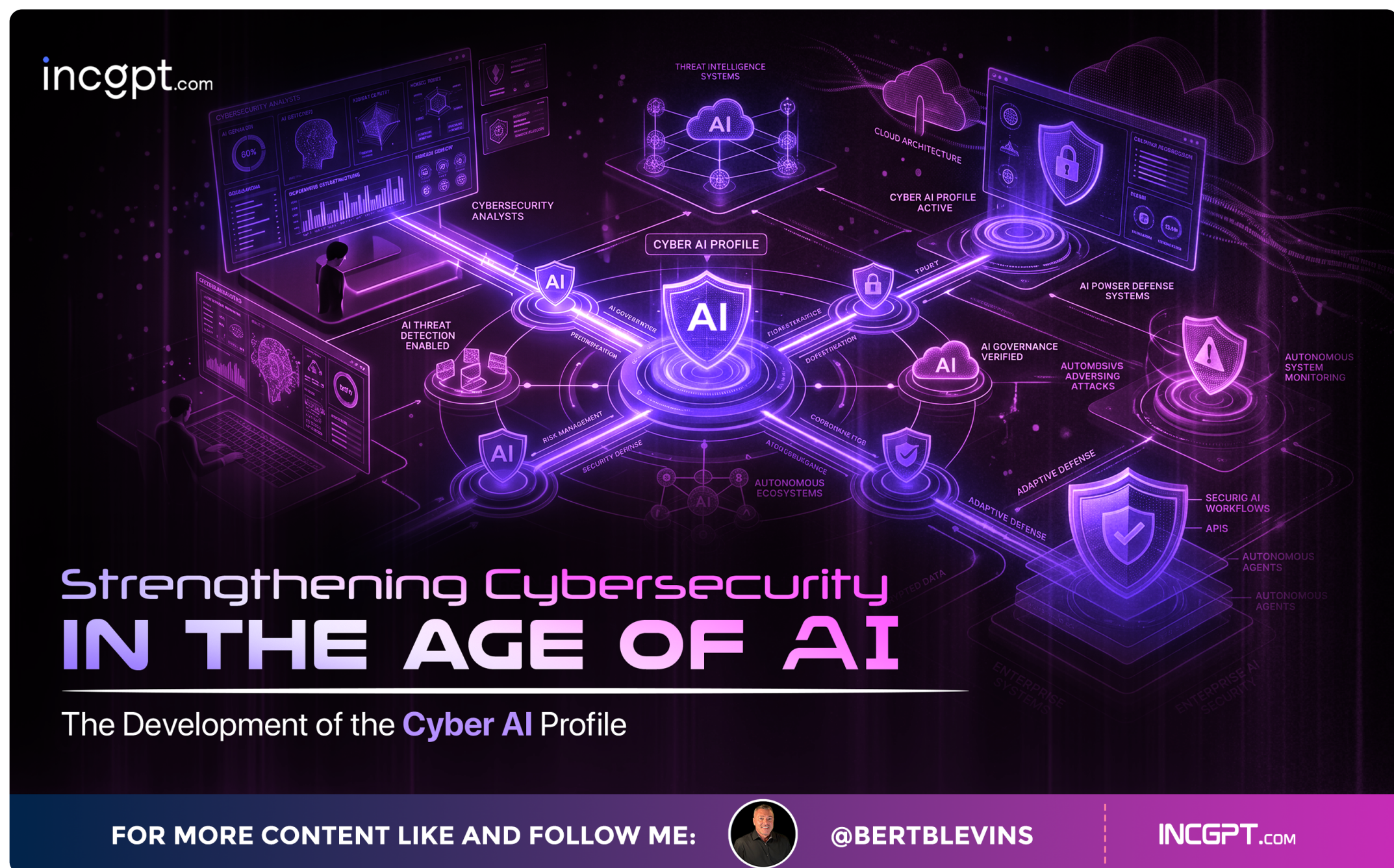


Strengthening Cybersecurity in the Age of AI: The Development of the Cyber AI Profile



Acknowledgements

The creation of the Preliminary Draft of the Cyber AI Profile owes much to the contributions of a wide range of stakeholders, including subject matter experts, workshop speakers, and session participants. These individuals played a pivotal role in shaping the discussions and providing feedback, which were crucial in forming the foundational elements of the document. Special thanks are extended to those who contributed invaluable insights during the public workshops and working sessions, as well as to the teams at NIST and MITRE Corporation, whose expertise in cybersecurity and AI was instrumental in the development process. Without their efforts, this work would not have been possible.

Emerging AI Opportunities in Cybersecurity

The rapid evolution of Artificial Intelligence (AI) has led to transformative opportunities and challenges within the cybersecurity landscape. AI's capabilities in automating tasks, analyzing vast amounts of data, and identifying complex patterns are revolutionizing how organizations approach security. However, the same technology also introduces novel vulnerabilities, as AI can be manipulated by adversaries or misused in cyberattacks. NIST recognizes the need to address both sides of the AI spectrum and is leveraging its expertise in cybersecurity and AI to support organizations. By doing so, NIST aims to help organizations navigate these emerging risks while taking full advantage of the benefits AI offers in improving security measures. The ongoing effort emphasizes the importance of keeping pace with these developments, fostering awareness, and implementing best practices to secure AI-driven systems.

For more content like and follow me:



@bertblevins

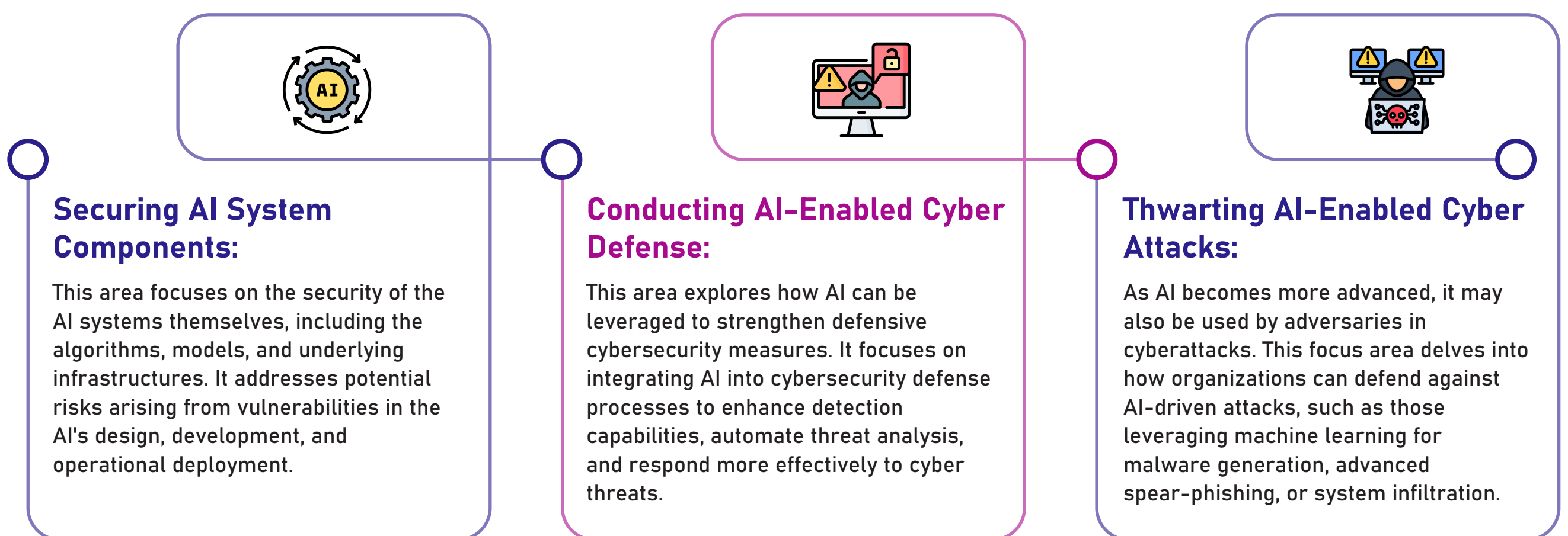
INCGPT.COM

Cyber AI Profile: A Framework for Cybersecurity and AI Integration

To guide organizations in integrating AI into their cybersecurity strategies, NIST is developing a comprehensive Cybersecurity Framework Profile specifically tailored to AI. This profile offers a structured, neutral, and technology-agnostic approach to managing AI-related cybersecurity risks. It will assist organizations in securing their AI systems, using AI to enhance their defenses, and mitigating adversarial AI attacks. As organizations increasingly adopt AI, it is crucial to establish clear, actionable guidelines that help secure the AI infrastructure. The Cyber AI Profile aims to offer a balanced framework that organizations can easily adapt and apply to both the operational and strategic aspects of cybersecurity, ensuring that AI adoption is done responsibly and securely.

Key Focus Areas of the Cyber AI Profile

The Cyber AI Profile is organized around three key focus areas, each addressing a different dimension of the AI-cybersecurity relationship:



These focus areas not only address how AI can be incorporated into an organization's security framework but also how it can be protected from potential misuse or exploitation by malicious actors.

01

Preliminary Draft of the Cyber AI Profile

The Preliminary Draft serves as a foundation for the ongoing development of the Cyber AI Profile. This draft outlines NIST's current approach to integrating AI into cybersecurity and is intended to gather public input to refine and improve the final version. Feedback from cybersecurity professionals, industry stakeholders, and AI experts is critical to ensuring that the profile remains relevant, practical, and effective in addressing emerging cybersecurity challenges related to AI.

02

NIST Cybersecurity Framework (CSF) 2.0

The NIST Cybersecurity Framework (CSF) 2.0 provides a well-established, voluntary approach for managing cybersecurity risks. NIST's AI Risk Management Framework (AI RMF) complements the CSF by addressing the unique risks posed by AI systems. Together, these frameworks provide organizations with a comprehensive methodology for understanding, mitigating, and managing the cybersecurity risks associated with AI technologies. The CSF's flexible structure allows organizations of various sizes and sectors to tailor their cybersecurity strategies, while the AI RMF introduces AI-specific guidelines to ensure that emerging AI risks are adequately addressed.



03

Development of the Cyber AI Profile

NIST has engaged a wide range of stakeholders from government, industry, and academia to shape the Cyber AI Profile. This collaborative process has been essential for understanding the cybersecurity challenges faced by organizations adopting AI. Through various workshops and public sessions, NIST has gathered input on the current state of AI-related cybersecurity, identified critical gaps, and discussed how AI can be better integrated into organizations' risk management strategies. This engagement has provided valuable perspectives that are being used to refine the profile.

04

Public Workshops and Working Sessions

In 2025, NIST conducted several public workshops and working sessions to collect feedback from the AI and cybersecurity communities. These sessions focused on identifying the specific cybersecurity needs that arise when integrating AI into organizational ecosystems. Discussions also explored how AI can be harnessed to improve security operations, and how organizations can prepare for the new threat landscape shaped by adversarial AI. The materials from these events continue to inform the development of the Cyber AI Profile, ensuring that it addresses the most pressing challenges faced by organizations.

05

Ongoing Literature Review and Stakeholder Input

An ongoing literature review, combined with continuous input from the AI and cybersecurity communities, has been a critical aspect of the Cyber AI Profile's development. As AI technology evolves rapidly, so too must the strategies for securing AI systems and defending against AI-driven threats. By incorporating the latest research and expert feedback, NIST ensures that the profile remains up-to-date and effective in addressing new cybersecurity risks as they emerge.

06

AI and Cybersecurity Considerations

The profile provides a deep dive into the various considerations organizations must take into account when securing AI systems and leveraging AI for cybersecurity defense. It highlights the challenges organizations face in securing AI systems, particularly when these systems are integrated into larger networks or used to support defensive measures. The document also emphasizes the need for resilience in AI-powered cybersecurity systems, focusing on how organizations can build defenses against adversarial AI attacks and mitigate risks arising from vulnerabilities in AI models or training data.

07

Tailoring Cyber AI Profile to Organizational Needs

One of the key strengths of the Cyber AI Profile is its adaptability. Organizations are encouraged to tailor the guidelines and recommendations to their specific needs, resources, and maturity levels. This flexibility allows organizations to prioritize the most relevant cybersecurity outcomes related to AI adoption and address them in a manner suited to their unique operational contexts.

08

Practical Guidance for Implementing AI in Cybersecurity

The Cyber AI Profile offers actionable guidance for organizations looking to integrate AI into their cybersecurity programs. It provides clear steps for assessing AI-related risks, prioritizing key cybersecurity efforts, and managing the complexities of AI adoption. Additionally, the profile helps organizations communicate their cybersecurity expectations with external stakeholders, ensuring that AI systems are securely implemented and maintained throughout their lifecycle.

