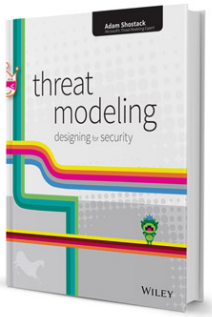
The B-MAD Approach to Threat Modeling

Adam Shostack

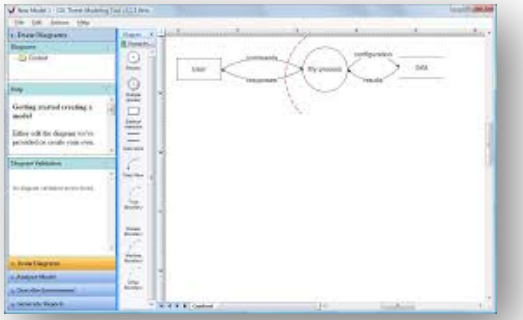
About Adam Shostack



Shostack & ASSOCIATES

https://associates.shostack.org

IriusRisk



Agenda

- Conflict between security and other teams
- Threat modeling
- The B-MAD approach

Security Teams and Conflict

Intro story

There’s a pattern here

- Security vs operations
- Security vs engineering
- Security vs the business

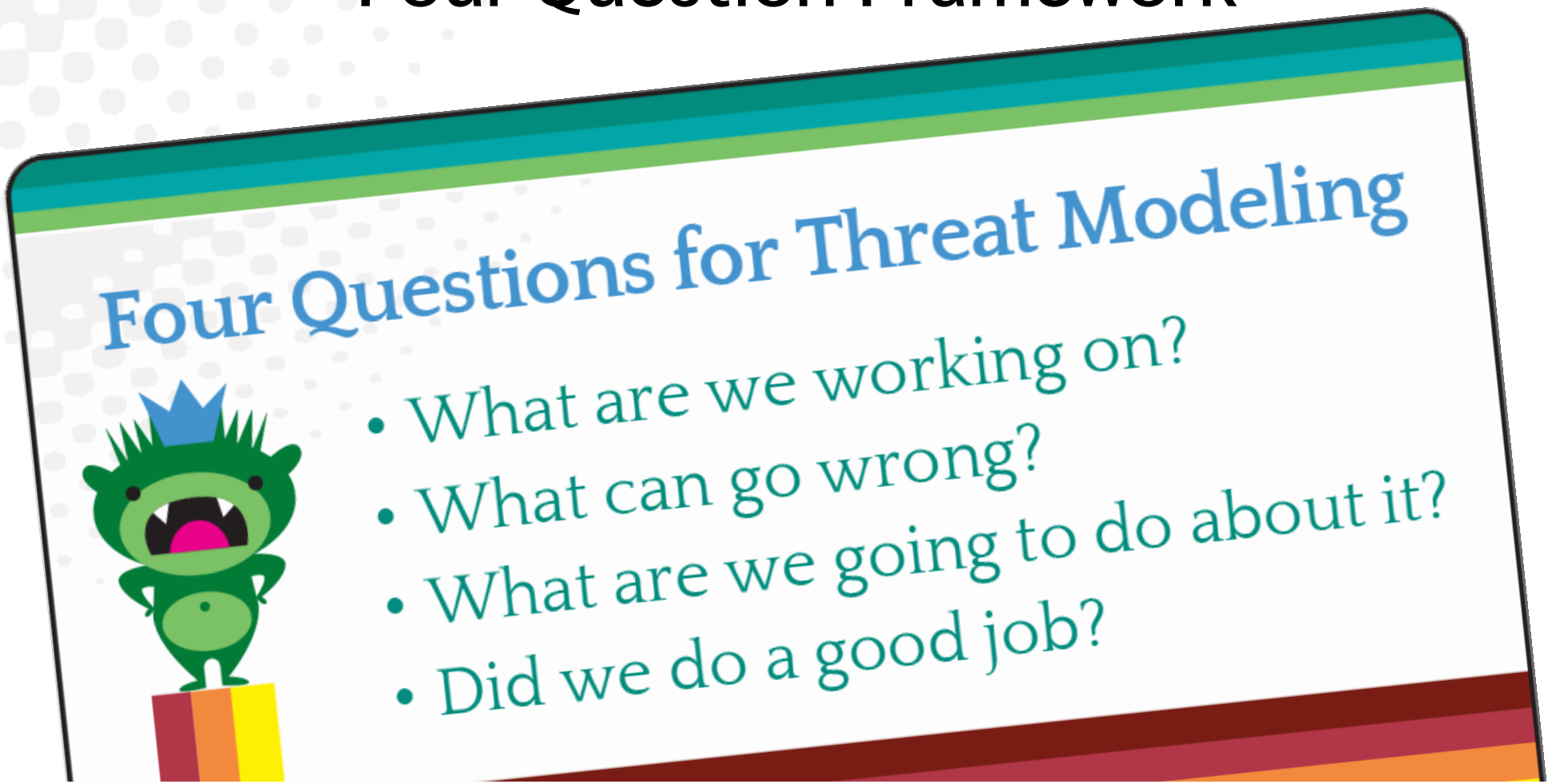
“Your failed relationships have one thing in common…”

Threat modeling

Introduction to threat modeling

- What is threat modeling?
- Threat modeling & threat intel
- Threat modeling is easy

Four Question Framework



STRIDE mnemonic

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges

... Helps us bring structured to “what can go wrong”

Threat modeling is full of traps

OMG SO MANY TRAPS

- This talk is about a clever trap that keeps getting us

The Jenga Model of threat modeling

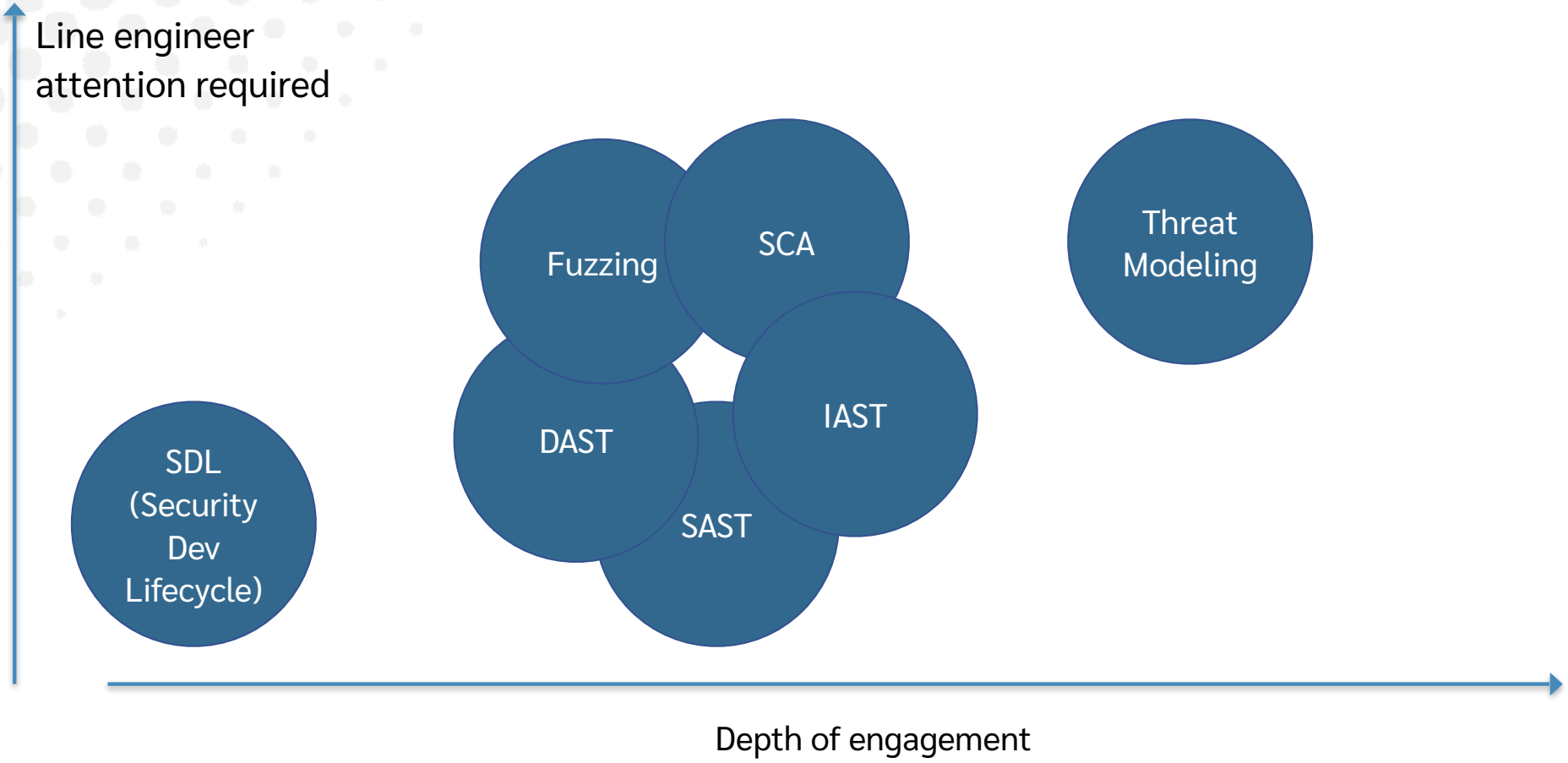
- Block types
  - Technical skills
  - Interpersonal skills
  - Organizational discipline

White paper at associates.shostack.org/whitepapers

This talk is “organizational”

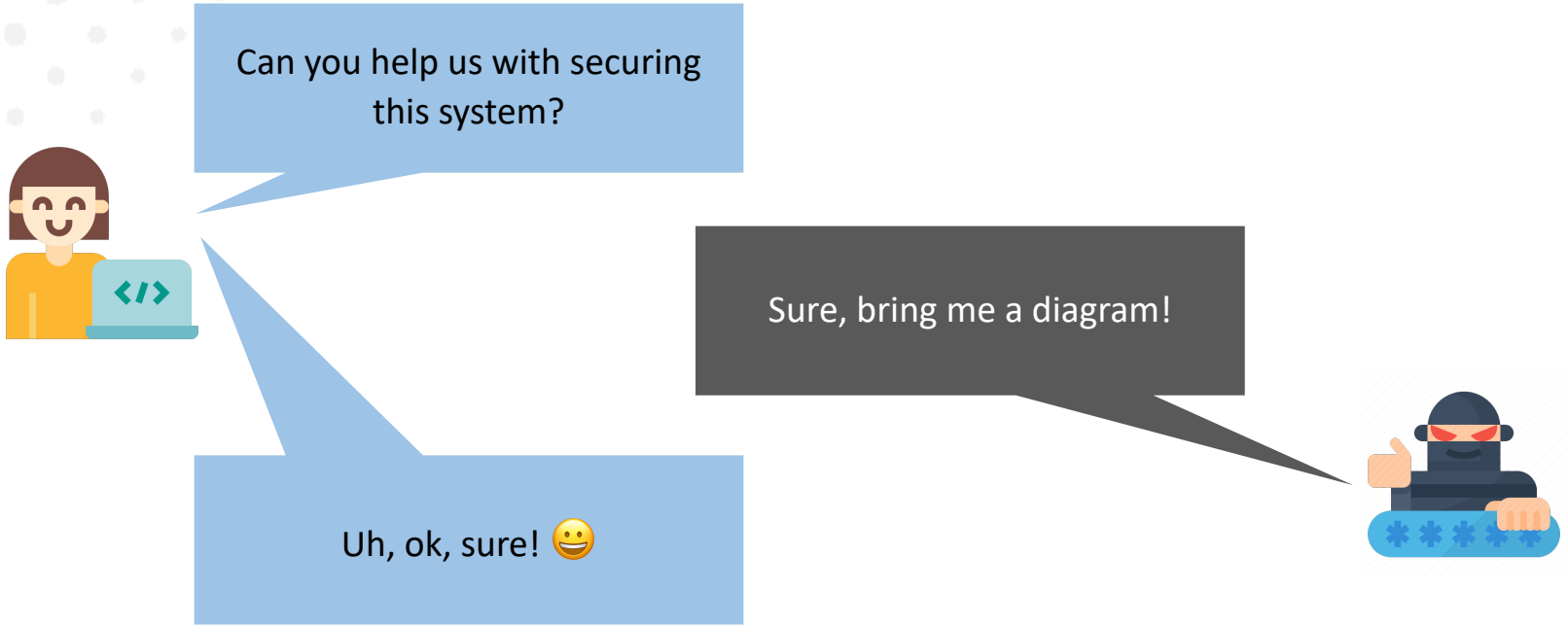
- It’s about conflict
- This conflict emerges from good intent
- Over and over

Software security tooling

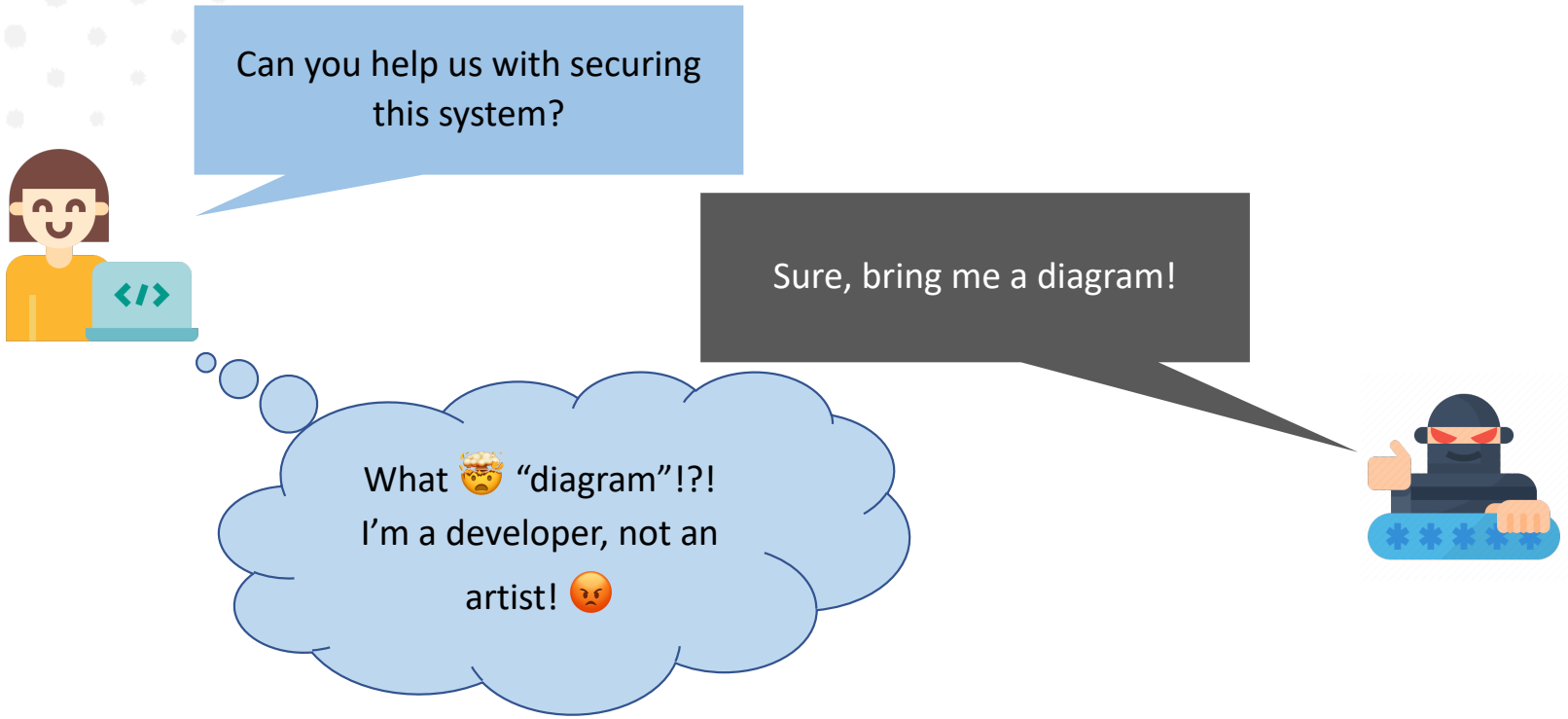


How B-MAD Causes Problems

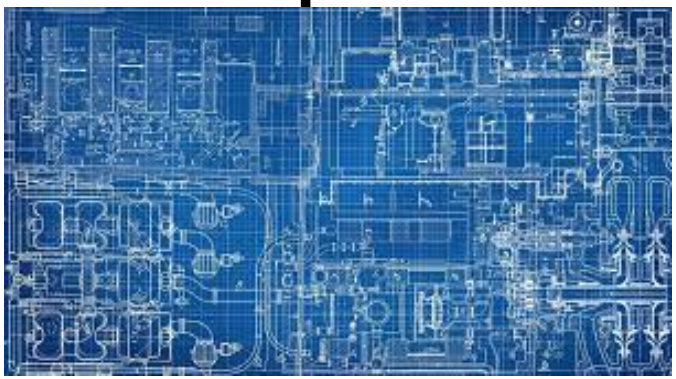
The B-MAD problem: developer view



B-MAD: developer view 2



The B-MAD problem: developer view 3



Hi, look, I made you a comprehensive design diagram!

Waaaaa?

STOP SHIP!
Let me tell you about the design flaws.

B-MAD: security team view

Can you help us with securing this system?

Can you help us with securing this system?

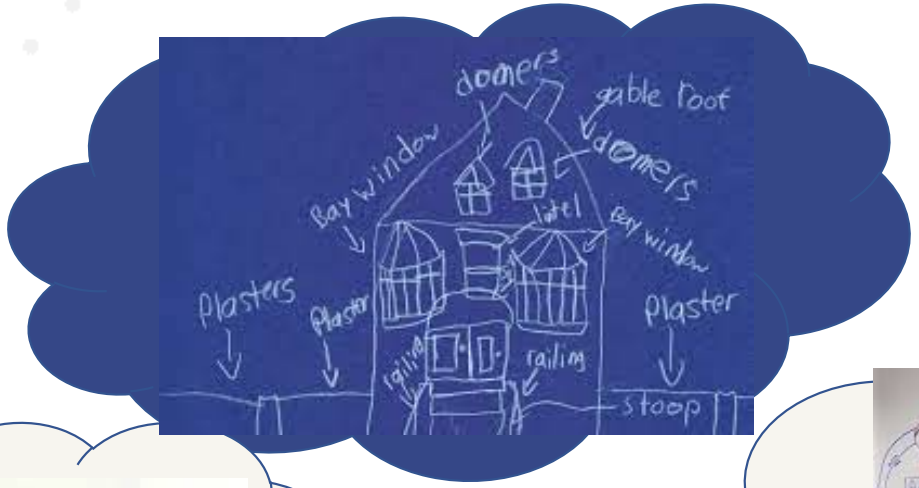
Can you help us with securing this system?

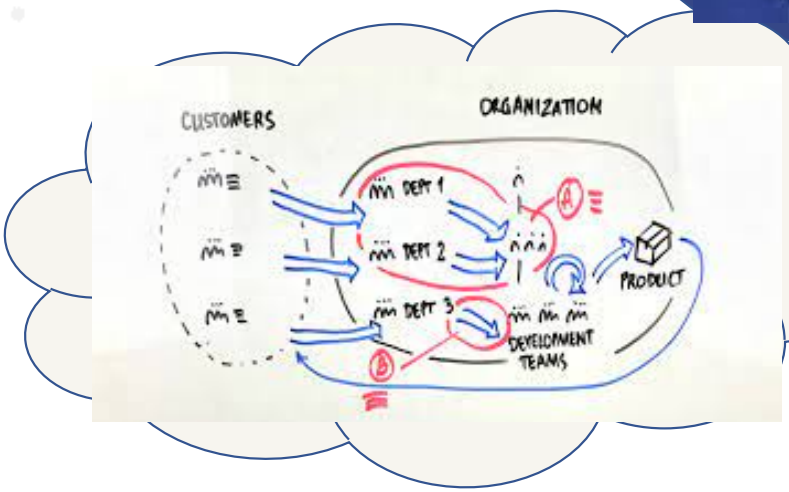
Bring me diagrams!

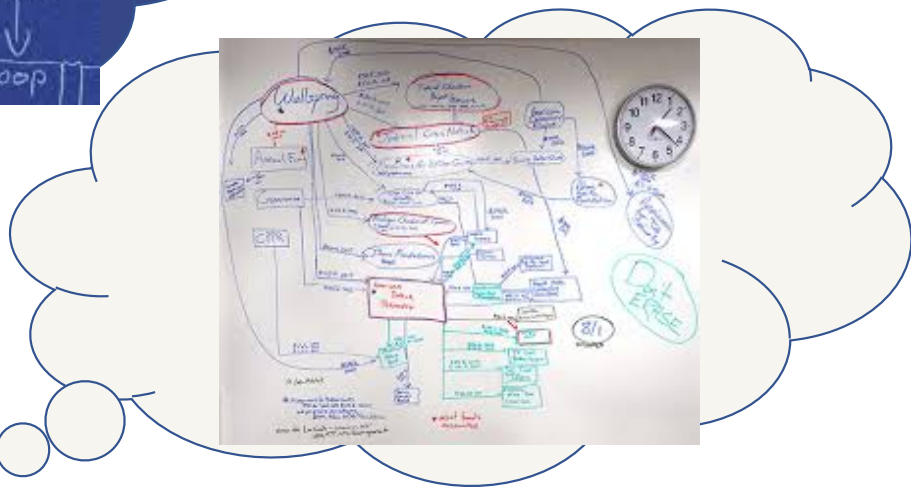
“I’m waiting!”

The B-MAD problem: security team view 2

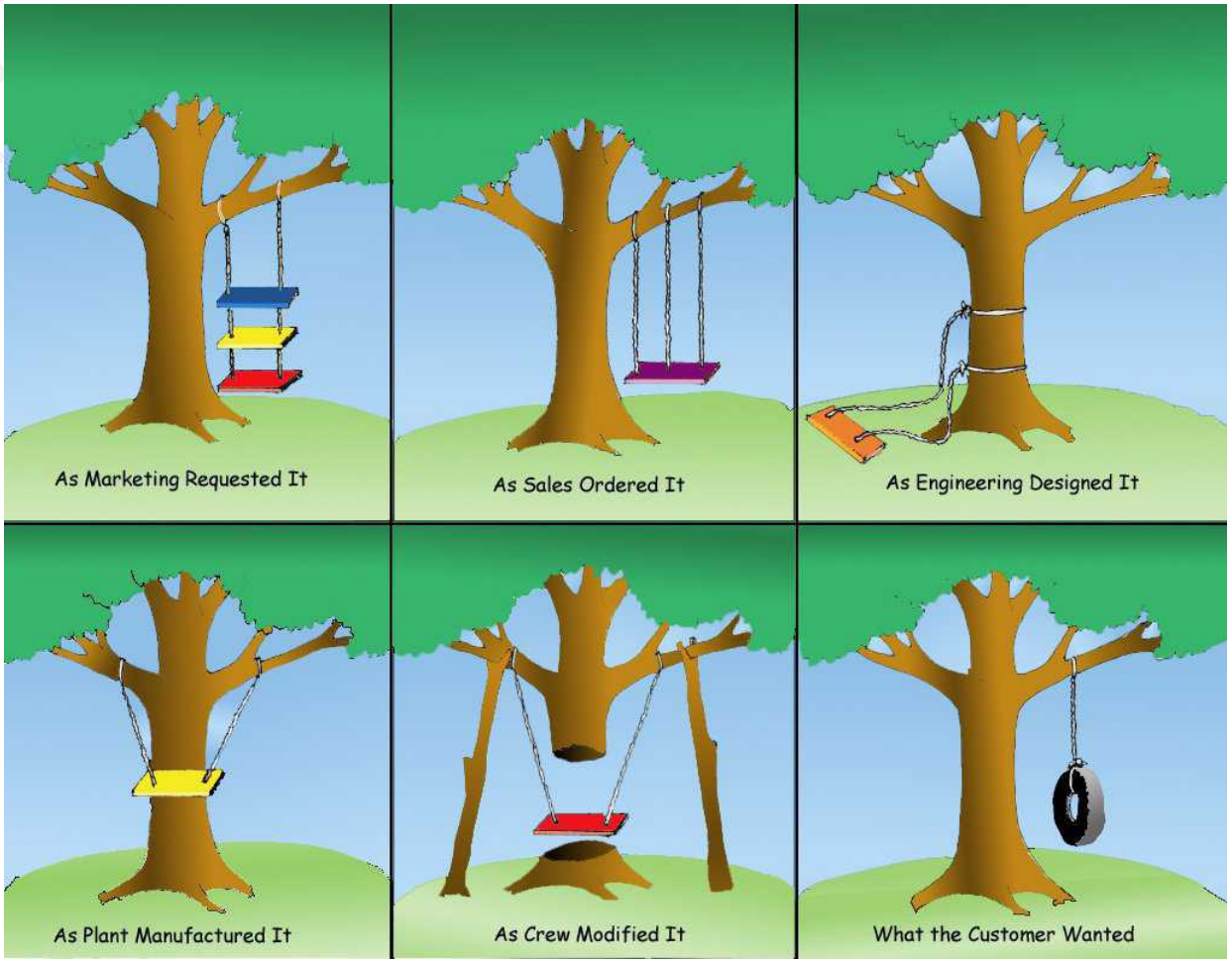
The diagrams security wants







“A failure to communicate”



So what's happening?

B-MAD: “Bring Me A Diagram!”

Can you help us with securing this system?

Can you help us with securing this system?

Bring me a diagram!

“I’m waiting!”

Contributors to the problem

- Security teams are highly loaded
  - Especially the unicorn appsec folks with design experience
- Security teams are learning about threat modeling
  - Lack practical experience
  - Also, some advice doesn't include retrospectives
- Development teams are getting more and more agile

Avoiding B-MAD

Technical

- How do we talk about ”what are we working on?”
  - Whiteboard threat modeling
  - TM every story (Izar Tarandach has talks on this)
  - Big Wall Maps (next slide)
- Deliverables
  - Samples
  - Align to the Four Question Framework, not threat modeling
- Measure skills in teams
  - Does security have more design skills or pen test skills?
  - Does dev or ops have security skills?

Big Wall Maps (Technical, continued)

- Large system maps to enable shared awareness
  - Wall space in offices is limited
  - Walk by
- “My story changes/doesn’t change this diagram”

Organizational

- Who delivers what to whom?
  - Some deliverables, like system models, may be collaborative
- Is “early and often” a win or a waste?
- How much design work can security team do?
  - Measure # of engagements
  - Time per engagement
  - Set reasonable goals
- How does that balance with other tasks?
  - High value work

Interpersonal

- Communicate expectations
  - Design collaboration or design review?
- Make it part of every meeting kickoff
  - “This is a collaborative working meeting to develop a system model. We’ll work through what can go wrong a bit here, and in more detail later.”
  - “This is a design review meeting, and 8 of 10 have no stop-ship issues.”

Thank you

adam@shostack.org

Shostack
& ASSOCIATES
https://associates.shostack.org

Resources

- threatmodelingmanifesto.org
- associates.shostack.org/whitepapers (Jenga white paper)