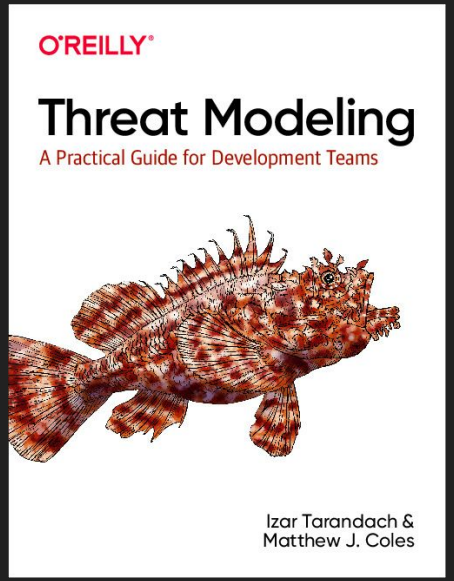
Threat Modeling

You don’t need to be paranoid, but it helps

Izar Tarandach - TNG Big Tech Day 2024

Your Speaker

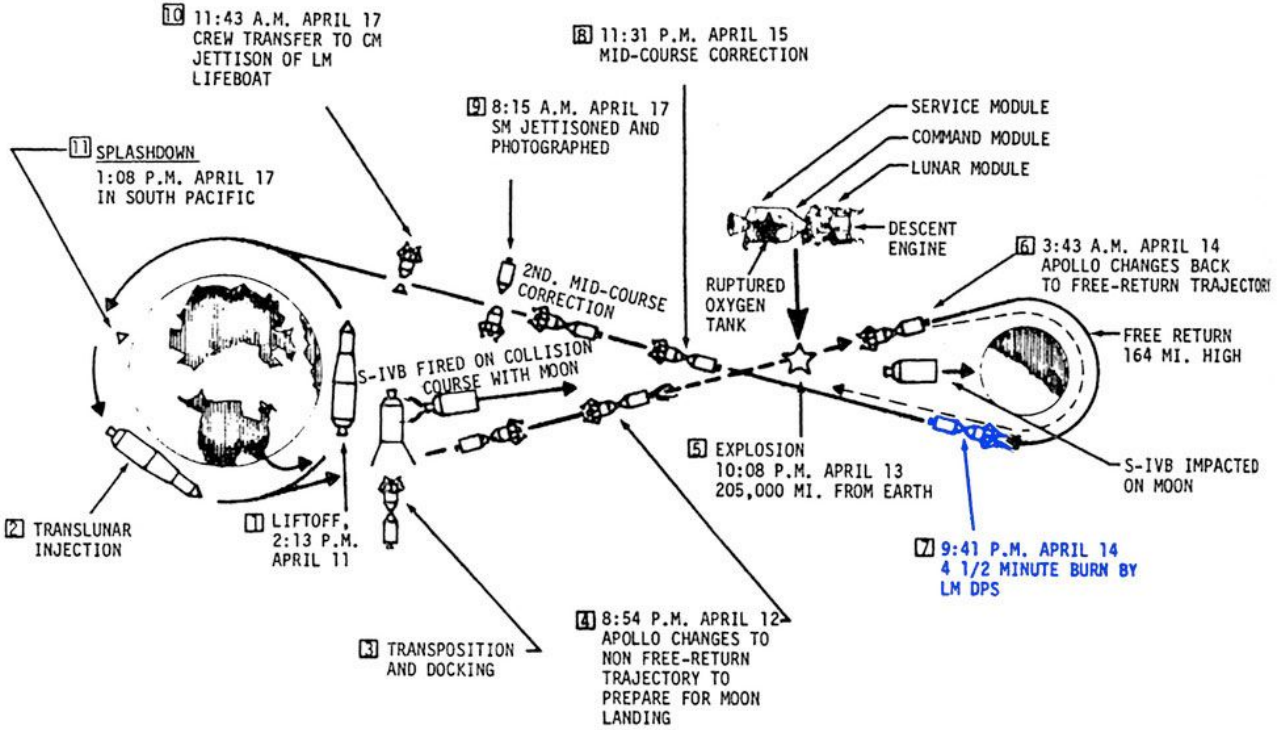
- Izar Tarandach, Sr. Principal Security Architect at a major broadcasting company
- doing security in a way or another since…well, a long time
- Many top and big companies, but some startups as well
- I've had lots of successes and a non-zero number of failures
- My focus is Threat Modeling, uses of AI in Security (like everyone else…) and improving security processes for developers. Big advocate of soft skills in Security
- Creator of CTM, co-author of this book →, some essays, co-author of the TMM and TMC documents, webinars and podcasts



“Houston, we have a problem.”

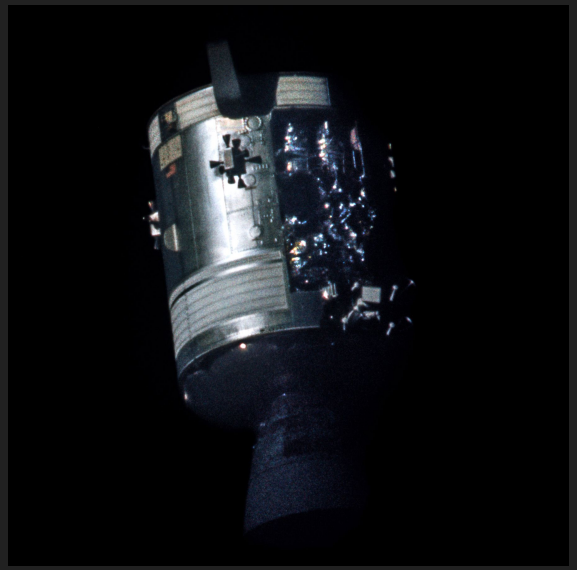
Apollo 13

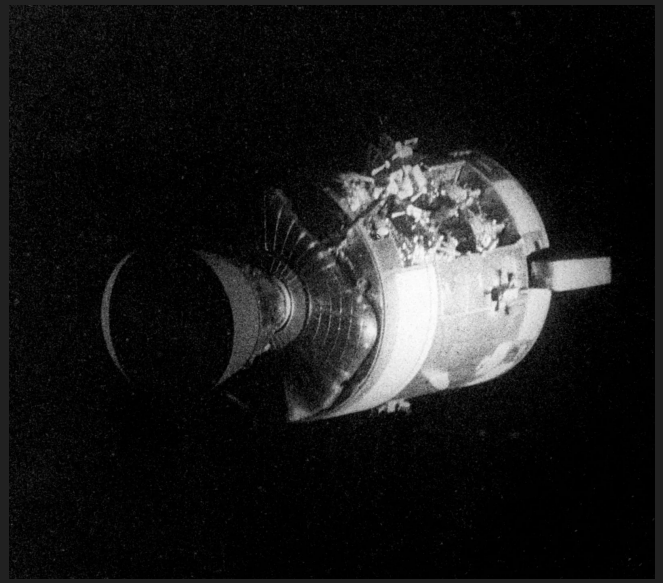
APOLLO 13 FLIGHT PROFILE

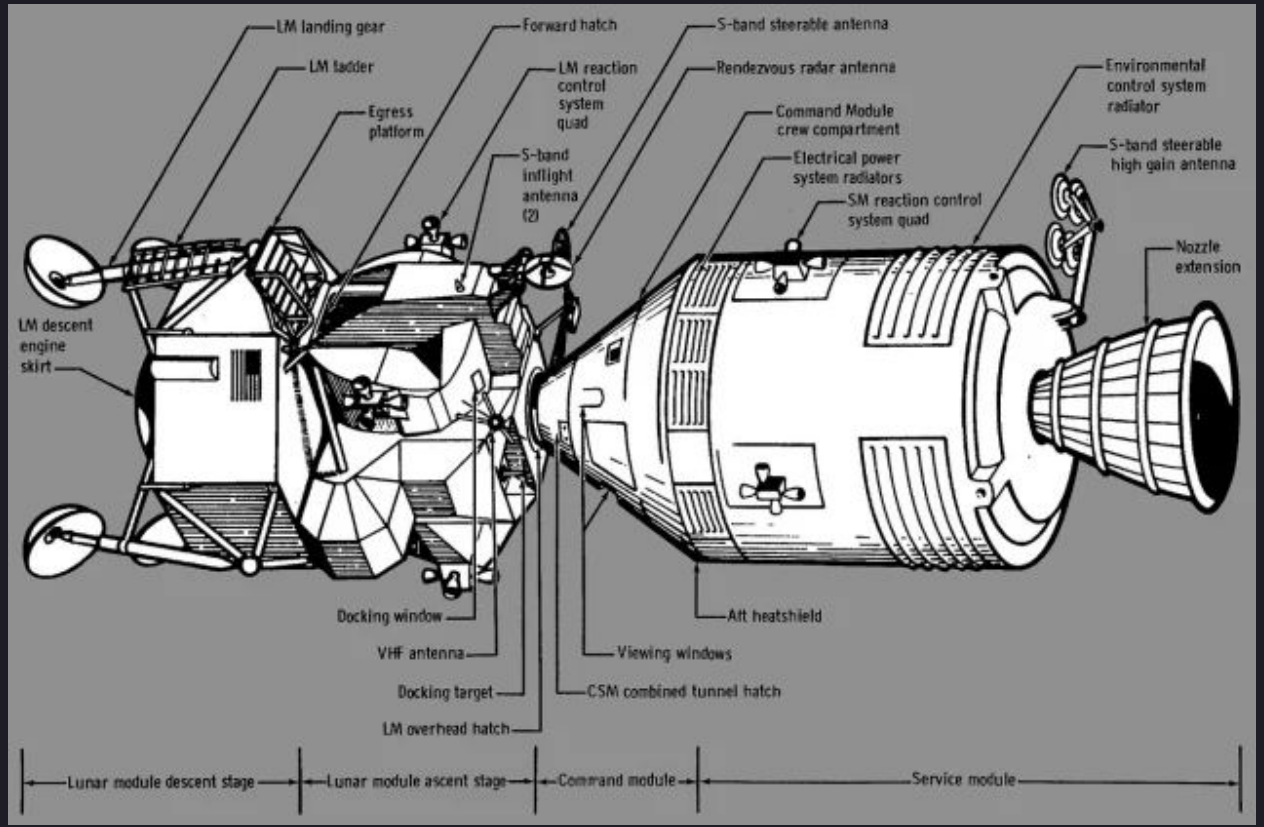


http://www.collectspace.com/review/andyanderson/apollo13_orientation01-lg.jpg

“Houston, we’ve had a problem here.”



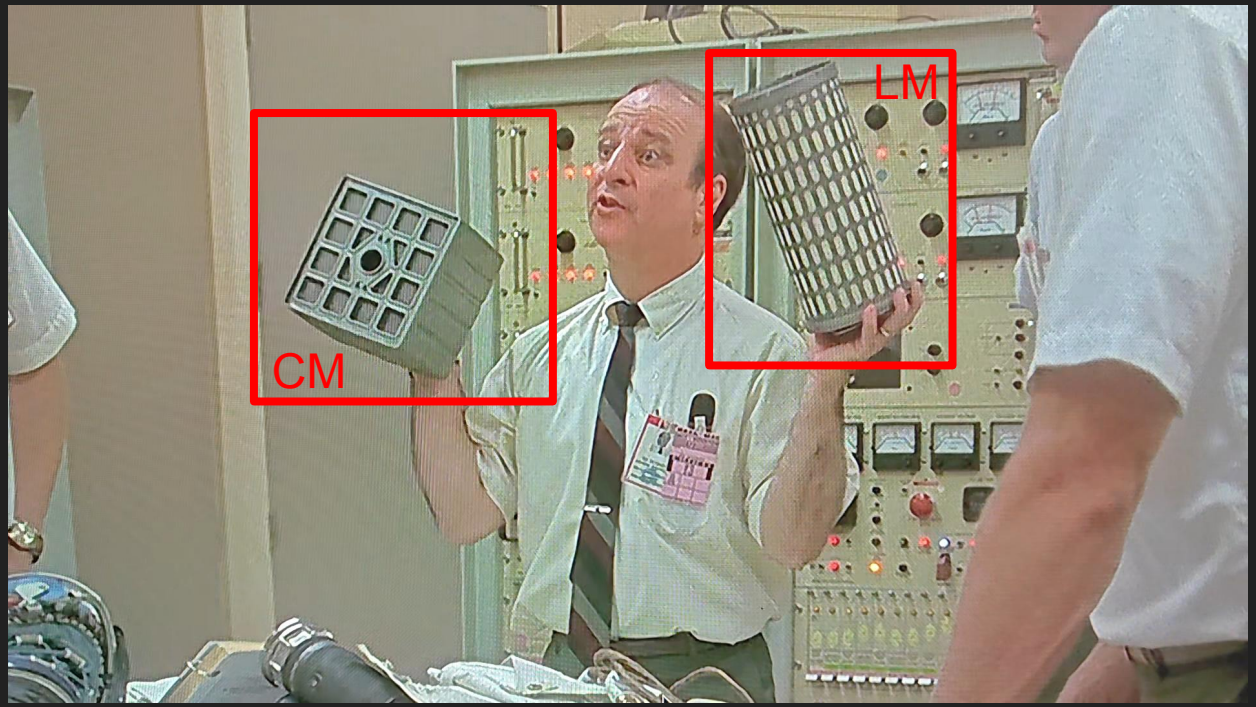




So this is the situation …

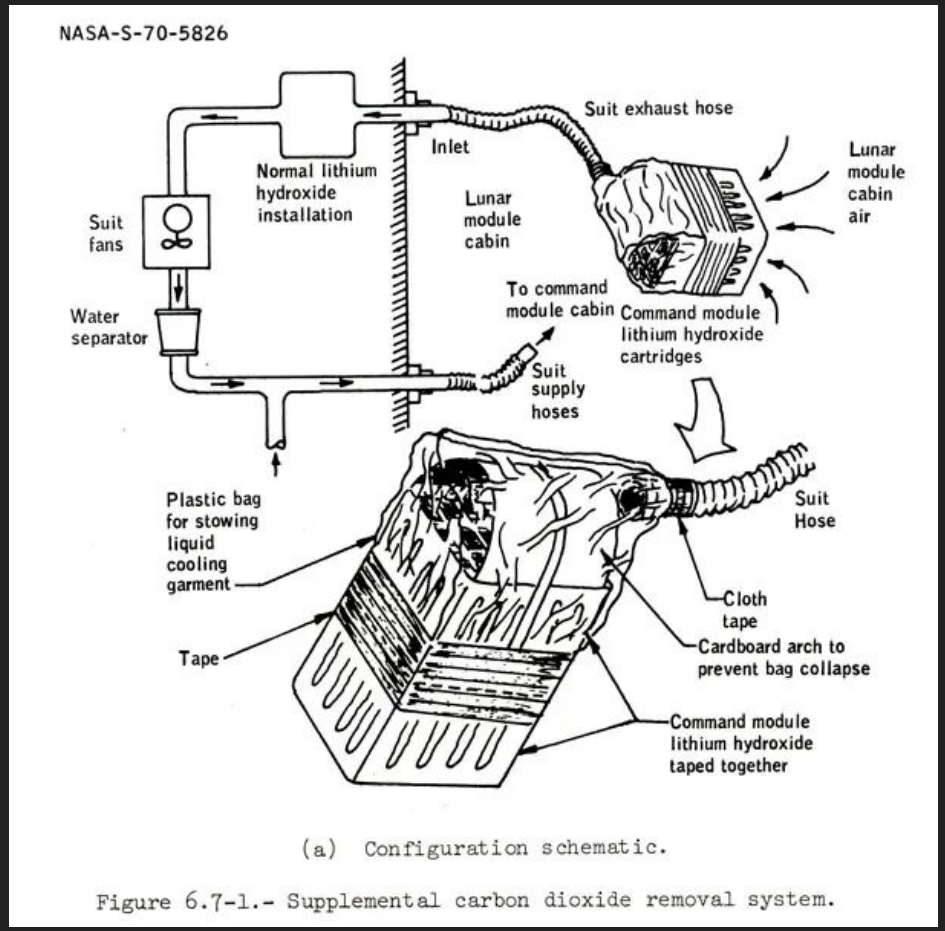
Flying back home

- New software written “on the flight” to use a different engine and nav comp
- Lots of math performed by the astronauts and checked at Mission control
- Lots of flight maneuvers made with only visual references
- About 10.000 things that needed to go absolutely right.
- The “mailbox” had to be imagined and built



“Apollo 13” - Universal Studios - 1995

The “Mailbox”



https://www.nasa.gov/wp-content/uploads/static/history/alsj/a13/ap13-S70-5826a-sm.jpg

The Point Of The Story

I am definitely not criticizing NASA design, I'm no rocket scientist

BUT

While there were contingency plans available…
… they couldn't take into consideration all the possible bad outcomes

The astronauts' life depended in large part on the ability of the ground team to know what was available, how it could be improvised, and create and transmit those instructions, with the astronauts performing flawlessly, under the stress of time and penalty of death.

The Point Of The Story - from the script of “Apollo 13”

GK - What about the scrubbers on the command module?

EE - They take square cartridges.

TM - The ones on the LM are round.

GK - Tell me this isn't a government operation.

TM - This isn't a contingency we've remotely looked at.

DR - Those CO2 levels are gonna be getting toxic.

Dealing with modes of failure

- A contingency plan is a strategic plan covering a possible bad outcome.
- It aims at emergencies or extraordinary situations.
- It is limited to what can be predicted, and can fail when faced with “different ways” the issue can happen.

- Solving a problem “by design” means removing the possibility of the mode of failure that can cause the problem.

…and so we get to Threat Modeling

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

– Threat Modeling Manifesto

….which is awesome, but what does it mean?

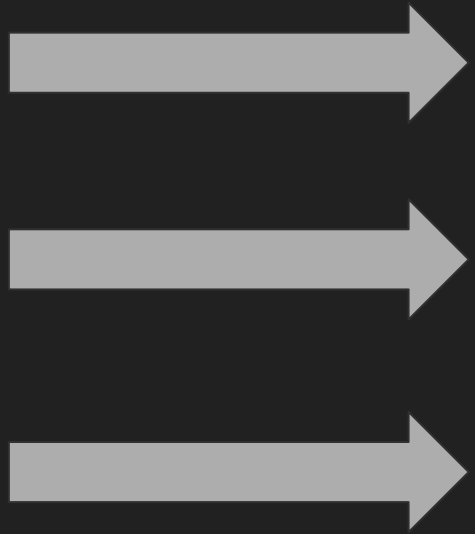
Threat Modeling is a process that intrinsically promotes those two newfangled approaches:

- Secure-by-design = “Secure-by-design” + Secure-by-default

If ALL the CO_2 scrubbers fit everywhere they are needed, then we CAN use them wherever needed whenever needed and no need for contingency plans.

4 Questions, 2 Parts, 1 artifact:

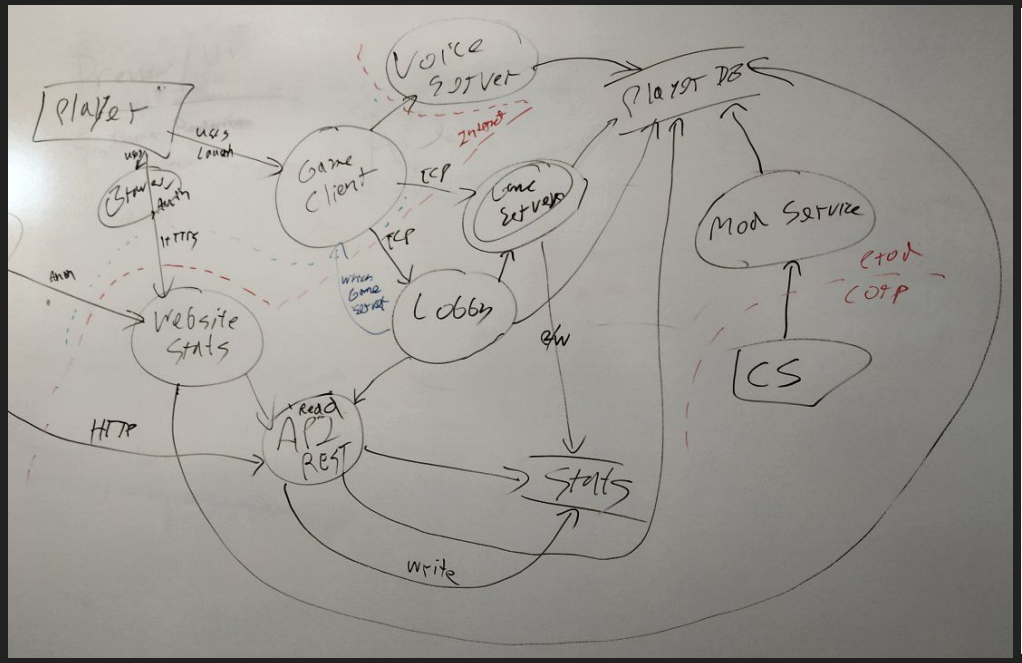
1. What are we building?
2. What could go wrong?
3. What will we do about it ?
4. Did we do a good job?

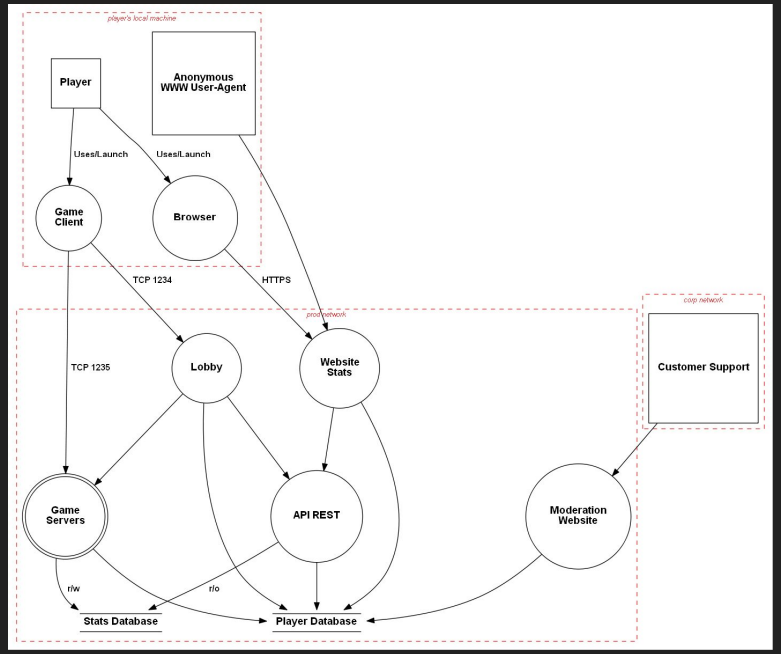


System Modeling

- Basically any way that suits the team: from formal modeling languages like SysML to a drawing on a napkin
- The important bit is that once the system is modeled, two things need to happen:
  - The participants can look back at the representation of the system, and recognize “this is what we are working on”
  - The representation is expressive enough to help elicit threats.

Dataflow Diagrams (DFDs) are a popular representation





https://github.com/OWASP/threat-model-cookbook/tree/master/Flow%20Diagram/online-battleroyale-game

Threat Elicitation

- What could go wrong?
- What could POSSIBLY go wrong?
- How BAD does it have to be?
- What if North Korea decides to break into my dog grooming business site?
- “Think like a hacker”. No. Really don’t.
- Threat libraries, security fundamentals, and everything in between

A bad example …

THREAT: something will break

MITIGATION: avoid something breaking

THREAT: secrets can leak

MITIGATION: stop secrets from leaking

A better example … THREAT/MITIGATION/PRIORITY

THREAT: too many requests too fast will cause the endpoint /abc to stop responding

MITIGATION: perform rate limitation, report on the number of requests/second, the number of successfully served and missed requests inside a configurable time period. This is a critical priority issue, as the endpoint is required for the service to run.

PRIORITY: MEDIUM - P2

THREAT: the key used for encrypting data at rest is available for any service account with read rights

MITIGATION: either accept this as a design feature, or limit access to the key to only the accounts that actually need to be able to use it, in which case this is a high priority issue

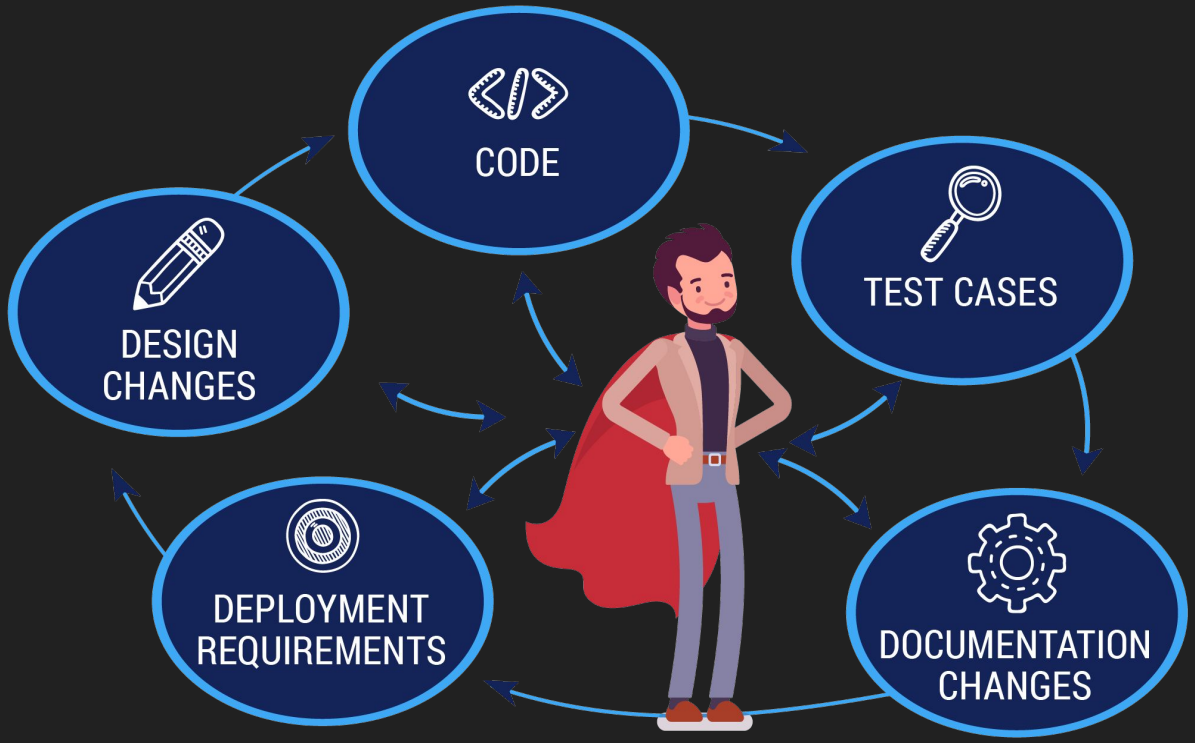
PRIORITY: REALLY IMPORTANT - P0

The result of a threat model should be ….

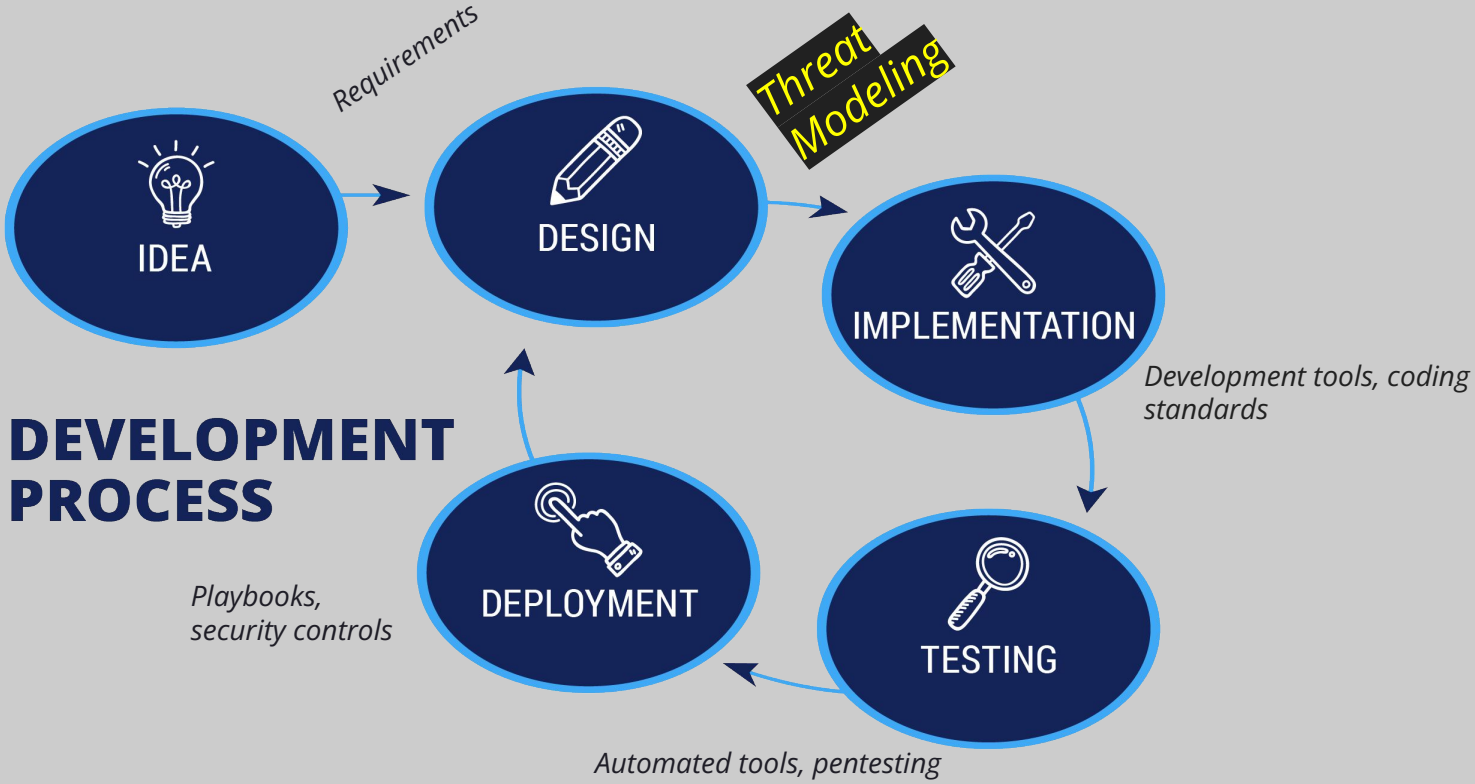
- A list of mitigations, for every flaw identified in the design that is open to exploitation by a threat actor via the existing attack surface

    - Actionable - developers, not security people
    - Shareable - among all who need to see it
    - Valuable - increments the security posture

The developer in today's Development Lifecycle



Threat Modeling in the Traditional SDLC



What value can Threat Modeling *actually* provide

Threat Modeling is an *expensive* process.

Design	*Secure-by-design*, eliminate whole classes of flaws, shrink attack surface
Implementation	*Secure-by-default* - secure libraries, known-good configurations, guardrails, paved road
Testing	Priorities and initial issues - what to test for and how - *the chewy bits*
Deployment	*Secure-by-default* - how the application interacts with its environment, secure services available, guardrails
Maintenance	New features tested in isolation, old code versus new threats

It is all about VALUE.

“The outcomes of threat modeling are meaningful when they are of value to stakeholders” - TMM

- There isn’t one magical methodology
  - There isn’t one perfect representation of a system
  - There are many ways to do threat elicitation
- The process takes time
  - Developers don’t like to give time to Security
  - Managers like even less
  - Training exists but is there is little absorption
- Requirements on developers:
  - Sparsely trained, but expected to provide perfect security
  - Security team is often a bottleneck

Threat Modeling Manifesto

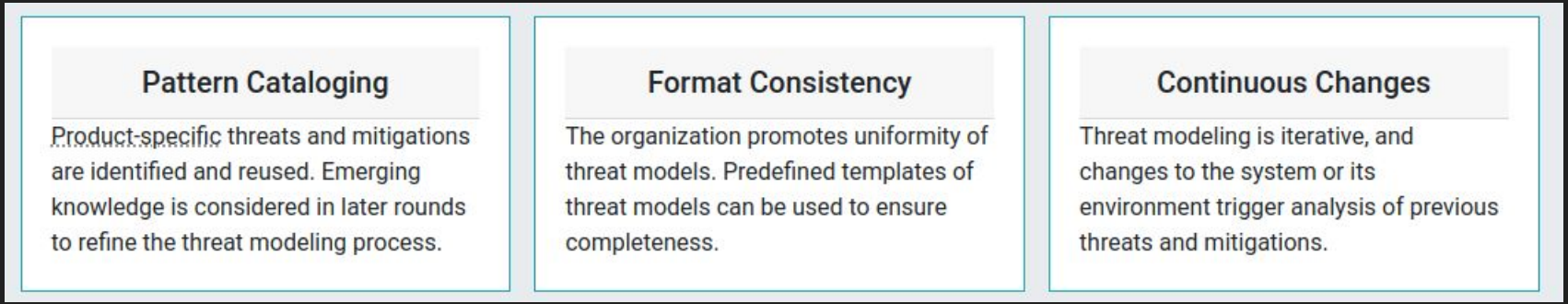
- 15 of the top voices in Threat Modeling education, research and execution sharing their experience

- 5 values:
  - A culture of finding and fixing design issues over checkbox compliance
  - People and collaboration over processes, methodologies, and tools
  - A journey of understanding over a security or privacy snapshot
  - Doing threat modeling over talking about it
  - Continuous refinement over a single delivery

- 4 principles
- 5 patterns
- 4 anti-patterns

Threat Modeling Capabilities

- Same authors, more or less
- It is a catalog of capabilities that help cultivate value from your threat modeling practice
- It is NOT a maturity document - we don't say how well you need to be doing something, only what you need to be threat modeling!
- 7 process areas



But there’s more!

- Managers love processes
- You can threat model processes as well

- In addition to developing contingencies and what-if-it-goes-wrong plans, you can apply threat modeling concepts to remove risk altogether!

- Let’s see a very simple example: going from home to the office

Threat Modeling Your Way Into The Office

- 0600AM! Wake up
  - What if my alarm doesn't ring ?
    - Double check it the night before
    - Set two separate alarms in two separate devices
- Get Dressed
  - My clothes are not presentable
    - Wear something else
    - Use a handheld vapor press
- Commute
  - It started raining
    - I didn't bring an umbrella!
- Arrive at the office
  - Have a spare change of clothes in the office, if your region has sudden rains

(better source and material: Dr. Michael Loadenthal, Univ. of Cincinnati - "Taking Threat Modeling Offline for IRL Human Application")

Threat Modeling Fails

- Do not bring value
  - Do not lead to security posture improvement
  - “Hero Threat Modeler”
  - “Admiration for the Problem”
- Do not express threats
  - At all
  - The *right* threats
    - “Tendency to Overfocus”
- Do not represent the system
  - “Perfect Representation”
- Dead threat models
  - No alignment to culture and practices

Orgs/teams/devs don't WANT to threat model

'Pushing security practices is a bit like selling insurance; people know they need it but nobody enjoys the associated costs.'

'...by adopting the perspectives of the decision-makers, we can grasp how they're likely to perceive our plans and attempts at persuasion.'

perspective-taking!

https://leaddev.com/security/supporting-influencing-and-leading-security-practitioner

How You Win

- People will start asking unprompted questions. When that happens, you won.
- People will refer to the threat model as part of documentation
- People will start asking “how can I ask better questions ?”
- People will start asking “where can I find security training ?”
- People will start asking “where is the threat model for X ?”
- Create a repeatable process and organize a threat modeling program

Takeaways

- It’s all about understanding your “customer” - try perspective-taking
- People cannot be forced to threat model, but they can be shown that they are already doing it
- Don’t expect perfection right at the start, threat modeling is an evolutionary practice
- A “bad” threat model is better than no threat model

More takeaways

- Make threat modeling a verb - say “let’s threat model this feature” rather than “bring me a threat model of this feature”
- Model and foster curiosity
- Everyone should threat model early and often
- You don’t need to be paranoid, but it helps!

Thank you! Questions?

Threat Modeling Manifesto - https://www.threatmodelingmanifesto.org

Threat Modeling Capabilities - https://www.threatmodelingmanifesto.org/capabilities/

“Threat Modeling: A Practical Guide For Development Teams” - https://amzn.to/3Ss8vlv

“Threat Modeling: Designing for Security”, Adam Shostack - https://amzn.to/3VLsXkq

“Building In Security At Agile Speed”, James Ransome & Brook Schoenfield - https://amzn.to/3MTDbuN

CISA “Secure By Design”, https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf