Who let the AI Dogs Out?

Kate Scarcella, Cybersecurity Architect

cd CON

They didn’t get out on their own


Bad Dog!

AI Puppies Running Loose

We Have Seen This Before!

- Hardcoded Credentials
- Flat Networks
- Implicit Trust
- Static Identities

Capability Before Governance

became **technical debt**

We'll secure it later

We Know Better

In cybersecurity:

* Hardcoded credentials ➜ easier today ➜ identity risk later

* Flat networks ➜ faster deployment ➜ lateral movement later

* Security after release ➜ faster shipping ➜ systemic exposure later

And now with AI:

* Release capability first

* Add constraints later

* Hope behavior sorts itself out

Secure it now

Systems Without Boundaries Fail

The problem is not intelligence

The problem is systems without boundaries.

Containment is not the absence of change.

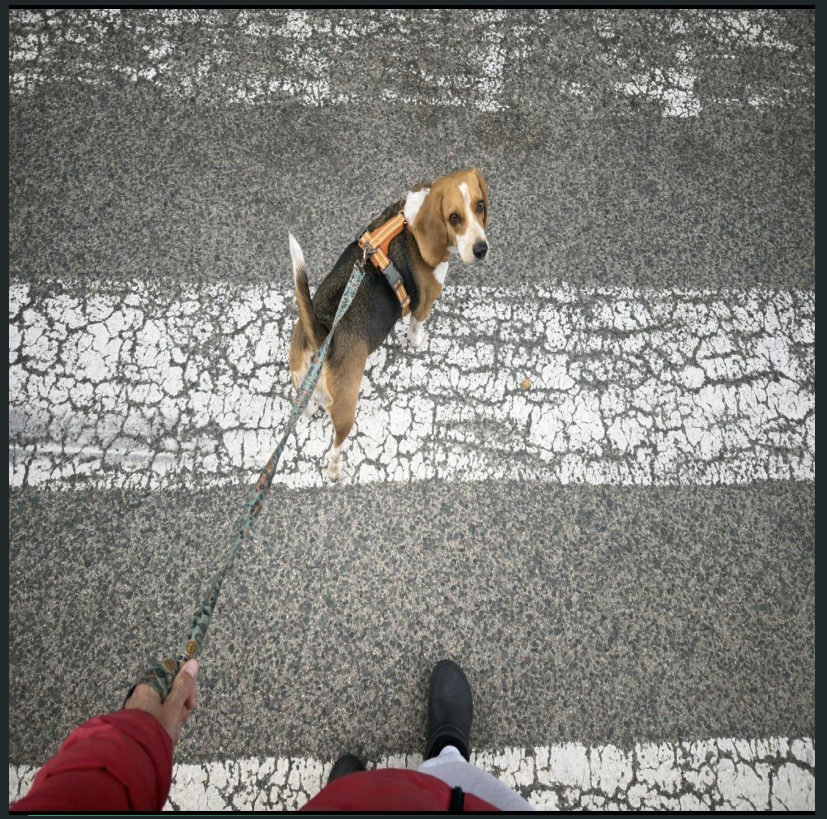
It is the preservation of order across change.

Containment Framework

1. Intent defines

2. Identity binds

3. Systems constrain actions of the actor



Language defines intent.

Traditional systems: documentation described systems.

AI Systems: language shapes systems

The control surface is no longer only code...it is language

Shape the guidance the community will rely on