

**threatworks**

**Solstice Event - AI in the Ring - Cybersecurity Face-Off**

THE TEAM

**One team.  
One focus.**

Offensive mindset, defensive actions.



**Teun  
Westbroek.**

Co-founder Threatworks.



**Jeoffrey  
Canters.**

Co-founder Threatworks.



**Today,  
AI is everywhere.**

THE NEW REALITY

# AI is everywhere. The question is what it's building.

From the kitchen to  
the codebase, AI is  
now part of daily life.



## AT HOME

Recipe & meal planning.



## AT WORK

Writing emails & reports.



## CREATIVE

Designing & generating  
visuals.



## PLANNING

Organising projects and tasks.



## PERSONAL

Medical & legal questions.



## YOUR BUSINESS

Building your applications.



**How does this affect  
software development?**

THE HACKATHON

**We wanted  
to know.  
So, we tested**

We took a real application  
built by AI, then tried  
to break it ourselves.

5.

Minutes to compromise an application built by AI.

TWO LEVELS

# AI makes mistakes *in two ways.*

One no scanner can see. One  
scanners might see.

## 0 1 Architecture

NOT SCANNABLE

Without context, AI makes design decisions nobody approved. The vulnerability lives in the architecture, no tool will flag it.

Insufficient RBAC

No security layer around the database

## 0 2 Code


SCANNABLE

AI generated code with missing controls and weak policies. The exact vulnerability classes SAST, SCA and DAST tools are built to find.

Missing authorization checks

Weak password policy

No brute-force protection



*In the age of AI,  
Secure-by-Design isn't optional.*  
**It's the only way to keep up.**

TWO LAYERS

# Tell AI what to build. *Verify it did.*

One layer defines the rules before the code is written. The other checks that those rules were followed after.

BEFORE THE CODE



## Secure by design.

Map the threat landscape. Define what needs protecting. Give AI explicit requirements, not vague instructions.

- Threat modeling
- Security requirements per feature
- AI inherits the guardrails

AFTER THE CODE



## Code scanning.

Automated tools verify what AI produced. Catch what slipped through, before it ships.

- Static analysis (SAST)
- Dependency & secrets scanning
- Validated against the threat model



***Thank you.***  
*Questions?*