Engineers & Exploits:

The Quest for Security

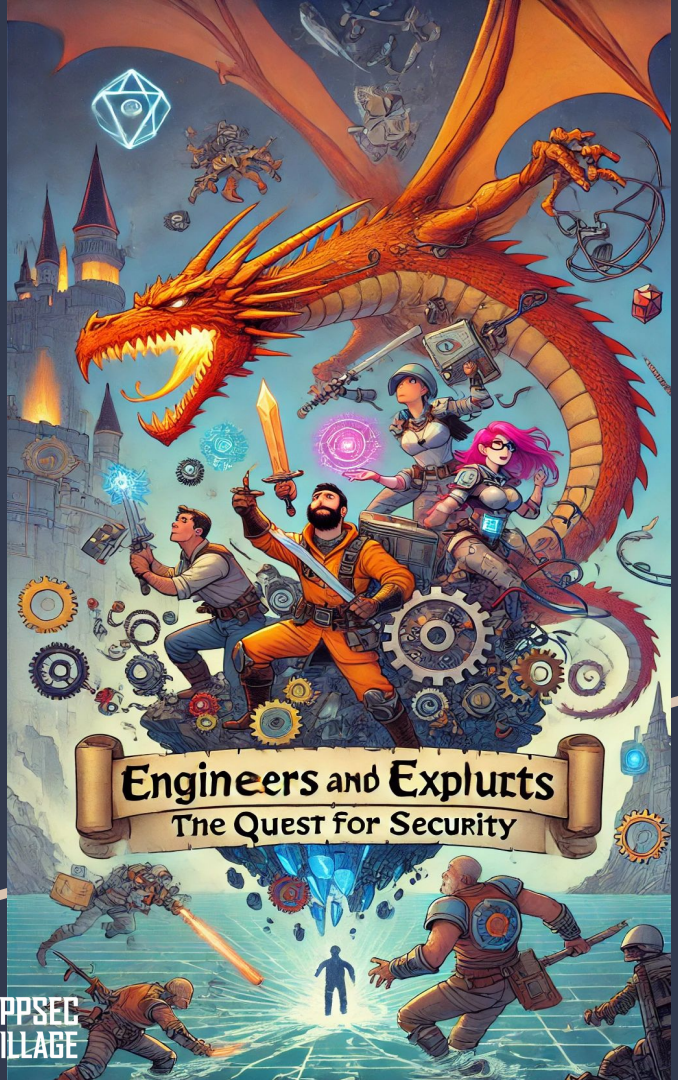
Andra Lezza OWASP/Sage

Spyros Gasteratos OWASP/Smithy

Sage

SMITHY

APPSEC VILLAGE



Summary

Threat Modelling

Insights

Cornucopia

Engineers & Exploits

whoami

Andra Lezza

Principal Application Security Specialist

OWASP London Chapter Leader

Spyros Gasteratos

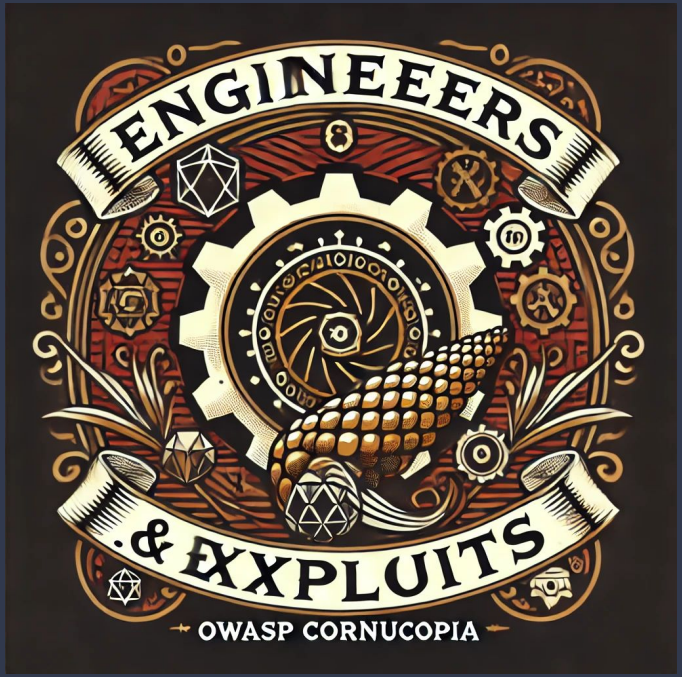
Security Engineer & Architect

OWASP OpenCRE Leader

APPSEC VILLAGE

Threat Modelling

The basics



APPSEC VILLAGE

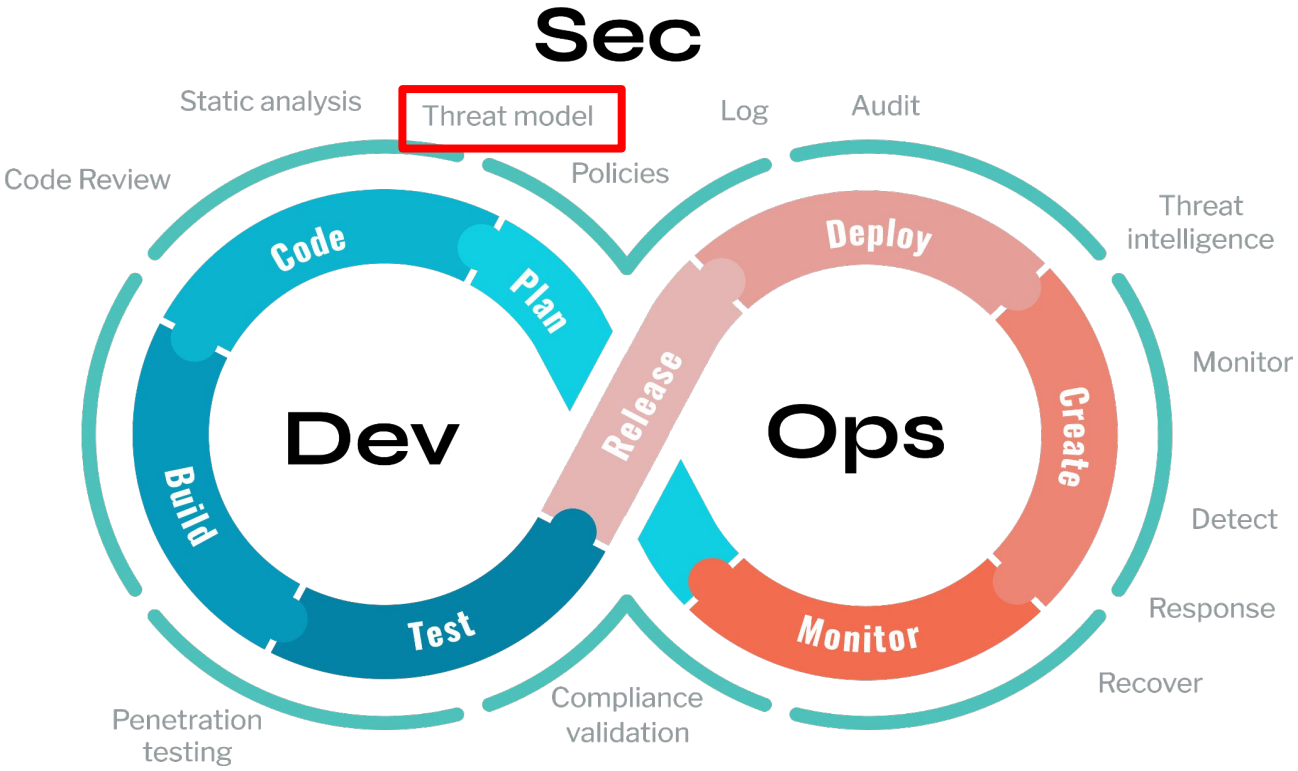
What is threat modelling?

Tabletop diagram ‘hacking’ 🤓
Security by design

*“a **structured, human-readable** representation of all the information that affects the security of a system. A view of the system and its environment through the lens of security.”*

APPSEC VILLAGE

When should we do threat modelling?

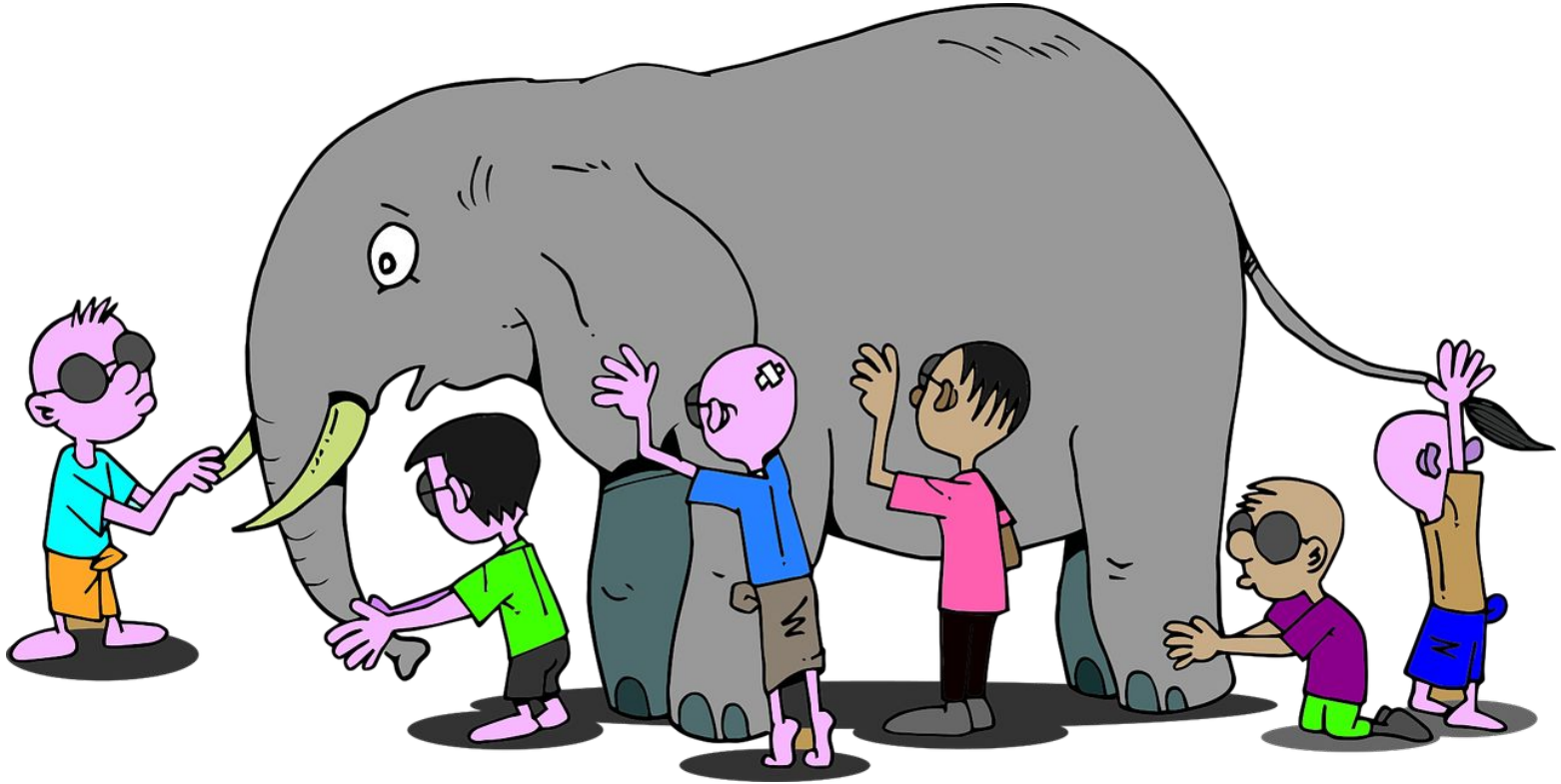


APPSEC VILLAGE

Security by design

APPSEC VILLAGE

Getting the full picture of a system/data flow



APPSEC VILLAGE

Exposure = Asset + Attack + Vulnerability

Asset	What we're trying to protect
Attack	What we're trying to protect against
Vulnerability	A weakness in our protection efforts
Exposure / Risk	What happens when an asset is vulnerable to an attack

APPSEC VILLAGE

The 4 questions

Framework

What are we building?

What can go wrong?

What are we going to do about it?

Did we do a good job?

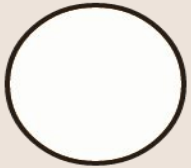
APPSEC VILLAGE

Data flow diagrams

External Entity

Any entiry controlled by the system or application

Process

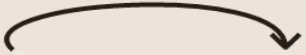


Command executables, libraries, services, endpoints

Data Store

Databases, files, queues, any data processed

Data Flow



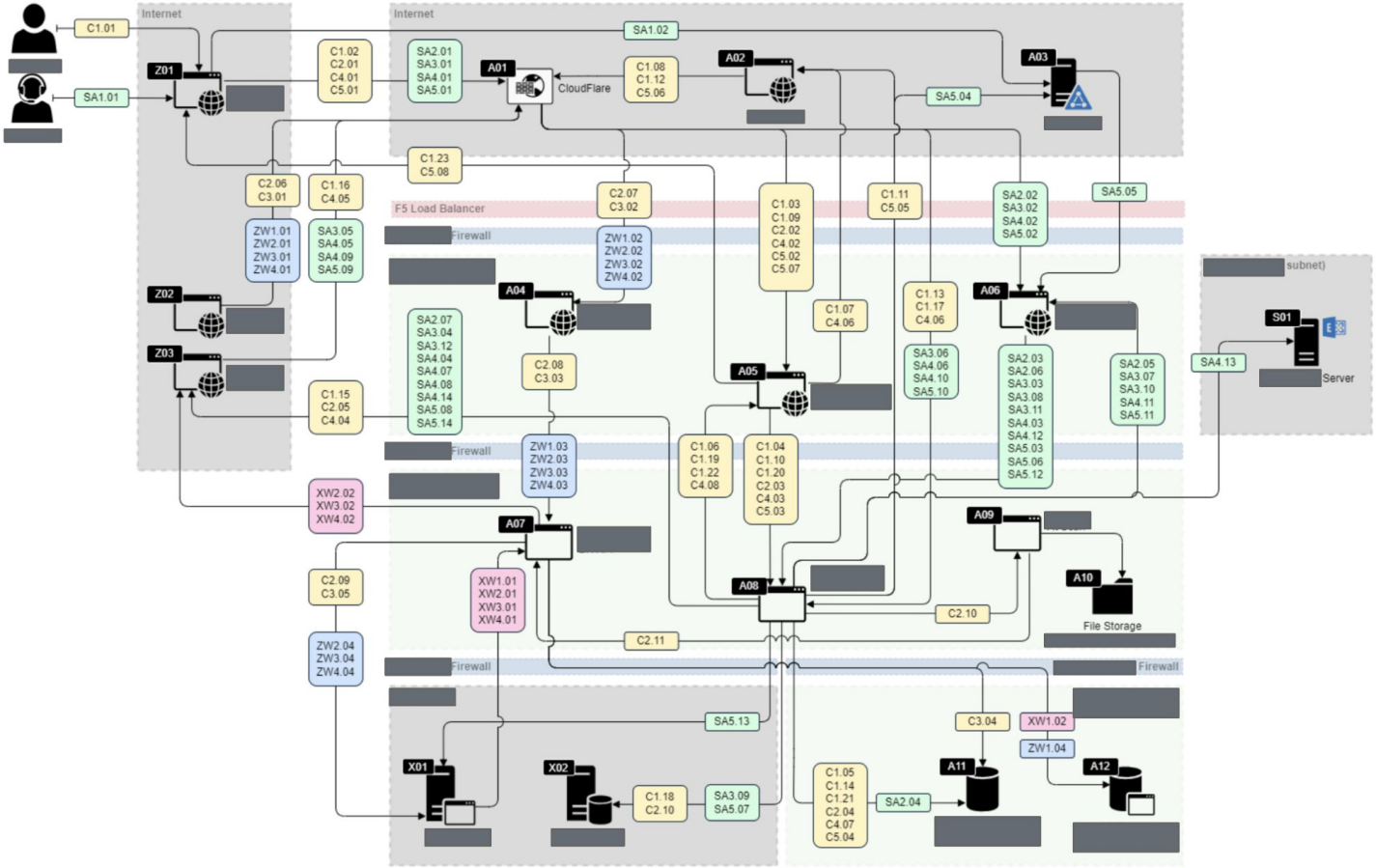
Any communication, traffic, call, etc between entities or process

Trust Boundary

Where trust levels change. Identifying the software's trust boundaries will help you focus on analyzing the areas of greater concern.

APPSEC VILLAGE

- Assets
→ Use cases
→ Dataflows
→ Threats



An example of a real world threat model - end goal

Approaches

STRIDE

PASTA

DREAD

LINDDUN

Attack trees

...

Tools

Games

- EoP
- Cornucopia

Threat modelling as code

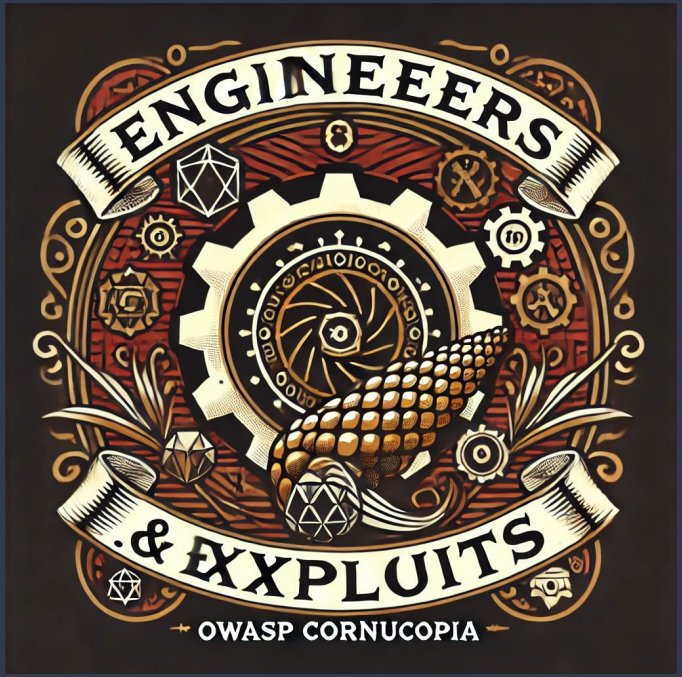
- PyTM
- Threagile
- HclTM

Threat modelling as diagrams/graphs

- ThreatDragon

Insights

Practical advice



APPSEC VILLAGE

Lessons learned ...
from the battle front of threat modelling in the real world

People have little **time**, engineers have even less

→ be efficient with the time you're given by the team

→ make sure everyone's on the same page about what's being built and delivered

Don't assume familiarity with **terms**

→ all of the above

→ SQLi, XSS, etc.

Don't just point and ask where the threats are on a data flow

Do not assume every threat needs to be mitigated - **context** matters!

Threat models can easily get out of hand

→ focus on parts of the system (**incremental** threat modelling)

→don't try to cover everything

APPSEC VILLAGE

Lessons learned …
from the battle front of threat modelling in the real world

People have little **time**, engineers have even less

→ be efficient with the time you're given by the team

→ make sure everyone's on the same page about what's being built and delivered

Lessons learned …
from the battle front of threat modelling in the real world

People have little **time**, engineers have even less

→ be efficient with the time you're given by the team

→ make sure everyone's on the same page about what's being built and delivered

Don't assume familiarity with **terms**

→ all of the above

→ SQLi, XSS, etc.

Lessons learned ...
from the battle front of threat modelling in the real world

People have little **time**, engineers have even less

→ be efficient with the time you're given by the team

→ make sure everyone's on the same page about what's being built and delivered

Don't assume familiarity with **terms**

→ all of the above

→ SQLi, XSS, etc.

Don't just point and ask where the threats are on a data flow

Lessons learned ...
from the battle front of threat modelling in the real world

People have little **time**, engineers have even less

→ be efficient with the time you're given by the team

→ make sure everyone's on the same page about what's being built and delivered

Don't assume familiarity with **terms**

→ all of the above

→ SQLi, XSS, etc.

Don't just point and ask where the threats are on a data flow

Do not assume every threat needs to be mitigated - **context** matters!

Lessons learned ...
from the battle front of threat modelling in the real world

People have little **time**, engineers have even less

→ be efficient with the time you're given by the team

→ make sure everyone's on the same page about what's being built and delivered

Don't assume familiarity with **terms**

→ all of the above

→ SQLi, XSS, etc.

Don't just point and ask where the threats are on a data flow

Do not assume every threat needs to be mitigated - **context** matters!

Threat models can easily get out of hand

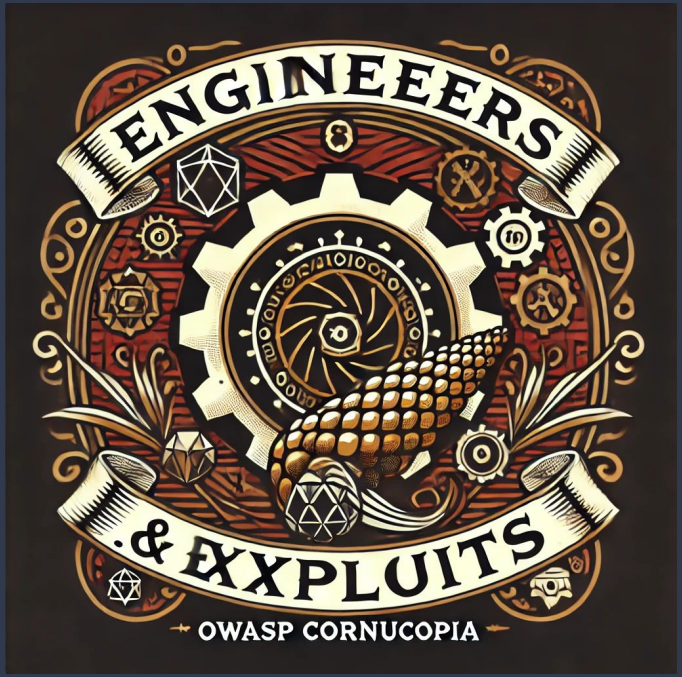
→ focus on parts of the system (**incremental** threat modelling)

→don't try to cover everything

APPSEC VILLAGE

Cornucopia

The game



APPSEC VILLAGE

What is Cornucopia?

- An OWASP® Project
- **Leaders & team**:
  - Colin Watson, Grant Ongers, Johan Sydseter, Xavier Godard
- Created & first user for developer training in **August 2012**
- 2 current decks
  - Web App & Mobile versions
- A threat modelling **mechanism** in the form of a card game
- Language & platform - agnostic
- Helps development teams
  - **identify** appsec requirements
  - **develop** security-based user stories

Web App suits

APPSEC VILLAGE

Pros

- Easy to start playing
- Tactile, has physical aspect / Fun online game
- Great for threat modelling with developers

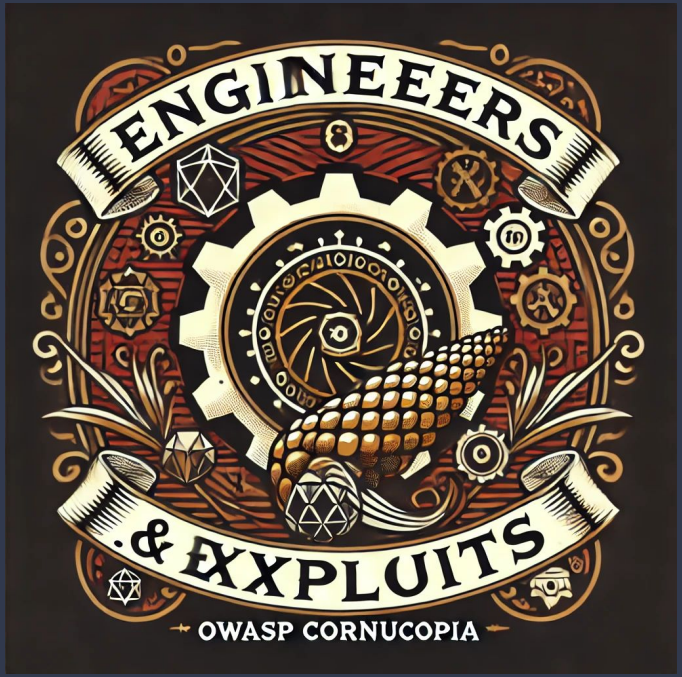
Cons

- Security people often struggle to pick it up
- If you play with specific threats in your mind, you can overlook exploits
- Security beginners struggle to go from “what is a risk” to “how do I rephrase the risk out of technical jargon”

Engineers & Exploits

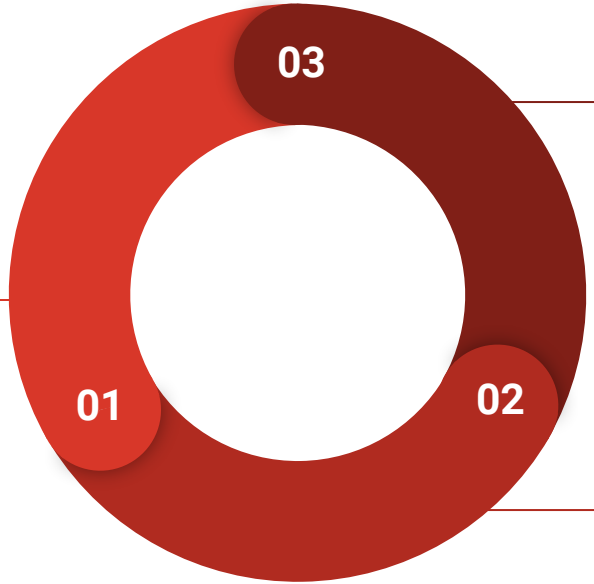
How it’s different

Why it helps



APPSEC VILLAGE

Threat modelling best done by teams in their own time



Teams become self-sufficient

AppSec trains the trainers*

Engineers & Exploits

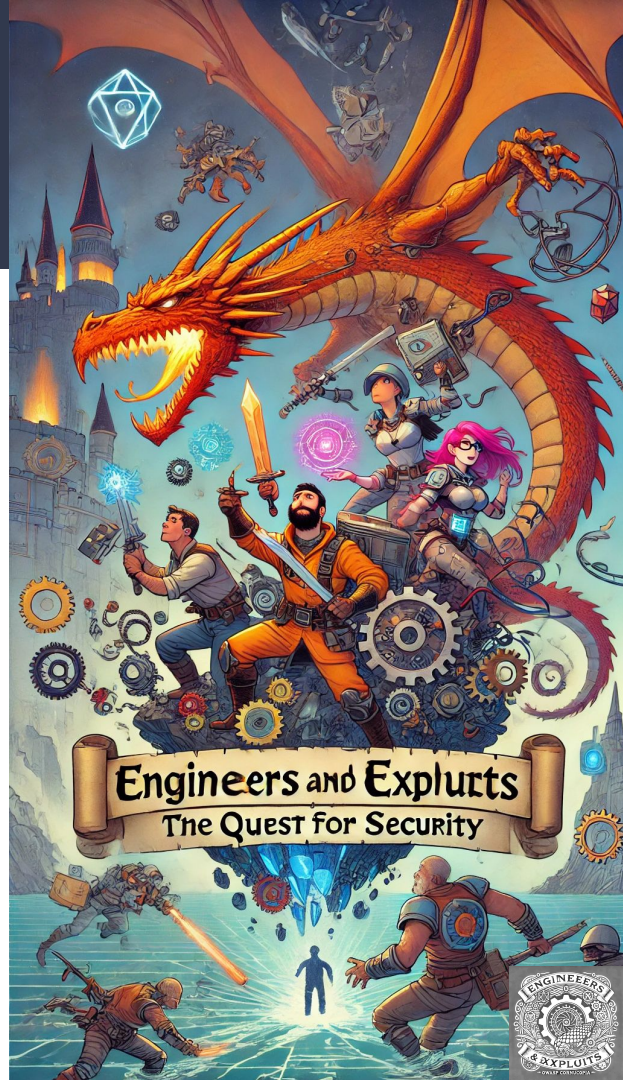
Trainers teach dev teams

APPSEC VILLAGE

*trainers = other security people, architects, developers, etc.

Introducing … Engineers & Exploits

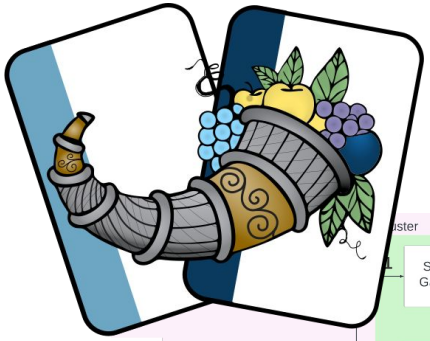
→ D&D for threat modelling nerds

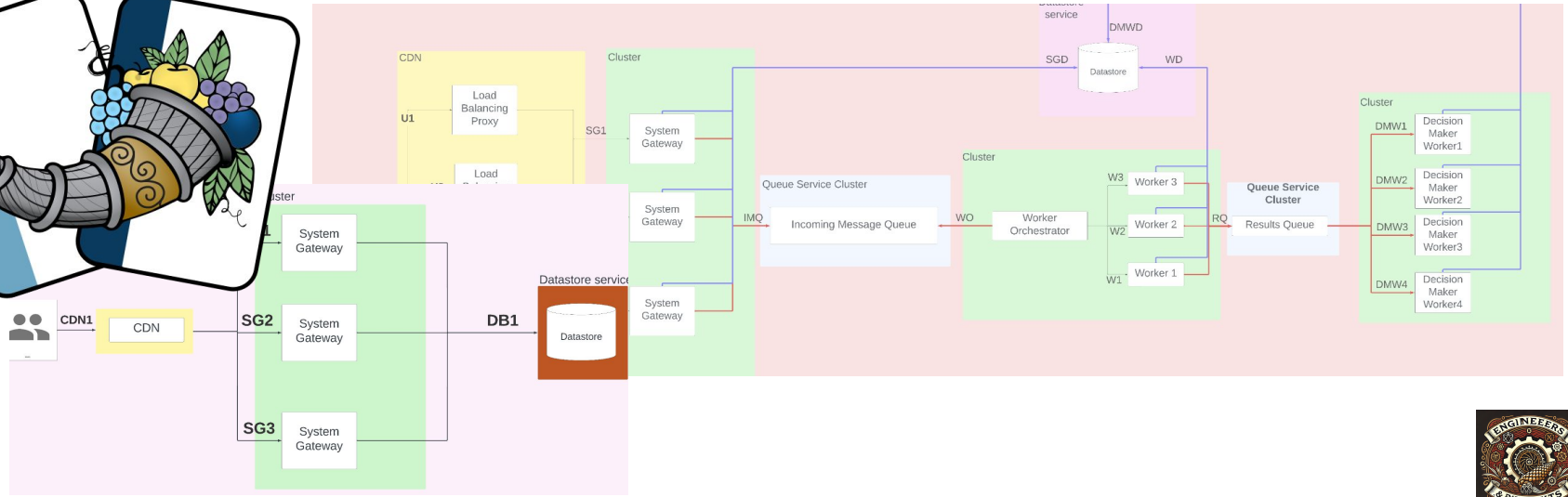


APPSEC VILLAGE

What is it?

- Sample diagrams → ***"What are we building?"***
- Reference app provided to introduce security people to threat modelling with **Cornucopia**
- As secure as the Game Master wants it to be 🤓





APPSEC VILLAGE

Rules

1 Game Master (preferably an experienced threat modeller / TheMostConfidentDevEver 🙄)

Up to **7** players (better with **4**) 👫👫👫

Players are threat modeling consultants: → ***"What can go wrong?"***

- take turns playing cards trying to find as many threats* as possible
- need to convince the GM that their threat is worth fixing

WIN: The person with the most threats wins ♠️

*You CAN steal points if a player can't explain a card, but you find it applicable otherwise

APPSEC VILLAGE

Tips & Tricks

As a Game Master

- You are a dev who's unaware of security - not thick
- Be a little bit precious with points - threats must be valid

→ ***What are we going to do about it?***

- Encourage a positive atmosphere

APPSEC VILLAGE

Tips & Tricks

As a player:

- You are there to learn a new way of hacking or organizing your thoughts
- Have fun!
- Play your cards
- Try to win, but in the end it’s all about learning

Activity: Threat modelling fun session with Cornucopia

📅 August 11, 11:00 - 13:00

APPSEC VILLAGE

Questions?

Andra Lezza - linkedin.com/in/andralezza/

Spyros Gasteratos - linkedin.com/in/spyr/

APPSEC VILLAGE