THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Global Threat Model Together Day - APAC Session

**October 23, 2025**

*The first community-led threat modeling bootcamp*

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Global Threat Model Together Day - EMEA Session

**October 23, 2025**

*The first community-led threat modeling bootcamp*

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Global Threat Model Together Day - Americas Session

**October 23, 2025**

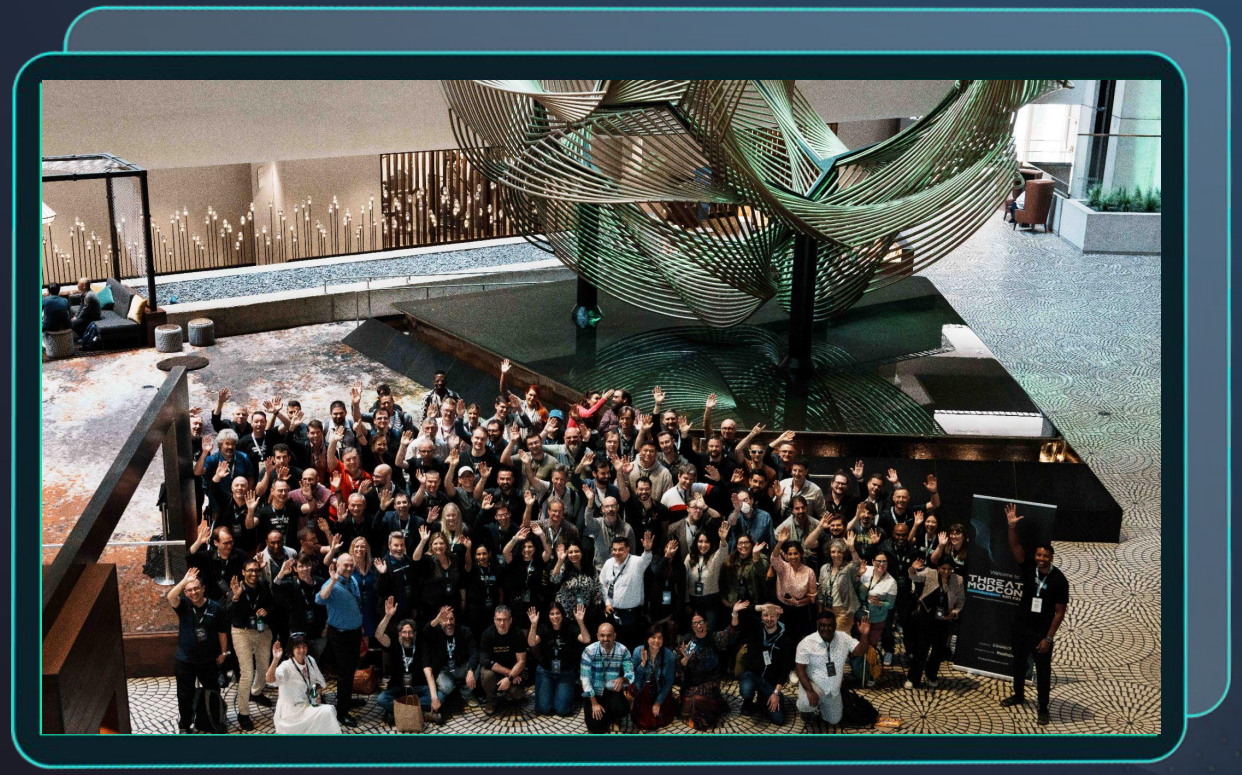
*The first community-led threat modeling bootcamp*

# Welcome to the Threat Modeling Connect (TMC) Community!


THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Who we are

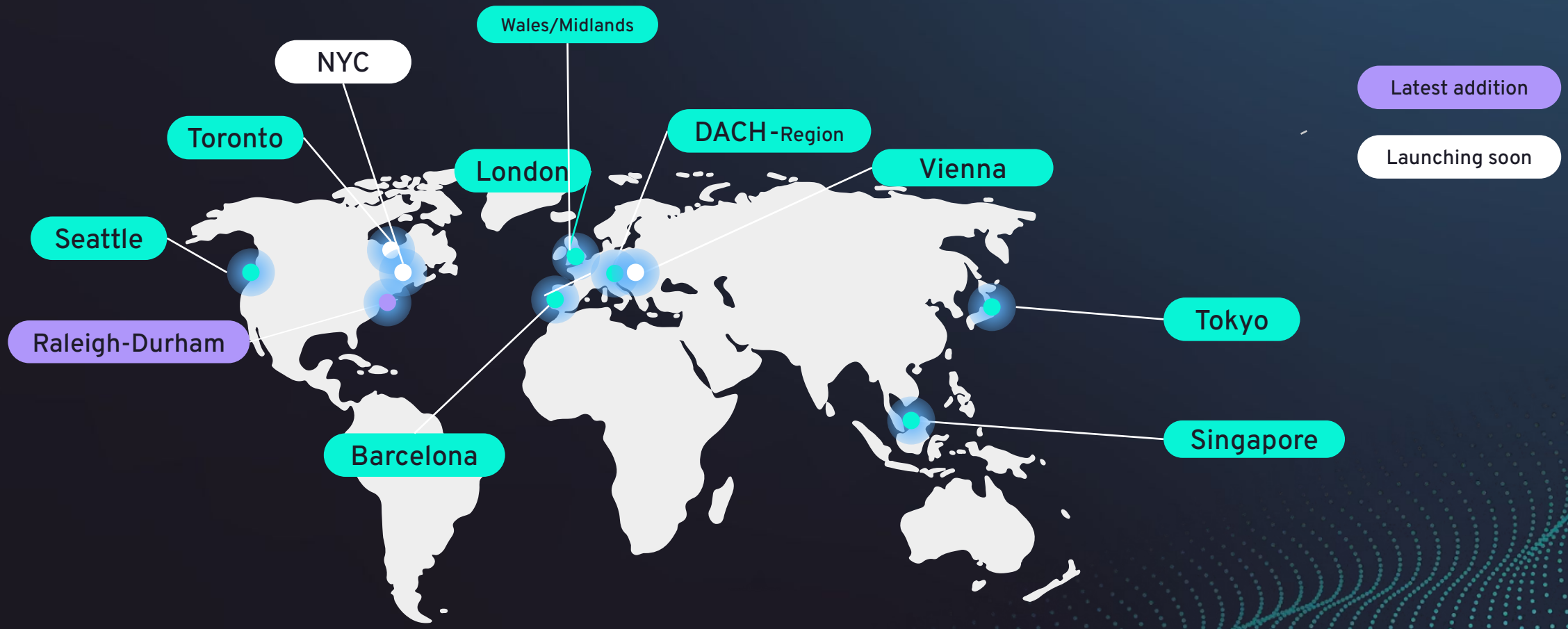
TMC is an open threat modeling community brought together by IriusRisk, with a mission to secure the software and systems that power the modern world by Threat Modeling.



THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# TMC Local Chapters

10 active chapters around the world and 1 coming up in New York City



THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Community and event sponsor

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Event Partner

# Photo time!

Camera on (/off)?

Name like you want it published? 😀?

Purpose: Event reports, social media, advertisements

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Agenda

01 – Today's Toolkit

02 – Playground / System Model

03 – Threat Model Together

04 – Insight Sharing

05 – Final Announcements

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Today's Toolkit

# What is Threat Modeling?

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

THREAT MODELING MANIFESTO

https://www.threatmodelingmanifesto.org/

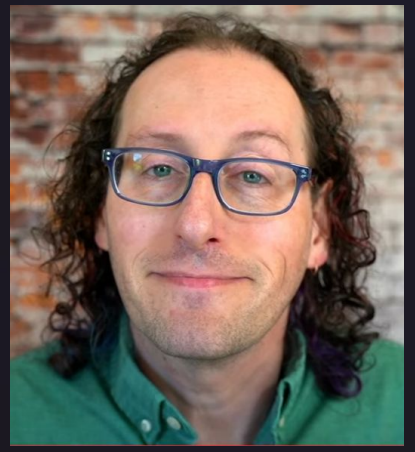
# Chris Romeo's Rule

[We are] not allowed to talk about Threat Modeling for more than 30 minutes, until people have to threat model.

https://www.youtube.com/watch?v=oioLnkQeVek&t=876s

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Shostack's 4 Question Framework for Threat Modeling



Q1 – What are we working on?

Q2 – What can go wrong?

Q3 – What are we going to do about it?

Q4 – Did we do a good job?

https://github.com/adamshostack/4QuestionFrame

# What is a Threat, Vulnerability and a Risk?

# Threat

*“A Threat is an action with the potential to cause harm”*

A boxer throwing a punch

# Vulnerability

*“A Vulnerability is a weakness that can be exploited”*

The boxer not using their guard to protect themselves

# Risk

*“The potential impact or result when a threat exploits a vulnerability”*

A boxer getting hit by a punch because they are not protecting themselves

# Threat & Vulnerability → Risk

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Go threat model: A day at the beach...

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Today's Toolkit
# \ What can go wrong?

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Today's Toolkit
# \ What can go wrong?
# \ Security

# STRIDE Threat Categories

**S** – Spoofing

**T** – Tampering

**R** – Repudiation

**I** – Information Disclosure

**D** – Denial of Service

**E** – Elevation of Privilege

- By Praerit Garg & Loren Kohnfelder, 1999
- Six threat categories
- Undermine six desired properties of a system

# STRIDE Threat Categories

- presented in a different order
- images from ThoughtWorks
  (licensed Creative Commons Attribution-ShareAlike 4.0 - https://thoughtworksinc.github.io/sensible-security-conversations/)

# Why reordered?

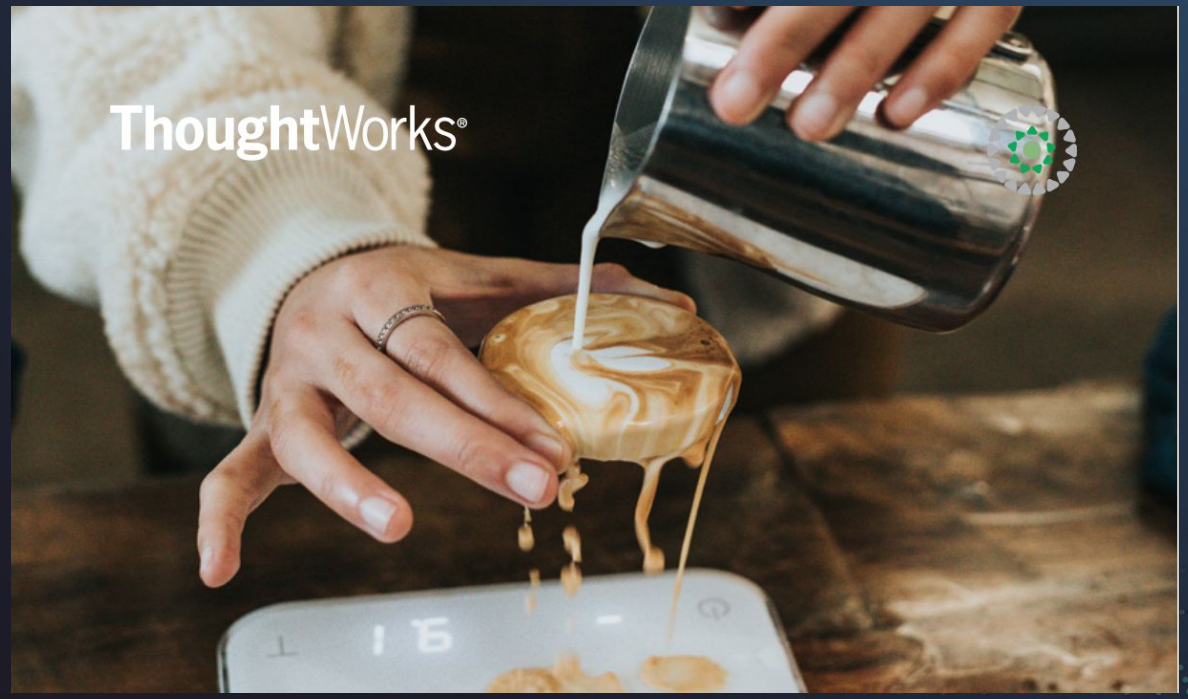
- First three correspond to popular CIA Triad
  - Information Disclosure ↔ Confidentiality
  - Tampering ↔ Integrity
  - Denial of Service ↔ Availability
- Two about getting there
  - Spoofing ↔ Authentication
  - Elevation of Privilege ↔ Authorization
- One about getting away
  - Repudiation

# STRIDE - Information Disclosure

- receiving information you were not supposed to see
- undermines Confidentiality
- Do we protect our secrets?

# STRIDE - Tampering

- manipulating data / communication / code
- undermines Integrity
- Can someone mess with our data or insert malicious snippets?



# STRIDE - Denial of Service

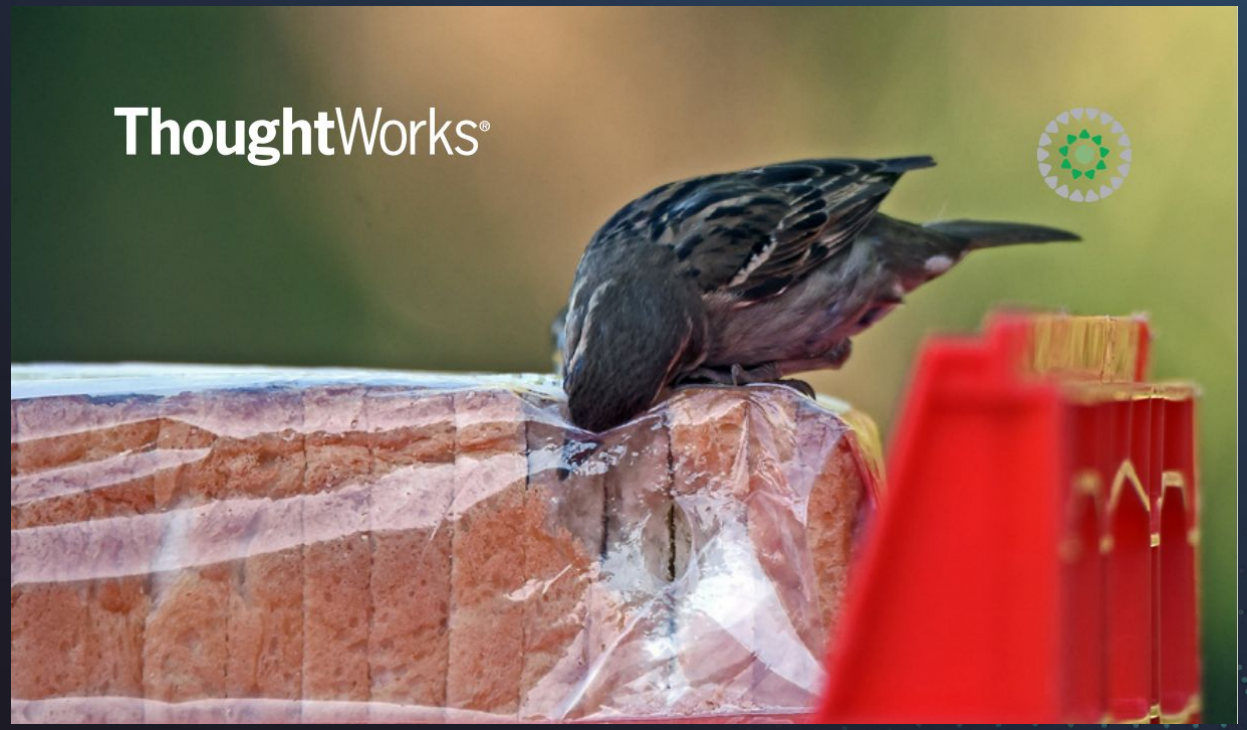
- making service unavailable for legit use
- undermines Availability
- Is our service up, even if someone wants to disrupt it?

# STRIDE - Spoofing

- pretending to be someone / something else
- undermines Authentication (Who are you?)
- Who can do this? How do we know it's really them?

# STRIDE - Elevation of Privilege

- achieving more than you should be able to do
- undermines Authorization (What can you do?)
- How do we enforce our permission system? Can it be bypassed?

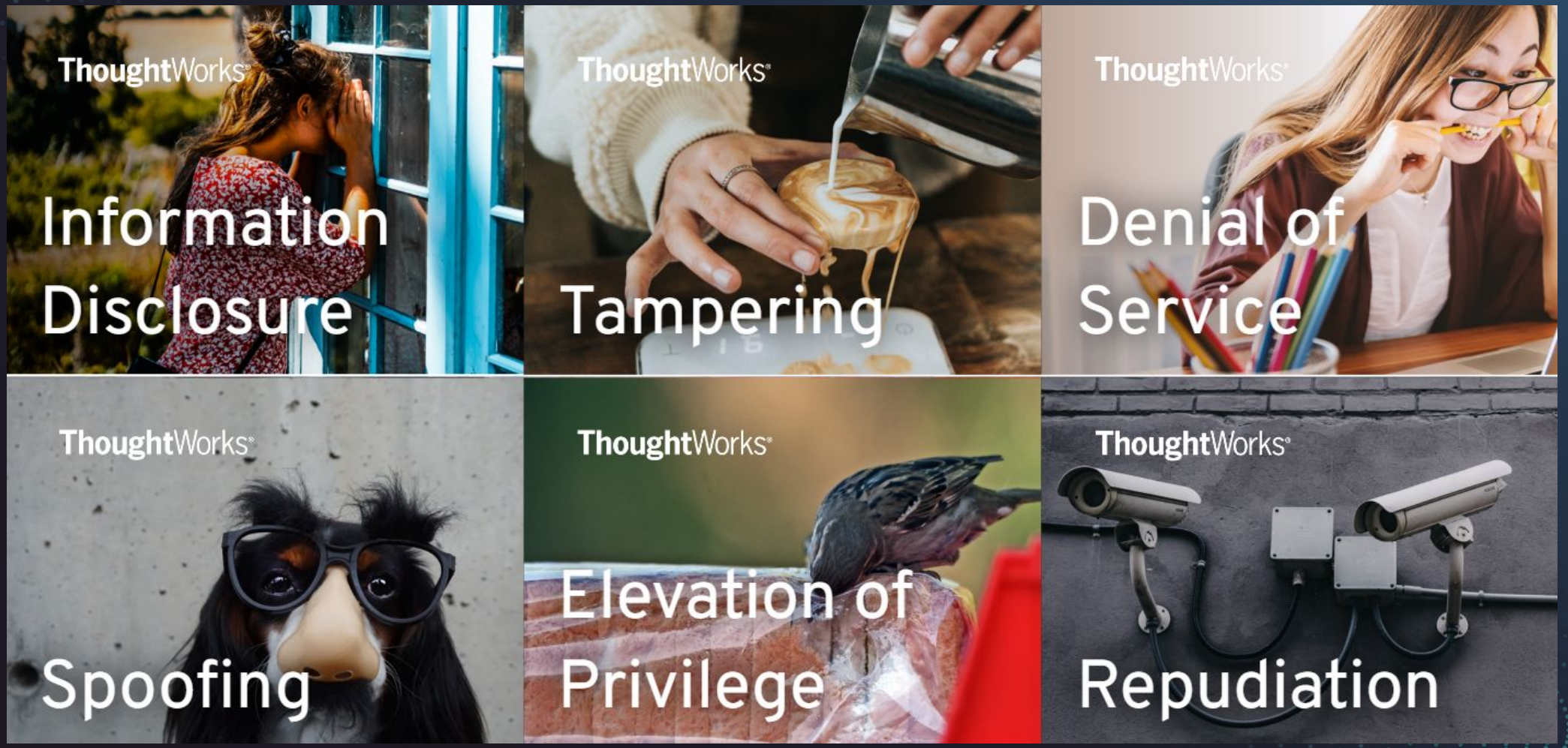


# STRIDE - Repudiation

- getting away with "I didn't do it" (after a malicious action)
- undermines Verifiability
- Can we detect & attribute critical actions?

# STRIDE (reordered)

THREAT MODELING CONNECT | POWERED BY IRIUSRISK



# STRIDE per Element

- Combine system components with the STRIDE categories
- More easily elicit threats because of focus

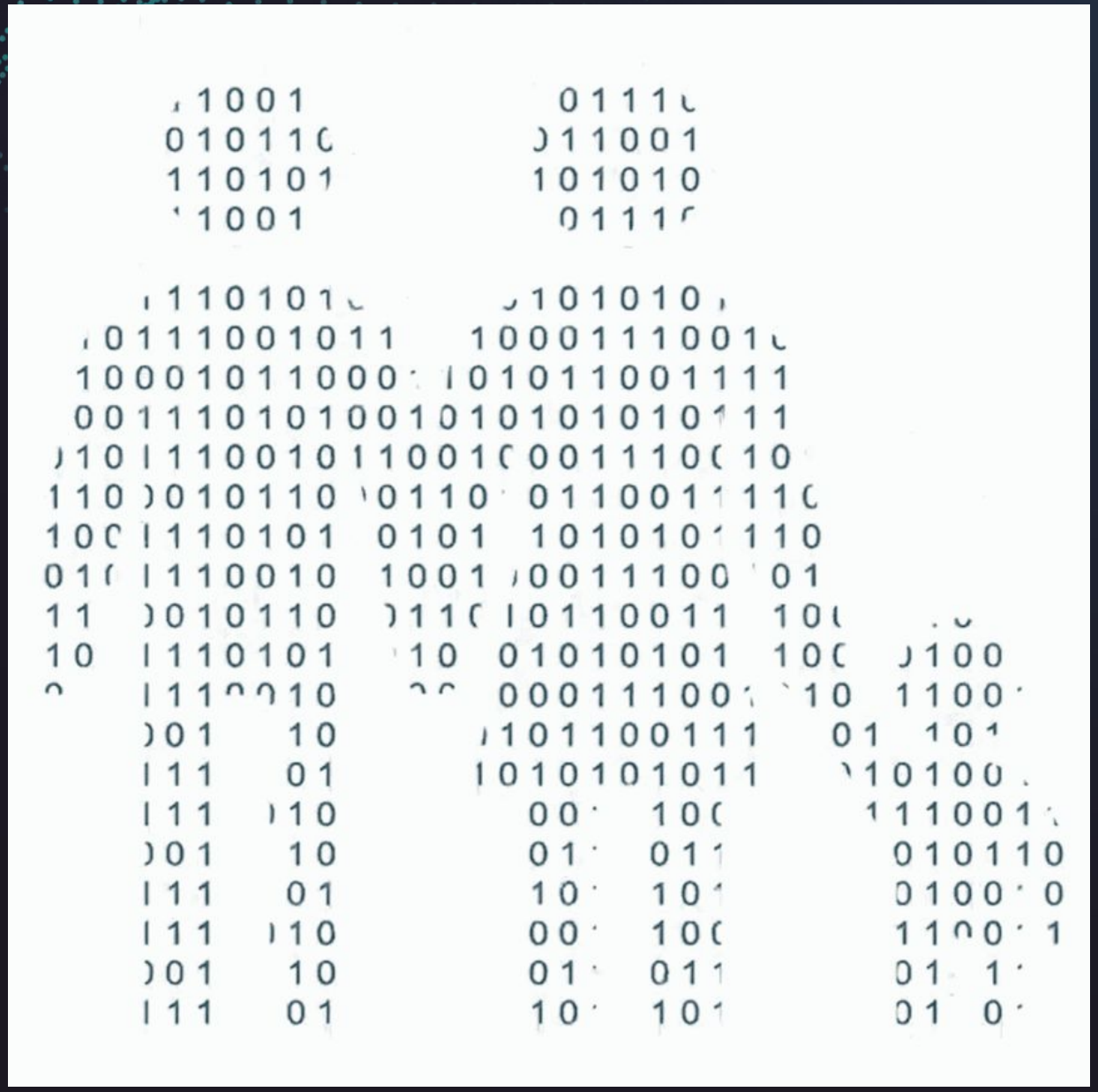
THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Today's Toolkit
# \ What can go wrong?
# \ Privacy

# Privacy


- We are not only processing data...

# Privacy



- We are not only processing data…
- It’s about people!

# Data subjects have rights!

- Data subjects want and deserve
  - adequate, minimal data about them collected/processed for a specific purpose
  - transparency
  - control

- Curious about more?
  Learn LINDDUN or checkout work of Kim Wuyts!

https://linddun.org

https://www.youtube.com/@KimWuyts-privacy

# Today's Toolkit
# \ What can go wrong?
# \ Usability

# Usability (ISO 9241-11:2018)

≈ how well your offer helps people achieve their goals

- Effectiveness: achieving the goal
- Efficiency: quality ↑ cost ↓
- Satisfaction: 🥰

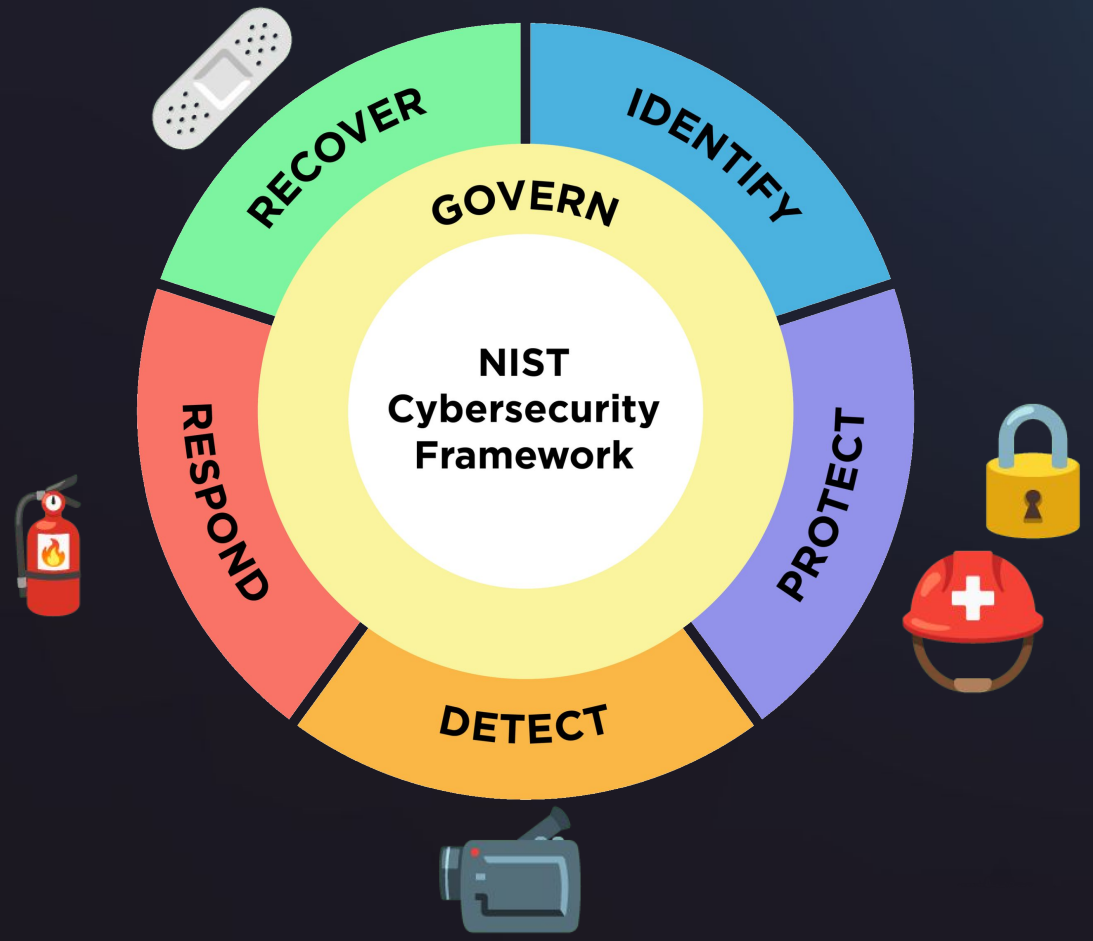
- Usability threats: Users frustrated, because they are not getting what they want from your system

https://www.iso.org/obp/ui/en/#iso:std:iso:9241:-11:ed-2:v1:en

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Today's Toolkit \ What are we going to do about it?

# Kinds of controls



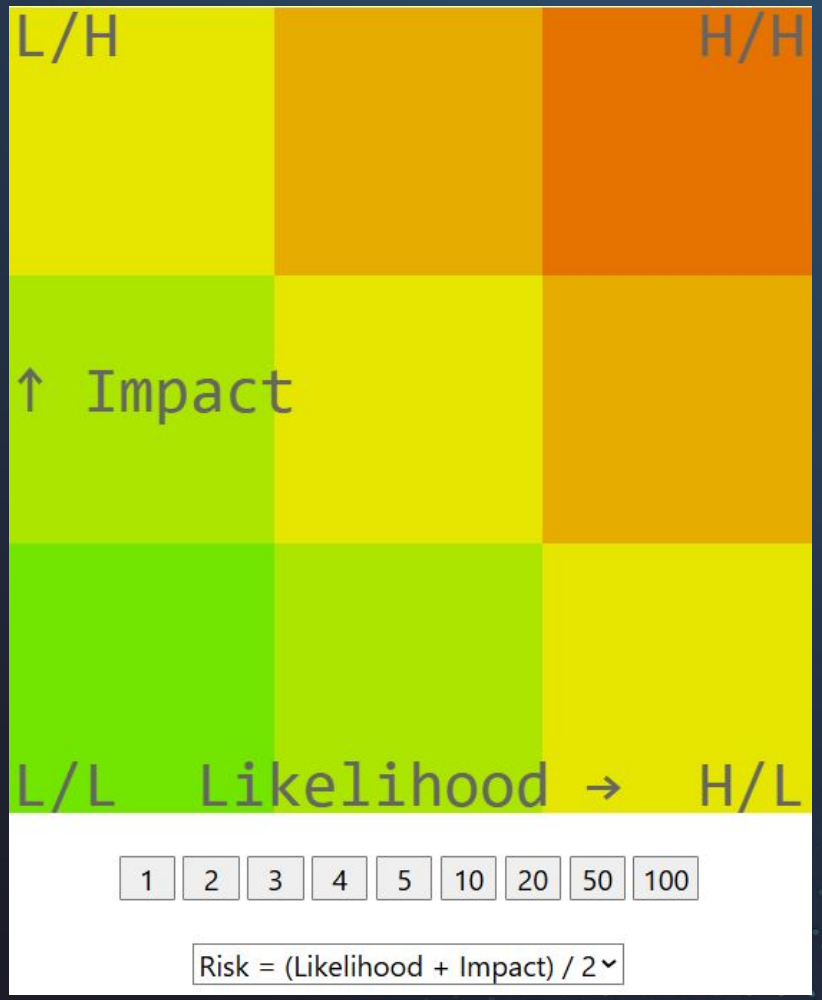

reduce likelihood

reduce harm

https://www.nist.gov/cyberframework

# Qualitative Risk

- Not all threats are equally severe
- How likely? How bad? → Risk
- LMH risk assessment:
  Judge likelihood & impact
  Low / Medium / High;
  get severity from matrix
- Before / After Principle:
  Improve severe risks with controls
  until they are acceptable




https://threat-modeling.net/likelihood-impact/

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Today, talk is cheap!

- Normally, risk & feasibility matter a lot.
- There's different approaches.

https://threatmodelingconnect.discourse.group/t/most-awesome-risk-assessment-style/889

- We don't actually want to secure that playground system.
- Let's only address risk & feasibility when it's fun!

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Agenda

01 – Today's Toolkit

**02 – Playground / System Model**

03 – Threat Model Together

04 – Insight Sharing

05 – Final Announcements

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Playground / System Model

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# System for today:

# Ordering food in the Global Threat Model Theme Park

📱➡️👩‍🍳➡️😋

# Scenario

After a successful ThreatModCon DC, Shuning wants to open her first “Global Threat Model Theme Park”.

All things awesome and threat modeled, of course!

We are in charge of building the food ordering experience! We have an early version of the design under construction.

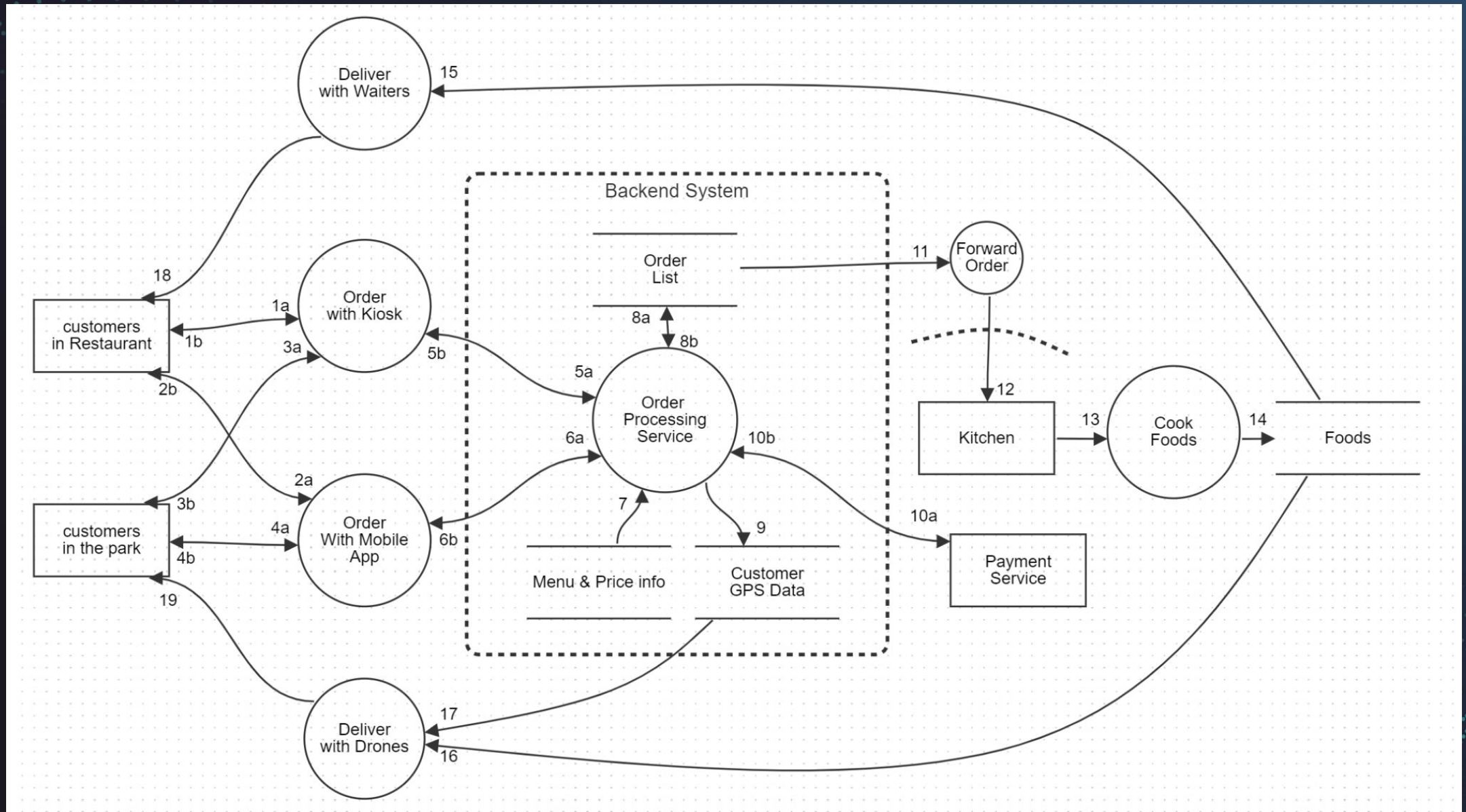
# System description

- New upcoming theme park has multiple restaurants.

- Ways to order:
  1. Traditional: Inside restaurant at a kiosk, have waiter deliver food
  2. Fancy: Inside the park with an app, have drones deliver with GPS / face recognition

# Data (& Food) Flow Diagram

THREAT MODELING CONNECT | POWERED BY IRIUSRISK



THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# What could possibly go wrong?

📱 ➡ 👨‍🍳 ➡ 😋

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Agenda

01 – Today's Toolkit

02 – Playground / System Model

**03 – Threat Model Together**

04 – Insight Sharing

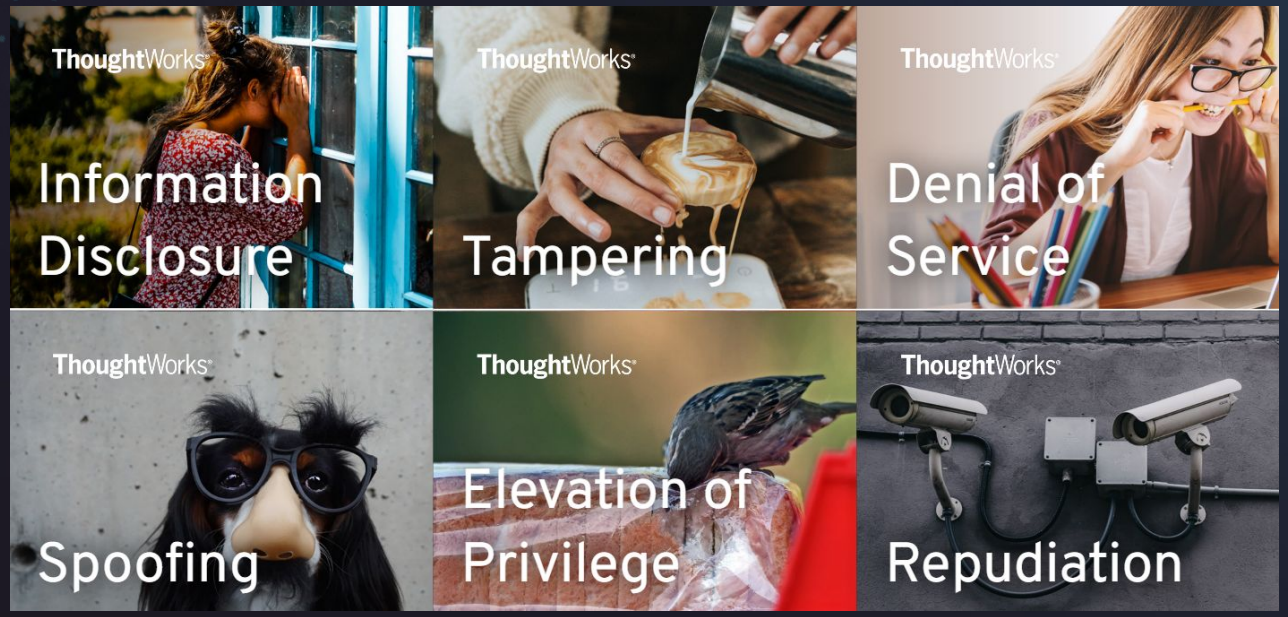
05 – Final Announcements

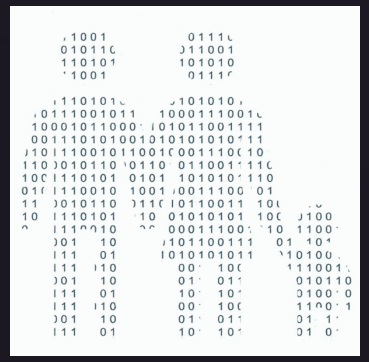
THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Threat Model Together

# Method cheat sheet

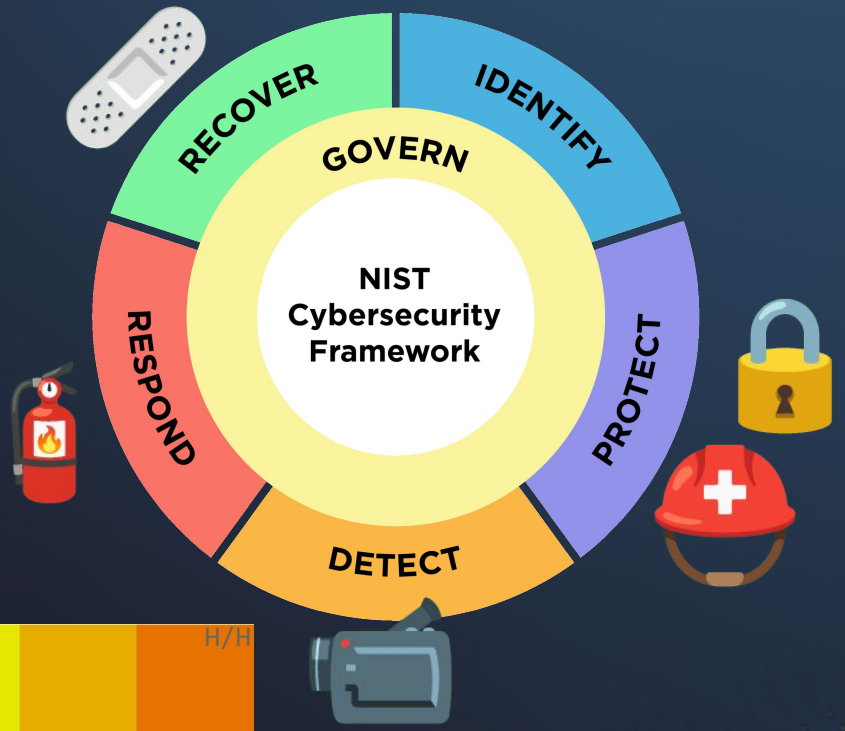


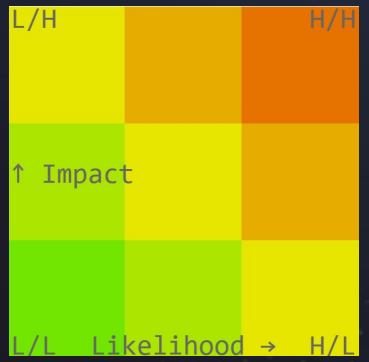


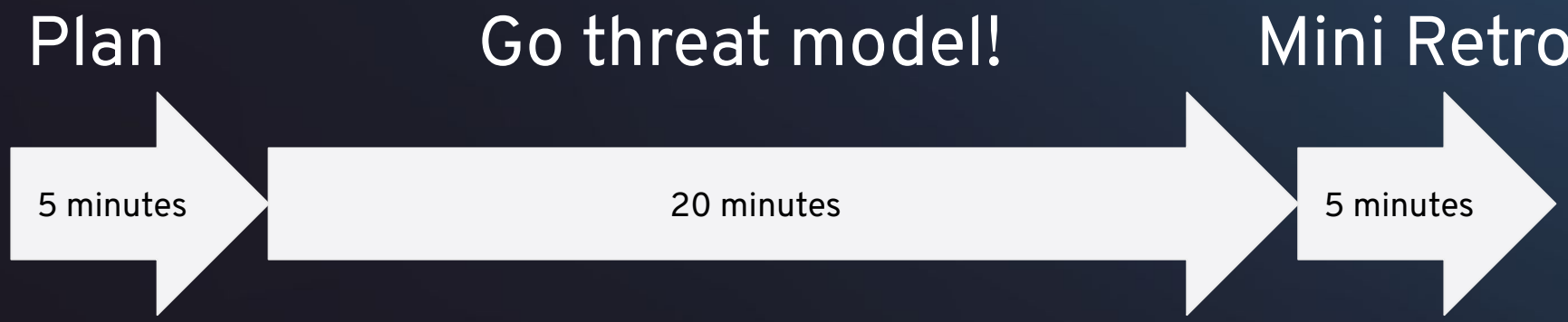
Privacy: Minimality, Transparency, Control

Usability: help users achieve their goals



# Agile Threat Modeling Mini Sprints




1. First sprint: ⛈️ Threats
2. Get together
3. Second sprint: ☂️ Mitigations
4. Insight sharing

# First sprint

- Topic: ⛈️ Threats

- Decide your focus!
- Elicit threats
  (Brainstorm / STRIDE / Privacy / Usability)
- Challenge: Also find one funny/#silly threat 😜

- Go threat model!
- Back in 30 minutes

# Get together

- What was your most interesting threat?

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Second sprint

- Topic: ☂️ Mitigations

- 🔐⛑️ Protect? 📹 Detect?
  🧯 Respond? 🩹 Recover?
- New follow-up threats from mitigations?

- Go threat model!
- Back in 30 minutes

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Agenda

01 – Today's Toolkit

02 – Playground / System Model

03 – Threat Model Together

**04 – Insight Sharing**

05 – Final Announcements

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Insight Sharing

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Insight Sharing

- How did the exercise work for you?
- What did you learn today?

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Agenda

01 – Today's Toolkit

02 – Playground / System Model

03 – Threat Model Together

04 – Insight Sharing

**05 – Final Announcements**

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

# Final Announcements

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

## Upcoming event

# ThreatModCon 2025 USA

Nov 7-8, 2025
Washington DC

—

The ONLY threat modeling conference on the planet & biggest annual gathering of the TMC community! ❤️

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

## Upcoming event

# TMC Vienna Meetup

Oct 30, 2025, 5-8PM
@ÖBB Open Innovation Factory

—

Hands-on threat modeling workshop, quantitative threat modeling seminar, happy hour!

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

## Save the date

# Hackathon 2026

February 1-27, 2026
Virtual

—

TMC's favorite spring tradition is back!
Registration opens in January. Limited seats available.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

## SOTM 2025-2026

# Community Survey opens next month!

Have your say and help shape the next SOTM report.
Stay tuned for updates coming November 2025!

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Member newsletter

# Events, content, projects news & so much more

threatmodelingconnect.com/join-the-community

Newsletter

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

We're on Slack!

# Connecting with fellow members is now easier

https://tinyurl.com/mrxydahn

Slack