Bosch Global Software Technologies
alt_future

BOSCH
Invented for life

Bosch AIShield

The core of AI systems security

Is your AI Secure?

AI Security is critical for Building Digital Trust

Where is AI Security today?

Widespread AI Adoption has profoundly exposed Machine Learning Models & associated Data to Vulnerabilities such as Model Theft/Extraction, Data Poisoning, Algorithm Evasion and loss of Intellectual Property.

Hackers can subvert machine learning systems for their own Profit, Skewed Ideology or cause harm to Individuals, AI Companies & Society at large.

- **89%** organizations did not have the right tools in place to secure their AI systems in 2021.
- **60%** AI providers will include a means to mitigate possible harm to their AI assets by 2024
- **80%** is the cost difference between cyberattack scenarios, where secure AI was deployed vs not deployed

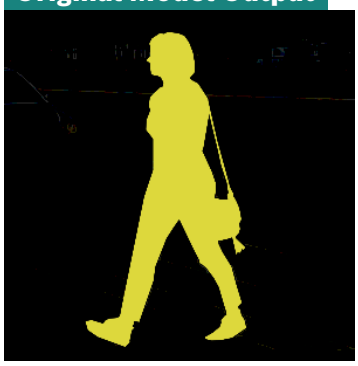
Case in Point

Bosch Ethical Hacking Case - Pedestrian Detection Algorithm

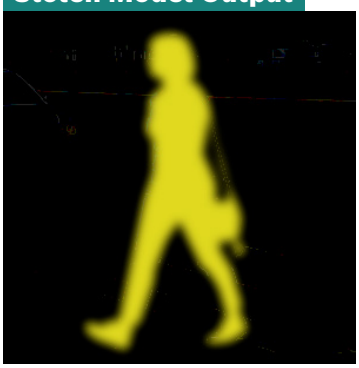
Developed with large proprietary data sets over 10 months costing Euro(€) 2 Mio

Original

Original Model Output



Stolen Model Output



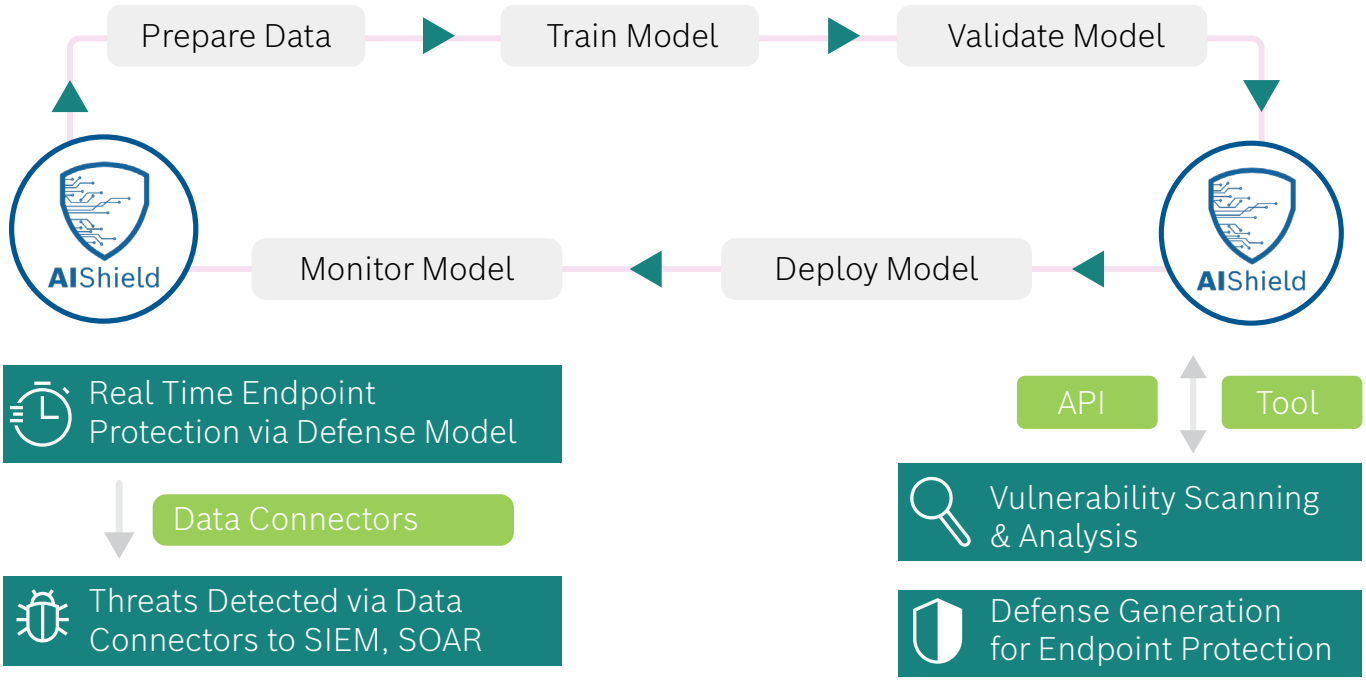
Stolen in <2 hours at Fraction of cost & less than 4% delta of model accuracy

The Problem

How to secure AI ecosystems against Adversarial Machine learning threats which could result in financial loss, reputation damage, loss of competitive advantage and intellectual property

" It's hard to patch or mitigate what you can't find !! "

How AIShield solves it?



Benefits

- **AI/ML Model Security**
- **Automation with MLOps**
- **Deployment Flexibility**
- **Safeguard AI Investments**
- **Trustworthy AI**
- **Brand & IP Protection**

Know more

Get in touch

Getting Started

Consulting

AI Security Impact Assessment & Mitigation Plan

Services

Customized Enterprise implementation of AI Security from PoC to Scale

Product

Consume & Realize AIShield benefits with MLOps integrated SaaS based subscription

For more information, send your enquiries to *AIShield.Contact@bosch.com*

Bosch Global Software Technologies Pvt. Ltd.
India | USA | Europe | Japan | Middle East | China

Bosch Global Software Technologies
alt_future