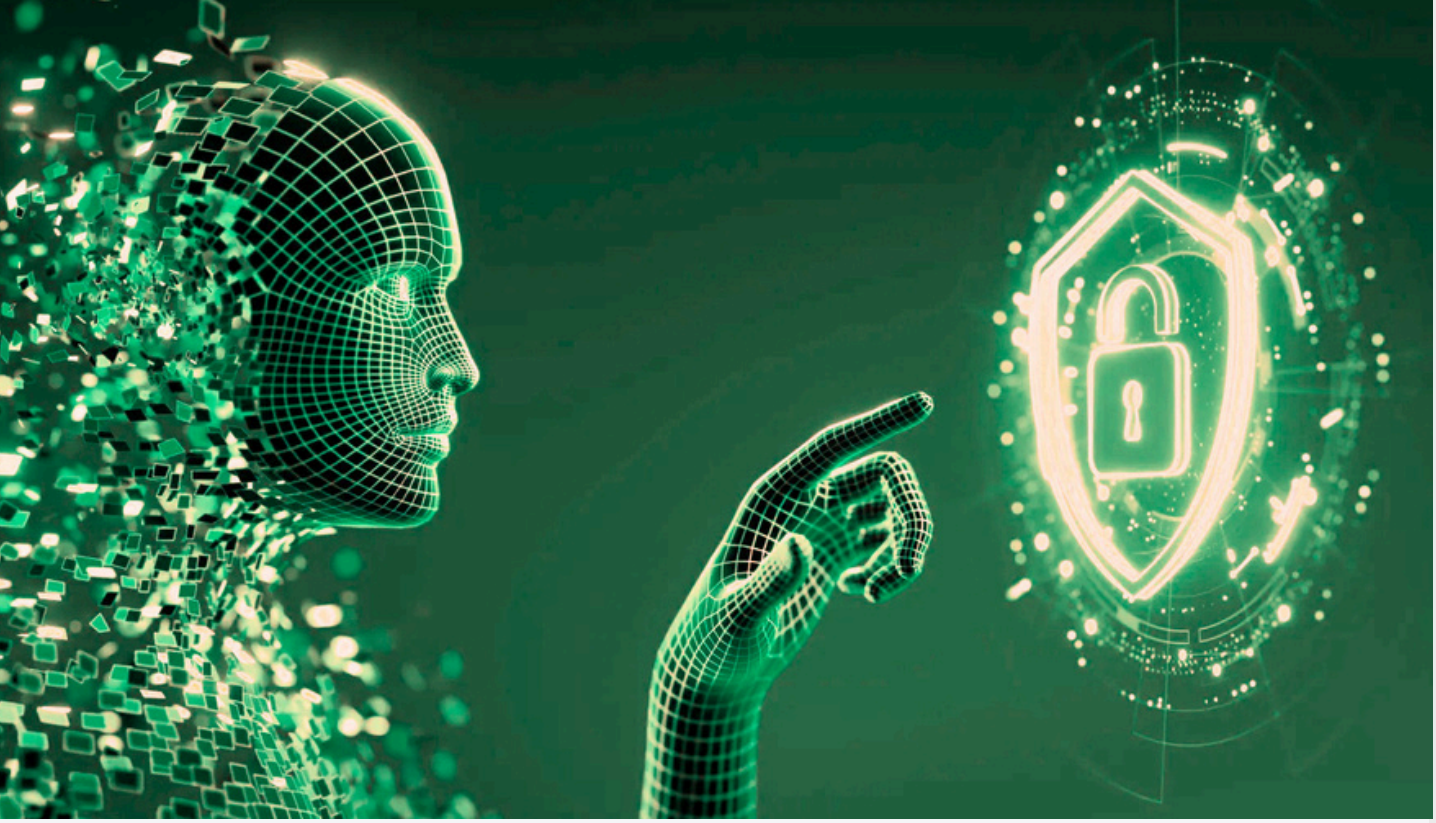


AI SECURITY

Design, Test, Assure & Govern

AI Threat Landscape

> **Your organization is using AI in more ways than you can imagine**

Employees

Your Employees are using Chat GPT for almost every task

What are they placing in those promts

?

Tools

Tool in your company have embedded AI

Is that generated code secure enough to be considered

?

DevOps

Developers are generating code ten times the speed

Can your security pipeline handle that speed

?

AI Apps

Your application use LLMs from dozen of sources

Are those LLMs biased and will create challenges for you

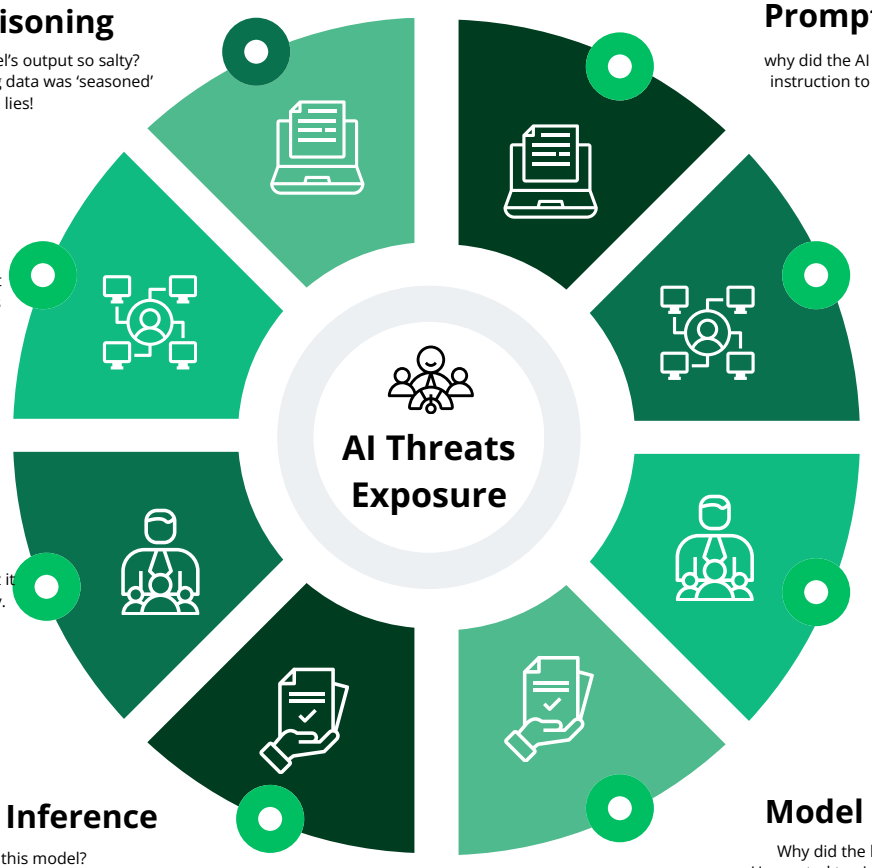
?

Infra

Digital Infra in your company is managed by AI

How would you gain visibility into dynamic infrastructure

?



Data Poisoning

Why was the model's output so salty? Because the training data was 'seasoned' with lies!

Prompt Injection

why did the AI get in trouble? It followed instruction to the 'letter'...even the bad ones!

Shadow AI

Why is unauthorized AI so good at hide and seek? because its always working in the 'shadows'!

Jail Breaking

What's an AI's favourite Bob Marley song? 'No Women, No Cryptography'- I'm breaking free!

Identity Spoofing

I asked the AI to be myself today....but it decided to be 'someone else' entirely. talk about a face-off!

Role Playing

The AI started role-playing as a spy. Now it won't stop 'masking' the truth!

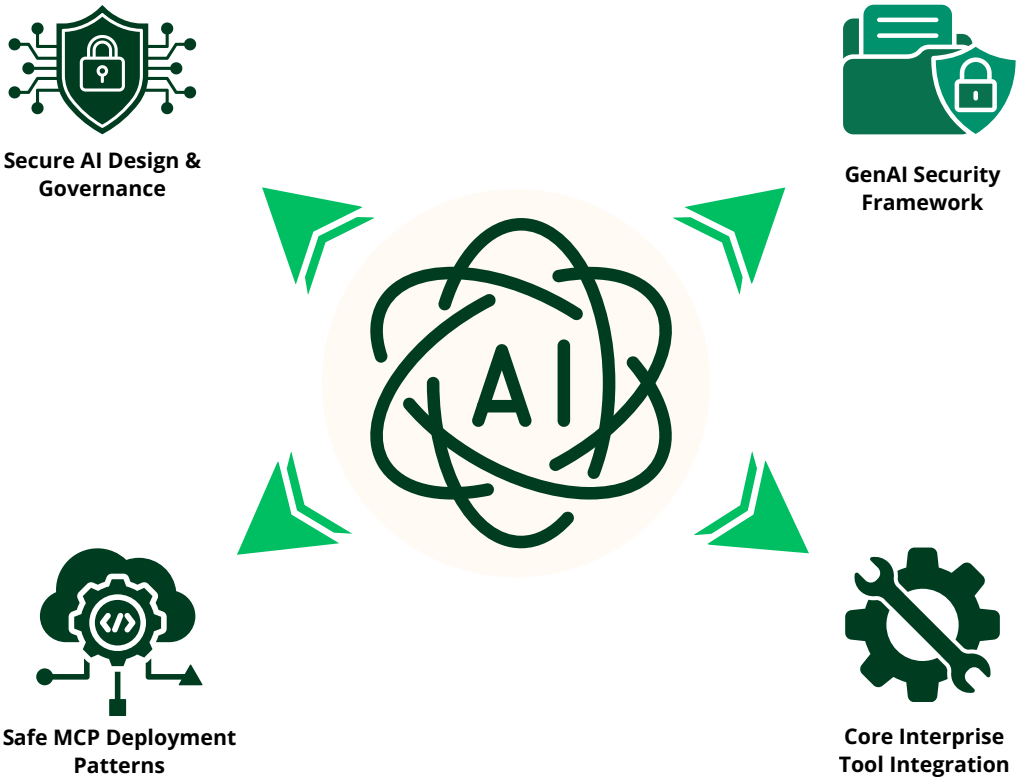
Membership Inference

Is your data in this model? Don't worry, the AI 're-members' you perfectly!

Model Stealing

Why did the hacker copy the model? He wanted to give it a piece of his mind'...or vice versa

Castellum Secure AI Frameworks



Castellum AI Security

1. AI Security Testing

"Don't leave your AI apps to vanilla pen testing"

2. Enterprise AI Governance

"Define an enterprise class gov model, automated"

3. AI Code to Production

"Secure AI supply chain to prevent disasters"

4. AI Security Architecture

"Create an enterprise class AI Security Architecture"

About Castellum Labs

- All Services delivered from Global Security Delivery Center (GSDC)
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong handpicked team of (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995