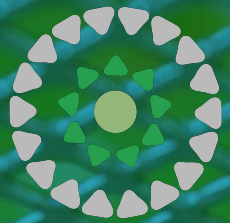


AGILE THREAT MODELLING

Continuous, timeboxed threat modelling to help teams talk about risk and build security in

ThoughtWorks®

THREAT MODELLING.

Thinking about things that can go wrong...

...so you can do something about them...

...***before*** they go wrong.


YOU ALREADY DO IT.

THREAT MODELLING IS...

... a process by which potential threats, such as structural vulnerabilities can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view - *Wikipedia*

... identifying, communicating, and understanding threats and mitigations within the context of protecting something of value - *OWASP*

... the use of abstractions to aid in thinking about risks - *Adam Shostack*

... Evil Brainstorming :) - *Tanya Janca*

It would be very remarkable if any system existing in the real world could be exactly represented by any simple model. The only question of interest is: ***"Is the model illuminating and useful?"***

GEORGE BOX

Statistician

METHODOLOGY. NO ‘BEST’ WAY

	Investment	Scope / System Model	Output	Good for
PASTA	Large	Exhaustive system model with multiple perspectives	Detailed risk assessments. countermeasures, system diagrams and essays	Comprehensive assurance exercises
Attack Trees	Take many hours to produce	Exhaustive for a single attacker motivation or goal	Graph like attack tree, overlaid with countermeasures. Can become quite complex	Focussing on a critical component in the context of a high risk attacker goal
😍 **Timeboxed STRIDE**	1 Hour Timebox Repeat iteratively	Small: This sprint’s changes Or big picture as security debt	Additional Acceptance Criteria, Tech Debt Stories, Additions to Definition of Done	**Agile teams**

Extended from Adam Shostack’s talk: https://i.blackhat.com/us-18/Wed-August-8/us-18-Shostack-Threat-Modeling-in-2018.pdf

WE ASK FOUR KEY QUESTIONS.

Agile Skills:

1. What are we building?

Component. Architecture and Flow Diagrams ✔

2. What can go wrong?

Brainstorming with STRIDE

3. What are we going to do about it?

User Stories, Acceptance Criteria, Definition of Done ✔

4. Did we do a good enough job?

Retrospectives ✔

WHO IS INVOLVED?

ENGINEERS

- Learn security
- Create a deeper understanding
- Guide secure design & testing
- Find threats missed by automation
- Shift security “left”

SECURITY TEAM

- Provide input in collaborative way
- Perspective of threat landscape
- Give context of controls
- Meet compliance needs
    - For example NIST 800-53

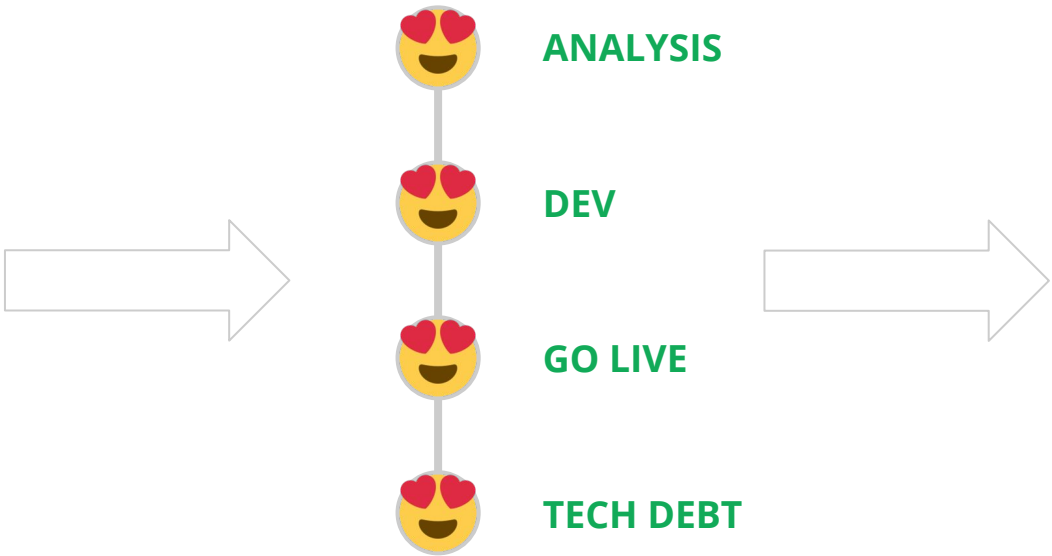
PRODUCT OWNER & BAs

- Prevent bad things from happening
- Save time doing security right
- Create a deeper understanding
- Prioritize according to risk
- Deliver on time

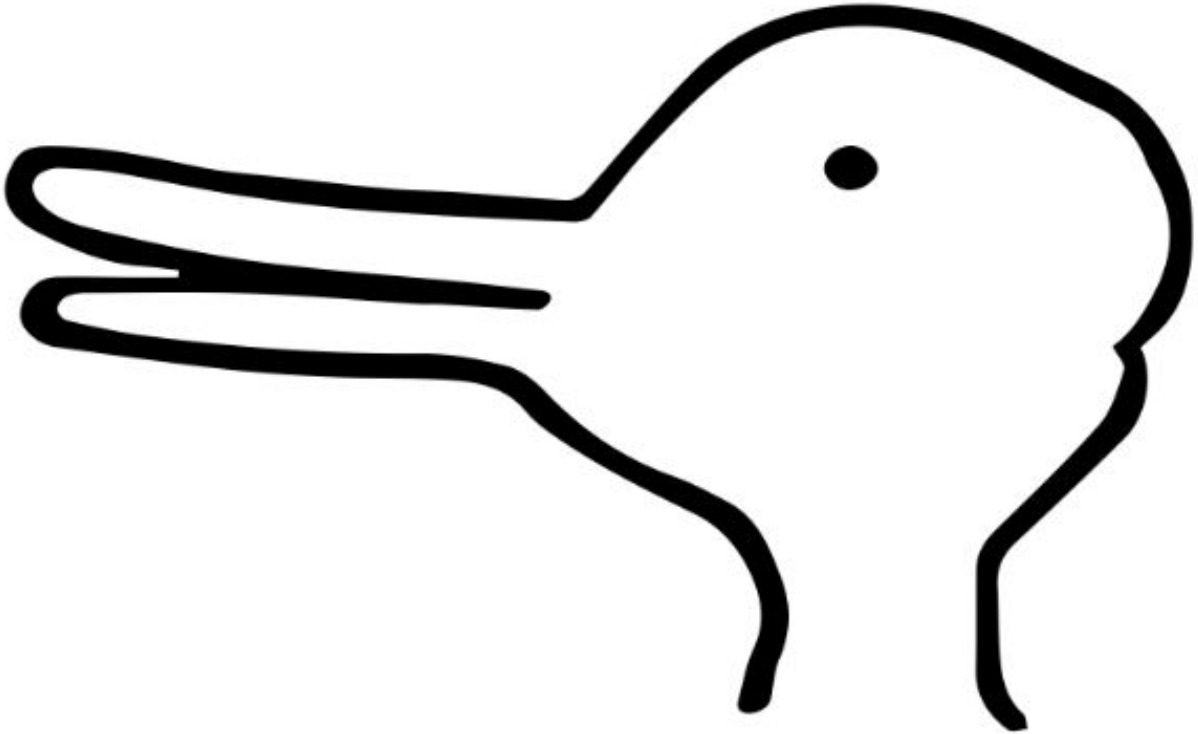
EVERYONE

- Reduce risk
- Greater confidence
- Breaks down silos

WHEN SHOULD WE DO IT?



BRAINSTORMING “WHAT CAN GO WRONG?”



SPOOFED IDENTITY

Can someone spoof an identity and then abuse its authority?

Spoofing identity allows attackers to do things they are not supposed to do.

KEY CONCEPTS:

- Identity
- Authentication

TAMPERING WITH INPUT

How hard is it for an attacker to modify the data they submit to your system?

Can they break a trust boundary and modify the code which runs as part of your system?

KEY CONCEPTS:

- Validation
- Integrity
- Injection

REPUDIATION OF ACTION

How hard is it for users to deny performing an action? What evidence does the system collect to help you to prove otherwise?

Non-repudiation refers to the ability of a system to ensure people are accountable for their actions.

KEY CONCEPTS:

- Non-Repudiation
- Logging
- Audit

INFORMATION DISCLOSURE

Can someone view information they are not supposed to have access to?

Information disclosure threats involve the exposure or interception of information to unauthorised individuals.

KEY CONCEPTS:

- Confidentiality
- Encryption
- Leakage
- Man in the middle

DENIAL OF SERVICE

Can someone break a system so valid users are unable to use it?

Denial of service attacks work by flooding, wiping or otherwise breaking a particular service or system.

KEY CONCEPTS:

- Availability
- Botnets
- DDoS / DDoSaaS

ESCALATION OF PRIVILEGE

Can an unprivileged user gain more access to the system than they should have?

Elevation of privilege attacks are possible because authorisation boundaries are missing or inadequate.

KEY CONCEPTS:

- Authorisation
- Isolation
- Blast radius
- Remote Code Execution


TIME FOR
THREAT MODELLING!

RETROSPECTIVE QUESTIONS

- Was there enough time?
- Did you have right resources?
- Was it easy to get started?
- Was the scope clear?
- Did you find the right range of threats?
- Could you perform this with your dev team?
- Who would you need in the room to get the most value out of the exercise?

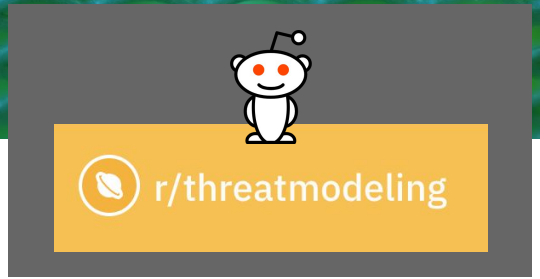
TAKEAWAYS

- You don’t have to be a security engineer or expert to threat model!
- You can pick up threats that you’ll never find with automation
- You can do threat modelling at any point in the delivery lifecycle
- Extend your existing ways of working and ask ‘what can go wrong?’
- There are lots of ways, but brainstorming with STRIDE is quick & flexible
- Actions might be stories, tasks, acceptance criteria or definition of done
- There’s a whole community out there to support with resources

LEARN MORE

Join 500 other threat modellers on #threat-modeling on OWASP's Slack

See Reddit :)



All things to do with threat and security modeling - from public examples to talks, tools and techniques

/r/threatmodeling/

Join the 'Security in our DNA' mailing list to ask questions and learn more

Security In Our DNA