KPMG

AI security framework design

KPMG AI Security Services

AI is being embedded into every business process and technology, but you probably don't know whether your AI is secure. KPMG AI Security Services looks to empower organizations to **assess** their AI ecosystem, **secure** their critical models, and **respond** to adversarial attacks.

A survey conducted by **Microsoft** found that **89%** of surveyed companies **do not have tools in place** to secure their AI systems

Source: Adversary Machine Learning, Redmond, USA (March 2021)

Today, **35%** of companies reported using AI in their business, and an **additional 42% reported they are exploring AI**

Source: IBM Global Adoption Index 2022, USA (May 2022)

Impending regulations, such as the **EU's AI Act**, will require organizations to ensure security and trustworthiness of their high-risk AI systems

Recent discoveries in the attack landscape have demonstrated that AI systems are a major target for attacks like poisoning, evasion, and extraction

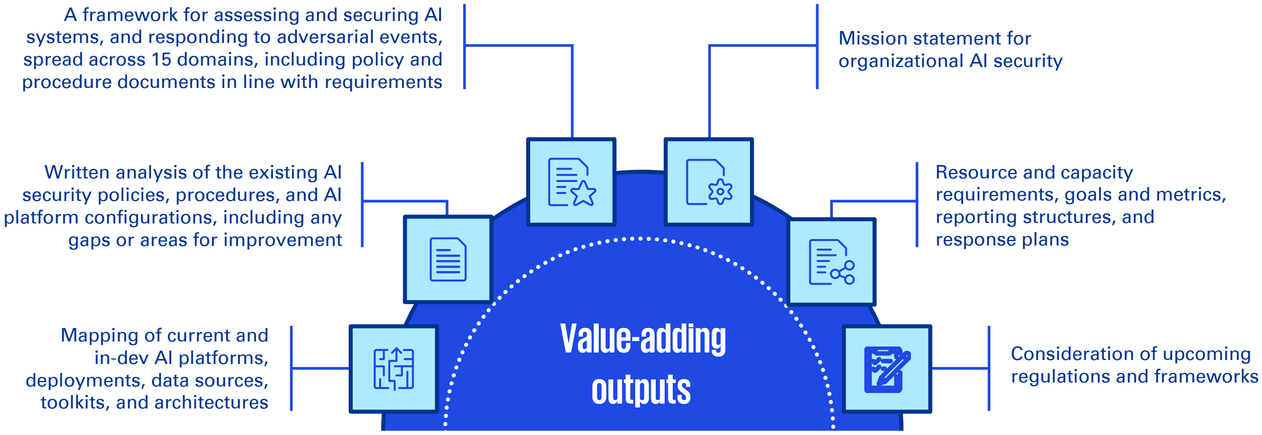
An immense cybersecurity void

As companies rapidly invest in automation of current-state processes with the help of AI models and systems, security considerations can be sacrificed or ignored completely. However, increased sophistication and feasibility of attacks, as well as regulatory pressure, will require organizations to ensure the security of their innovative AI solutions.

A comprehensive AI security framework

Our AI security framework design provides security teams with a playbook to proactively assess their organization's AI systems in development and production environments; it helps to secure those systems against threats such as backdoor attacks and model inversion, and respond effectively in the event of an attack. Our AI security professionals tailor the approach to meet the requirements, platforms, and capabilities of different organizations to deliver an effective and accepted security strategy.

The value-adding outputs of an AI security framework engagement can include:



Value-adding outputs

A framework for assessing and securing AI systems, and responding to adversarial events, spread across 15 domains, including policy and procedure documents in line with requirements

Mission statement for organizational AI security

Written analysis of the existing AI security policies, procedures, and AI platform configurations, including any gaps or areas for improvement

Resource and capacity requirements, goals and metrics, reporting structures, and response plans

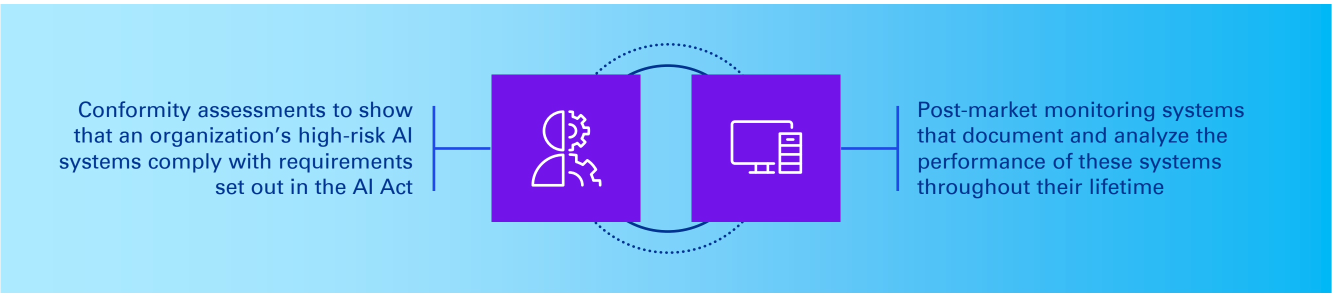
Mapping of current and in-dev AI platforms, deployments, data sources, toolkits, and architectures

Consideration of upcoming regulations and frameworks

Why act now?

As organizations push to reinvent existing processes with the support of AI, more and more critical business processes are reliant on deployed AI models. Attacks against these systems present unique cybersecurity problems, as unlike traditional systems, many AI models cannot simply be turned off in-flight, such as those supporting autonomous vehicles or medical devices. Additionally, the overall technical complexity underpinning the operation of AI systems enhances the difficulty of detecting and remediating an adversarial attack.

Regulatory bodies are currently developing requirements for organizations to ensure the trustworthiness and security of their high-risk AI systems. The EU's AI Act, for example, will require providers of high-risk AI systems to implement the following governance mechanisms:



Conformity assessments to show that an organization's high-risk AI systems comply with requirements set out in the AI Act

Post-market monitoring systems that document and analyze the performance of these systems throughout their lifetime

In addition to the regulatory pressures, a variety of standards centered around AI systems are in development, such as NIST's AI Risk Management Framework (AI RMF) and MITRE's Adversarial Threat Landscape Against AI Systems (ATLAS).

Rather than waiting for breaches to occur or regulations to hit, proactive organizations will take steps today to get a full view of the AI operating in their organization, understand the risks associated with these systems, and secure against any discovered vulnerabilities. KPMG AI Security Services professionals bring the requisite security knowledge, as well as the necessary technical data science skillsets, to support organizations in accomplishing this goal.

KPMG AI Security Services is a leading suite of AI security service offerings that provide effective security approaches for AI systems and models. Our risk-based approach provides targeted prioritization to secure an organization's most critical systems.

Stay ahead of sophisticated threats against your AI systems and models, as well as regulations requiring robust security of high-risk AI models

Empower your data-science teams to continue experimenting and transforming current processes while helping to keep critical systems safe

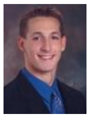
Contact us:

Matthew Miller
Principal
T: +1 571 225 7842
E: matthewpmiller@kpmg.com

Charles Jacco
Principal
T: +1 212 954 1949
E: cjacco@kpmg.com

Jonathan Dambrot
Principal
T: +1 908 361 6438
E: jdambrot@kpmg.com

Mitushi Pitti
Managing Director
T: +1 848 247 8445
E: mitushipitti@kpmg.com



Brad Raiford
Director
T: +1 832 527 5624
E: braiford@kpmg.com

Daniel Christman
Senior Associate
T: +1 832 866 7039
E: dchristman@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

KPMG is a global organization of independent professional services firms providing Audit, Tax and Advisory services. KPMG is the brand under which the member firms of KPMG International Limited ("KPMG International") operate and provide professional services. "KPMG" is used to refer to individual member firms within the KPMG organization or to one or more member firms collectively.

For more detail about our structure, please visit home.kpmg/governance.