How to make security shut up

(without getting fired)

Byron Pogson
hello@bpog.cloud

www.bpog.cloud

PLATINUM SPONSORS

MAKERX

PATIENT ZERO

GOLD SPONSORS

SKAO

aws

Qoria

Microsoft

VERSENT

Octopus Deploy

VGW

DIGITAL SPONSORS

AFG

UWA DATA INSTITUTE

Keystart.

WA DATA SCIENCE INNOVATION HUB
Powering an AI Future

AKKODIS

Insight

ROOM SPONSORS

interfuze.
Seriously good technology consultants.

software one

PERTH COMMUNITY

HELLO INITIATIVE.

BUILD CLUB

breast cancer partners

SHE{CODES}

Bloom

WAITTA

Hello, I’m Byron

- Developer and solution architect
- 8 years at Amazon Web Services
- Accidental security person
- Security champion at AWS

Confession: security conferences make me question working in security

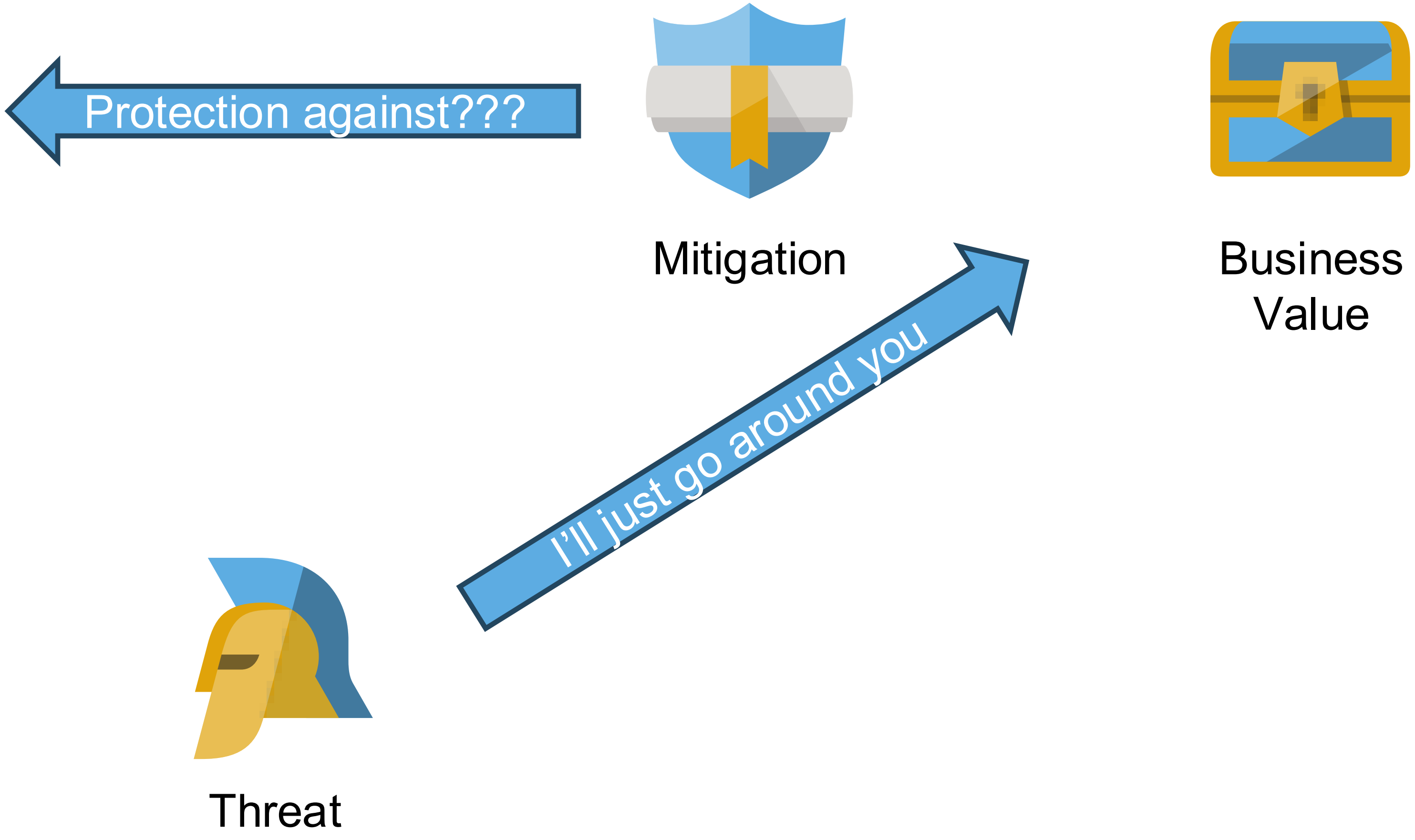
Bla bla bla bad people etc

Threat

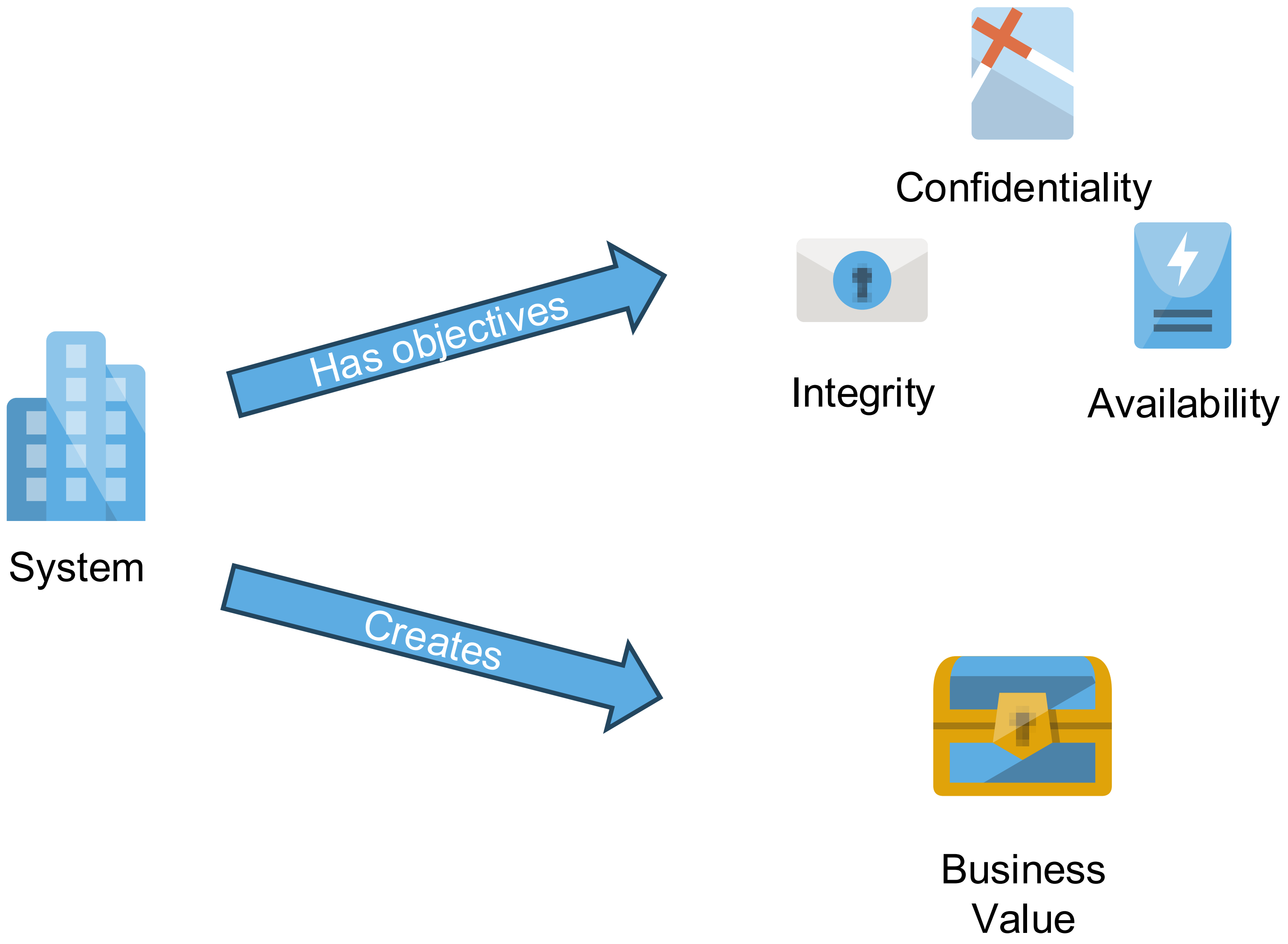
???

Excuse me sir, this is a Wendy’s

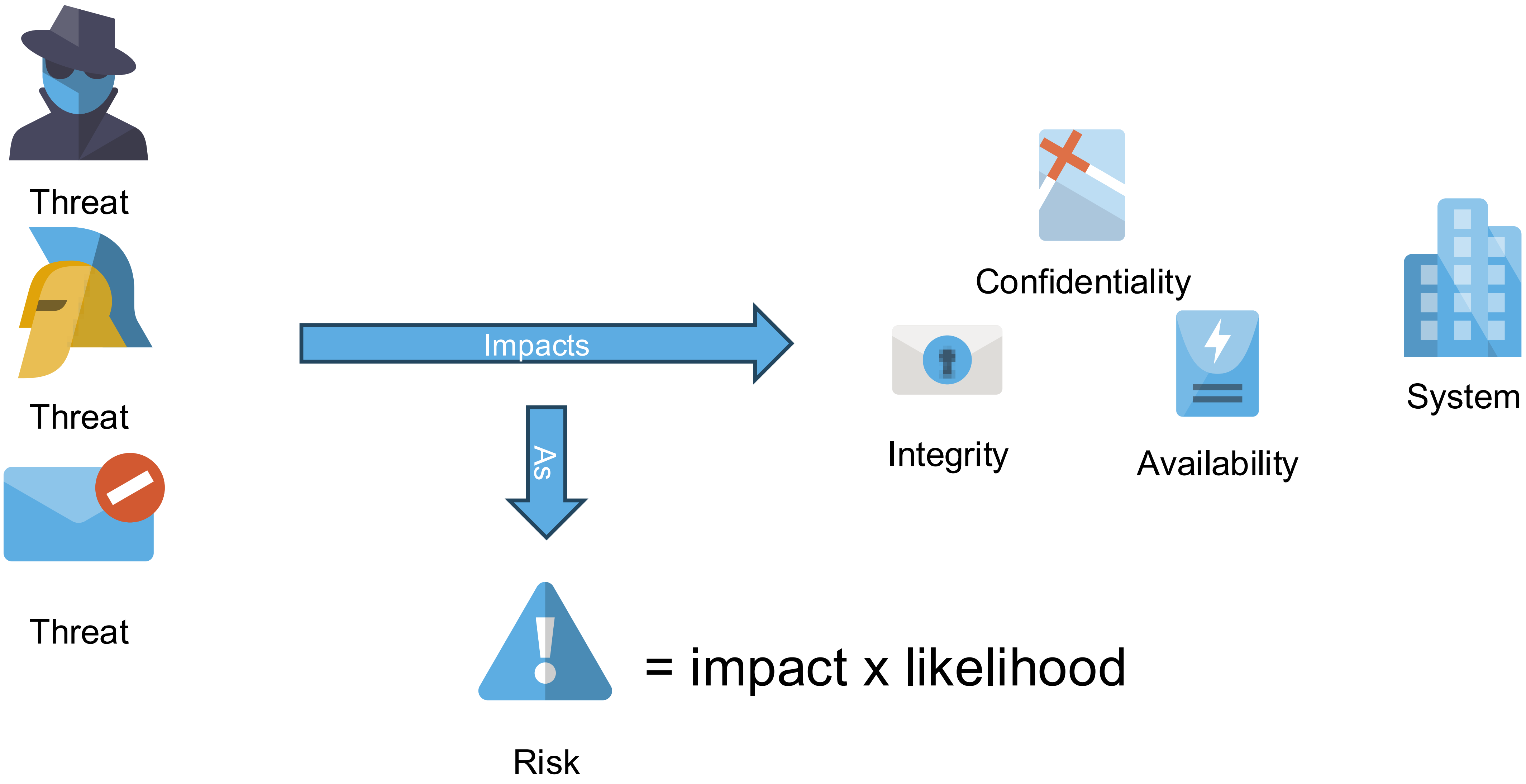
Do this because I said so



Information security 101



Information security 101



Threat

Threat

Threat

Impacts

As

Confidentiality

Integrity

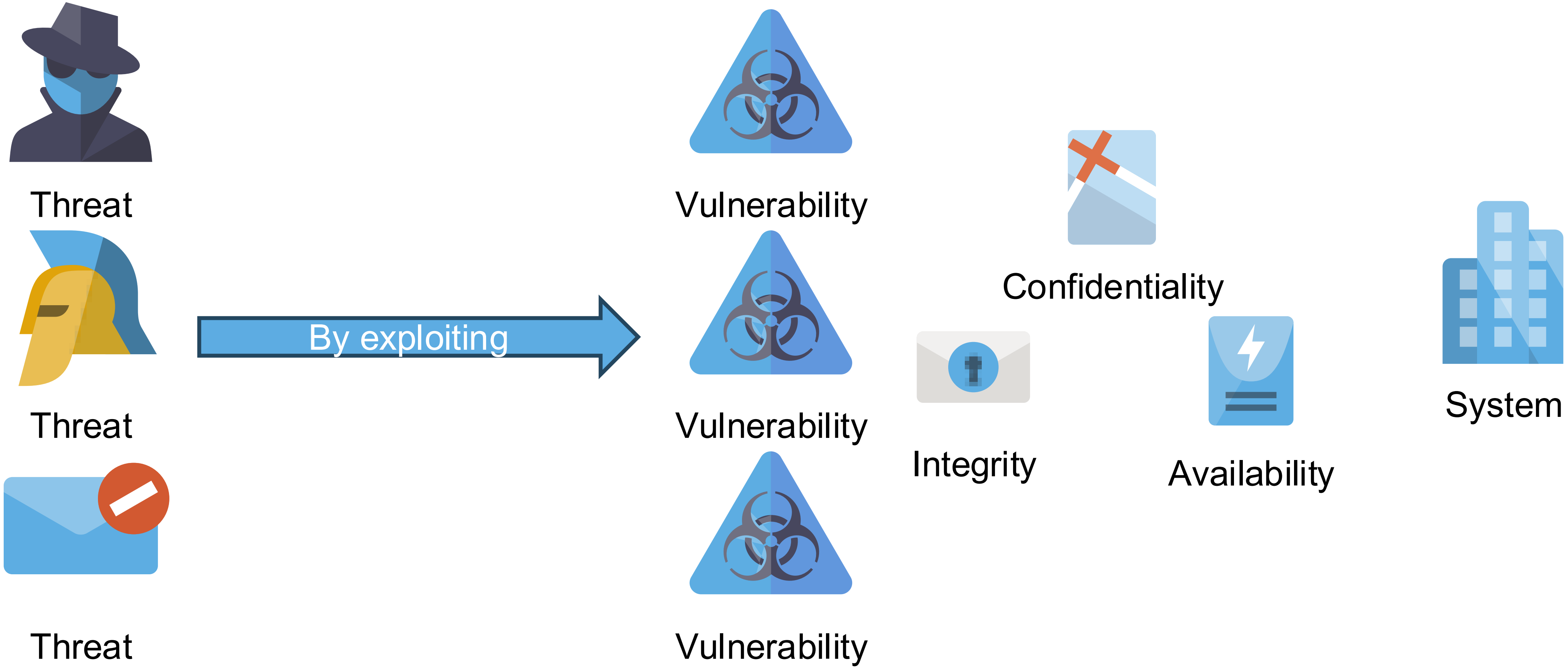
Availability

System

Risk

= impact x likelihood

Information security 101



Threat

Threat

Threat

By exploiting

Vulnerability

Vulnerability

Vulnerability

Confidentiality

Integrity

Availability

System

Information security 101

Threat

Threat

Threat

Mitigation

Mitigation

Mitigation

Vulnerability

Vulnerability

Vulnerability

Confidentiality

Integrity

Availability

System

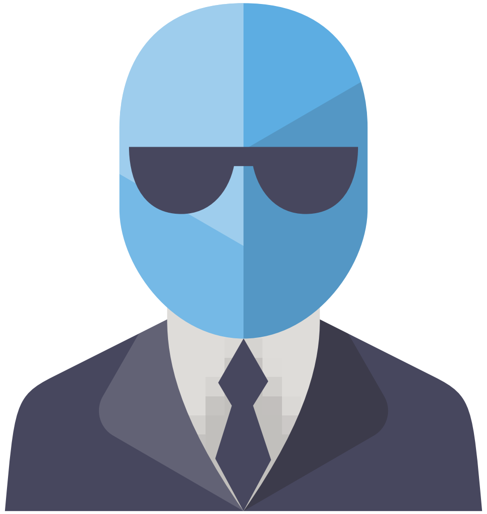
Thank you!

Do you have any questions?

hello@bpog.cloud

www.bpog.cloud

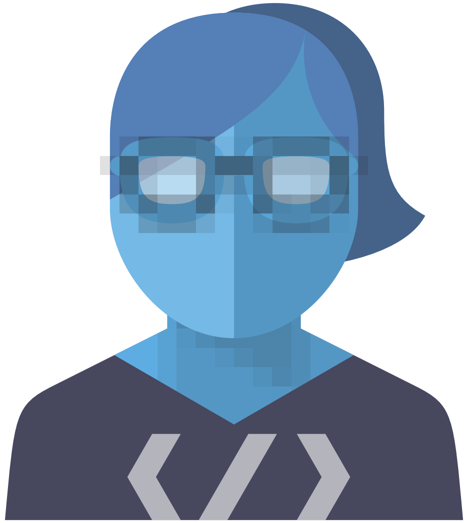
Security/development disconnect



Security

We want to protect the business but don't know the application

We know what we're building, we're not intentionally making it insecure



Development

THREAT MODELING MANIFESTO

- The best use of threat modeling is to **improve the security** and privacy of a system through early and **frequent analysis**
- Threat modeling must **align with an organization's development practices** and follow design changes in iterations that are each scoped to manageable portions of the system
- The outcomes of threat modeling are meaningful when they are **of value to stakeholders**
- **Dialog** is key to establishing the common understandings that lead to value, while documents record those understandings, and enable measurement

https://www.threatmodelingmanifesto.org/

Four key questions

What are we working on?

What can go wrong?

What are we going to do about it?

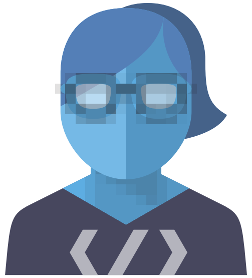
Did we do a good job?

But I don’t know how!

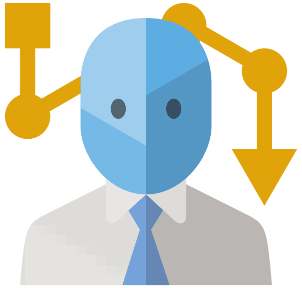
Threat modeling is natural

There’s no such thing as an incorrect model.

Get started: assemble a team



Development

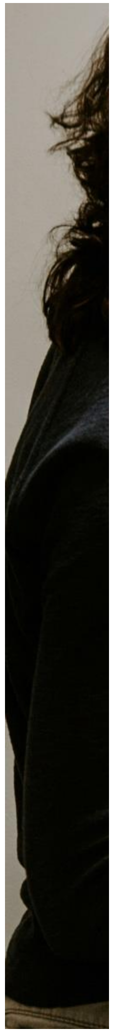


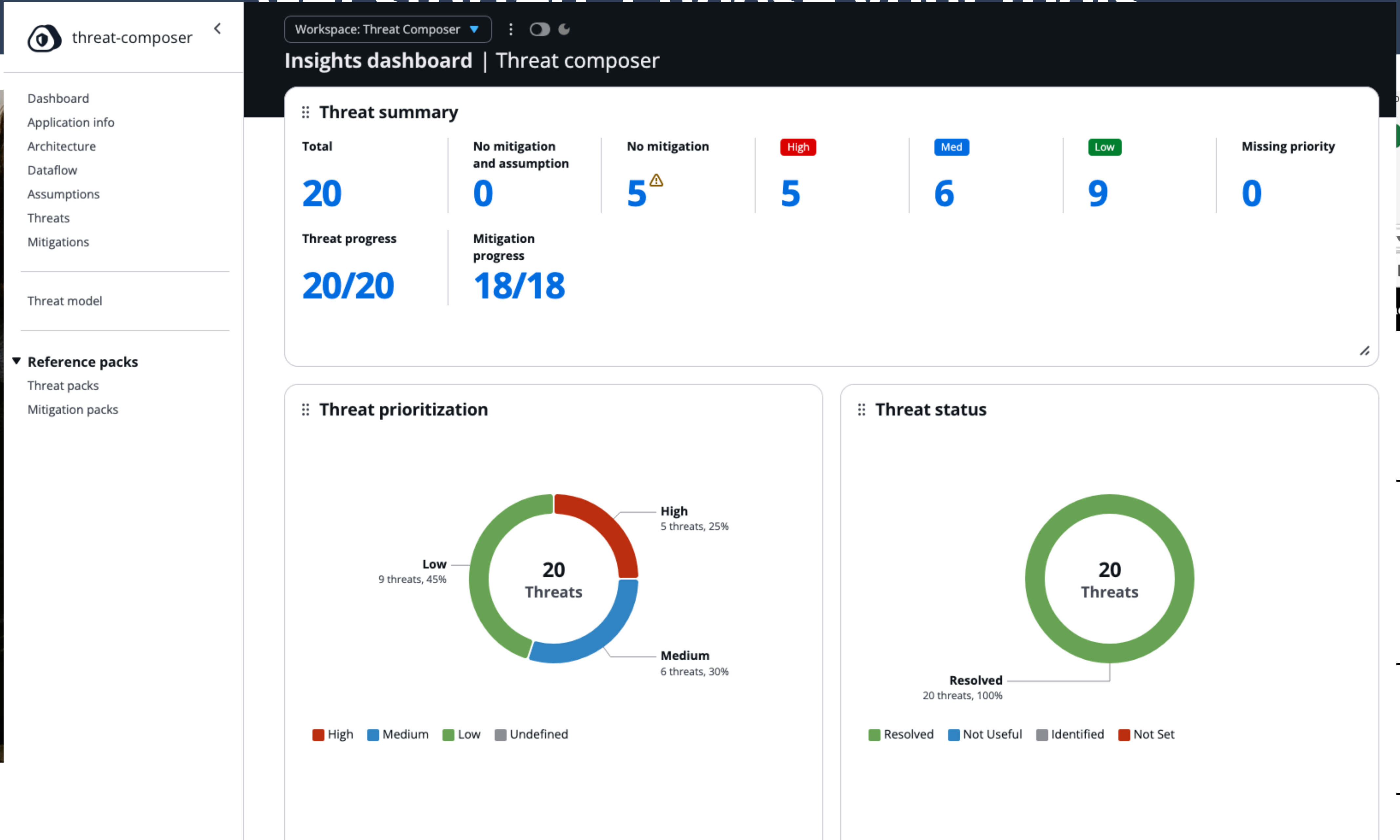
Operations

Product management

Security

Get started: choose your tools





threat-composer

- Dashboard
- Application info
- Architecture
- Dataflow
- Assumptions
- Threats
- Mitigations

Threat model

▼ **Reference packs**

- Threat packs
- Mitigation packs

Workspace: Threat Composer ▼

Insights dashboard | Threat composer

Threat summary

Total	No mitigation and assumption	No mitigation	High	Med	Low	Missing priority
20	0	5 ⚠	5	6	9	0

Threat progress	Mitigation progress
20/20	18/18

Threat prioritization

Threat status

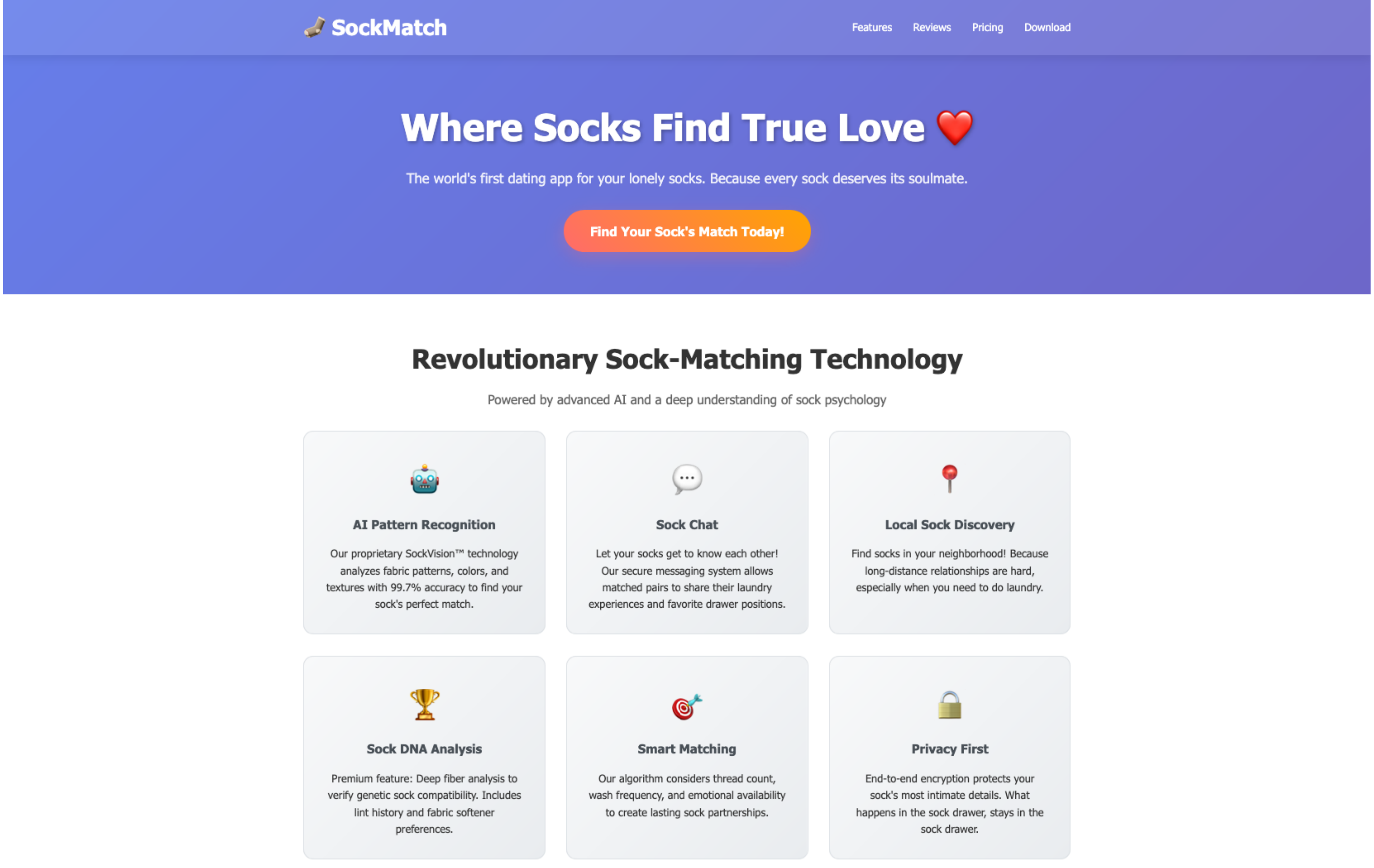
Four key questions

What are we working on?

What can go wrong?

What are we going to do about it?

Did we do a good job?



Where Socks Find True Love ❤️

The world's first dating app for your lonely socks. Because every sock deserves its soulmate.

Revolutionary Sock-Matching Technology

Powered by advanced AI and a deep understanding of sock psychology

🤖

AI Pattern Recognition

Our proprietary SockVision™ technology analyzes fabric patterns, colors, and textures with 99.7% accuracy to find your sock's perfect match.

💬

Sock Chat

Let your socks get to know each other! Our secure messaging system allows matched pairs to share their laundry experiences and favorite drawer positions.

📍

Local Sock Discovery

Find socks in your neighborhood! Because long-distance relationships are hard, especially when you need to do laundry.

🏆

Sock DNA Analysis

Premium feature: Deep fiber analysis to verify genetic sock compatibility. Includes lint history and fabric softener preferences.

🎯

Smart Matching

Our algorithm considers thread count, wash frequency, and emotional availability to create lasting sock partnerships.

🔒

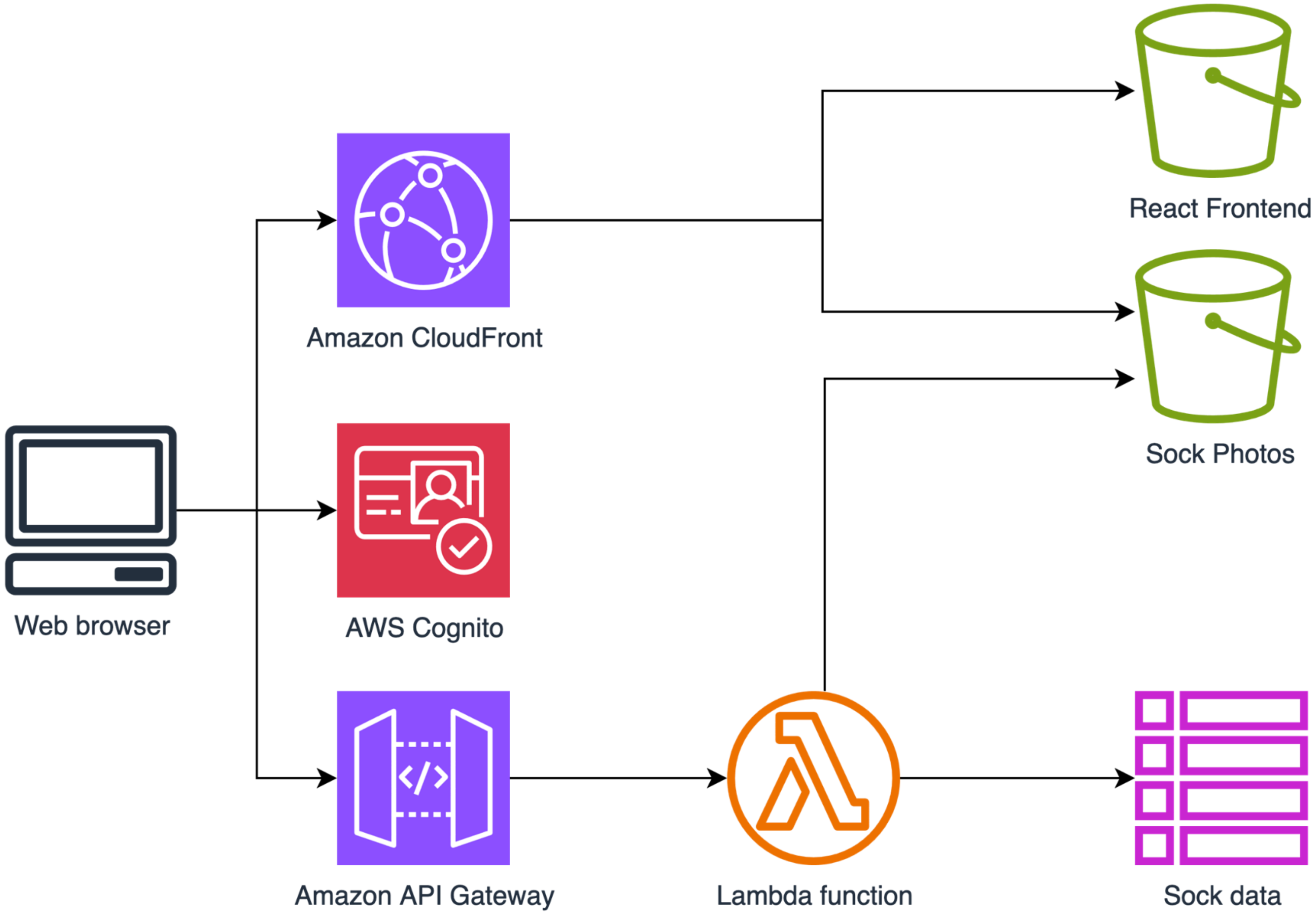
Privacy First

End-to-end encryption protects your sock's most intimate details. What happens in the sock drawer, stays in the sock drawer.

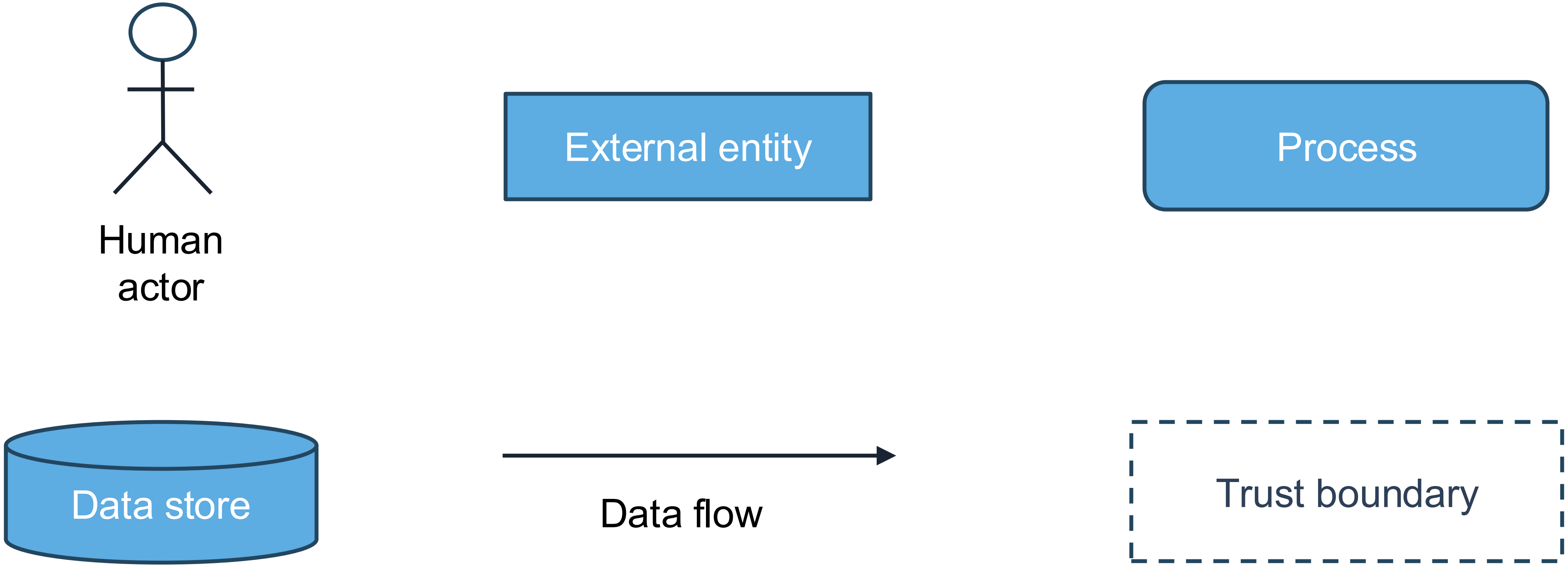
Tip: Scope your problem

- Decompose the problem
- Align to software development lifecycle
- Think about similar systems
- Reuse and start a threat library

Tinder for socks



Data flow diagrams



Human actor

External entity

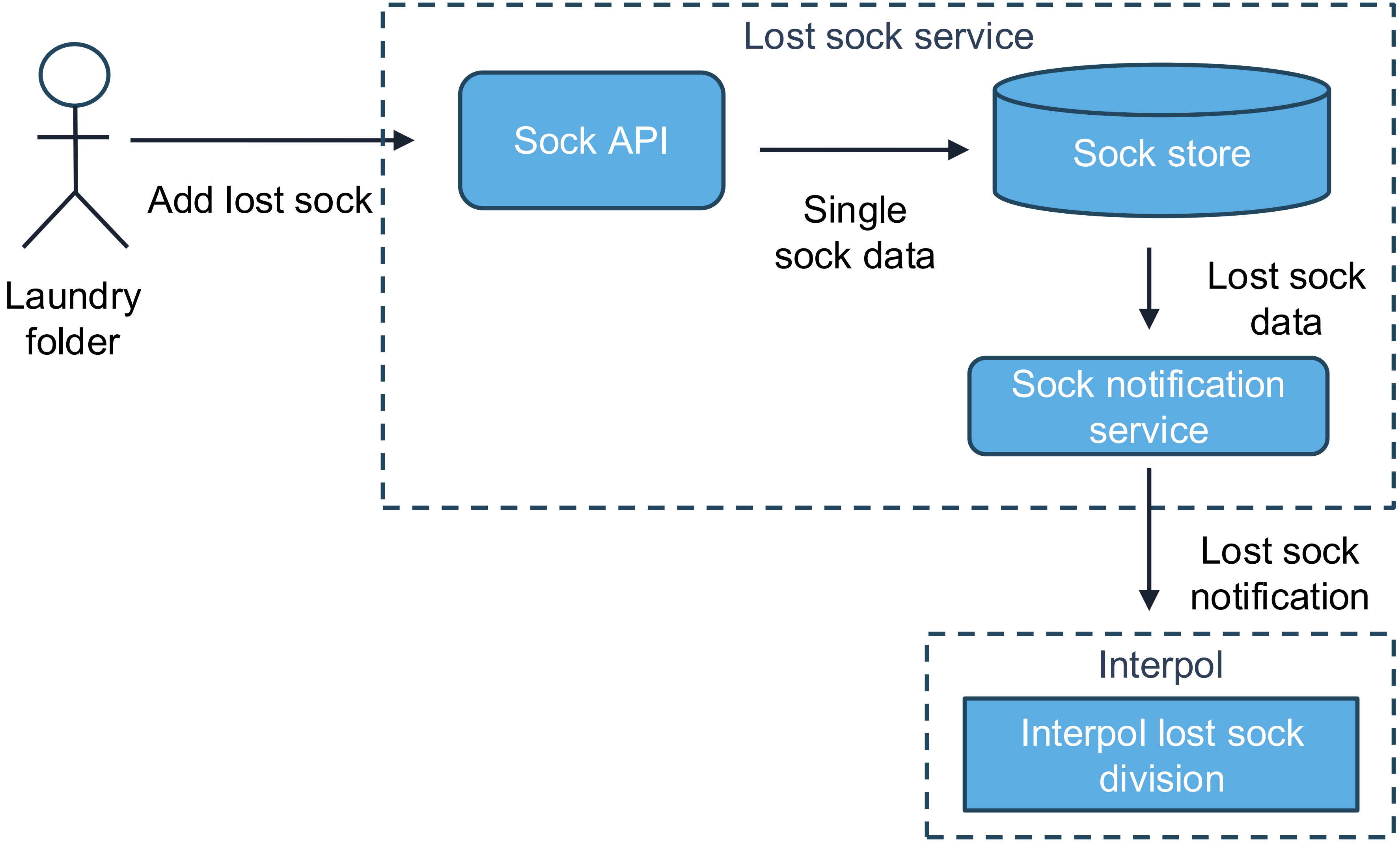
Process

Data store

Data flow

Trust boundary

Data flow diagrams



Use assumptions

- Move quickly
- Linked to threats and mitigations
- Allows for focus
- Pitfall: don’t state mitigations as an assumption

Assumption ID	Description
Assumption-1	Users web browsers are up to date
Assumption-2	AWS managed keys are sufficient for KMS encryption
Assumption-3	We are using a single AWS account per environment

Tips for what are we working on

- Does this help think about what can go wrong?
- Ensure you can tell a story
- Include all sometimes/also scenarios
- Data can’t move itself!

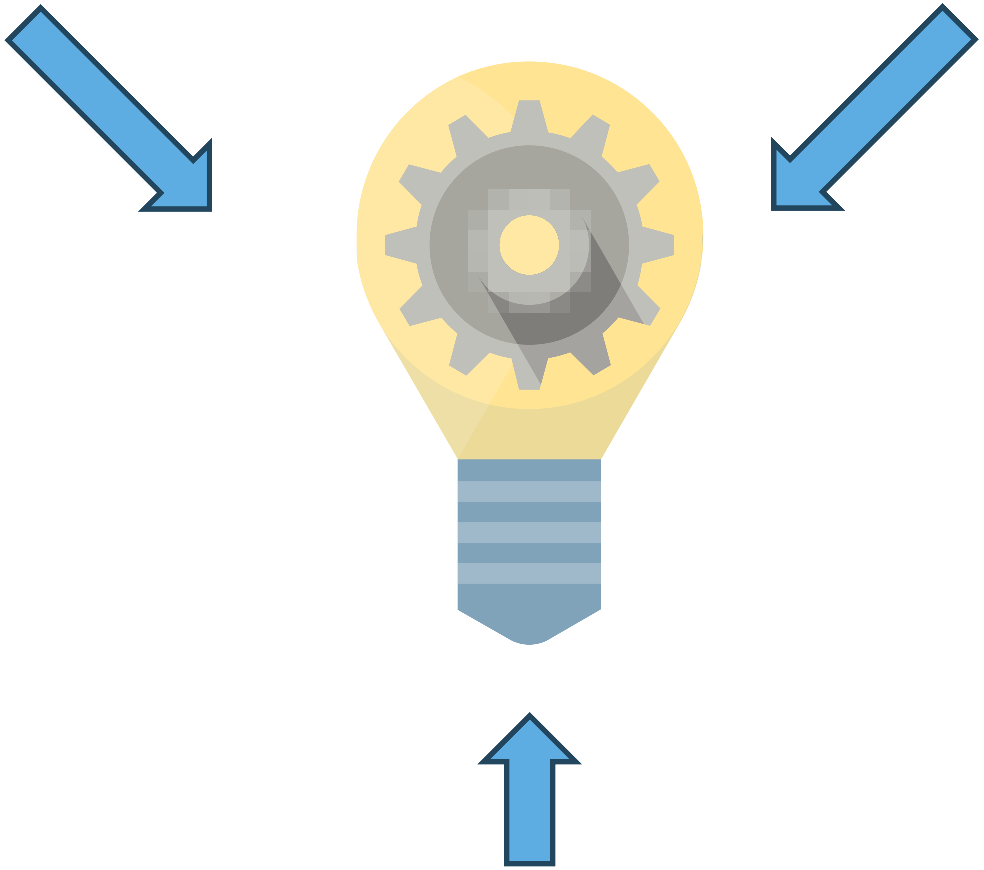
Four key questions

What are we working on?

What can go wrong?

What are we going to do about it?

Did we do a good job?



Brainstorm

OWASP Top Ten
Threat library

STRIDE

Spoofing

- Violates authentication
- "Is this person/machine who they say they are?"

Tampering

- Violates integrity
- "Is this data intact?"

Repudiation

- Violates non-repudiation (trust)
- ”Can we identify who did the thing?

Information disclosure

- Violates confidentiality
- “Can data only be viewed by those who should?”

Denial of services

- Violates availability
- “Are our resources being used correctly?”

Elevation of privilege

- Violates authorization
- “We should only take actions that the user/machine is allowed to take?

[threat source] [prerequisites] can [threat action] which leads to [threat impact], resulting in reduced [impacted goal] of [impacted asset].

Threat syntax

[An internet-based user] [with the ability to see traffic packets] can [intercept messages to Interpol] which leads to [message interception], resulting in reduced [confidentiality] of [the mandatory reporting service].

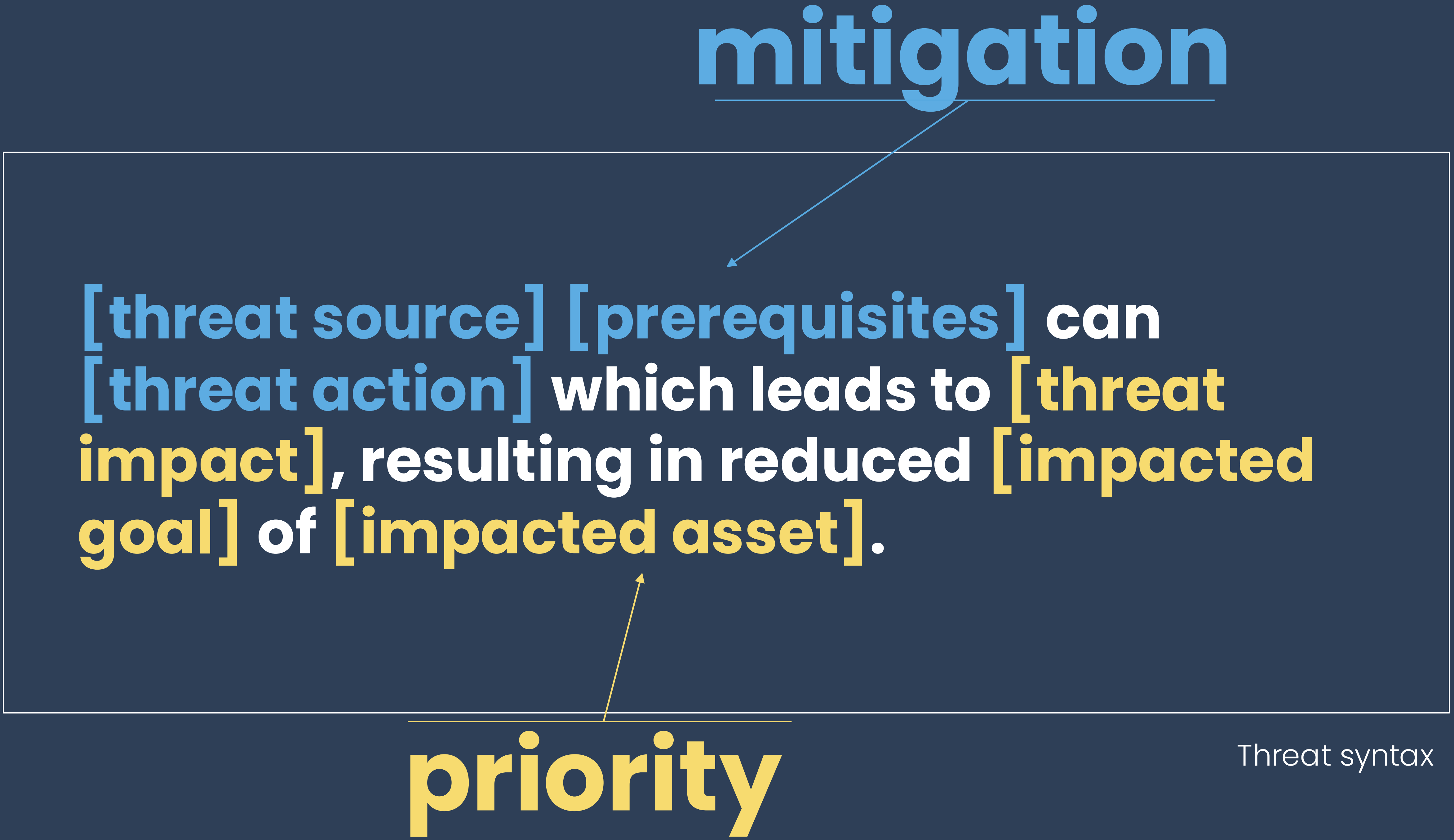
Threat syntax

Risk = impact x likelihood

likelihood

[threat source] [prerequisites] can [threat action] which leads to [threat impact], resulting in reduced [impacted goal] of [impacted asset].

impact



mitigation

[threat source] [prerequisites] can [threat action] which leads to [threat impact], resulting in reduced [impacted goal] of [impacted asset].

priority

Threat syntax

Threat examples

Threat ID	Description	STRIDE	Related assumption
Theat-001	An internal actor with admin access can update the database to match with socks they want leading to reduced integrity in the matching service	T	Assumption-2
Threat-002	An internet-based user can make thousands of concurrent requests which leads to blocking user access to the application resulting in reduced availability of SockMatch	D	
Threat-003	An internet-based user can enter any ID into the request parameter for a sock which leads to the viewing of that sock’s data leading to reduced confidentiality in the sock information service	E	

Tips for what can go wrong

- Threats cluster around boundaries
- Listen for more assumptions
- Note mitigations but move on
- Record things that have been mitigated too!
- Use threat libraries

Four key questions

What are we working on?

What can go wrong?

What are we going to do about it?

Did we do a good job?

Four options

Mitigate it

Risk = impact x likelihood

Mitigation examples

Threat ID	Description	Related Mitigation
Theat-001	An internal actor with admin access can update the database to match with socks they want leading to reduced integrity in the matching service	Mit-001, Mit-002

Mitigate ID	Mitigation	Related Threat	Related assumption
Mit-001	Admin access is only provided on a temporary basis	Threat-001	Assumption-2
Mit-002	Human access to the database is logged and monitored	Threat-001	

Mitigation examples

Threat ID	Description	Related Mitigation
Threat-002	An internet-based user can make thousands of concurrent requests which leads to blocking user access to the application resulting in reduced availability of SockMatch	Mit-003, Mit-004

Mitigate ID	Mitigation	Related Threat	Related assumption
Mit-003	SockMatch will be placed behind a load balancer connected to an auto-scaling group to absorb any excess load	Threat-002	
Mit-004	The WAF will implement rates-based limiting	Threat-002	

Mitigation examples

Threat ID	Description	Related Mitigation
Threat-003	An internet-based user can enter any ID into the request parameter for a sock which leads to the viewing of that sock's data leading to reduced confidentiality in the sock information service	Mit-004

Mitigate ID	Mitigation	Related Threat	Related assumption
Mit-003	The sock information service will only display information for socks that a user is authorized to see by validating that the sock with the matching ID belongs to them	Threat-003	

Spoofing

- Authentication
- Machines and humans

Tampering

- Authorization
- Encryption
- Logging

Repudiation

- Fraud prevention
- Logs
- Cryptography

Information disclosure

- Access control
- Encryption

Denial of services

- Build for high-availability
- Detection and response
- Access control

Elevation of privilege

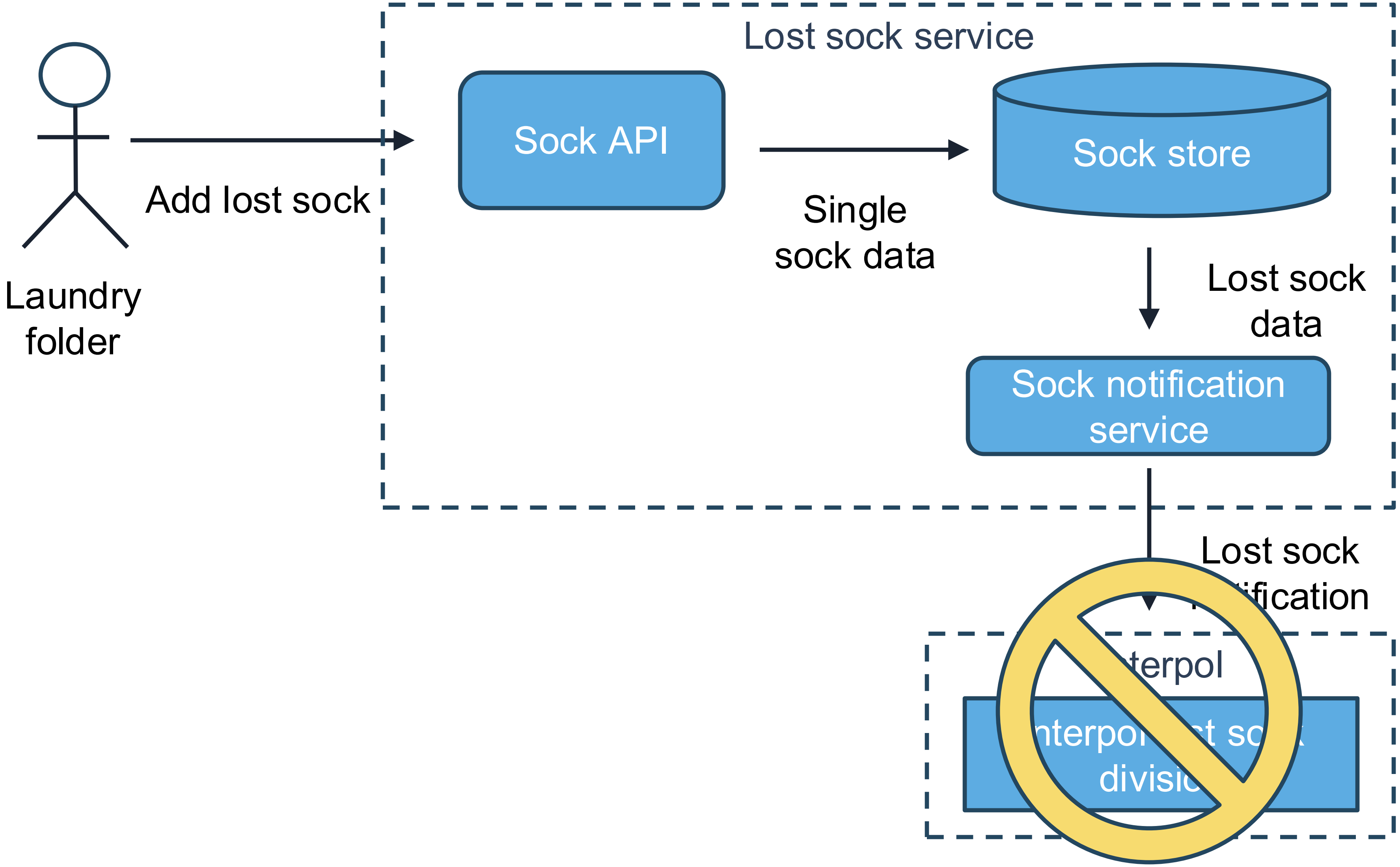
- Authorization

Four options

Mitigate it

Eliminate it

Data flow diagrams



Lost sock service

Laundry folder

Add lost sock

Sock API

Single sock data

Sock store

Lost sock data

Sock notification service

Lost sock
ification

terpol

nterpo st so
divisi

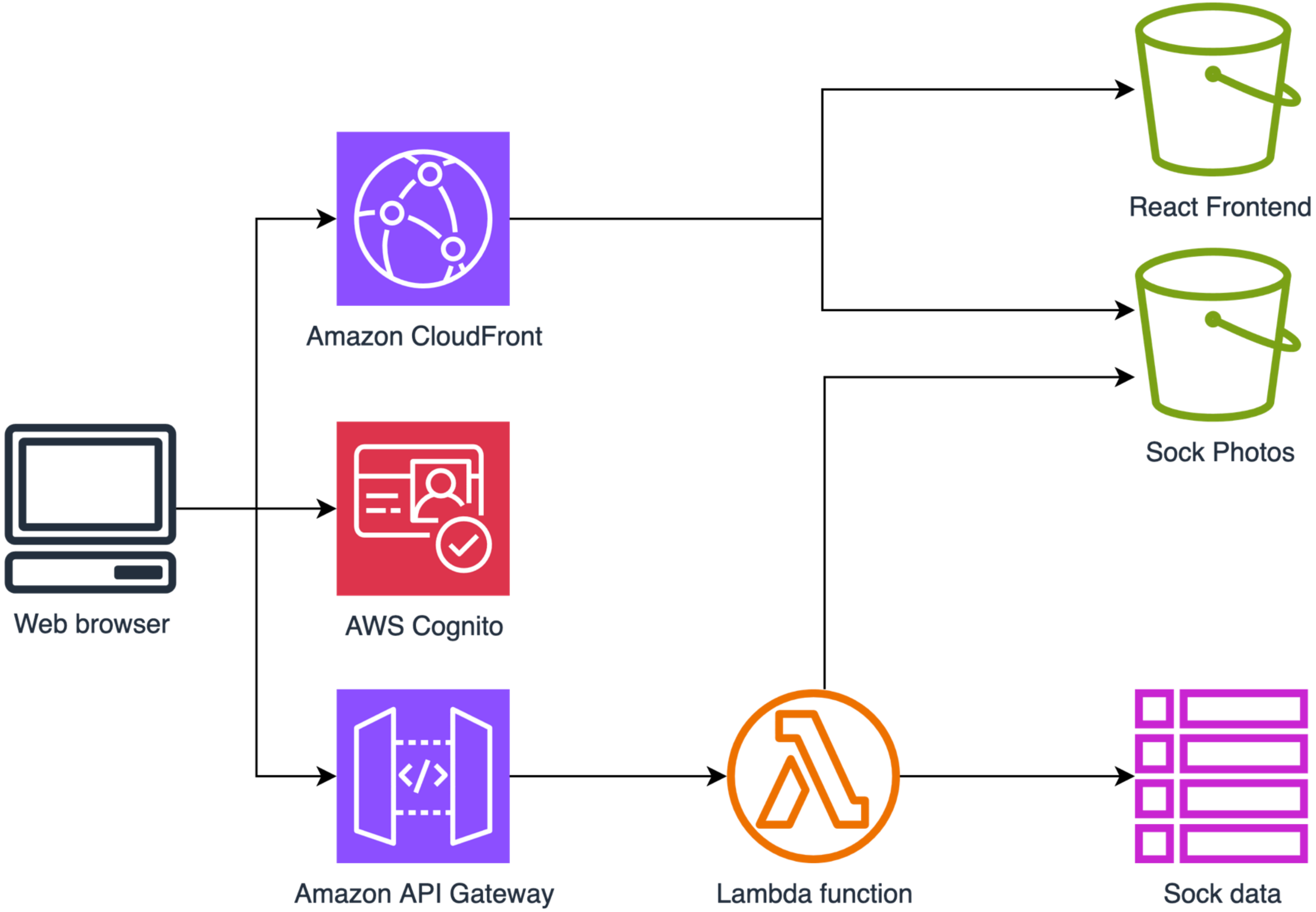
Four options

Mitigate it

Eliminate it

Transfer it

Tinder for socks



Four options

Mitigate it

Eliminate it

Transfer it

Accept it

* Not pictured: sticking your head in the sand

Tips for what are we going to do

- Layer mitigations
- Detective control must also have a response
- Don’t reinvent the wheel
- “If I gave you an example of where someone did that would you fix it?”
- Don’t be the most senior person to know about a risk

Four key questions

What are we working on?

What can go wrong?

What are we going to do about it?

Did we do a good job?

There’s no such thing as an incorrect model.

Tips for did we do a good job

- Consider human factors
- Remember no good or bad

STRIDE per element

	S	T	R	I	D	E
Human actor External entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data store		✓	?	✓	✓	
Data flow		✓		✓	✓	

Four key questions

What are we working on?

What can go wrong?

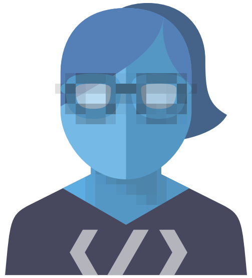
What are we going to do about it?

Did we do a good job?

What to do with your threat model

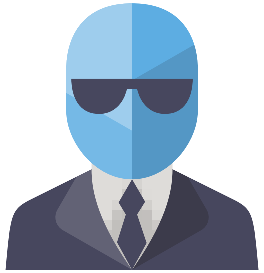
- Add work to the backlog
- Test mitigations
  - Test it works
  - Test to bypass it
- Create a threat library

Scaling threat modeling



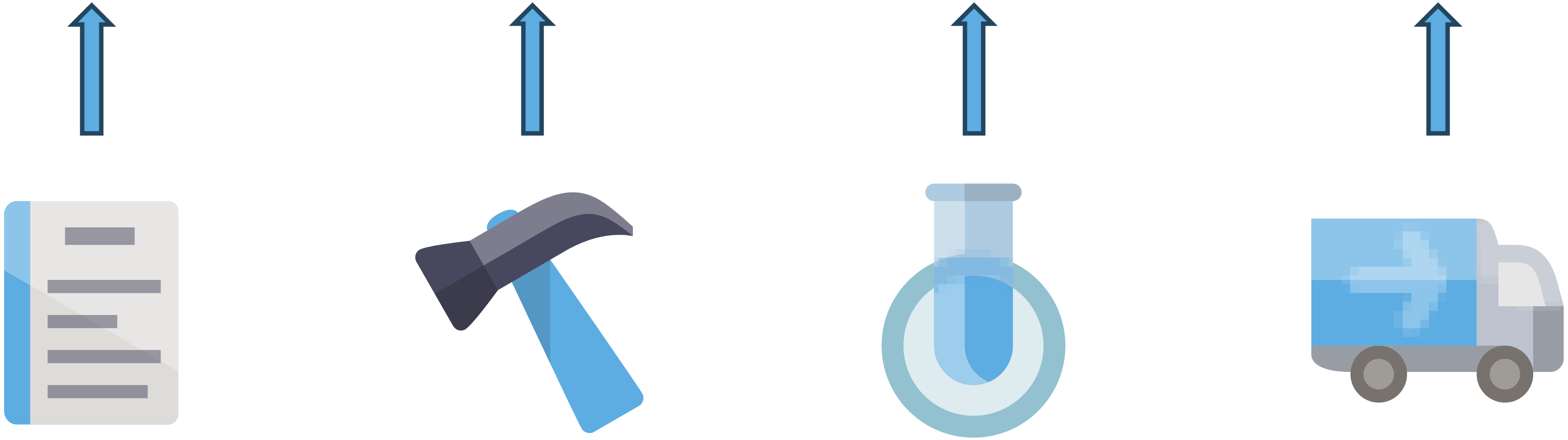
Development

Product management



Security

Consider other elements in your pipeline



Code scanning
Git hooks

Code

Static analysis
Dependency analysis

Build

Dynamic analysis
Pen testing

Test

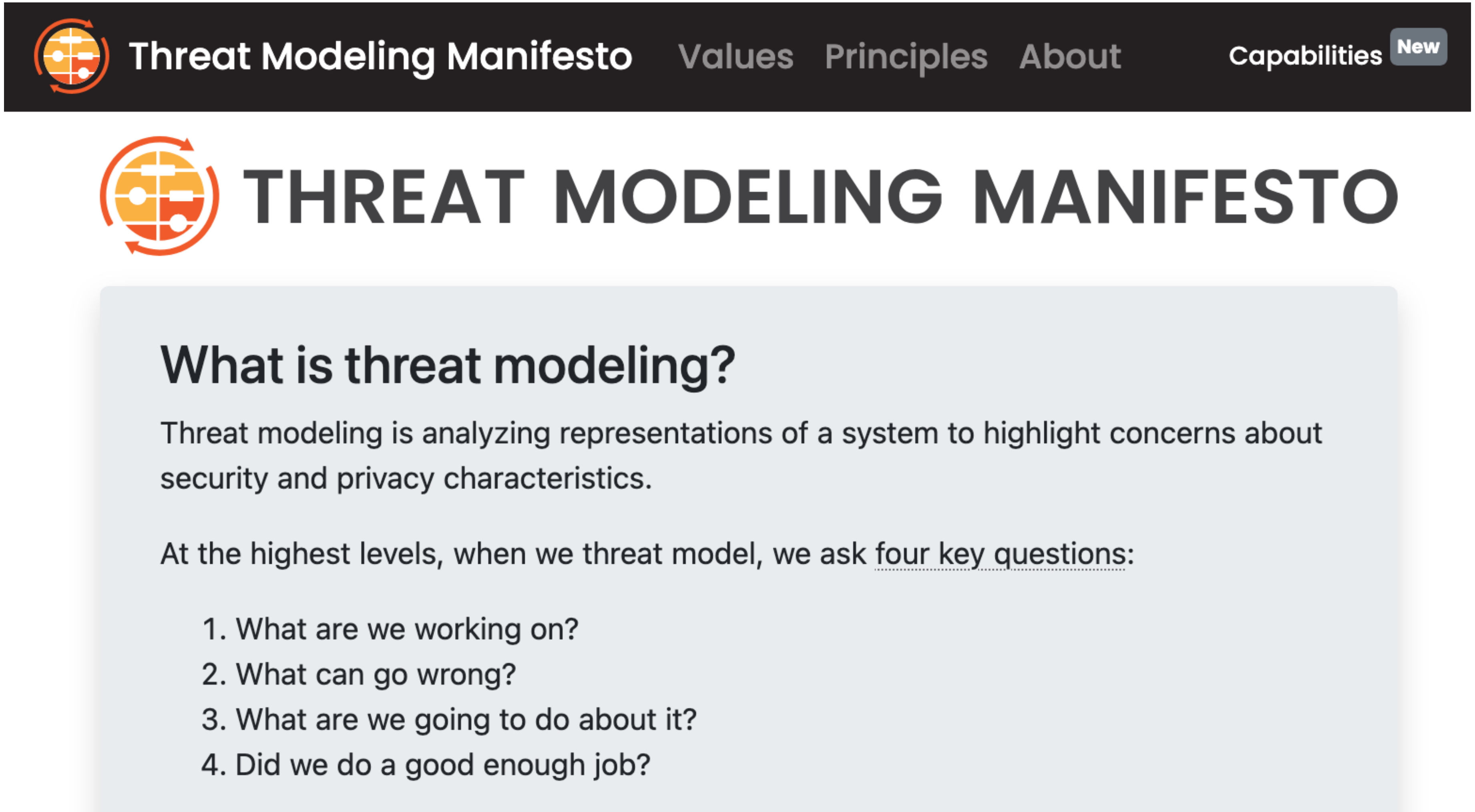
Vuln. monitoring

Deploy

So, what do we say to security?

- What’s the threat you’re trying to mitigate?
- What is the business impact of this risk?
- Remind them they don’t own the risk
- Here’s where it fits in our threat model

Start with



THREAT MODELING MANIFESTO

What is threat modeling?

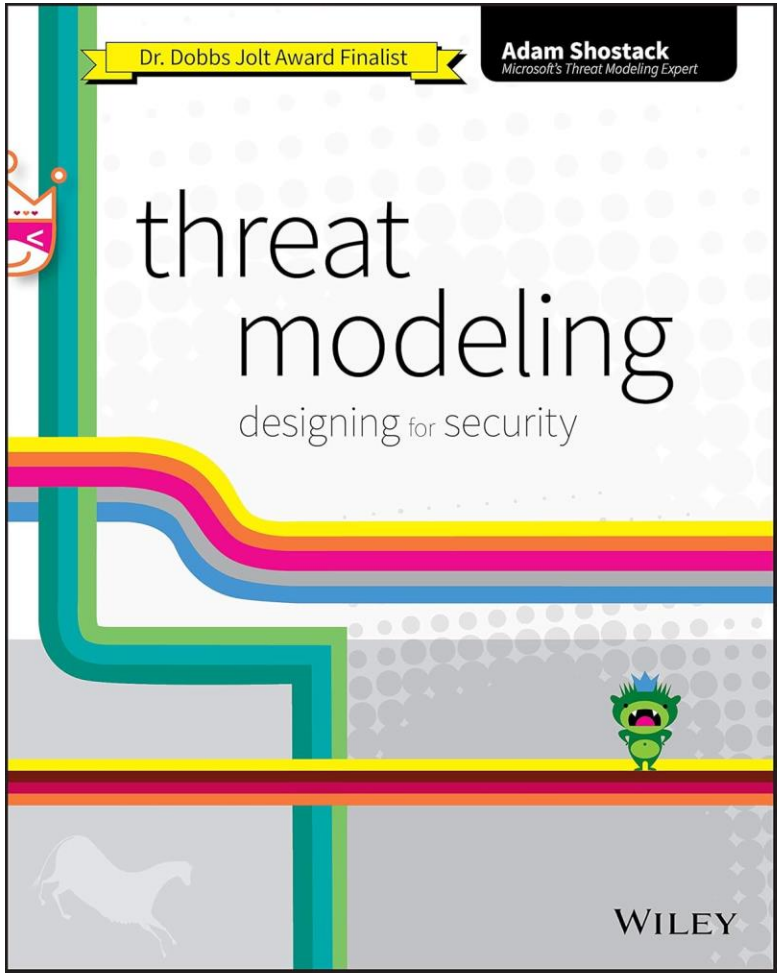
Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.

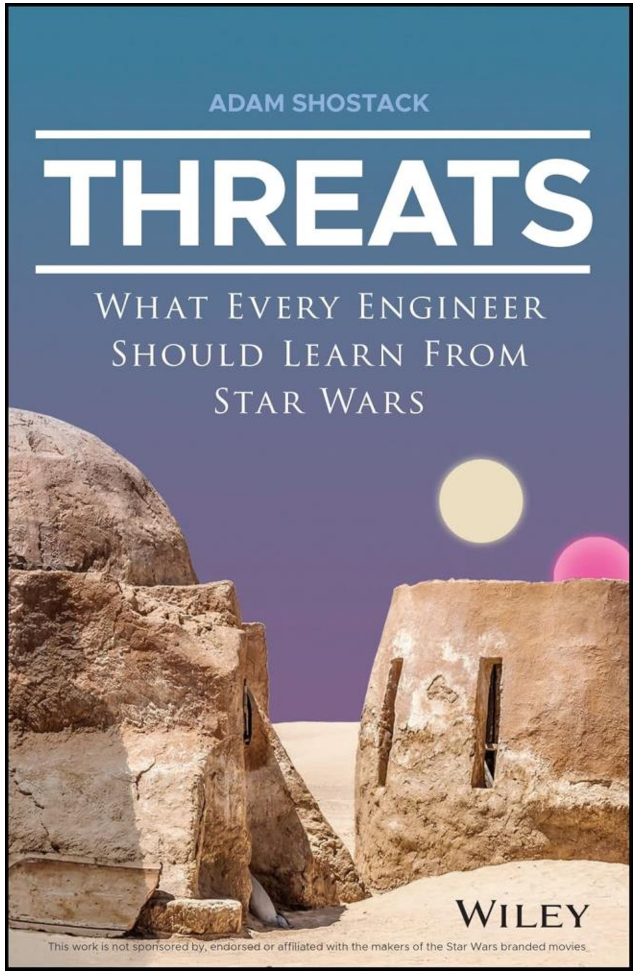
At the highest levels, when we threat model, we ask four key questions:

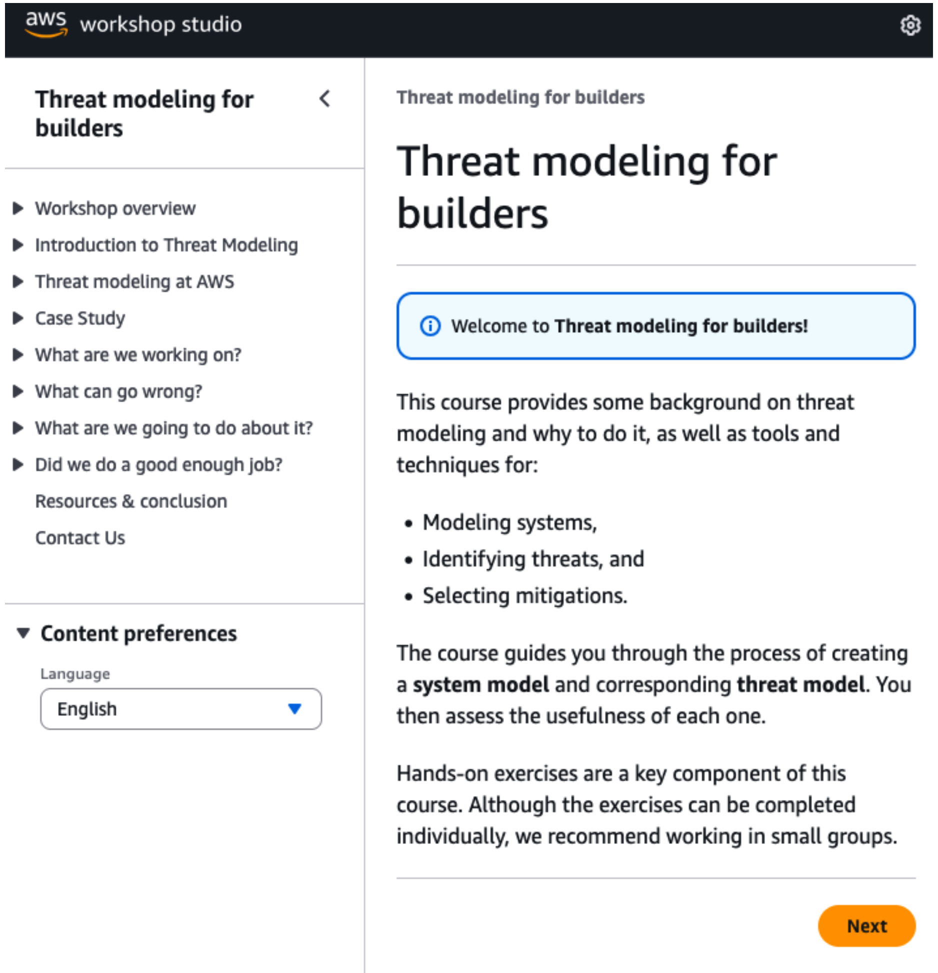
1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

https://www.threatmodelingmanifesto.org/

Further reading


Dr. Dobbs Jolt Award Finalist
Adam Shostack
Microsoft's Threat Modeling Expert
threat modeling
designing for security
WILEY


ADAM SHOSTACK
THREATS
What Every Engineer Should Learn From Star Wars
WILEY
This work is not sponsored by, endorsed or affiliated with the makers of the Star Wars branded movies.



Threat modeling for builders

Threat modeling for builders

Welcome to **Threat modeling for builders!**

This course provides some background on threat modeling and why to do it, as well as tools and techniques for:

- Modeling systems,
- Identifying threats, and
- Selecting mitigations.

The course guides you through the process of creating a **system model** and corresponding **threat model**. You then assess the usefulness of each one.

Hands-on exercises are a key component of this course. Although the exercises can be completed individually, we recommend working in small groups.

Thank you!

Do you have any questions?

hello@bpog.cloud

www.bpog.cloud