From Startup to Scale: *Choosing the Right AppSec Path*

A five-year security rollercoaster with Alex

Real story. Real pain. Real pizza.

German OWASP Day 2025

Meet Your Speakers

Vanessa Sutter

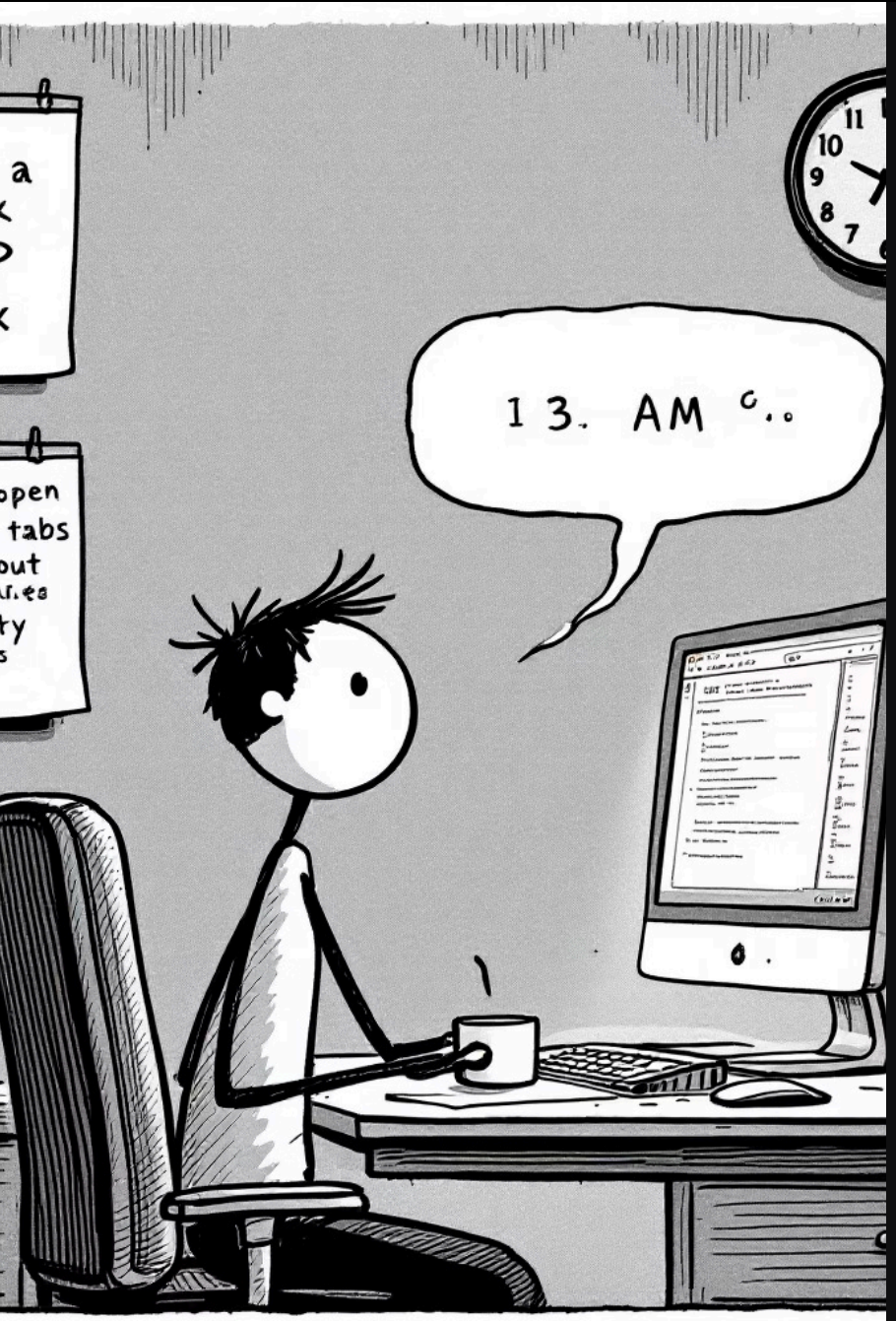
Product Security Lead

Frontify

Javan Rasokat

DevOps Security

Sage



Act I: The Accidental Hero

Alex, fullstack dev, thought fixing a CSP header would be a side quest

Narrator: It was not a side quest

The First Tools

Security Budget

Burp Suite

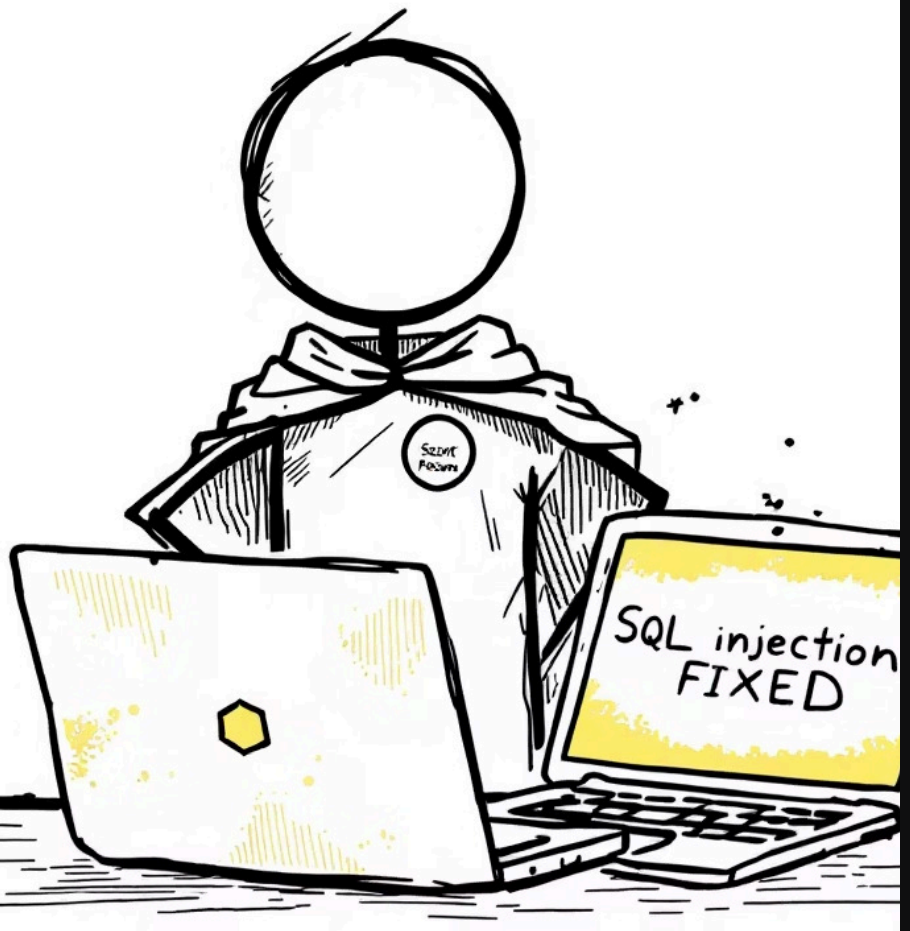
(Community Edition)

+ Free Coffee

from the break room

(the stale kind)

Corporate investment in security: $0.00



Early Wins

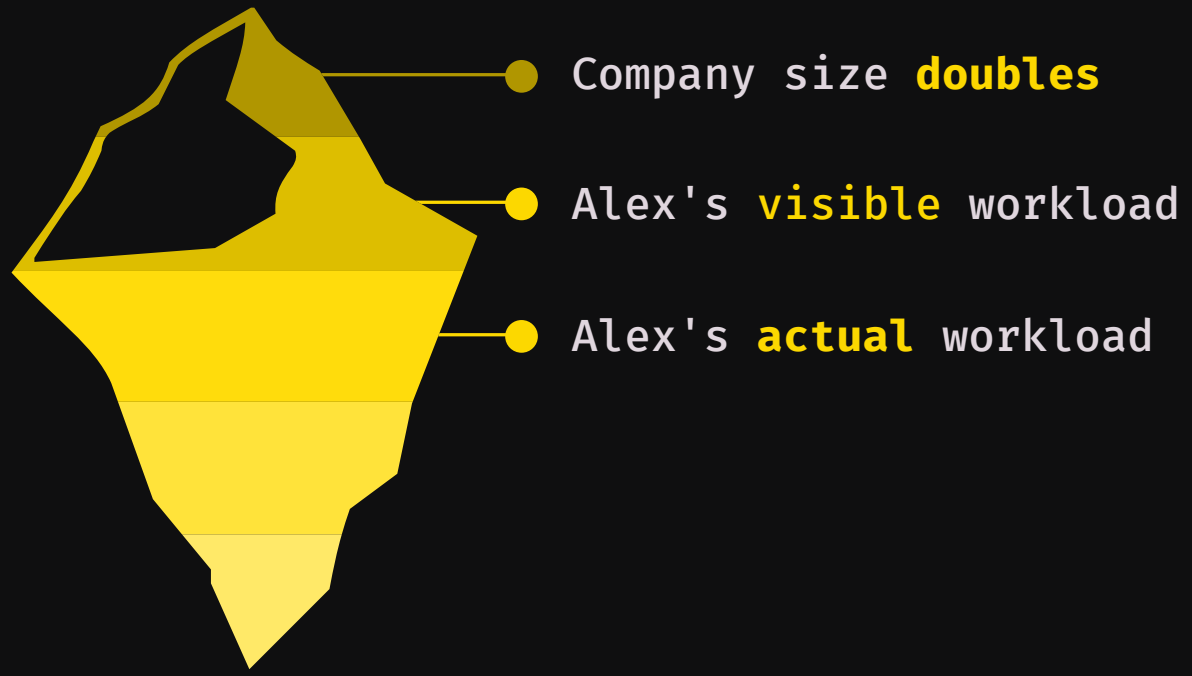
The Patches

- SQL injection: **fixed**
- XSS vulnerability: **patched**
- CSRF tokens: **implemented**

Alex gains title: "The Security Person"

Pride → Recognition → Pressure

Structure is Destiny



> *"Growth's hidden cost: your lone-wolf security model doesn't scale. It shatters."*

The City Metaphor

As your company grows, your security must evolve

Centralized

One lock on the city gate

Embedded

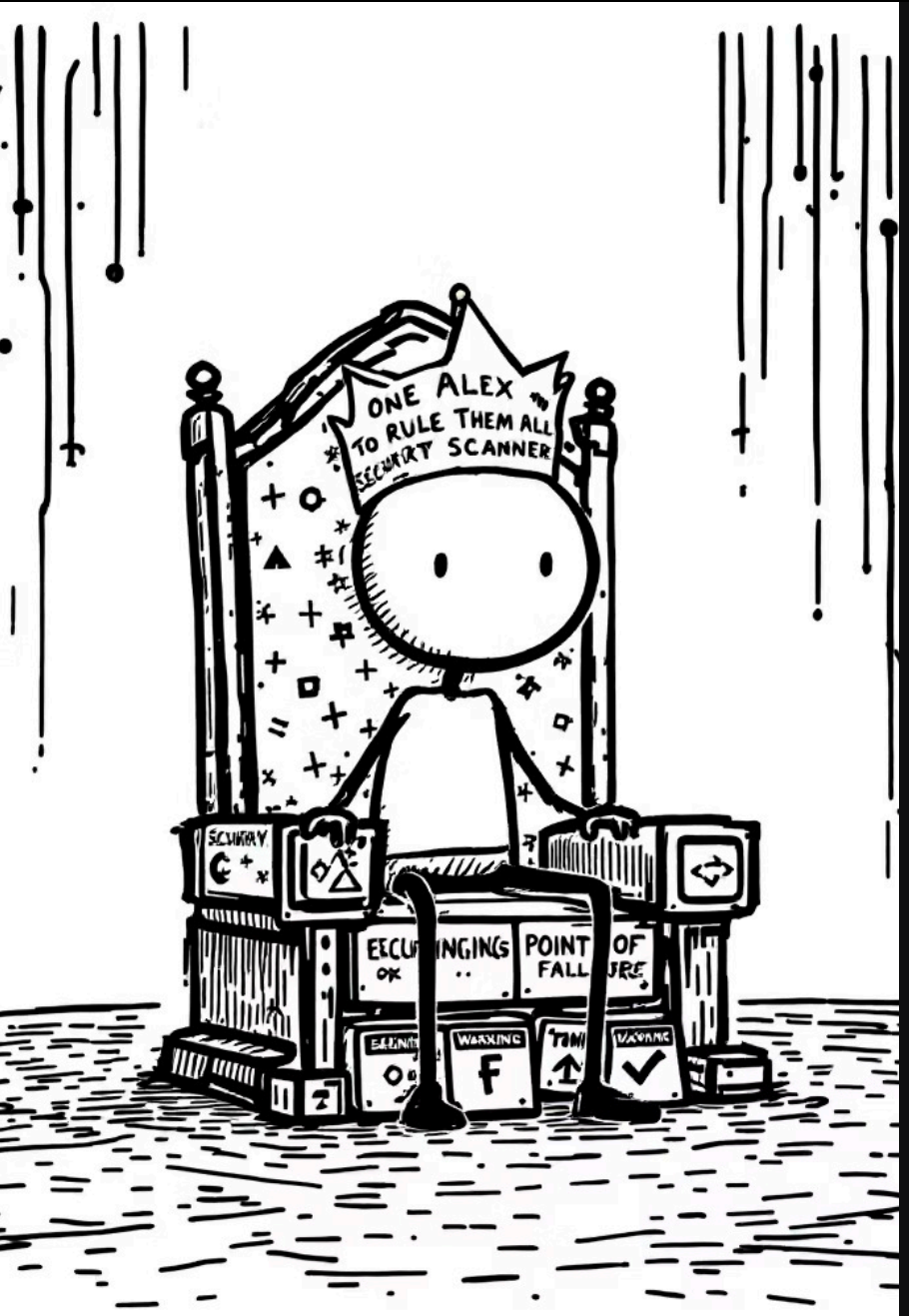
Defenders in every tower

Platform

Self-repairing fortifications

Champions

Architects teaching the city to defend itself



Act 2: One Alex to Rule Them All

Pros ✓

- High control
- Clear ownership
- Consistent decisions
- Hero status

Cons ?

- Zero scalability
- Single point of failure
- Bottleneck incarnate
- Burnout guaranteed

Centralized AppSec: heroic beginnings, tragic endings

Burnout Hits

- **Pager bleeps**

  3 AM vulnerability alert

- **Coffee maker bleeps**

  Empty again (tragic)

- **Balance fails**

  Alex can't keep up

> *"Centralized security: works beautifully until complexity arrives. Then it implodes."*

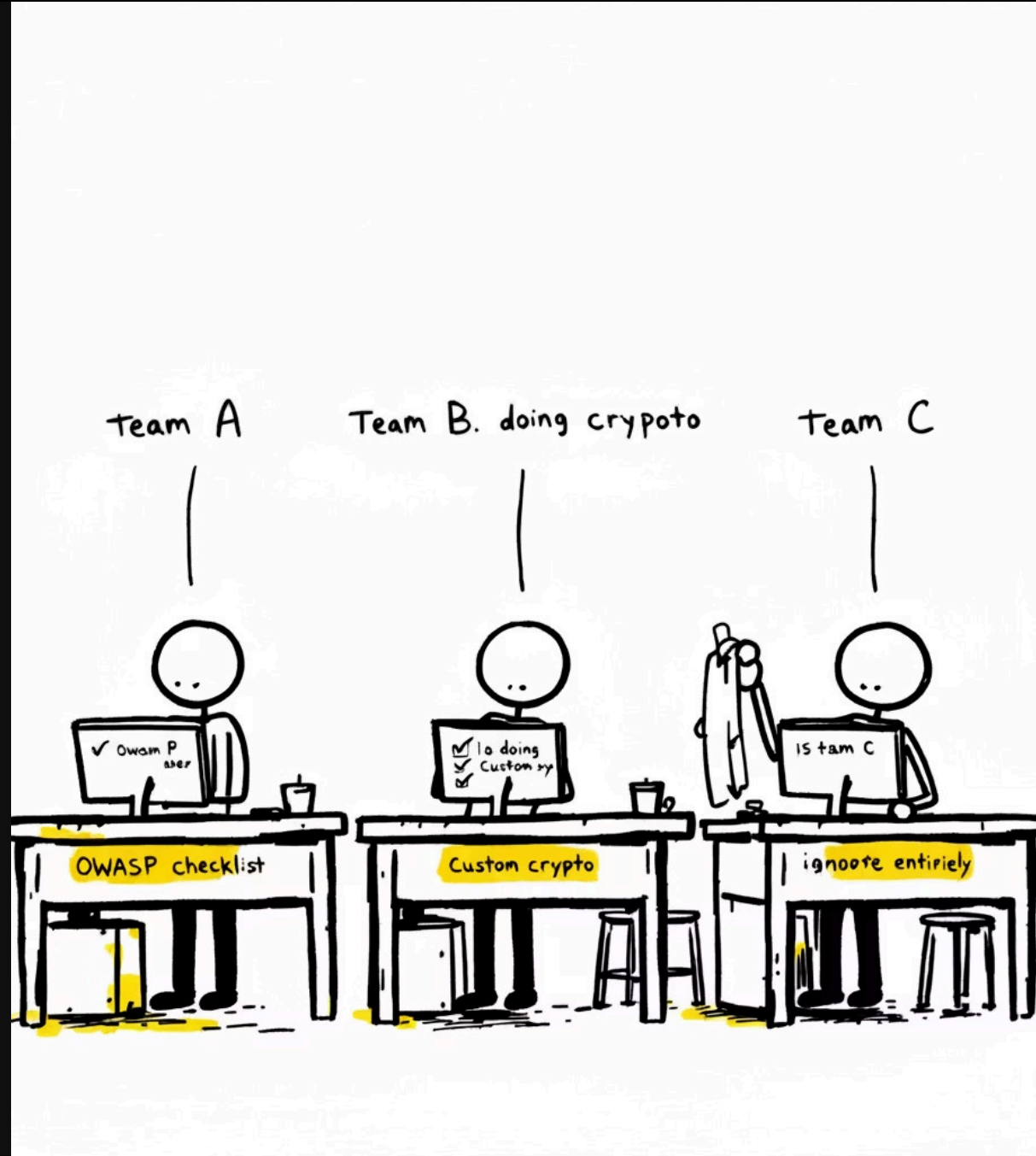
Act 3: Embedded Engineers

Relief arrives (briefly)

Team grows → Security engineers embedded in product teams

- Security closer to dev work
- Faster feedback loops
- Context-aware decisions
- Alignment increases

Hope rises for the first time in months

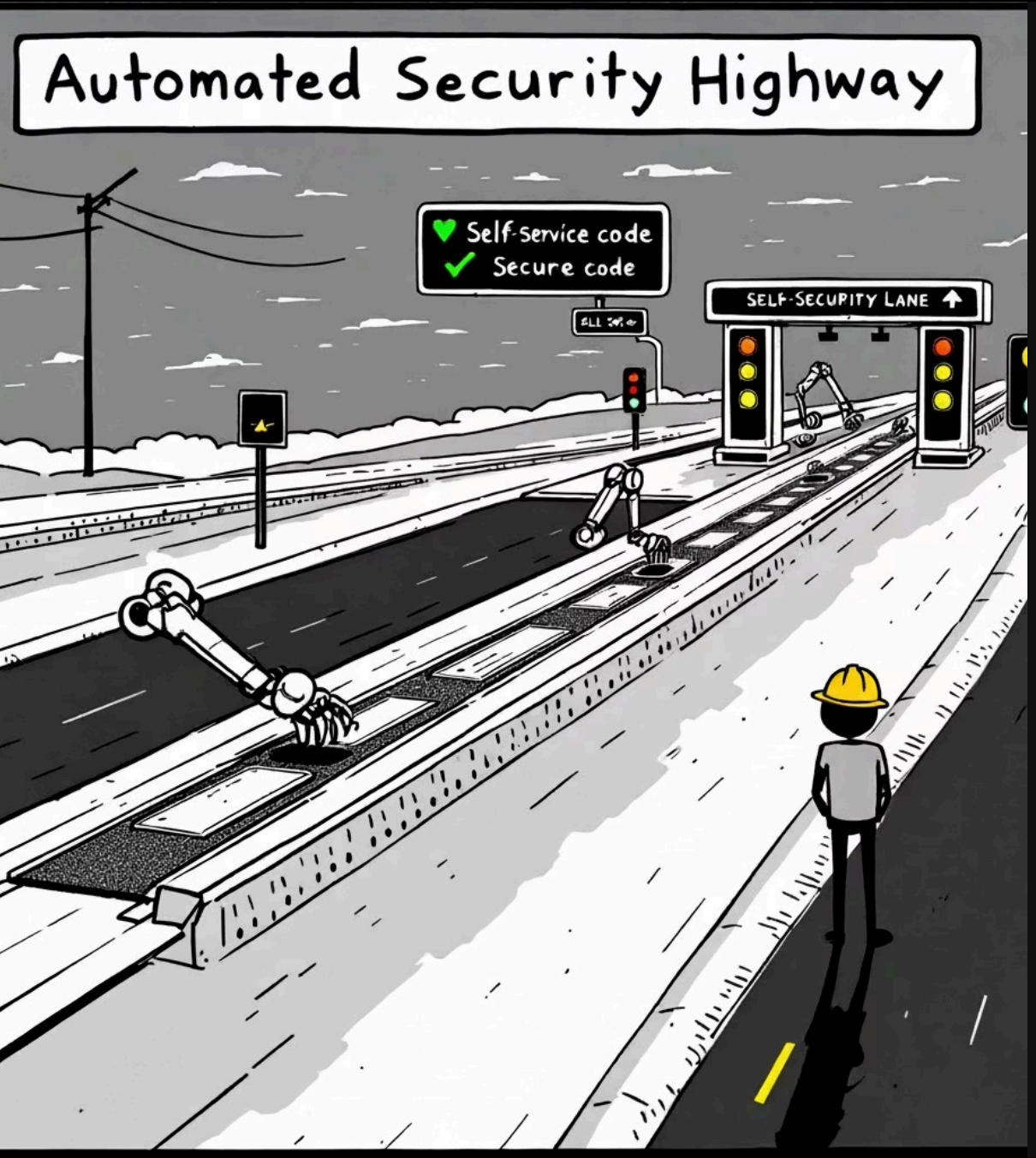


Fragmentation and Chaos

Team A's "Secure"	Team B's "Secure"	Team C's "Secure"
Password complexity rules	Zero trust everything	Whatever ships fastest
OWASP Top 10 checklist	Custom crypto (yikes)	"We'll fix it later"

Security stories compete with features (features win)

Community without consistency = chaos



Act 4: The Perfect Portal

Automate to scale (finally!)

Dashboards

Real-time metrics

Pipelines

Automated scanning

Automation

Self-service tools

Innovation brings hope (again)

The Portal Nobody Uses

Tools exist

But no one looks

Security feels *imposed* not *owned*

Technology failure? No.

Human adoption failure.

Act 5: Trust Beyond Tools

The Champions Network emerges

Step 1

🍕 Pizza party

(recruitment)

Step 2

👕 Hoodies

(incentive)

Step 3

📚 Free training

(enablement)

Champions as a Force Multiplier

Pros ✓

- Broad reach across teams
- Early threat detection
- Product ownership mentality
- Scales with company

Cons ?

- Quality varies wildly
- Needs ongoing support
- Champions need champions
- Time investment required

Empowerment replaces exhaustion

Reality Is Messy

Hybrid models: the only honest approach

Centralized

Core policy

Incident response

Champions

Cultural change

Distributed ownership

Embedded

Team expertise

Deep context

Platform

Automated tools

Self-service

No perfect model. Just the right model for right now.

Metrics and Trust

Key to scaling security

<24h

MTTR

Mean time to resolution

87%

Coverage

Services with security scans

142

Champions

Active security advocates

94%

Adoption

Teams using security tools

Trust matters more than automation alone

What Alex Wishes He Knew Earlier

Topology mutates

Devs are the key

Automate pain, not process

Support champions properly

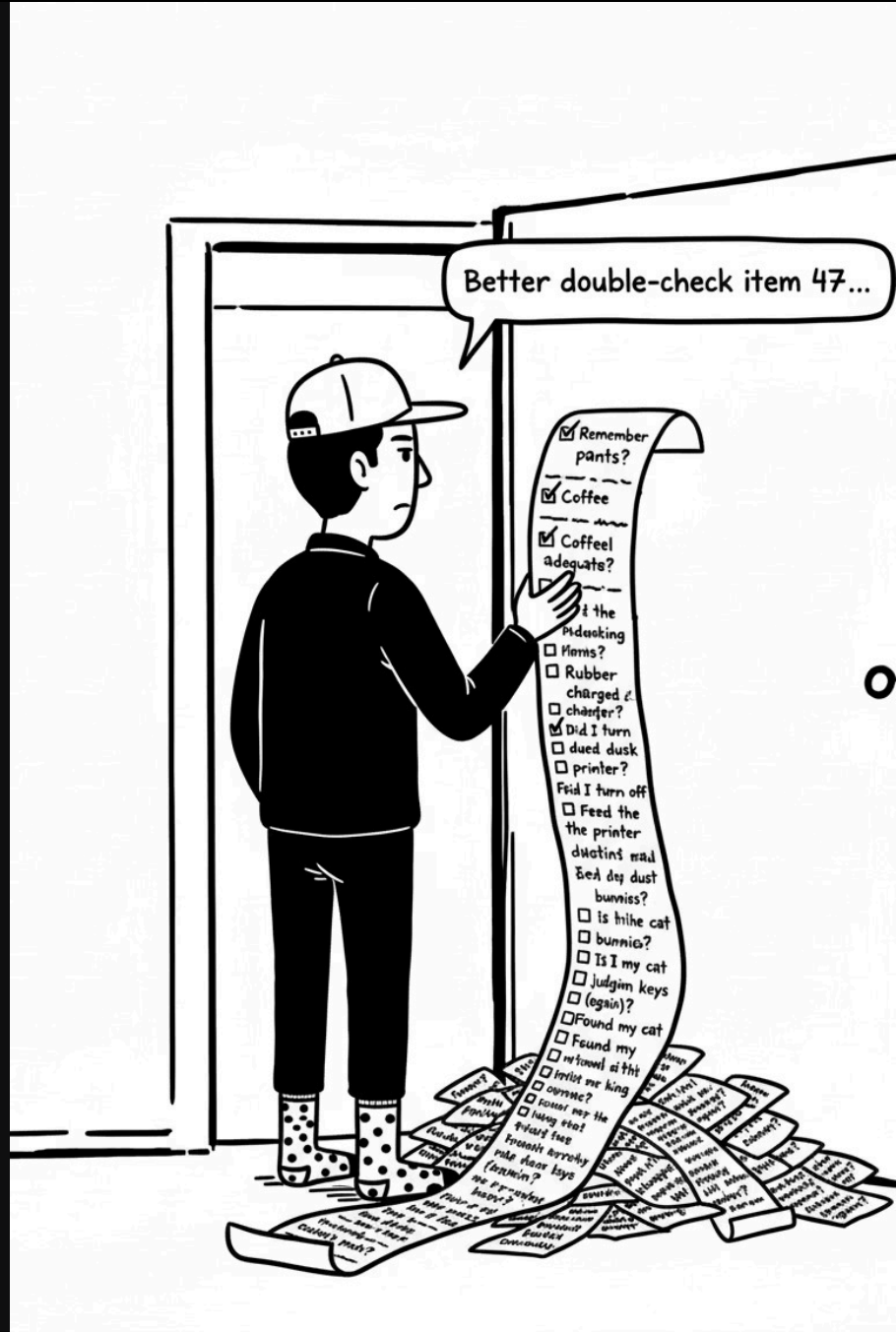
Culture grows slow

Advice for New Hires

Questions to ask before accepting that AppSec role

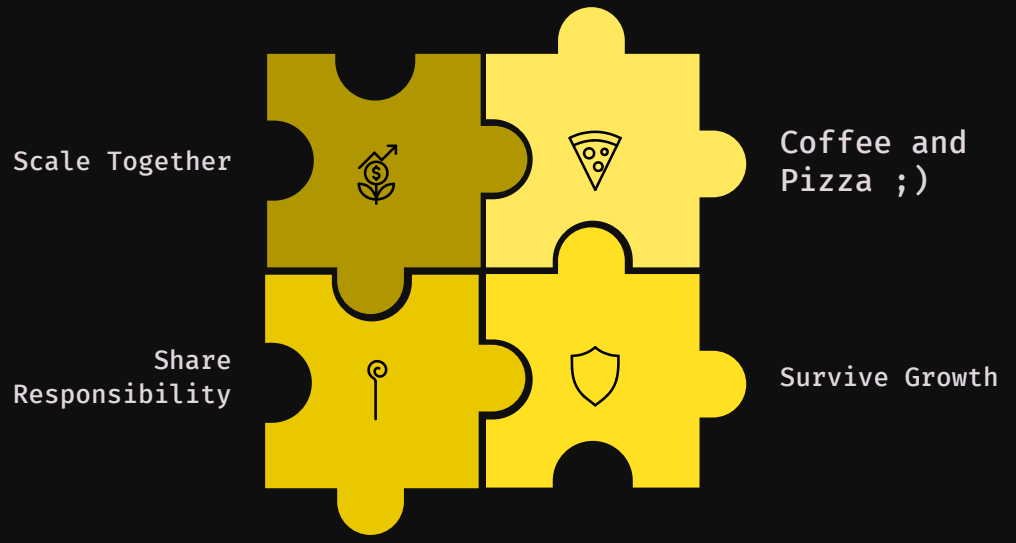
- What's the current **security topology**?
- How fast is the company scaling?
- Who builds the security platform?
- What **metrics** define success?
- Is there free coffee? (critical)

Savvy newcomers avoid pitfalls



AppSec Isn't a Department

It's a Strategy



> *"Security is everyone's job. But someone needs to buy the pizza."*
>
> — Alex

Key Takeaways

Surviving SaaS growth without losing your mind

- Right-size your model
- Automate the pain
- Build allies

Survival over perfection


Thanks for Riding the Roller Coaster with us