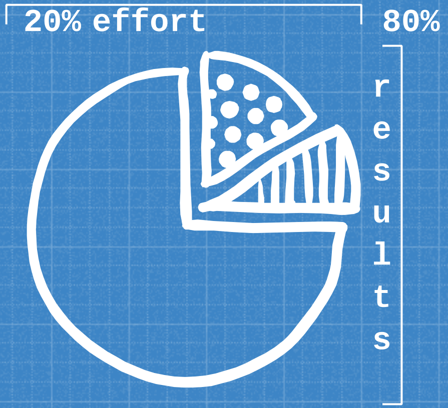
Old Pareto had a chart

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

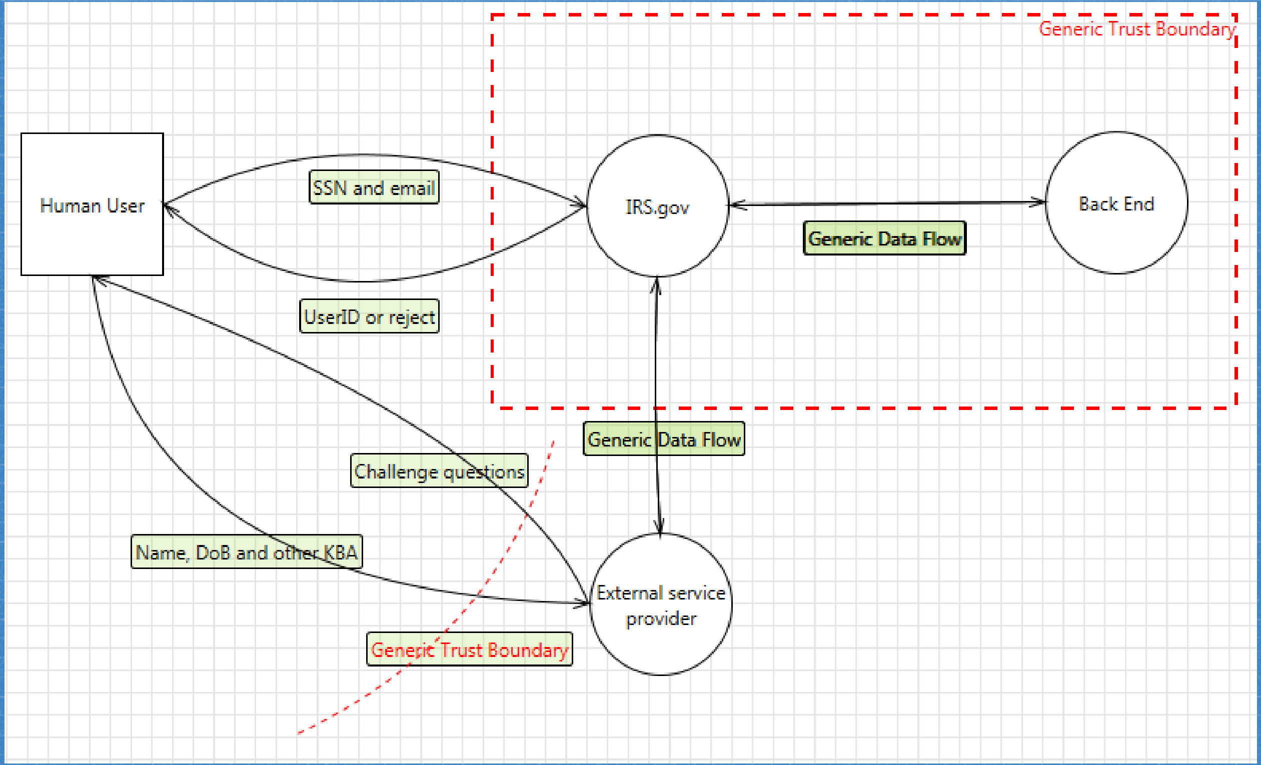
What is Threat Modelling?

And why do I care?

Software-centric Threat Modelling

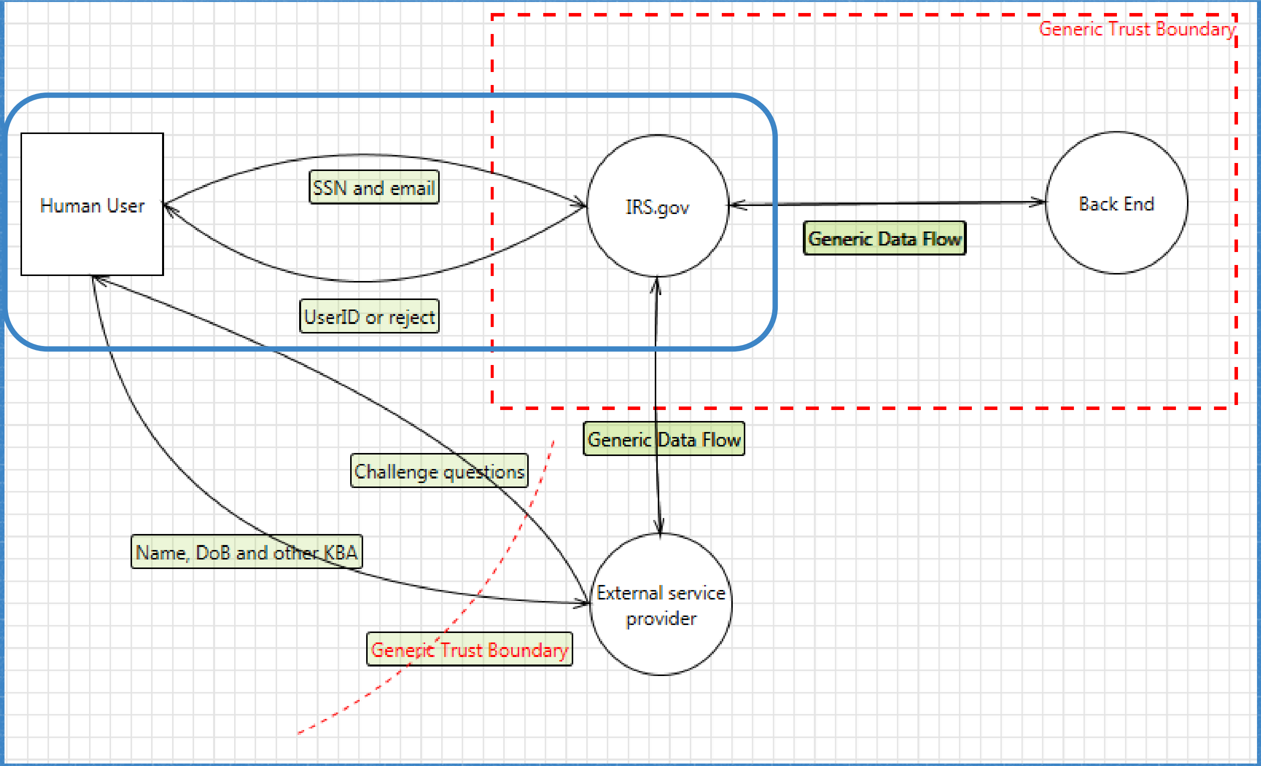
1. **What are we building?**
2. **What can go wrong?**
3. **What are we going to do about that?**
4. **Have we done a good enough job?**

Data Flow Diagrams

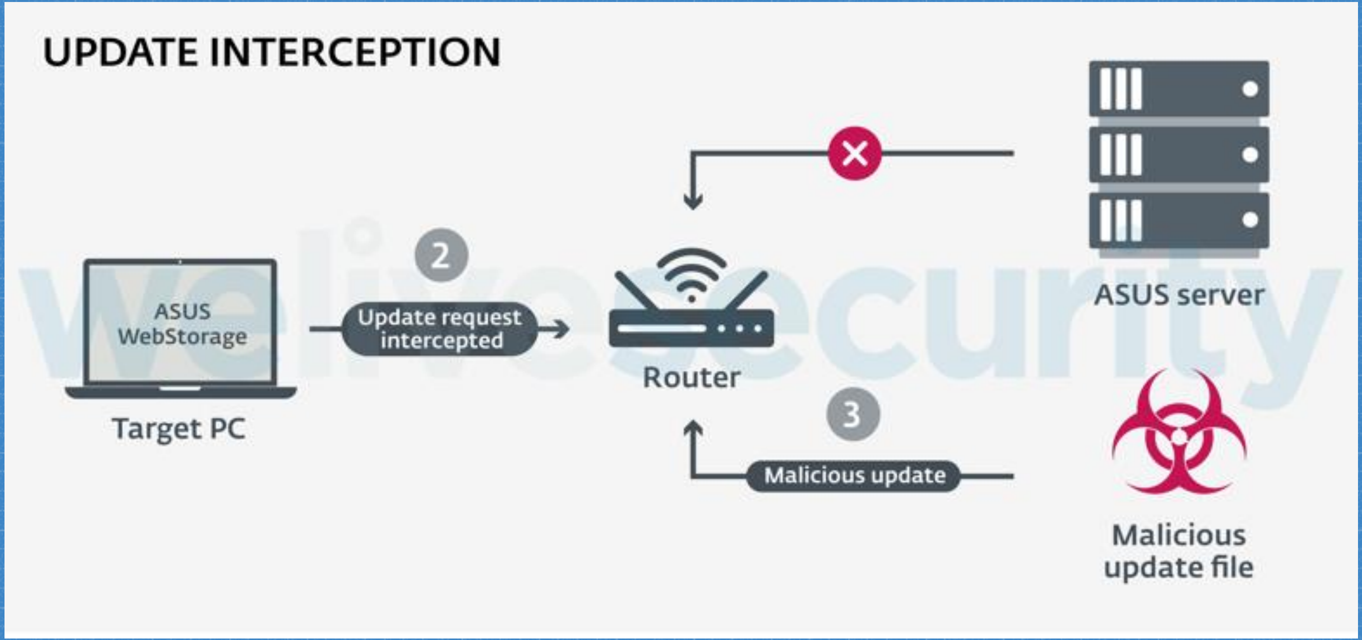


Threat	Property	Definition
Spoofing	**Authentication**	Impersonating something or someone else
Tampering	**Integrity**	Modifying data or code
Repudiation	**Non-repudiation**	Claiming to have not performed an action
Information Disclosure	**Confidentiality**	Exposing information to non-authorised party
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



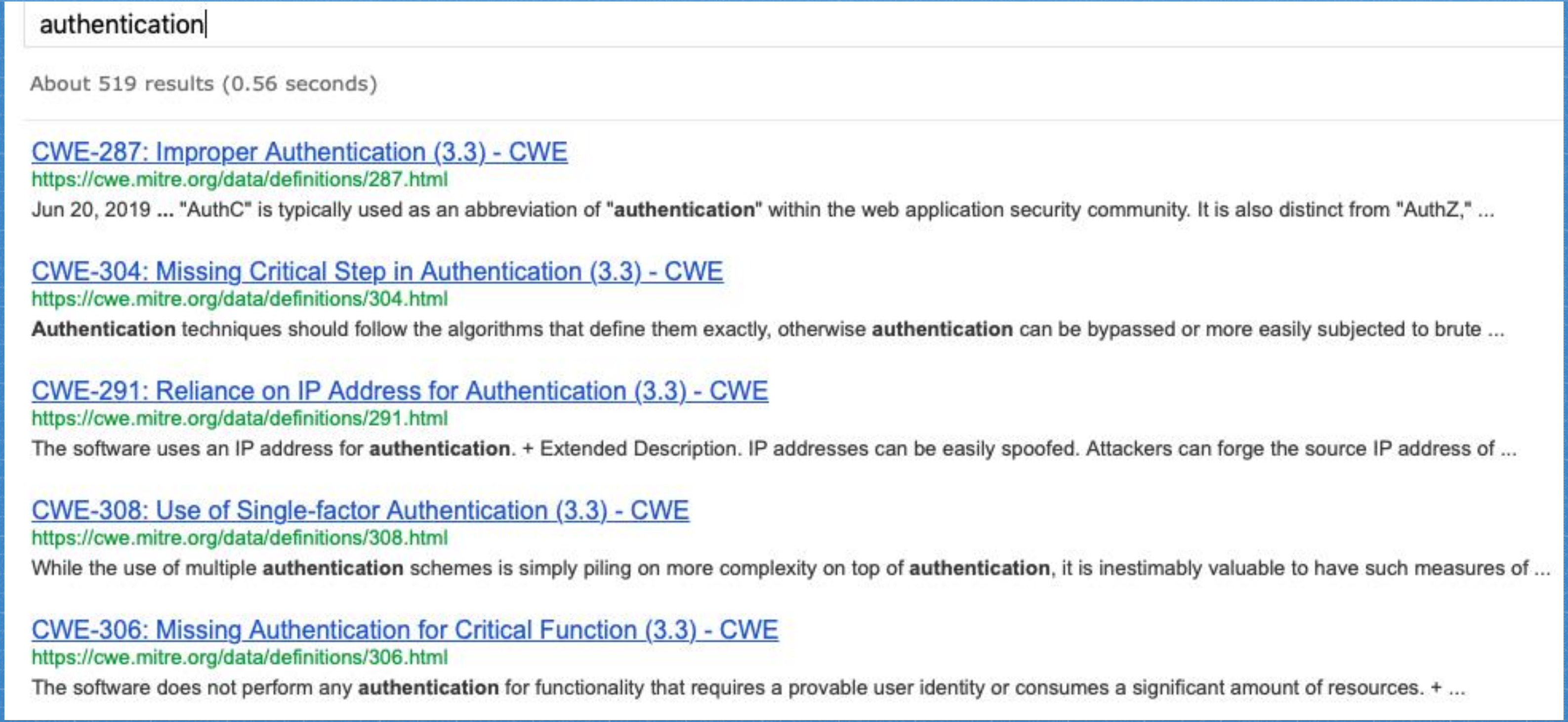
Source: https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage

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



authentication

About 519 results (0.56 seconds)

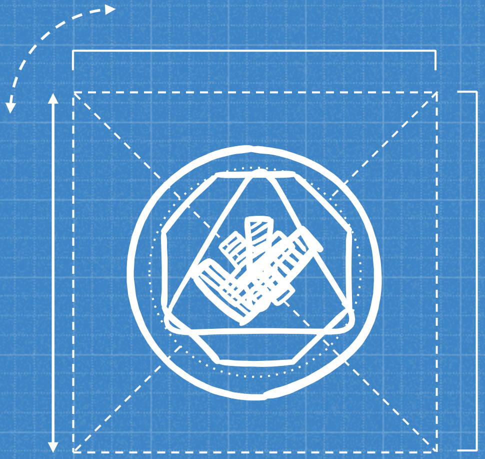
CWE-287: Improper Authentication (3.3) - CWE
https://cwe.mitre.org/data/definitions/287.html
Jun 20, 2019 ... "AuthC" is typically used as an abbreviation of "**authentication**" within the web application security community. It is also distinct from "AuthZ," ...

CWE-304: Missing Critical Step in Authentication (3.3) - CWE
https://cwe.mitre.org/data/definitions/304.html
Authentication techniques should follow the algorithms that define them exactly, otherwise **authentication** can be bypassed or more easily subjected to brute ...

CWE-291: Reliance on IP Address for Authentication (3.3) - CWE
https://cwe.mitre.org/data/definitions/291.html
The software uses an IP address for **authentication**. + Extended Description. IP addresses can be easily spoofed. Attackers can forge the source IP address of ...

CWE-308: Use of Single-factor Authentication (3.3) - CWE
https://cwe.mitre.org/data/definitions/308.html
While the use of multiple **authentication** schemes is simply piling on more complexity on top of **authentication**, it is inestimably valuable to have such measures of ...

CWE-306: Missing Authentication for Critical Function (3.3) - CWE
https://cwe.mitre.org/data/definitions/306.html
The software does not perform any **authentication** for functionality that requires a provable user identity or consumes a significant amount of resources. + ...



Security Team

Need one example of “Good”

2

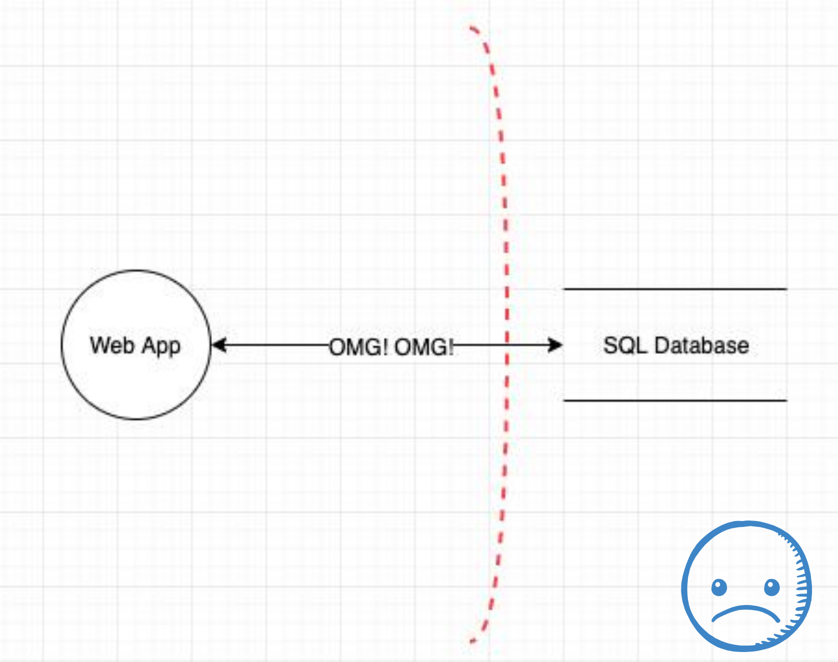
Threat Modelling aids

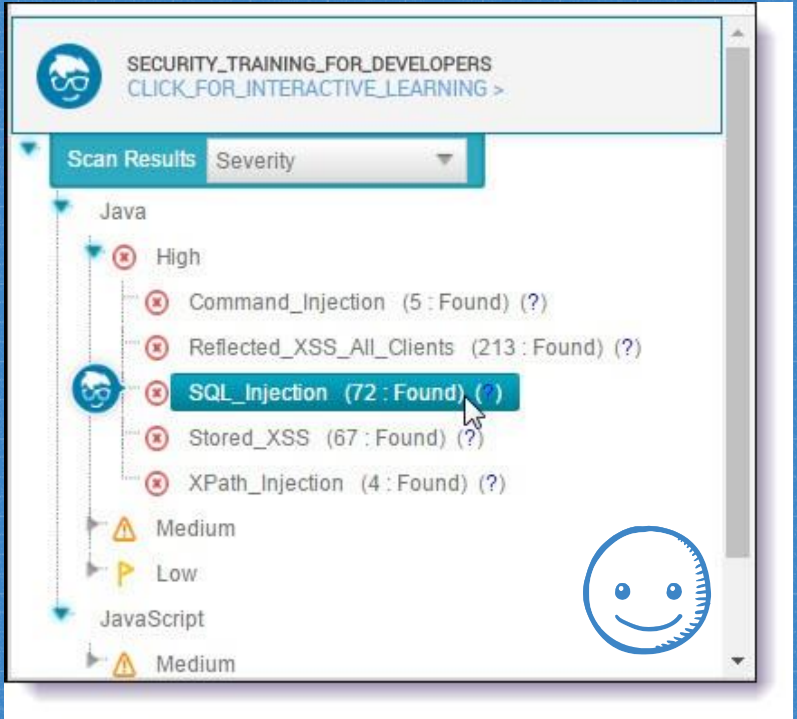
Automated and semi-automated

Secure Development tools

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

People’s time is precious



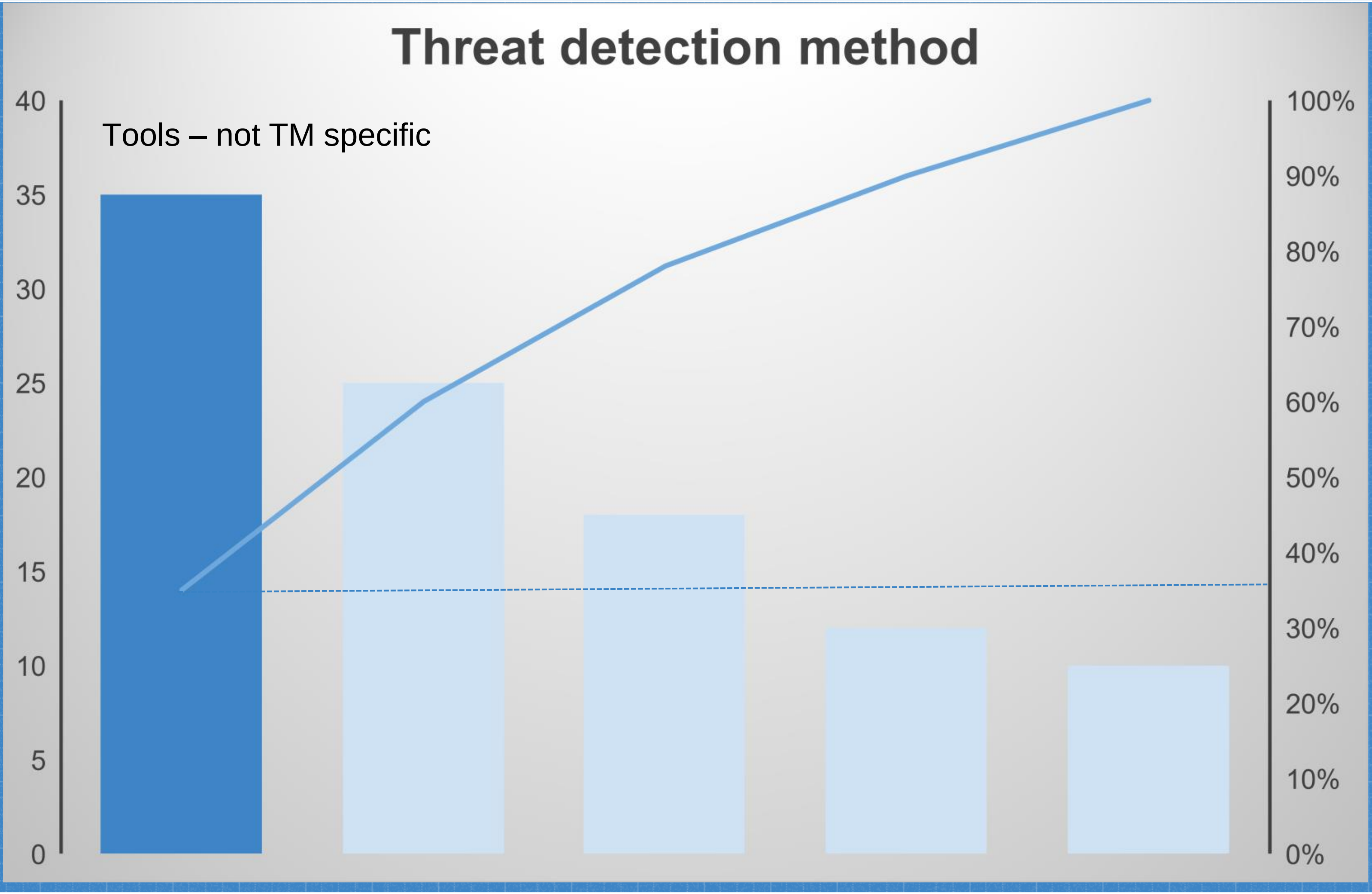


SECURITY_TRAINING_FOR_DEVELOPERS
CLICK_FOR_INTERACTIVE_LEARNING >

Scan Results: Severity

- Java
  - High
    - Command_Injection (5 : Found) (?)
    - Reflected_XSS_All_Clients (213 : Found) (?)
    - SQL_Injection (72 : Found) (?)
    - Stored_XSS (67 : Found) (?)
    - XPath_Injection (4 : Found) (?)
  - Medium
  - Low
- JavaScript
  - Medium

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

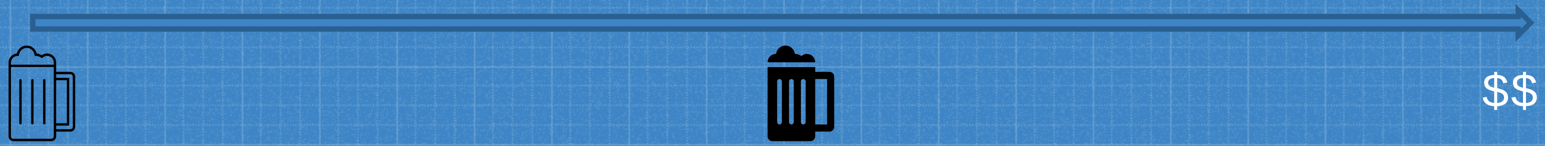

Threat detection method
Tools – not TM specific
40
35
30
25
20
15
10
5
0
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

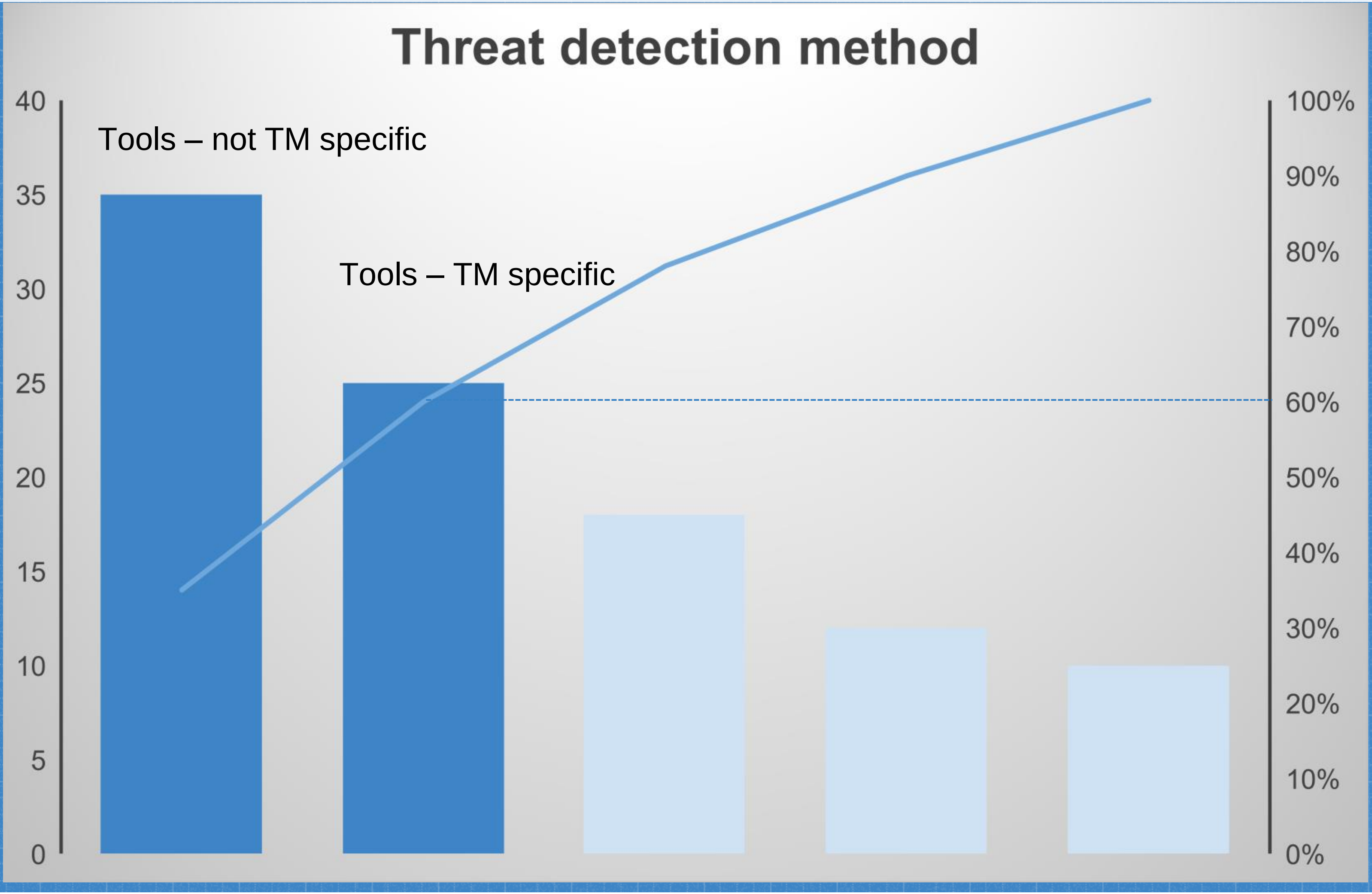
Threat modelling tools

- Microsoft Threat Modeling tool
- OWASP ThreatDragon
- Threats Manager Studio

- Tutamantic
- IriusRisk

- ThreatModeler
- SDElements
- SecuriCAD



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

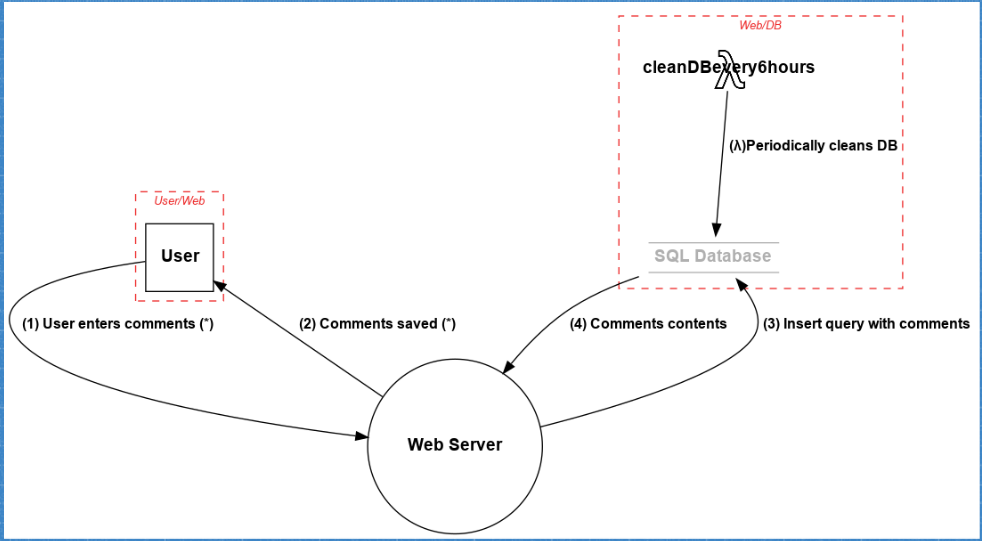
DevSec Collaboration

Add Ops for extra marks

pytm: A Pythonic framework for threat modeling

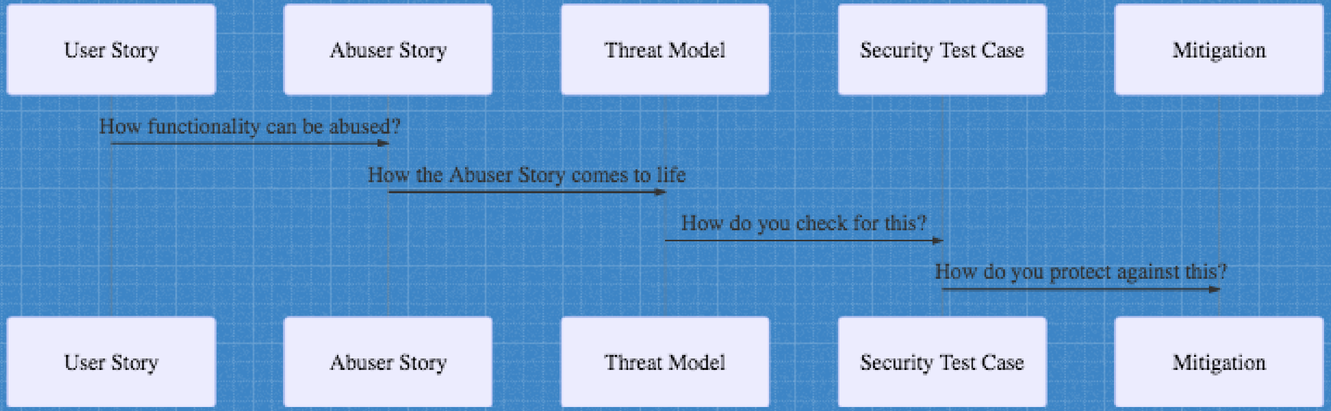
- https://github.com/izar/pytm
- @izar_t

```
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
```



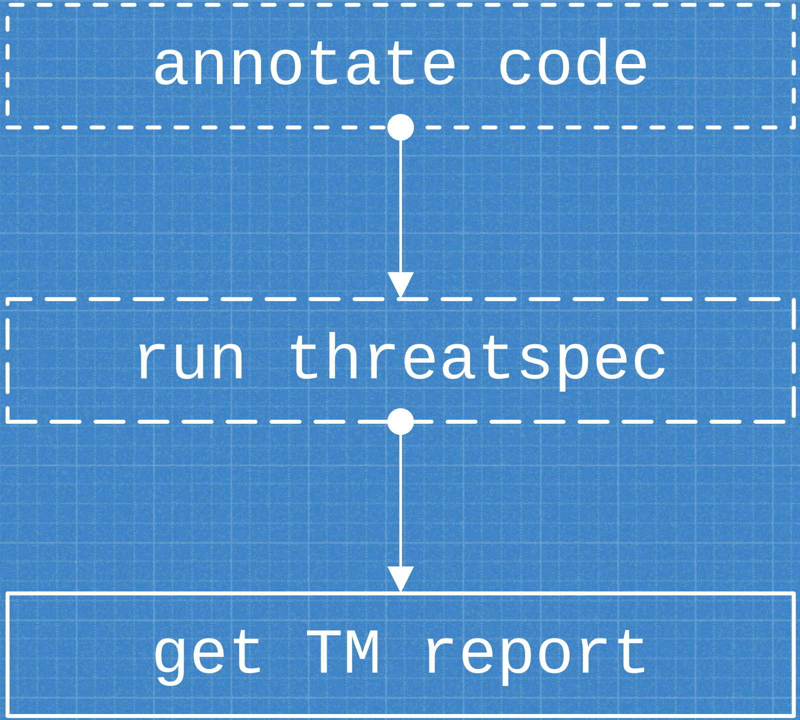
ThreatPlaybook

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


User Story
Abuser Story
Threat Model
Security Test Case
Mitigation
How functionality can be abused?
How the Abuser Story comes to life
How do you check for this?
How do you protect against this?
User Story
Abuser Story
Threat Model
Security Test Case
Mitigation

https://threatspec.org

- @zeroXten



annotate code

run threatspec

get TM report

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

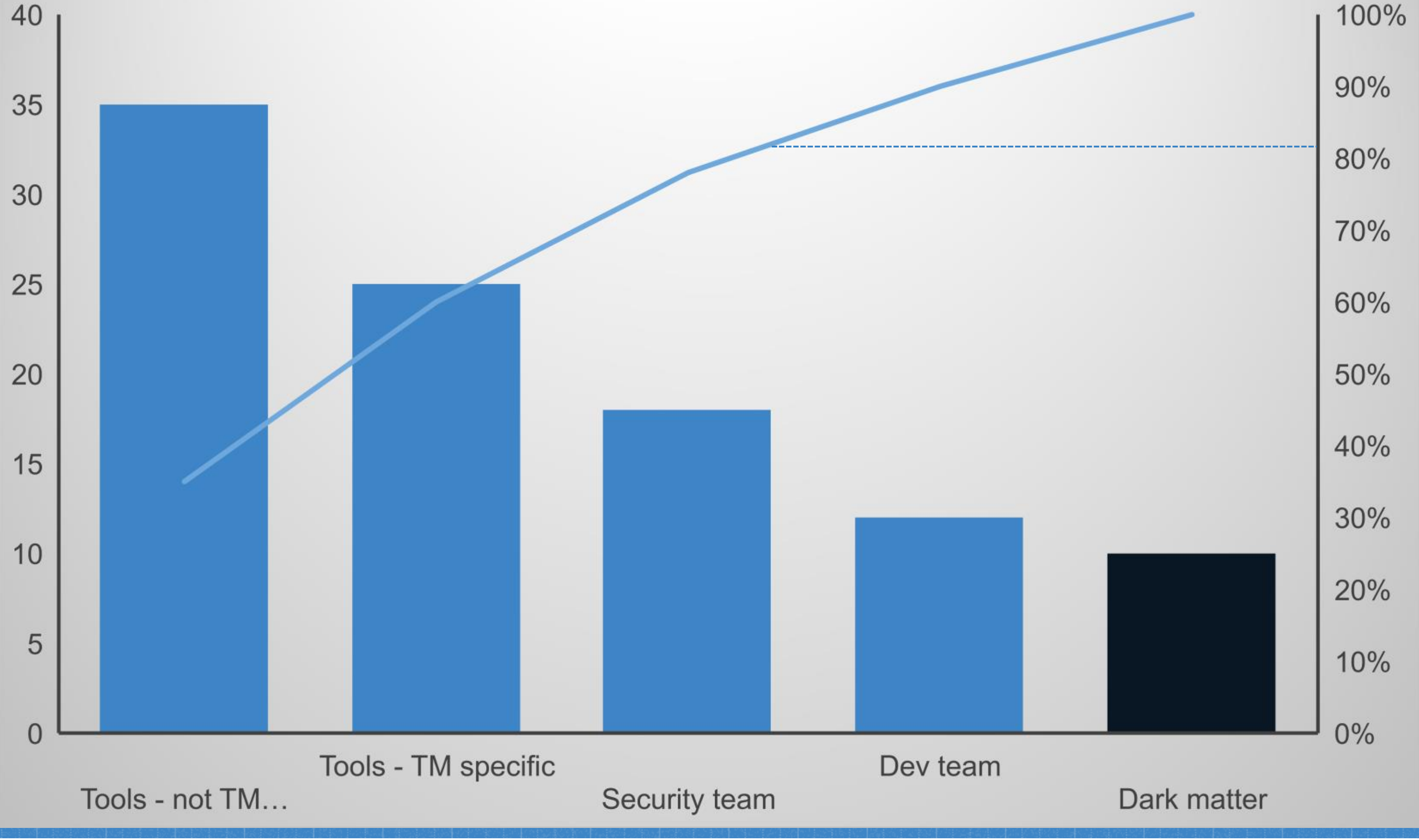
- https://github.com/secmerc/materialize-threats
- Parse draw.io diagrams
- Enumerates threats
- Suggests mitigations and tests

Good collaboration practices

ent

patterns

Threat detection method



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