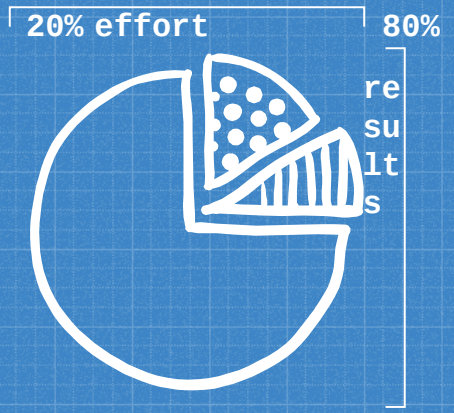
Old Pareto had a chart

Getting 80% benefits of threat modelling with 20% of effort

”Innovative software and secure development practices are not a contradiction.”

You can find me at:

@IreneMichlin



1

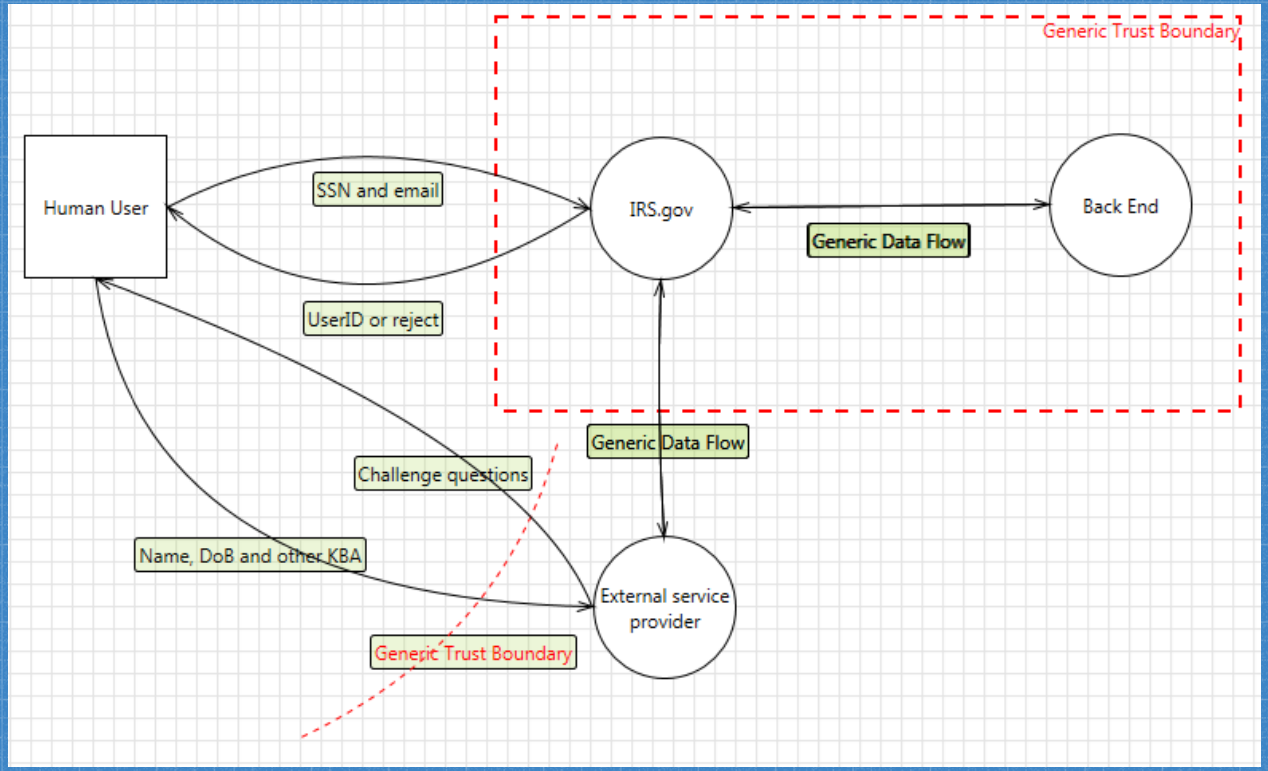
What is Threat Modelling?

And why do I care?

Software-centric Threat Modelling

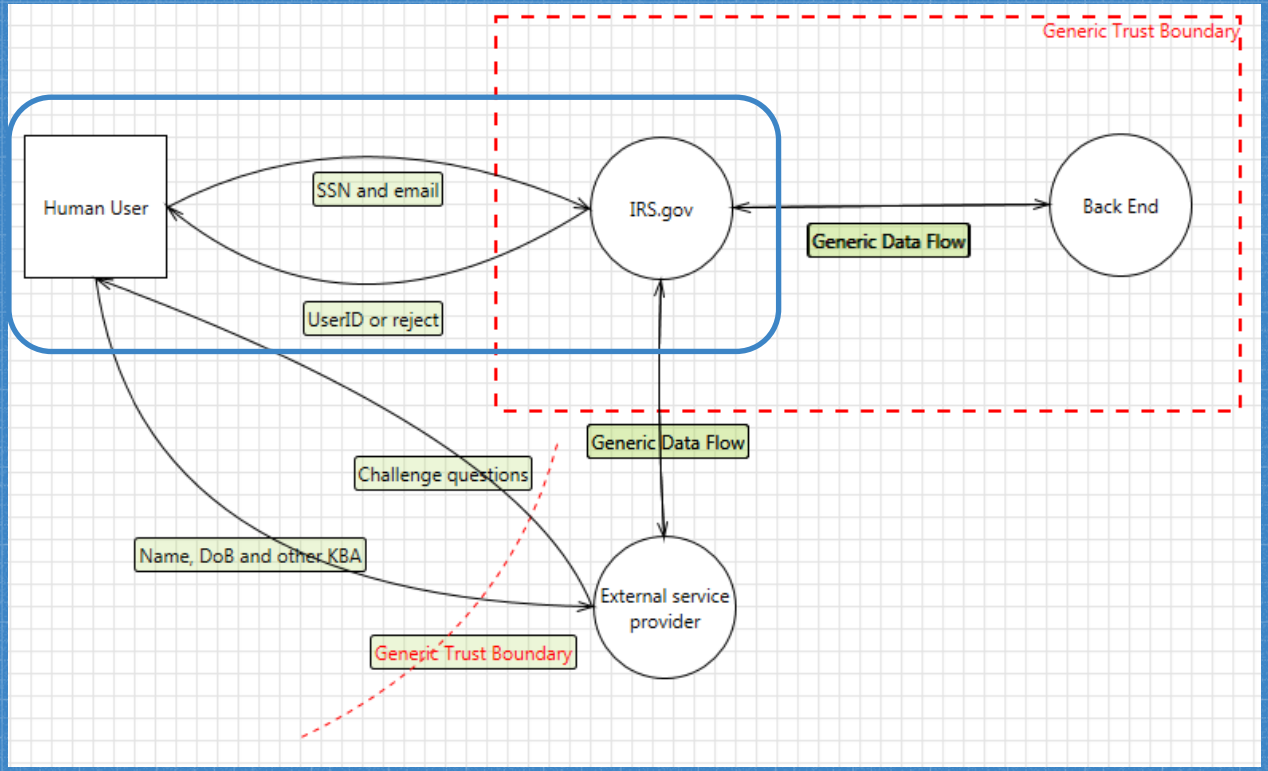
1. **What are we building?**
2. **What can go wrong?**
3. **What are we going to do about that?**
4. **Have we done a good enough job?**

Data Flow Diagrams

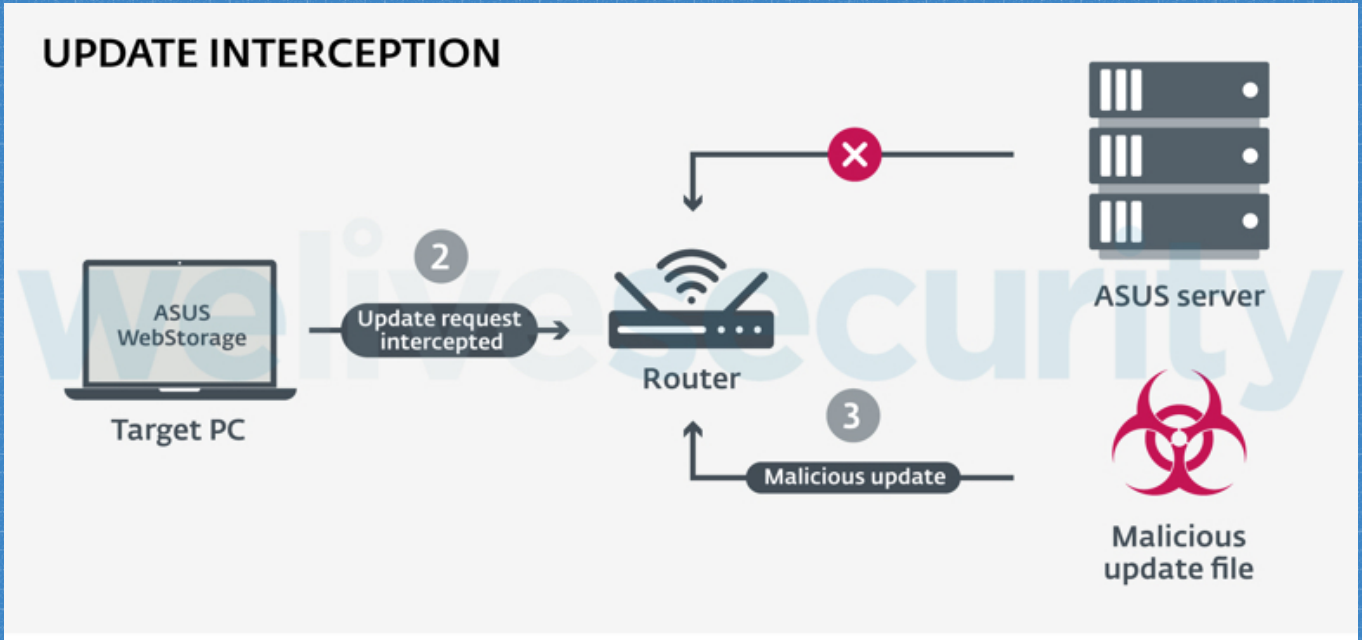


Threat	Property	Definition
Spoofing	**Authentication**	Impersonating something or someone else
Tampering	**Integrity**	Modifying data or code
Repudiation	**Non-repudiation**	Claiming to have not performed an action
Information Disclosure	**Confidentiality**	Exposing information to non-authorised party
Denial of Service	**Availability**	Deny or degrade service
Elevation of Privilege	**Authorization**	Gain capabilities without proper authorisation

Spoofing


Generic Trust Boundary
Human User
SSN and email
IRS.gov
Back End
Generic Data Flow
UserID or reject
Generic Data Flow
Challenge questions
Name, DoB and other KBA
External service provider
Generic Trust Boundary

Tampering



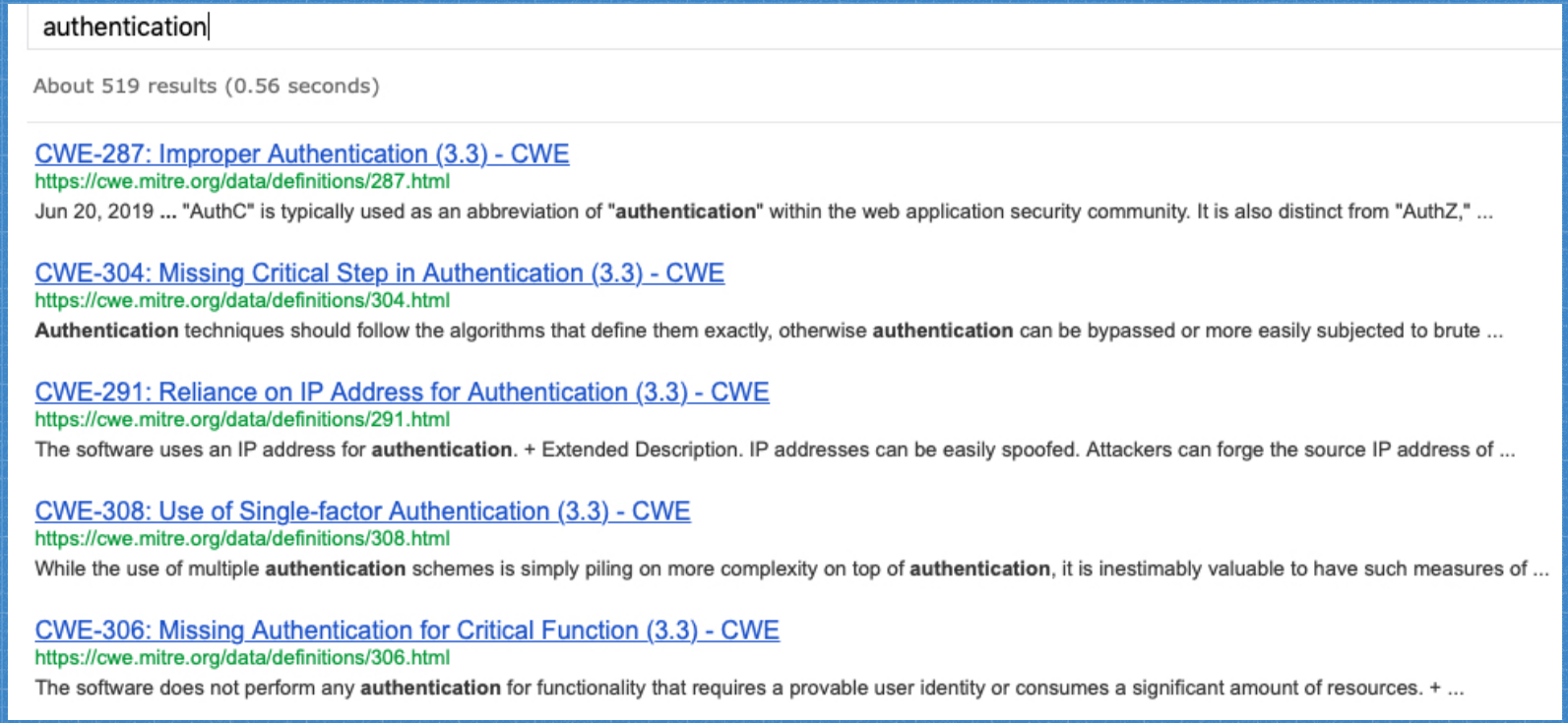
Source: https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage

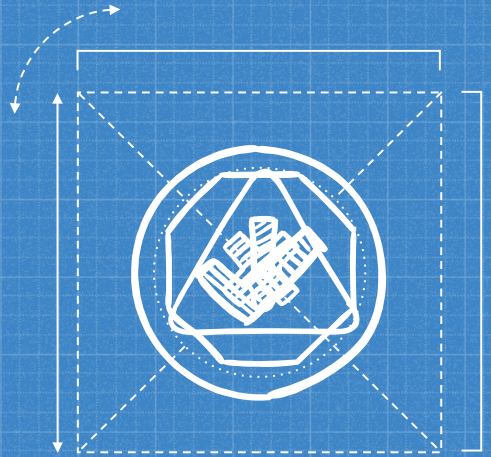
Other sources of threats

- Attack trees
- https://www.owasp.org/index.php/OWASP_Cloud_Security_Project
- CWE: https://cwe.mitre.org/data/definitions/1008.html
- SANS TOP25: https://www.sans.org/top25-software-errors
- ATT&CK: https://attack.mitre.org
- OWASP Top 10: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Domain specific threat libraries

Irene, are you kidding? Stop throwing extra work at us!

Can’t remember all of that all the time





Security Team

Need one example of “Good”

2

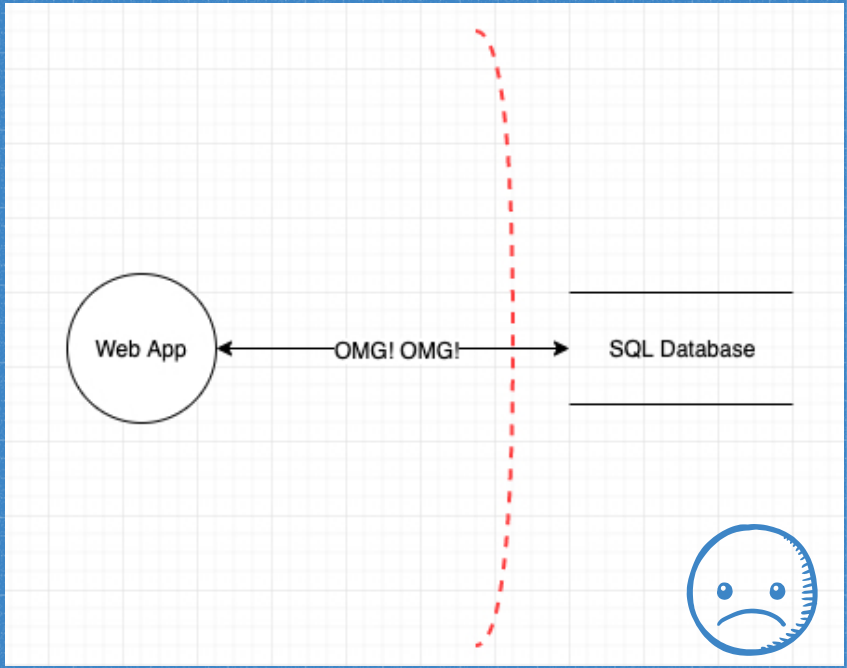
Threat Modelling aids

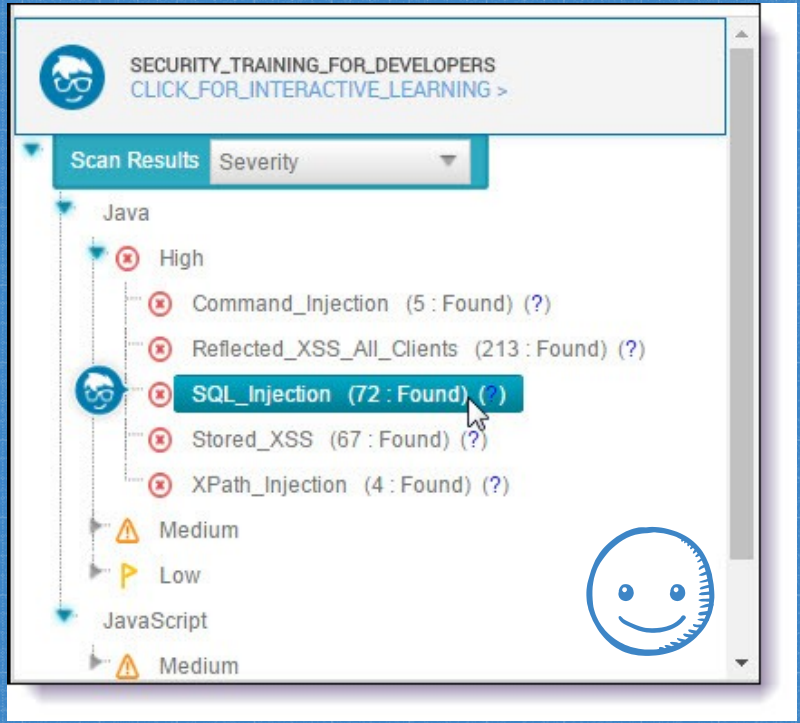
Automated and semi-automated

Secure Development tools

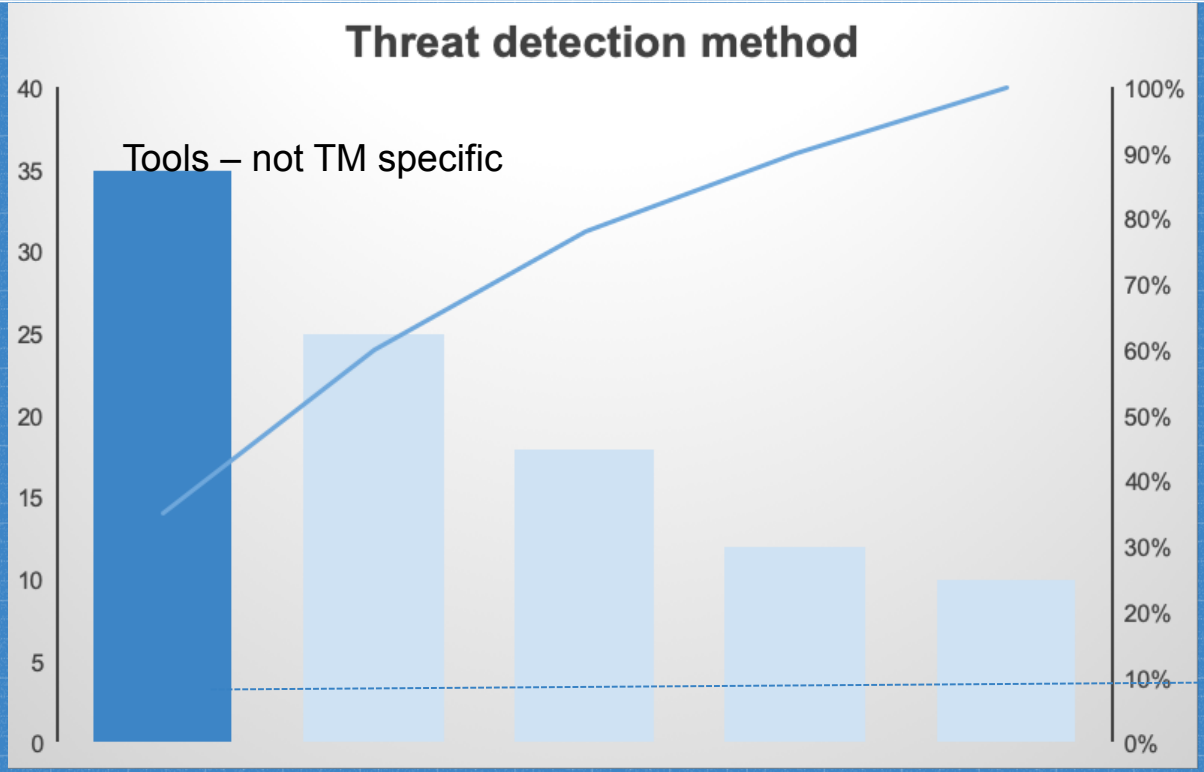
- Static Analysis
- Dynamic Analysis
- Fuzzing
- Open Source Analysis
- Code quality automated checks
- Compliance automated checks

People’s time is precious



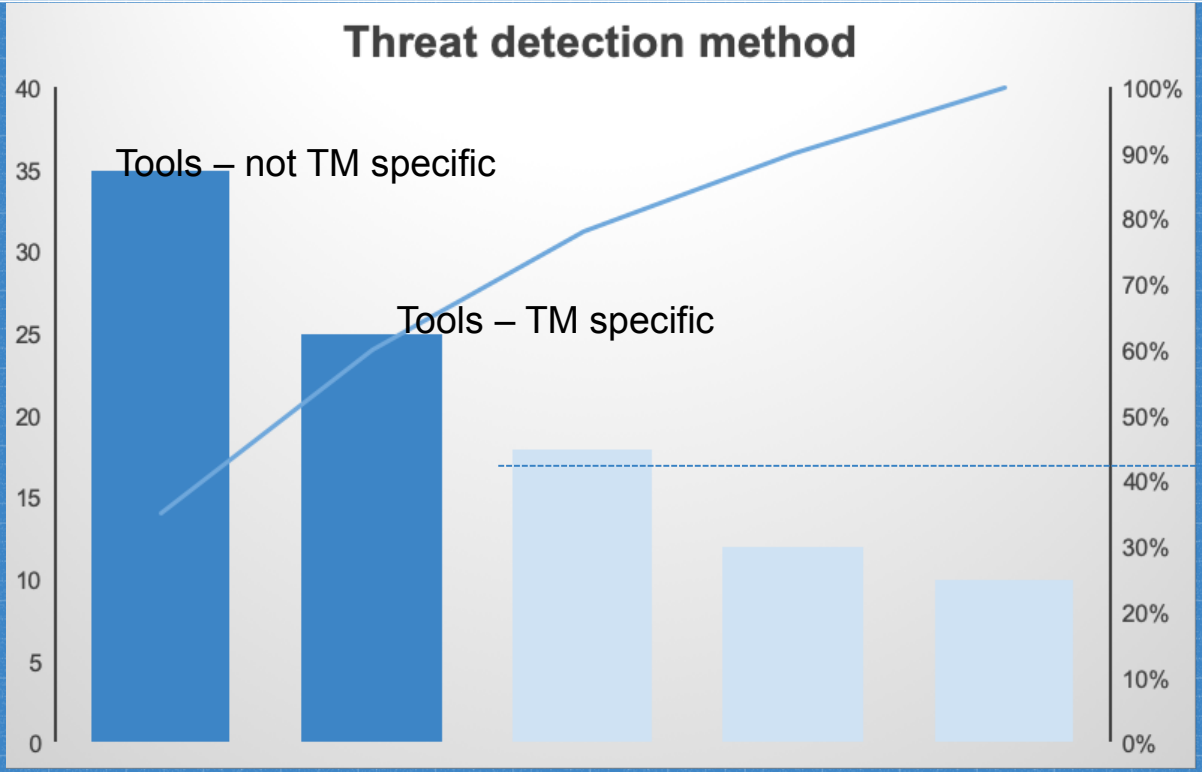


https://checkmarx.atlassian.net/wiki/spaces/KC/pages/78544949/Scan+Results+Example+v8.2.0


Threat detection method
Tools – not TM specific
40
35
30
25
20
15
10
5
0
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

Threat modelling tools

- Microsoft Threat Modeling tool (free)
- ThreatModeler
- IriusRisk (free community edition)
- SDElements
- OWASP ThreatDragon (free)
- Tutamantic (free community edition)


Threat detection method
40
35
30
25
20
15
10
5
0
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Tools – not TM specific
Tools – TM specific

3

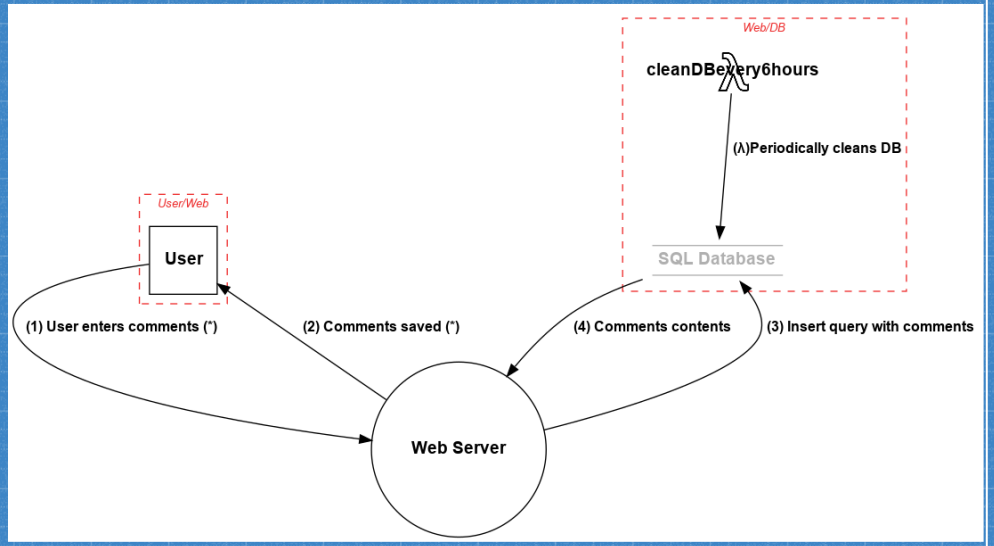
DevSec Collaboration

Add Ops for extra marks

pytm: A Pythonic framework for threat modeling

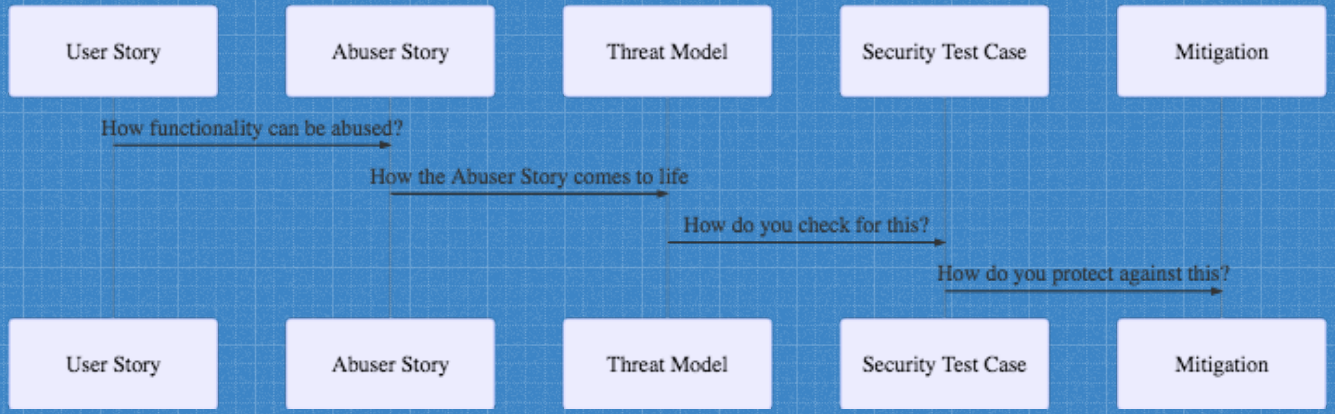
- https://github.com/izar/pytm
- @izar_t

```
User_Web = Boundary("User/Web")
Web_DB = Boundary("Web/DB")

user = Actor("User")
user.inBoundary = User_Web

web = Server("Web Server")
web.OS = "CloudOS”
web.isHardened = True
```



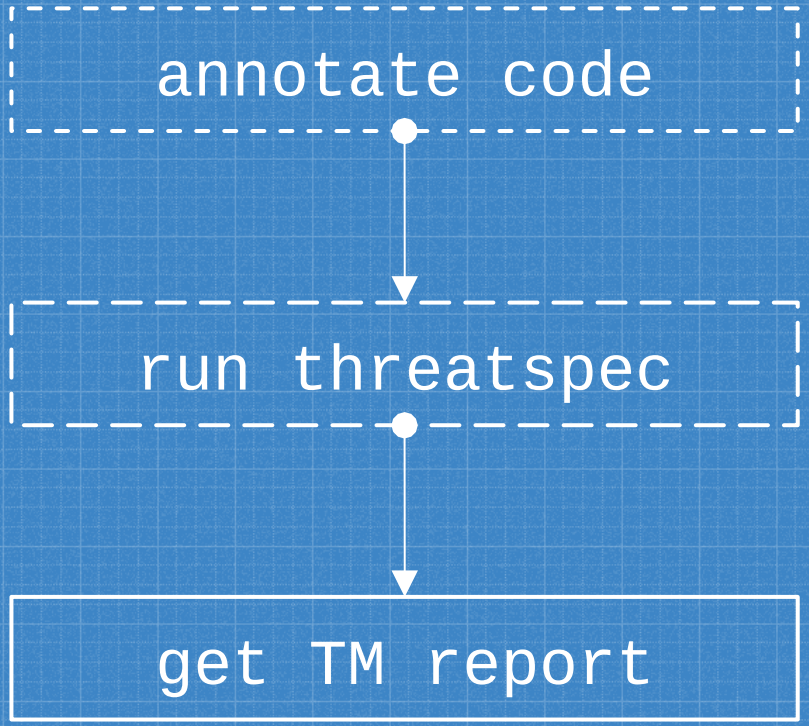
ThreatPlaybook

- https://github.com/we45/ThreatPlaybook
- @abhaybhargav



https://threatspec.org

- @zeroXten



Threagile

- https://threagile.io
- @cschneider4711
- Threat Models as declarative YAML file
  - Data Assets
  - Components
  - Communication Links
  - Trust Boundaries
- Generates diagrams and threat reports

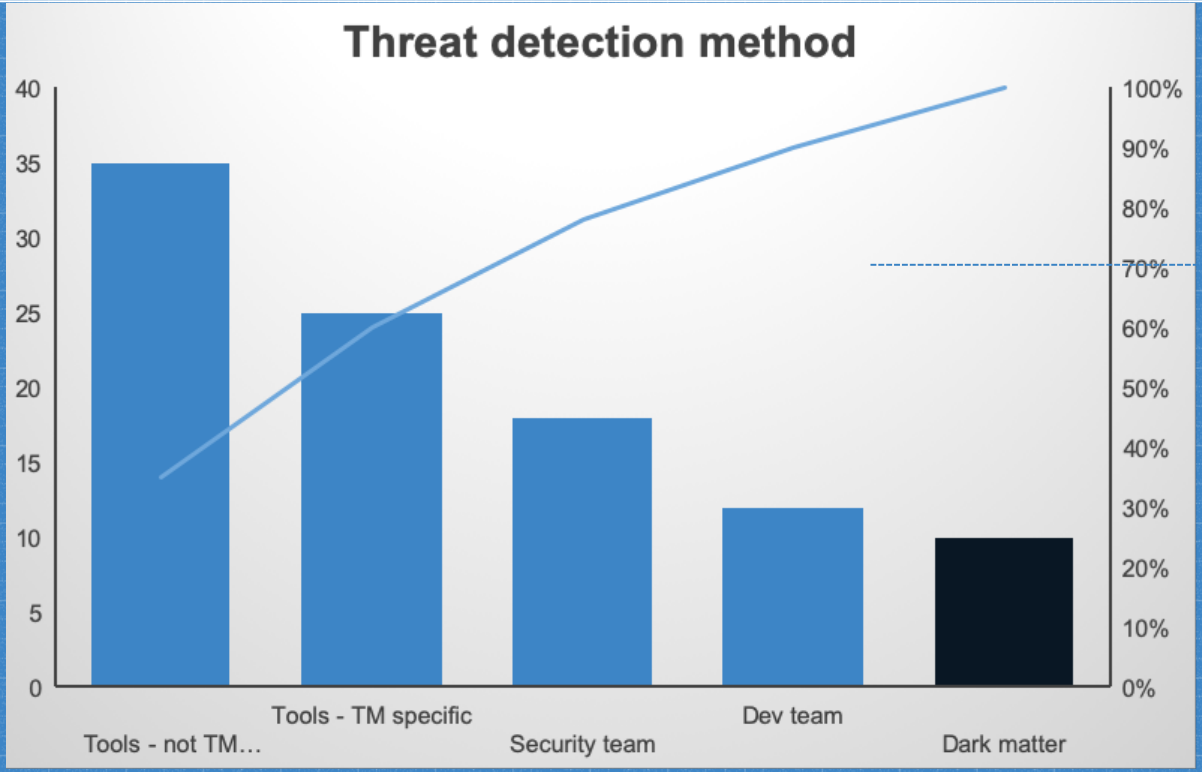
materialize-threats

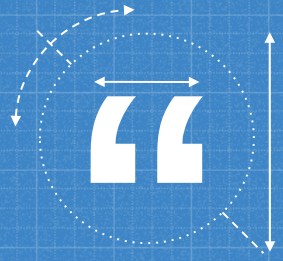
- https://github.com/secmerc/materialize-threats
- Parse draw.io diagrams
- Enumerates threats
- Suggests mitigations and tests

Good collaboration practices

-
-
-
-

ent
patterns


Threat detection method
40
35
30
25
20
15
10
5
0
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Tools - not TM…
Tools - TM specific
Security team
Dev team
Dark matter



All models are wrong, but some are useful

https://www.threatmodelingmanifesto.org

- Use the Manifesto as a guide to develop or refine a methodology that best fits your needs.

Thanks!

ANY QUESTIONS?

You can find me at:

@IreneMichlin

irene221b@gmail.com

CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash