AIShield
Powered by Bosch

DATASHEET

AISHIELD PROFESSIONAL SERVICES

With our deep technology and industry implementation expertise, let us guide you through the rough and complex landscape of AI security to proactively assess, detect and defend your AI assets.

WHY NOW

In today's business landscape, Artificial Intelligence (AI) is increasingly playing a pivotal role. Widespread AI adoption is giving rise to new attack surfaces for cyber adversaries to exploit while businesses are left grappling to manage such complex AI security risks. Hence, securing AI infrastructure is paramount as breaches can result in severe consequences like brand damage, loss of intellectual property, and financial repercussions. Imminent regulatory frameworks like the European AI Act and the U.S. Executive AI Order underscore the urgency of compliance and security.

WHY US

AIShield stands as an essential AI security partner, providing a holistic suite of services tailored to safeguard your AI systems. Our team , boasting over 70+ years of combined expertise in cybersecurity engineering, data science and adversarial AI, system engineering, threat intelligence, and adversarial engineering empowers your organization to adeptly assess, detect and defend your AI systems. We excel in technical proficiency and practical, front-line defense against significant AI and ML model breaches. We proactively research and mitigate vulnerabilities in MLOps/ LLMOps platforms to safeguard the public. Moreover, our commitment to innovation is highlighted by an average of 4 patents per team member, showcasing our strategic approach to developing cutting-edge solutions in AI Security.

BENEFITS

AIShield's suite of services, provides strategic insights to shield your AI investments effectively. We equip your team with the tools to anticipate and neutralize threats, ensuring your AI operates with unmatched resilience and security, perfectly aligned with your business goals.

Empower Teams

- Learn from the leading experts in Adversarial Machine Learning

Staying ahead of threats

- Gain a clear understanding of the threats facing your AI models.
- Discover the most vulnerable points in your ML operations and models.

Smoother AI Integrations

- Protect your ML/LLM operations with unmatched security measures.
- Strategically prepare for AI threat detection and response.
- Safely accelerate the adoption of Large Language Models in your organization.

DATASHEET

WHAT WE OFFER

AI Security Risk Evaluation

Understand the unique security risks of your AI/ML and GenAI applications. We identify vulnerabilities, offer solutions, and ensure your AI complies with crucial standards, best practices, and laws (e.g., NIST AI RMF, MITRE ATLAS, OWASP Top 10, EU AI Act, ISO 42000 and 27000).

01

AI Security Technical Risk Assessment

Gain insights into technical risks in your AI/ML and GenAI operations. We highlight issues from model vulnerabilities to data integrity, with strategies to strengthen your defenses, securing your AI infrastructure and pipelines against future attacks.

02

AI Application Security Posture Evaluation

Receive detailed assessments of your AI applications' security, identifying misconfigurations and deviations from best practices related to architecture, design, planning, and tooling.

03

Red Team Augmentation

Boost your red team's ability to anticipate and simulate realistic AI-specific threat scenarios with our advanced hands-on session. Learn from the adversarial tactics, techniques, and procedures (TTPs) that could target your AI systems and how to test for them.

04

AIShield Implementation Services

Integrate the AIShield Platform into your AI development and operations (MLOps) to improve security and efficiency. Our service enhances your AI's defense mechanisms and your team's response capabilities, maximizing your AI investments.

05

AIShield Defense Integration Services

Focus on integrating detection models and defensive strategies tailored to your environment, ensuring comprehensive protection for your AI systems.

06

Red Team/ Blue Team Exercise

Enhance your cybersecurity team's skills with a simulated attack scenario using the AIShield Platform as a Red Team. Learn from our experts as Blue Team to defend against sophisticated threats targeted at your industry.

07

AI Security Training

AIShield offers comprehensive training sessions ranging from 4 hours to 2 days, designed for AI and security teams at all levels, including specialized sessions for C-level executives .

08

ABOUT AISHIELD

AIShield is a Gartner-recognized AI application security startup of Robert Bosch GmbH with a vision to secure AI/ML systems of the world. Founded in May 2022, AIShield is a leading provider of products and solutions, backed by 45+ patents, that ensure the cybersecurity of Artificial Intelligence-based workloads and assets. More than 40+ customers globally trust AIShield to secure their AI systems across the lifecycle, deployment scenarios, and any model. (Discriminative AI, Machine Learning models, Deep Learning & Generative AI Large Language models).

Address: 123 Industrial Layout, Koramangala, Hosur Main Road, Bengaluru, Karnataka 560095

Website: www.boschaishield.com

Contact us at: aishield.contact@bosch.com