PASTA and OCTIVE and STRIDE, Oh My!

Bringing Threat Modeling Out of the Woods


DELTA
SkyWest
604
BL137

Hacker and Researcher

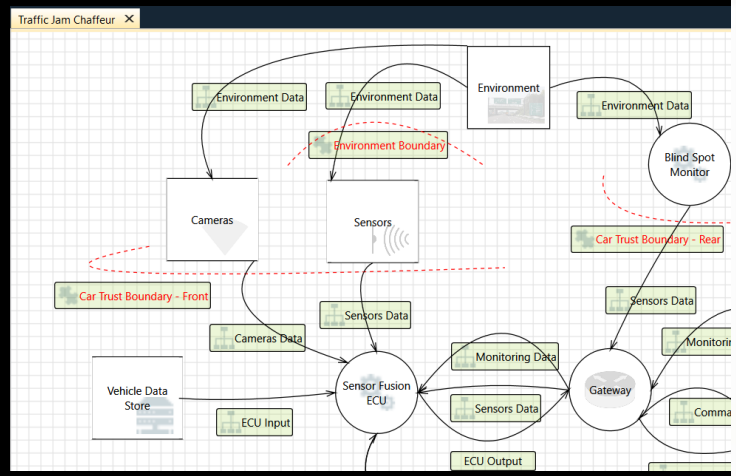
BISO* - S&P Global Ratings

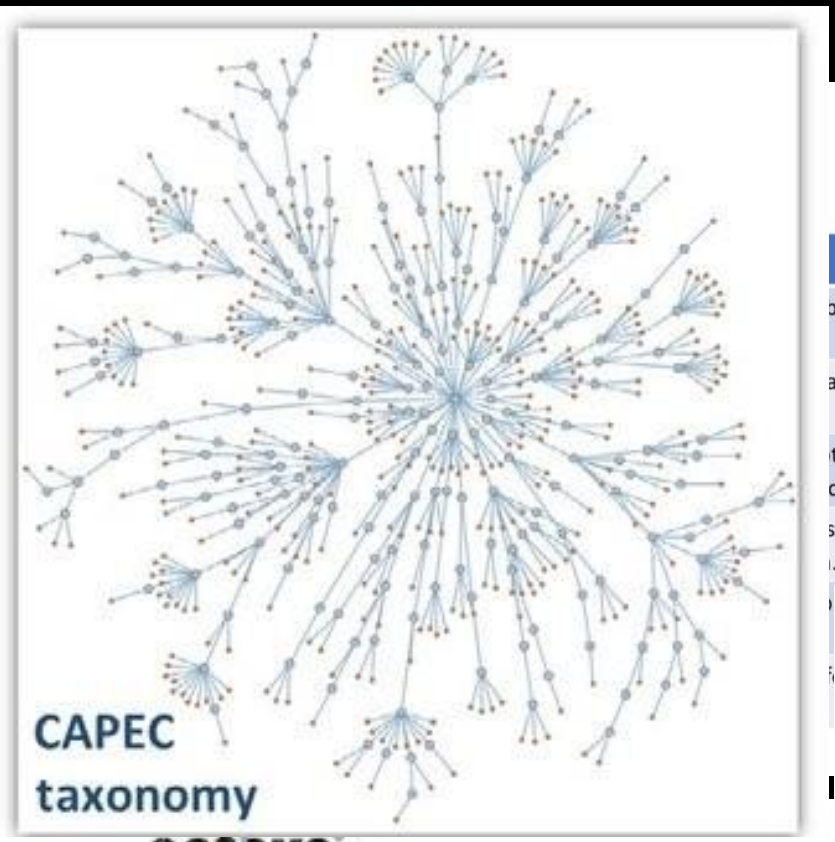
Author & Blogger

Former Software Developer

***What is a BISO? - https://alyssa.link/BISO**

https://alyssasec.com





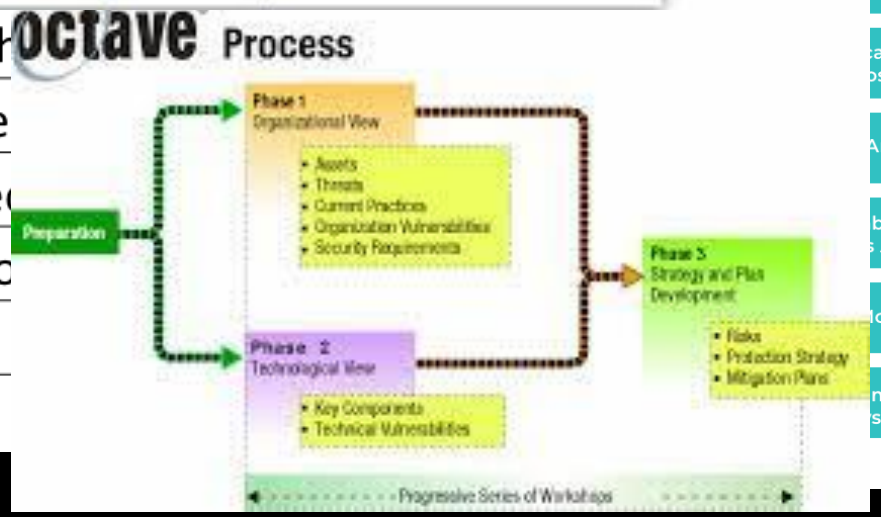
STRIDE

	Property	Example
be someone else.	Authentication	Hack victim's email and use to send messages in name of the victim.
a or code.	Integrity	Software executive file is tampered by hackers.
t to do a ction.	Non-repudiation	"I have not sent an email to Alice".
sensitive .	Confidentiality	Credit card information available on the internet.

DREAD+D

Damage	How bad would
Reproducability	How easy to recreate th
Exploitability	How easy to launch the
Affected Users	How many are impacte
Discoverability	How easy to discover fo
Detection	How hard to detect for

ConFoo Vancouver 2016

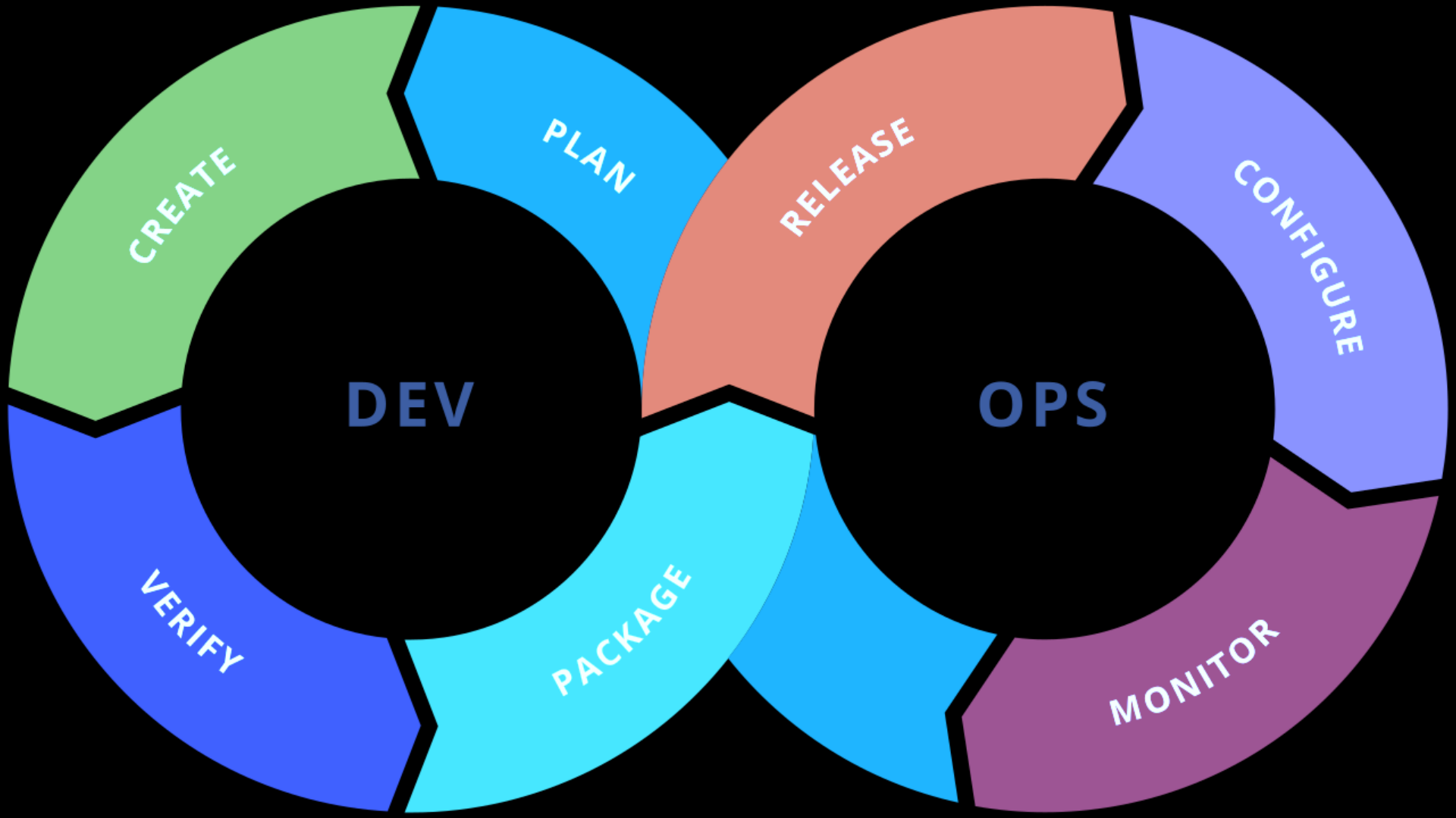


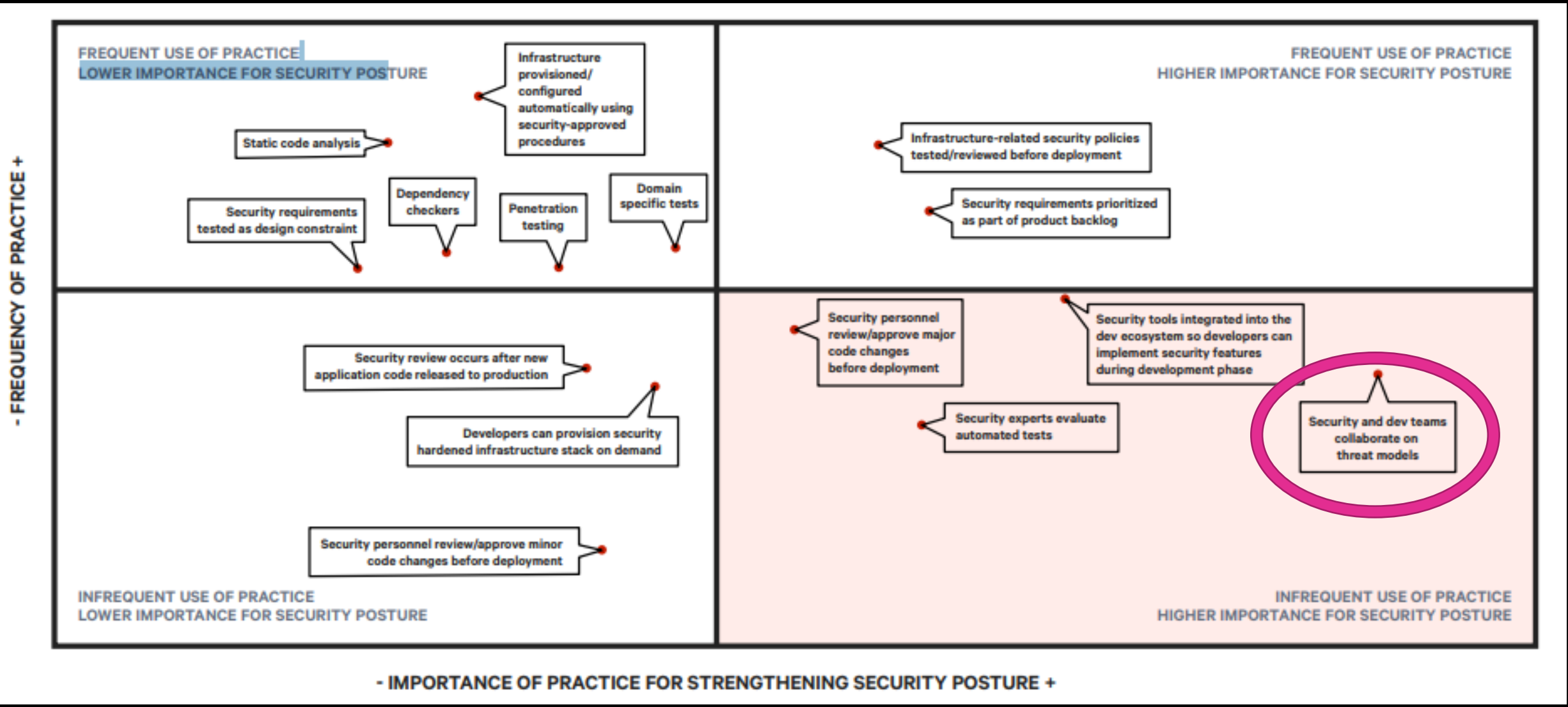
PASTA Methodolgy

1. Define Objectives	• Identify Business Objectives • Identify Security & Compliance Requirements • Business Impact Analysis
2. Define Technical ...e	• Capture the boundaries of the technical environment • Capture Infrastructure / Application / Software / Dependencies
...cation ...position	• Identify Use Cases / Define App Entry Points & Trust levels • Identify Actors / Assets / Services / Roles / Data Sources • Data Flow Diagramming (DFDs) / Trust Boundaries
...Analysis	• Probabilistic Attack Scenarios Analysis • Regression Analysis on Security Events • Threat Intelligence Correlation & Analytics
...bility & ...s Analysis	• Queries of Existing Vulnerability Reports & Issues Tracking • Threat to Existing Vulnerability Mapping Using Thread Trees • Design Flaw Analysis Using Use & Abuse Cases
...odeling	• Attack Surface Analysis • Attack Tree Development / Attack Library Mgt • Attack to Vulnerability & Exploit Analysis using Attack Trees
...mpact ...sis	• Quality & Quantify business impact • Countermeasure Identification & Residual Risk Analysis • ID risk mitigation strategies

DICEUS

That’s so 2008





Source: https://puppet.com/resources/report/state-of-devops-report/
Puppet/Circle-CI 2019 State of DevOps Report

What is Threat Modeling?

Why do we Threat Model?

“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

“Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.”

THREAT MODELING MANIFESTO

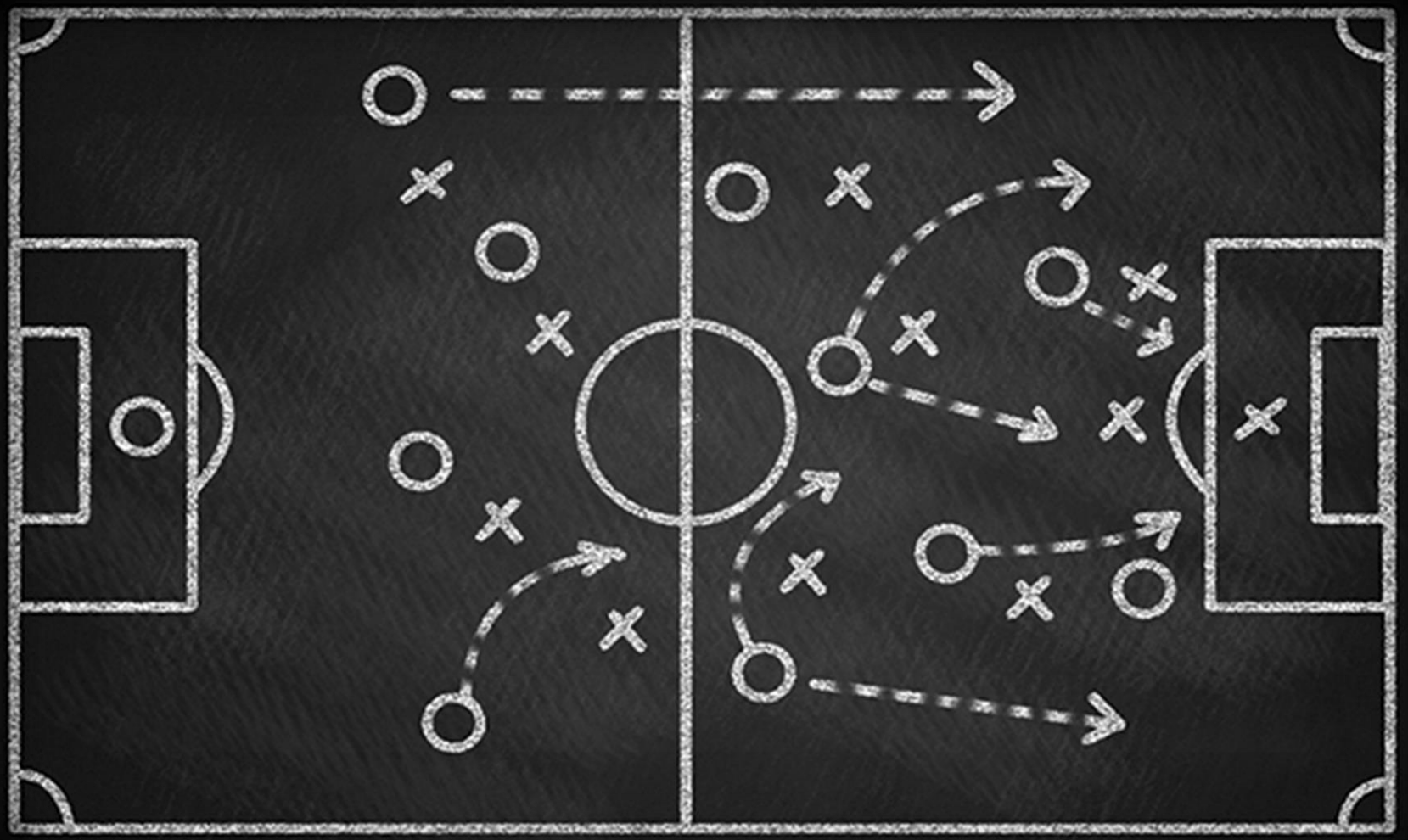
https://www.threatmodelingmanifesto.org/


But 'Why?'

“The output of the threat model…informs decisions that you might make in subsequent design, development, testing, and post-deployment phases.”

https://www.threatmodelingmanifesto.org/

Building your methodology



“A value in threat modeling is something that has relative worth, merit, or importance. That is, while there is value in the items on the right, we value the items on the left more.”

THREAT MODELING MANIFESTO

https://www.threatmodelingmanifesto.org/

A culture of finding and fixing design issues…

…over checkbox compliance

People and collaboration…

…over processes, methodologies, and tools

A journey of understanding…

…over a security or privacy snapshot

Doing threat modeling…

…over talking about it

Continuous refinement…

…over a single delivery

“A principle describes the fundamental truths of threat modeling.”

THREAT MODELING MANIFESTO

https://www.threatmodelingmanifesto.org/

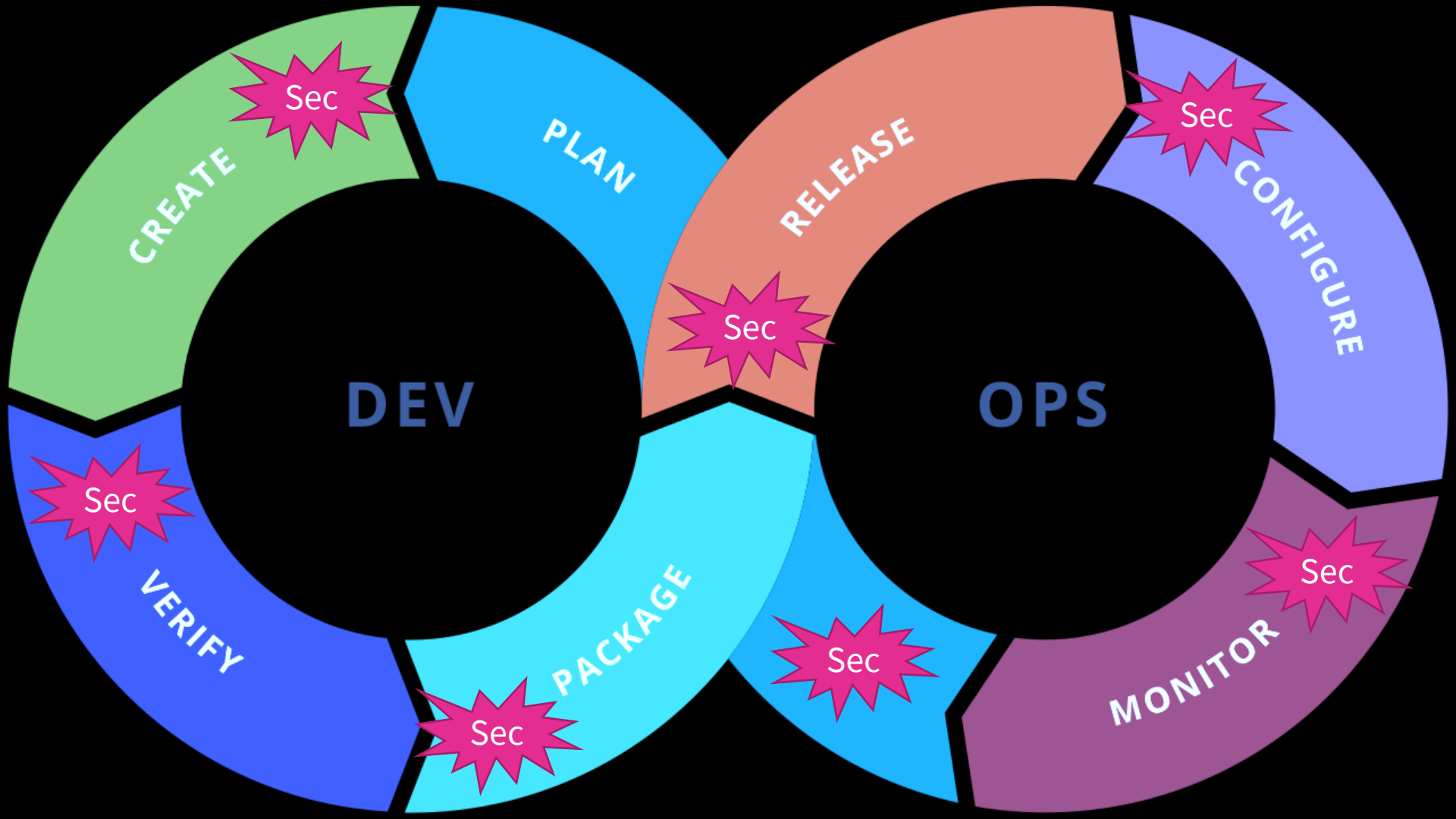
Early and frequent analysis

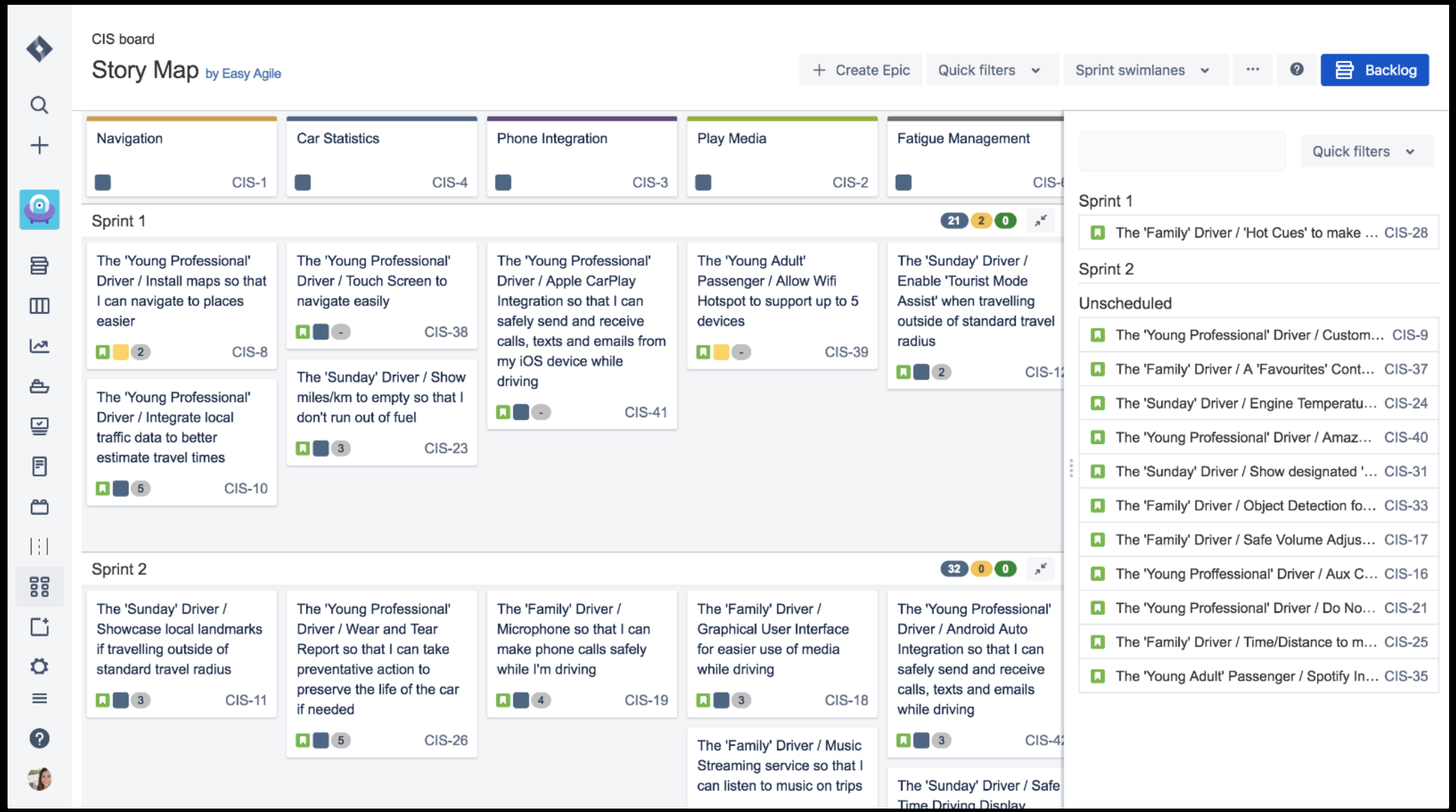
Of value to stakeholders

Iterations, manageable portions

Dialog is key, documents record

Let's Do Real DevSecOps




CIS board
Story Map by Easy Agile
Create Epic
Quick filters
Sprint swimlanes
Backlog
Navigation
CIS-1
Car Statistics
CIS-4
Phone Integration
CIS-3
Play Media
CIS-2
Fatigue Management
Sprint 1
21 2 0
The 'Young Professional' Driver / Install maps so that I can navigate to places easier
CIS-8
The 'Young Professional' Driver / Touch Screen to navigate easily
CIS-38
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
The 'Young Professional' Driver / Integrate local traffic data to better estimate travel times
CIS-10
The 'Sunday' Driver / Show miles/km to empty so that I don't run out of fuel
CIS-23
Sprint 2
32 0 0
The 'Sunday' Driver / Showcase local landmarks if travelling outside of standard travel radius
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
CIS-26
The 'Family' Driver / Microphone so that I can make phone calls safely while I'm driving
CIS-19
The 'Family' Driver / Graphical User Interface for easier use of media while driving
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
The 'Sunday' Driver / Safe
Quick filters
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

As a Car driver

I want to Enter a destination name

So that I can navigate w/o an address

** I want you to:

Protect My search history

From Being accessed by attackers

Threat Information

Plan

Security Requirements

Build

Security Controls

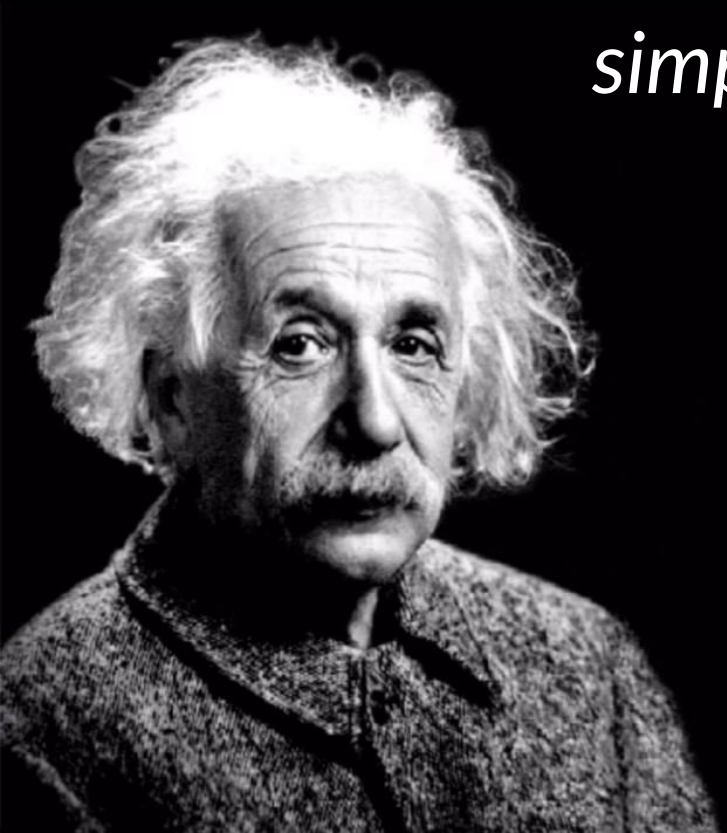
Test

Test Cases

Deploy

Monitoring

```
asset:
  name: search_terms
  description: Destination names entered by users
  threats:
    - theft-via-rest-svc:
      - countermeasures: [client-cert,session-token]
    - theft-via-db:
      - countermeasures: [field-encrypt]
```



“Genius is making complex ideas simple, not making simple ideas complex.”

– Albert Einstein

https://alyssasec.com

@AlyssaM_Infosec

/in/alyssam-infosec

https://alyssasec.com

Thank You

Alyssa
MILLER

@alyssam_infosec

https://alyssasec.com