Alyssa MILLER

Security in the User Story

DevOps Compatible Threat Modeling

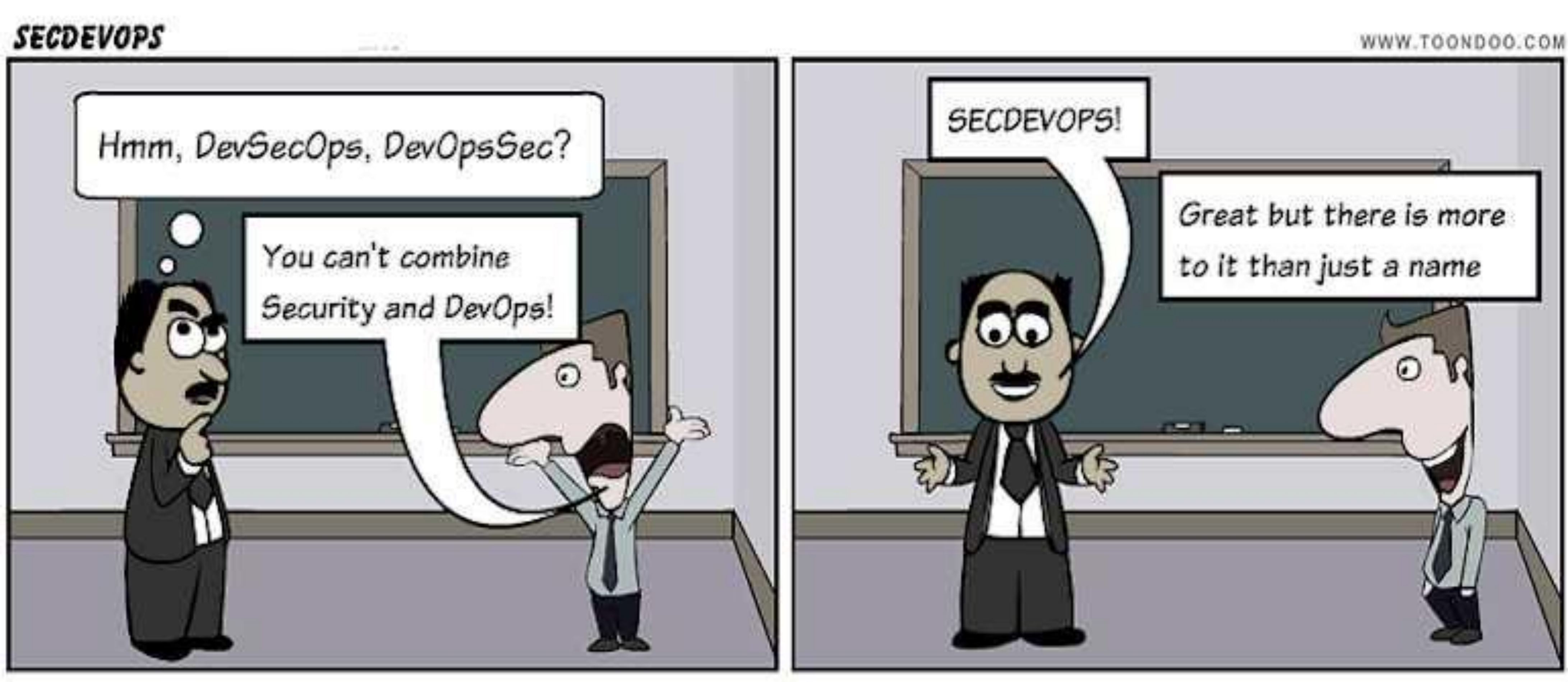
Hacker/Researcher

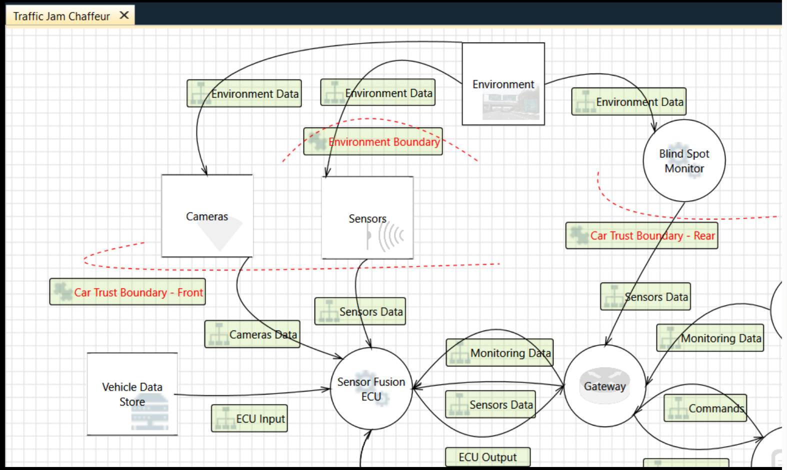
Security Advocate

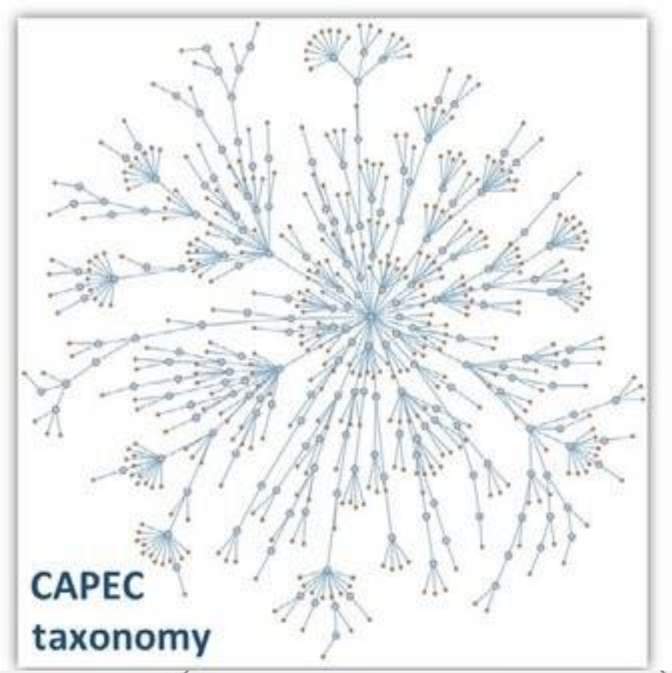
Author & Blogger

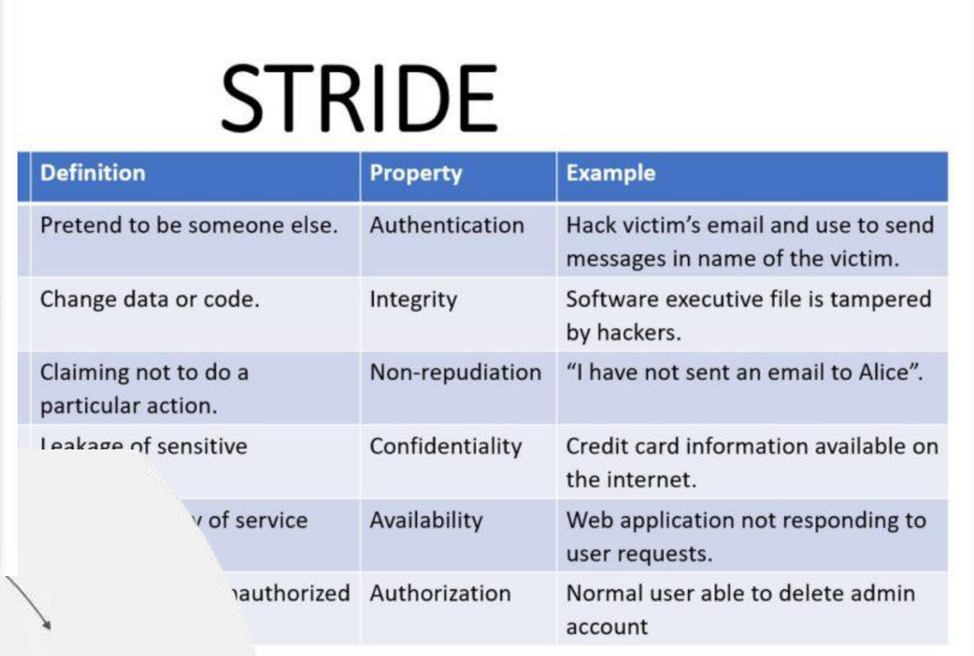
Reformed Developer ☺

snyk


SECDEVOPS
WWW.TOONDOO.COM
Hmm, DevSecOps, DevOpsSec?
You can't combine Security and DevOps!
SECDEVOPS!
Great but there is more to it than just a name

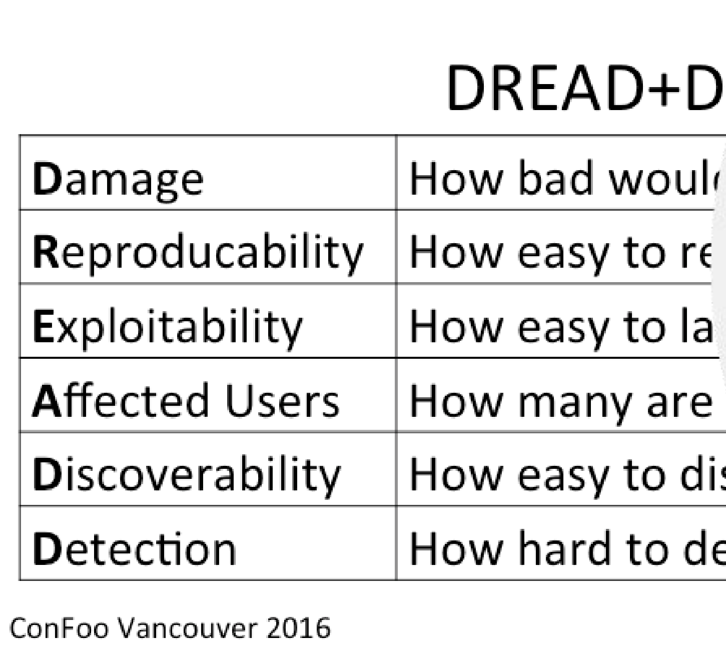






STRIDE

Definition	Property	Example
Pretend to be someone else.	Authentication	Hack victim’s email and use to send messages in name of the victim.
Change data or code.	Integrity	Software executive file is tampered by hackers.
Claiming not to do a particular action.	Non-repudiation	“I have not sent an email to Alice”.
Leakage of sensitive	Confidentiality	Credit card information available on the internet.
y of service	Availability	Web application not responding to user requests.
authorized	Authorization	Normal user able to delete admin account

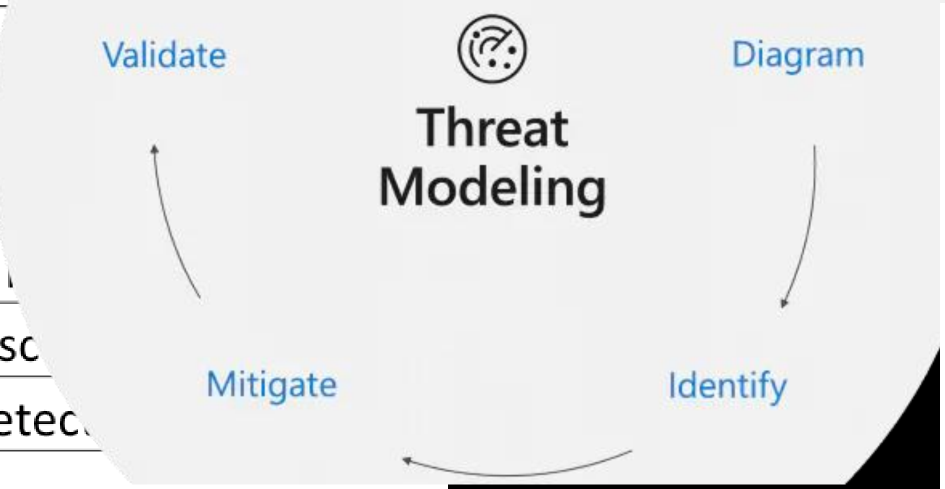


DREAD+D

Damage	How bad woul
Reproducability	How easy to re
Exploitability	How easy to la
Affected Users	How many are
Discoverability	How easy to disc
Detection	How hard to detec

ConFoo Vancouver 2016

@jschauma



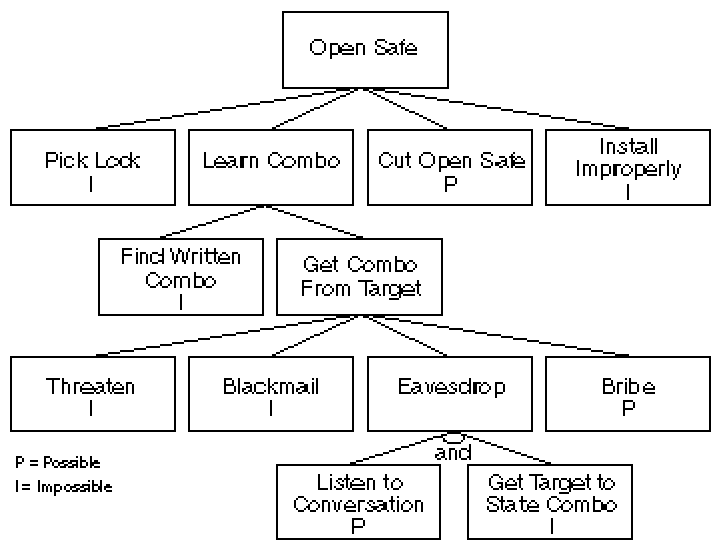
Threat Modeling

Validate

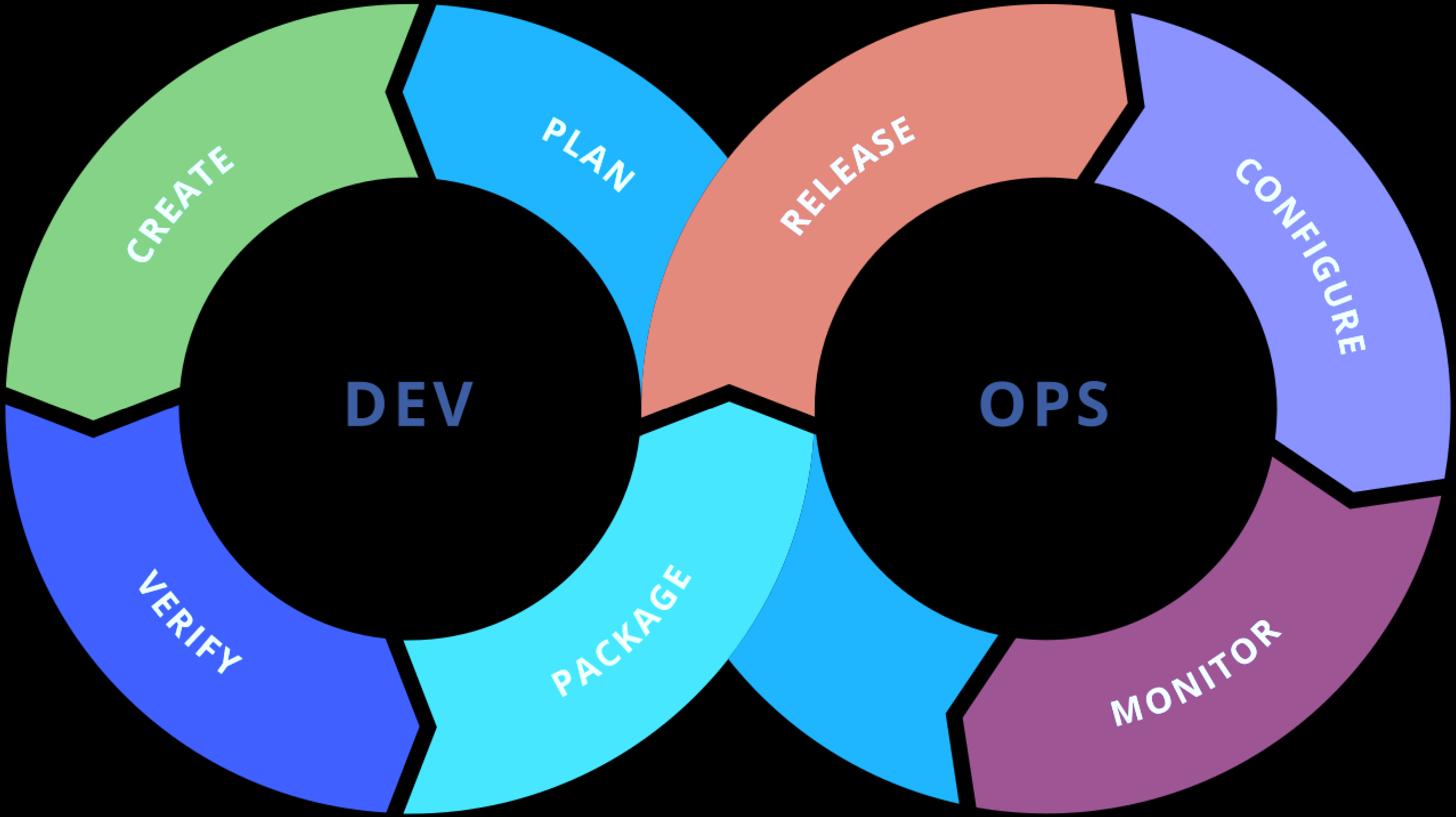
Diagram

Identify

Mitigate



That’s so 2008



“Threat modeling is a family of activities for improving security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (failure of a Storage Device). Threat modeling is a planned activity for identifying and assessing application threats and vulnerabilities.”

Source: https://www.owasp.org/index.php/Category:Threat_Modeling

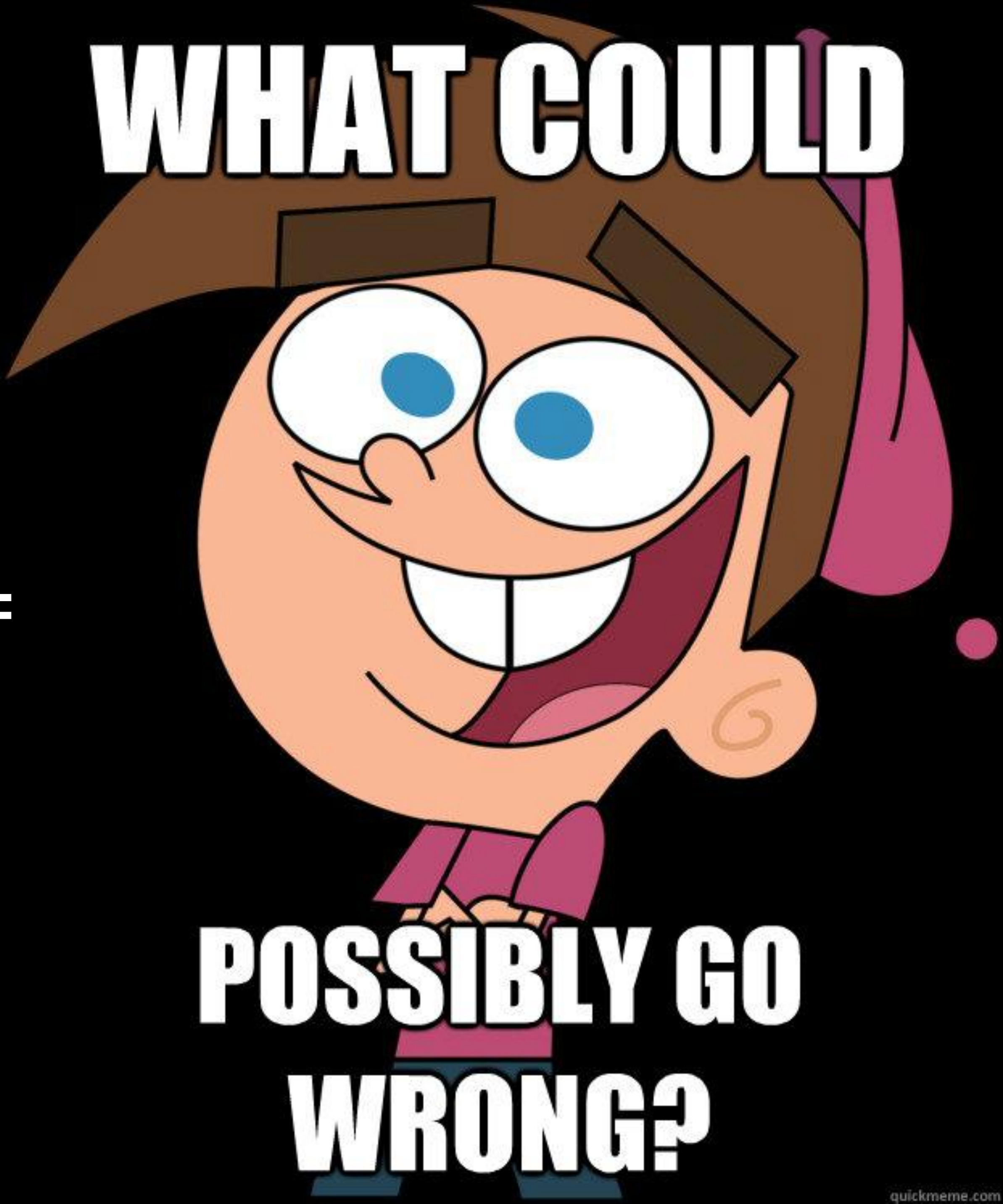
“The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker’s profile, the most likely attack vectors, and the assets most desired by an attacker. Threat modeling answers questions like ‘Where am I most vulnerable to attack?’, ‘What are the most relevant threats?’, and ‘What do I need to do to safeguard against these threats?’”.

Source: https://en.wikipedia.org/wiki/Threat_model

“[Threat Modeling is] an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application. You can use threat modeling to shape your application's design, meet your company's security objectives, and reduce risk.”

Source: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

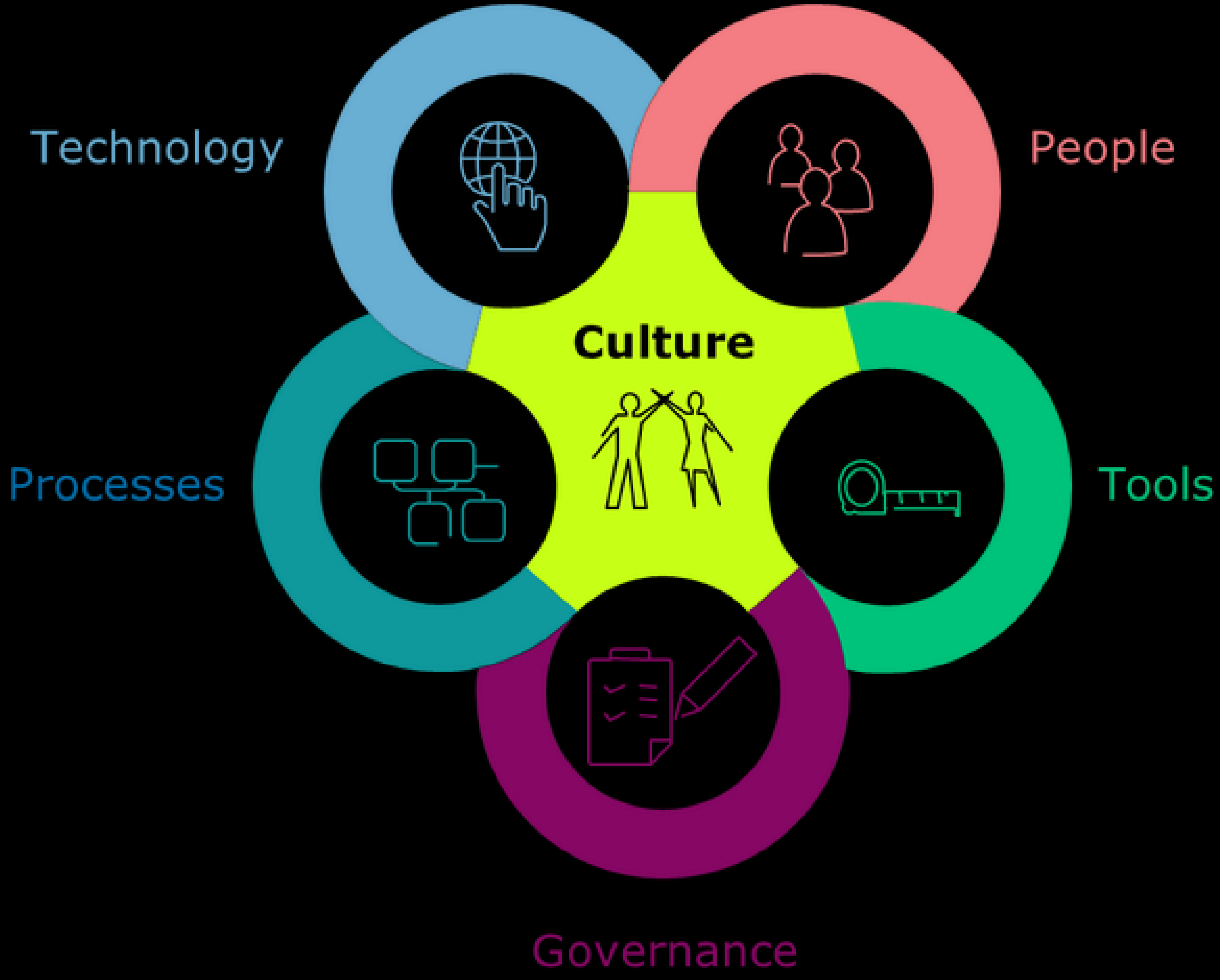
Threat Modeling ==

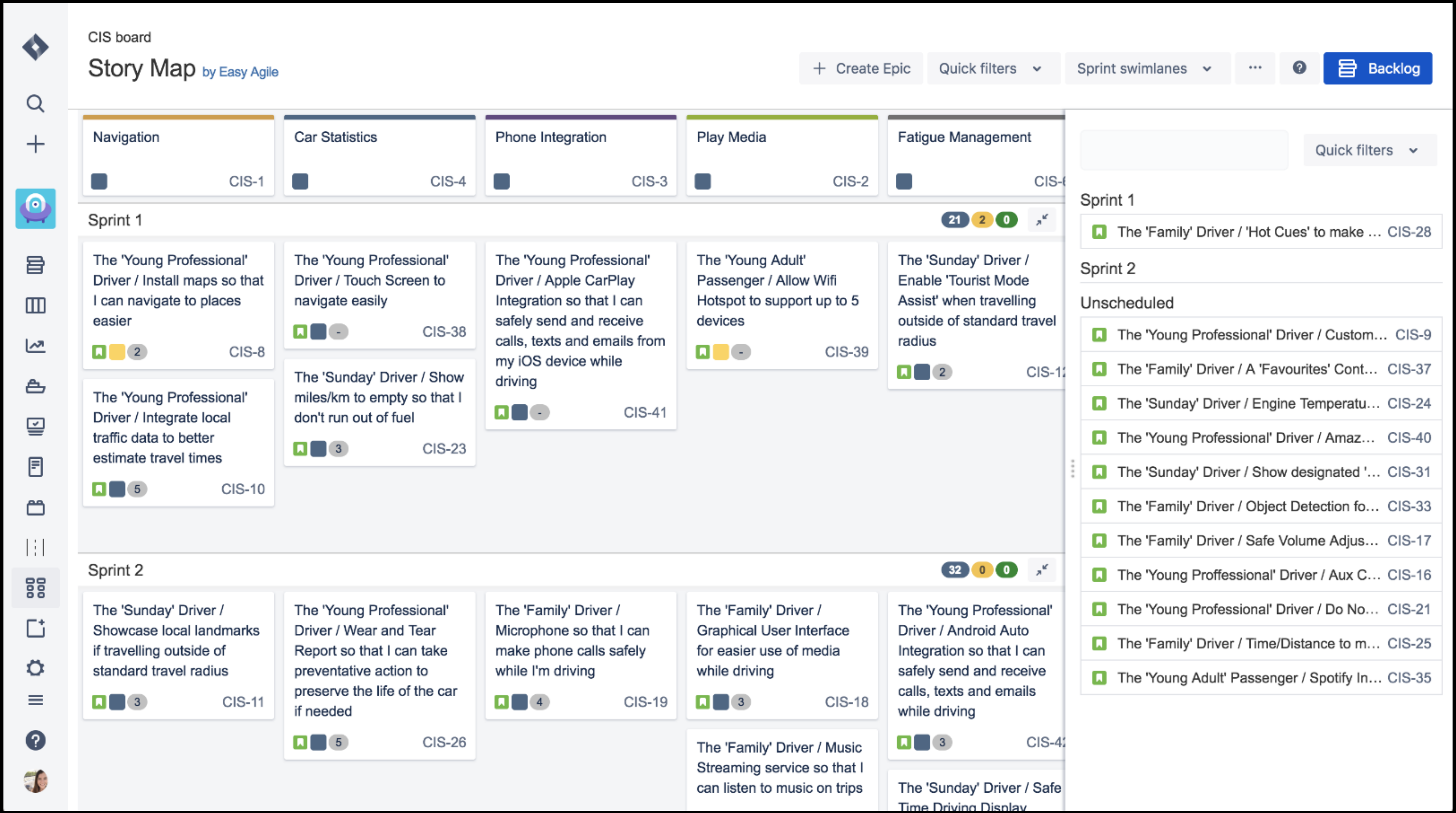


“Identify the likely threats to a system to inform the design of security countermeasures”

Source: Alyssa Miller

This is DevSecOps





CIS board

Story Map by Easy Agile

Navigation CIS-1

Car Statistics CIS-4

Phone Integration CIS-3

Play Media CIS-2

Fatigue Management CIS-

Sprint 1 — 21 2 0

The 'Young Professional' Driver / Install maps so that I can navigate to places easier — 2 — CIS-8

The 'Young Professional' Driver / Integrate local traffic data to better estimate travel times — 5 — CIS-10

The 'Young Professional' Driver / Touch Screen to navigate easily — - — CIS-38

The 'Sunday' Driver / Show miles/km to empty so that I don't run out of fuel — 3 — CIS-23

The 'Young Professional' Driver / Apple CarPlay Integration so that I can safely send and receive calls, texts and emails from my iOS device while driving — - — CIS-41

The 'Young Adult' Passenger / Allow Wifi Hotspot to support up to 5 devices — - — CIS-39

The 'Sunday' Driver / Enable 'Tourist Mode Assist' when travelling outside of standard travel radius — 2 — CIS-1

Sprint 2 — 32 0 0

The 'Sunday' Driver / Showcase local landmarks if travelling outside of standard travel radius — 3 — CIS-11

The 'Young Professional' Driver / Wear and Tear Report so that I can take preventative action to preserve the life of the car if needed — 5 — CIS-26

The 'Family' Driver / Microphone so that I can make phone calls safely while I'm driving — 4 — CIS-19

The 'Family' Driver / Graphical User Interface for easier use of media while driving — 3 — CIS-18

The 'Family' Driver / Music Streaming service so that I can listen to music on trips

The 'Young Professional' Driver / Android Auto Integration so that I can safely send and receive calls, texts and emails while driving — 3 — CIS-4

The 'Sunday' Driver / Safe Time Driving Display

Sprint 1

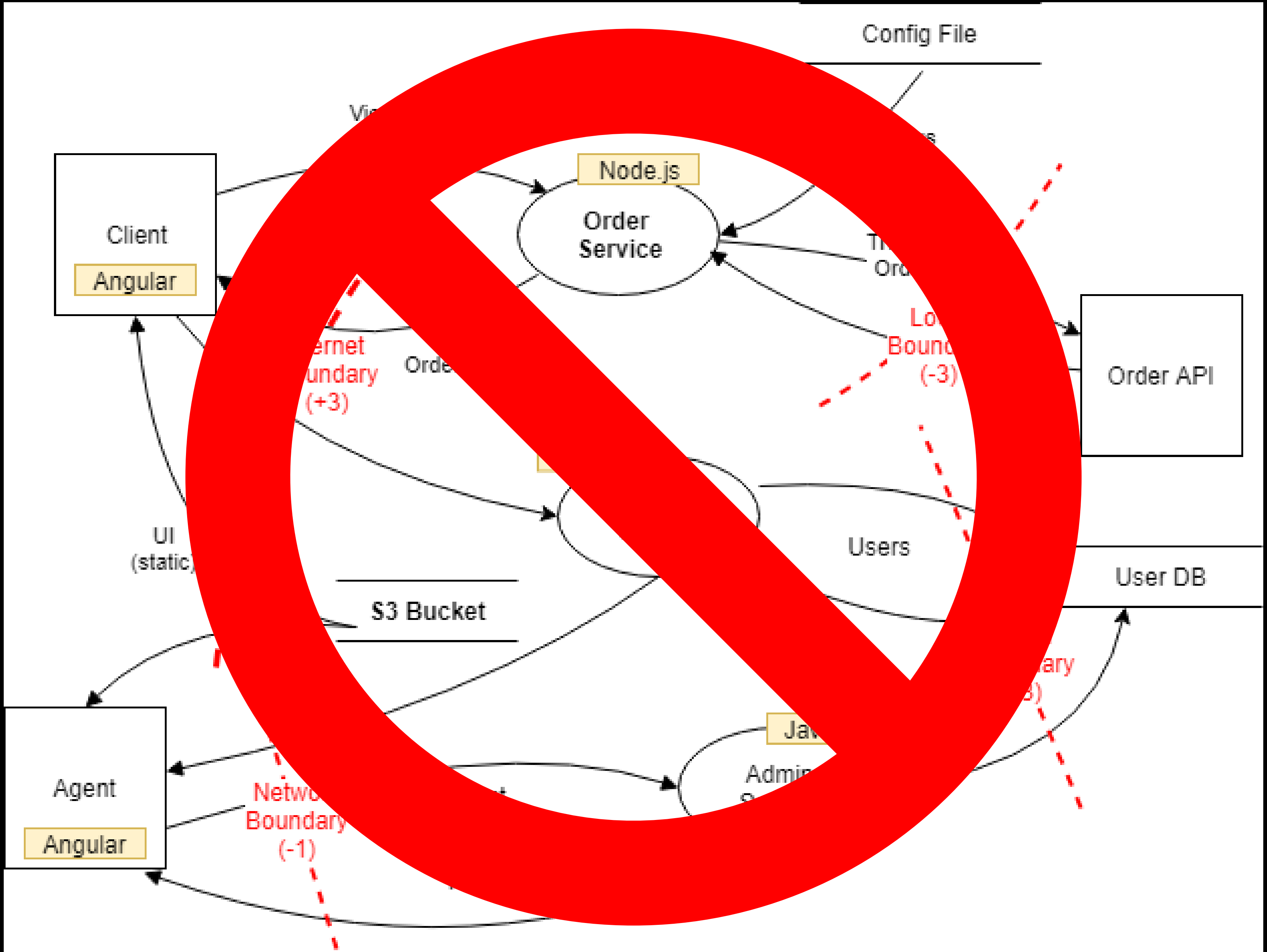
The 'Family' Driver / 'Hot Cues' to make … CIS-28

Sprint 2

Unscheduled

The 'Young Professional' Driver / Custom…	CIS-9
The 'Family' Driver / A 'Favourites' Cont…	CIS-37
The 'Sunday' Driver / Engine Temperatu…	CIS-24
The 'Young Professional' Driver / Amaz…	CIS-40
The 'Sunday' Driver / Show designated '…	CIS-31
The 'Family' Driver / Object Detection fo…	CIS-33
The 'Family' Driver / Safe Volume Adjus…	CIS-17
The 'Young Proffessional' Driver / Aux C…	CIS-16
The 'Young Professional' Driver / Do No…	CIS-21
The 'Family' Driver / Time/Distance to m…	CIS-25
The 'Young Adult' Passenger / Spotify In…	CIS-35

WHAT'S THE WORST THING THAT COULD HAPPEN?
imgflip.com


Config File
Vi
s
Node.js
Order
Service
Client
Angular
Tr
Ord
Lo
Bound
(-3)
ernet
undary
(+3)
Orde
Order API
UI
(static)
Users
User DB
S3 Bucket
ary
3)
Jav
Admin
Agent
Angular
Netwo
Boundary
(-1)

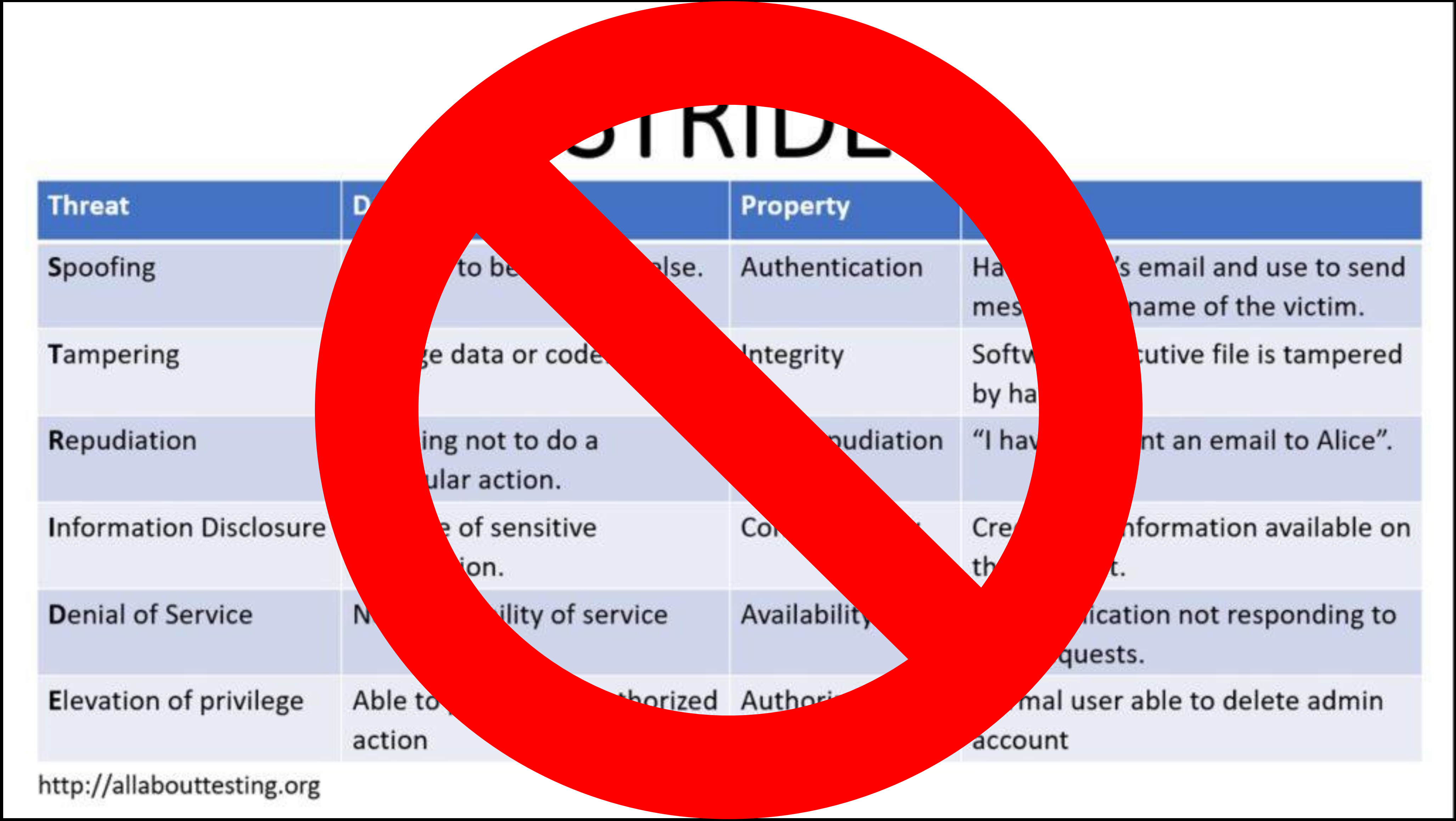
PRIVATE DATA

CRITICAL FUNCTIONS

FINANCIAL ASSETS

PEOPLE ASSETS

SECRETS



STRIDE

Threat	D	Property	
Spoofing	to be else.	Authentication	Ha 's email and use to send mes name of the victim.
Tampering	ge data or code	Integrity	Softw cutive file is tampered by ha
Repudiation	ing not to do a ular action.	pudiation	"I hav nt an email to Alice".
Information Disclosure	e of sensitive ion.	Co	Cre nformation available on th t.
Denial of Service	N ility of service	Availability	ication not responding to quests.
Elevation of privilege	Able to thorized action	Authori	mal user able to delete admin account

http://allabouttesting.org

THEFT

FRAUD

EXPOSED DATA

INTERRUPTED BUSINESS

“We cannot change where we’re headed by doing the same things that got us here”

– Unknown

@AlyssaM_Infosec

/in/alyssam-infosec

https://alyssasec.com

Thank You

Alyssa
MILLER