

RSA® Conference 2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: DSO-T02

What Could Possibly Go Wrong? Plain Language Threat Modeling in DevSecOps

Alyssa Miller

BISO (Business Information Security Officer)
S&P Global Ratings
@AlyssaM_InfoSec



Disclaimer

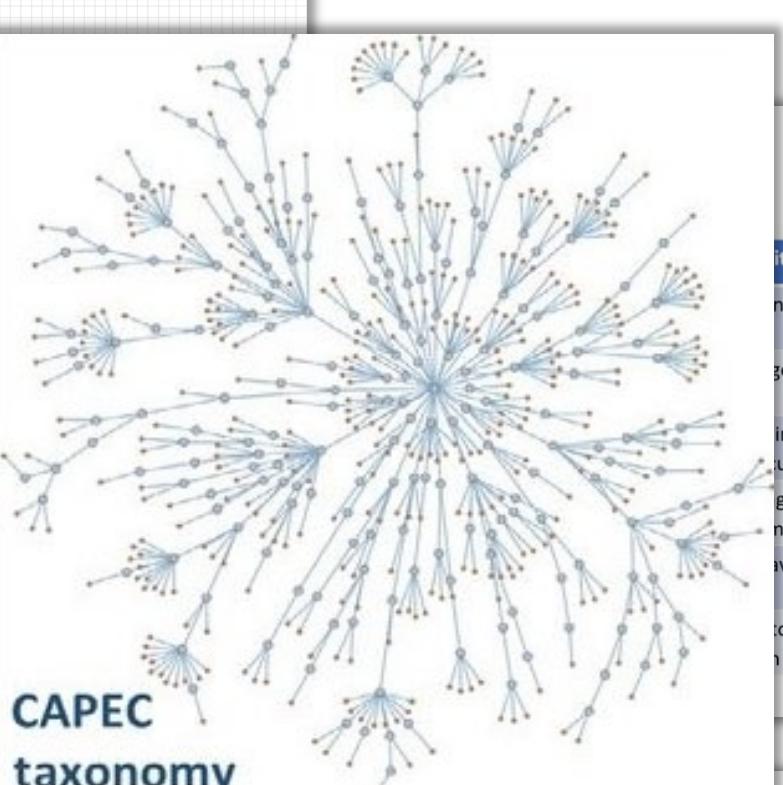
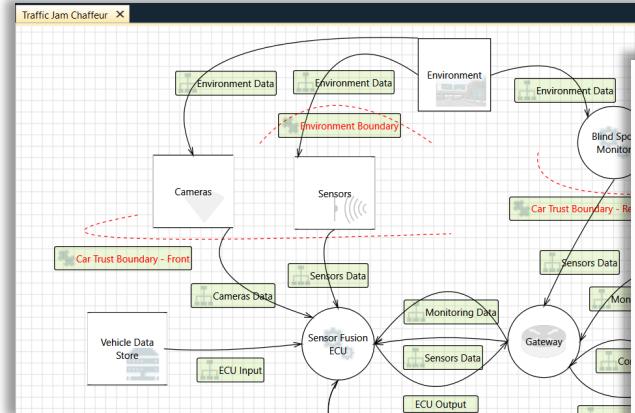
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

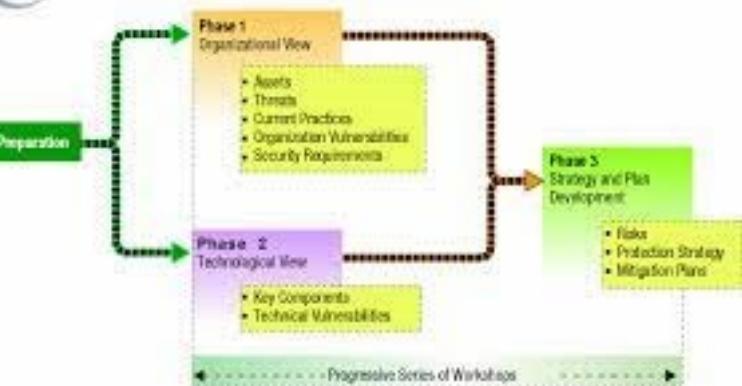
No opinions, views, or other content presented in this session represent those of S&P Global or its subsidiaries. All content presented is the sole work of the presenter.





CAPEC taxonomy

octave Process



Damage	How bad would it be?
Reproducability	How easy to reproduce?
Exploitability	How easy to launch the attack?
Affected Users	How many are impacted?
Discoverability	How easy to discover for a threat?
Detection	How hard to detect for detection?

ConFoo Vancouver 2016

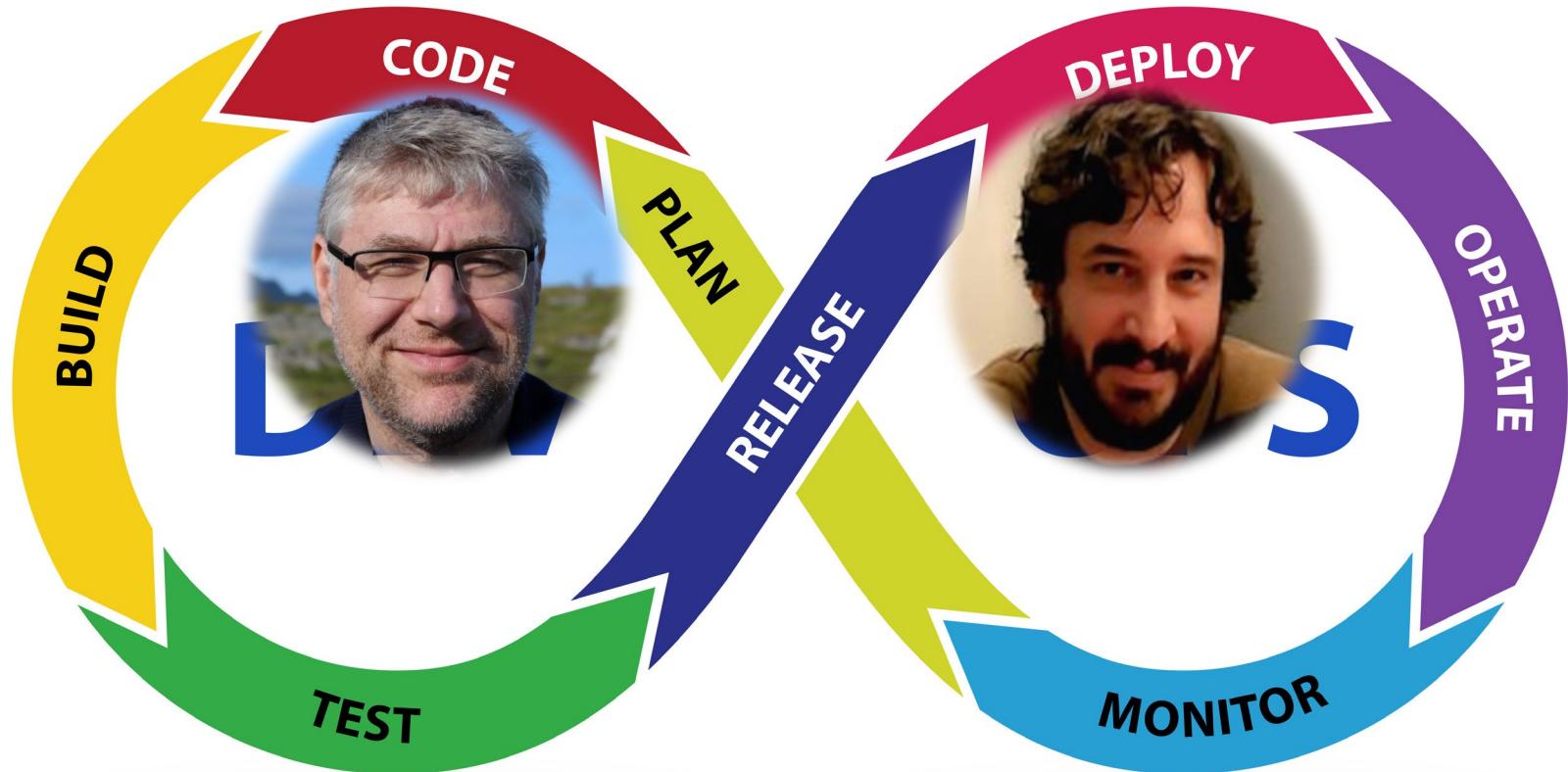
STRIDE

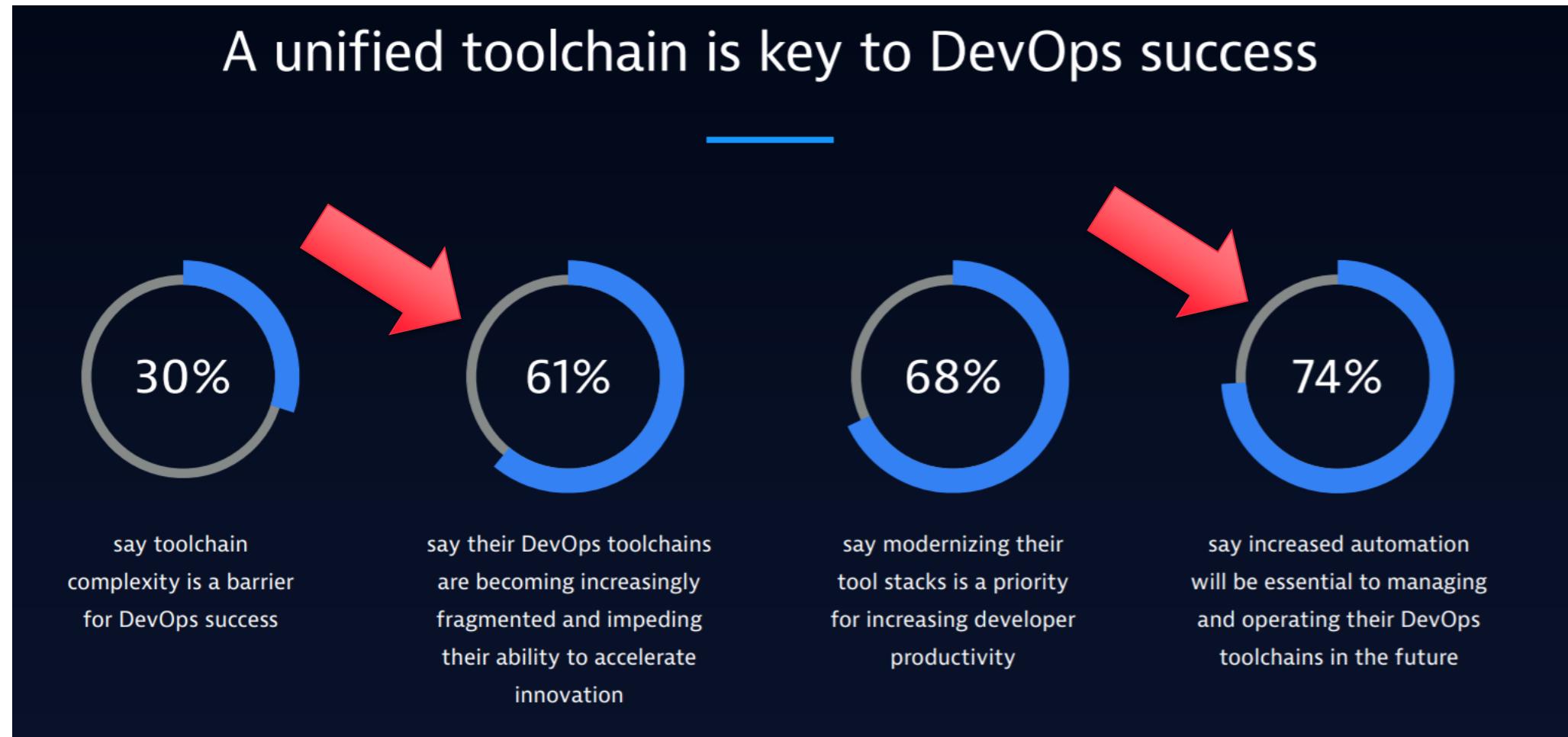
Condition	Property	Example
Want to be someone else.	Authentication	Hack victim's email and use to send messages in name of the victim.
Change data or code.	Integrity	Software executive file is tampered by hackers.
Wanting not to do a particular action.	Non-repudiation	"I have not sent an email to Alice".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

PASTA Methodology

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

Meanwhile, in 2008...





Dynatrace 2021 DevOps Report

<https://www.dynatrace.com/monitoring/solutions/devops-report>

What is Threat Modeling?



Why do we Threat Model?

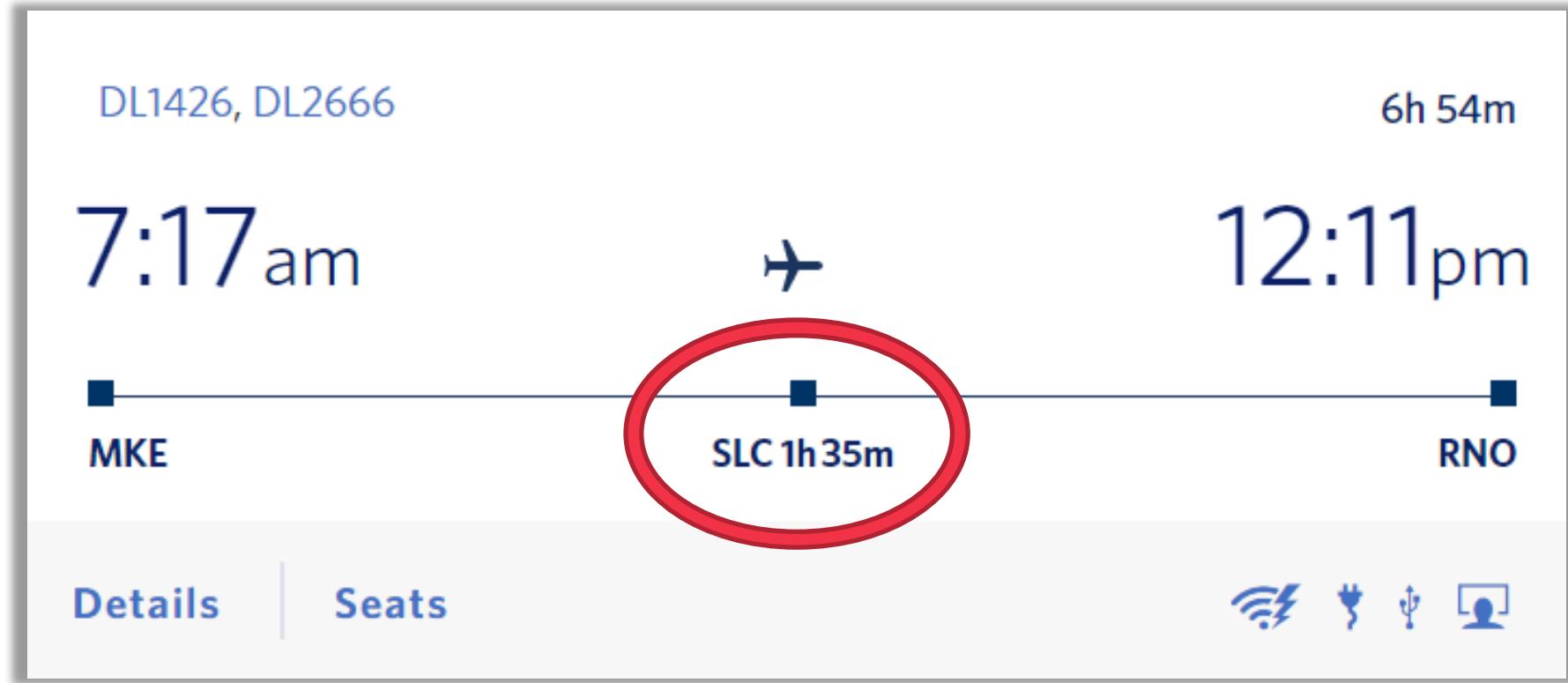
What is Threat Modeling?



Answering Two Questions:

What is most important?
What could possibly go wrong?

Why do we Threat Model?



So we can take action to avoid those outcomes

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



THREAT
MODELING
MANIFESTO

<https://www.threatmodelingmanifesto.org/>



THREAT MODELING MANIFESTO

“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/>



THREAT
MODELING
MANIFESTO

Each organization should have a tailored methodology that aligns to their unique business objectives and structure.

<https://www.threatmodelingmanifesto.org/>

Five Values of Threat Modeling

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



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

Four Principles of Threat Modeling

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





Early and frequent analysis

Of value to stakeholders



Iterations, manageable portions



Dialog is key, documents record

Building a Methodology in DevSecOps

“The Manifesto contains ideas, but is not a how-to, and is methodology-agnostic.



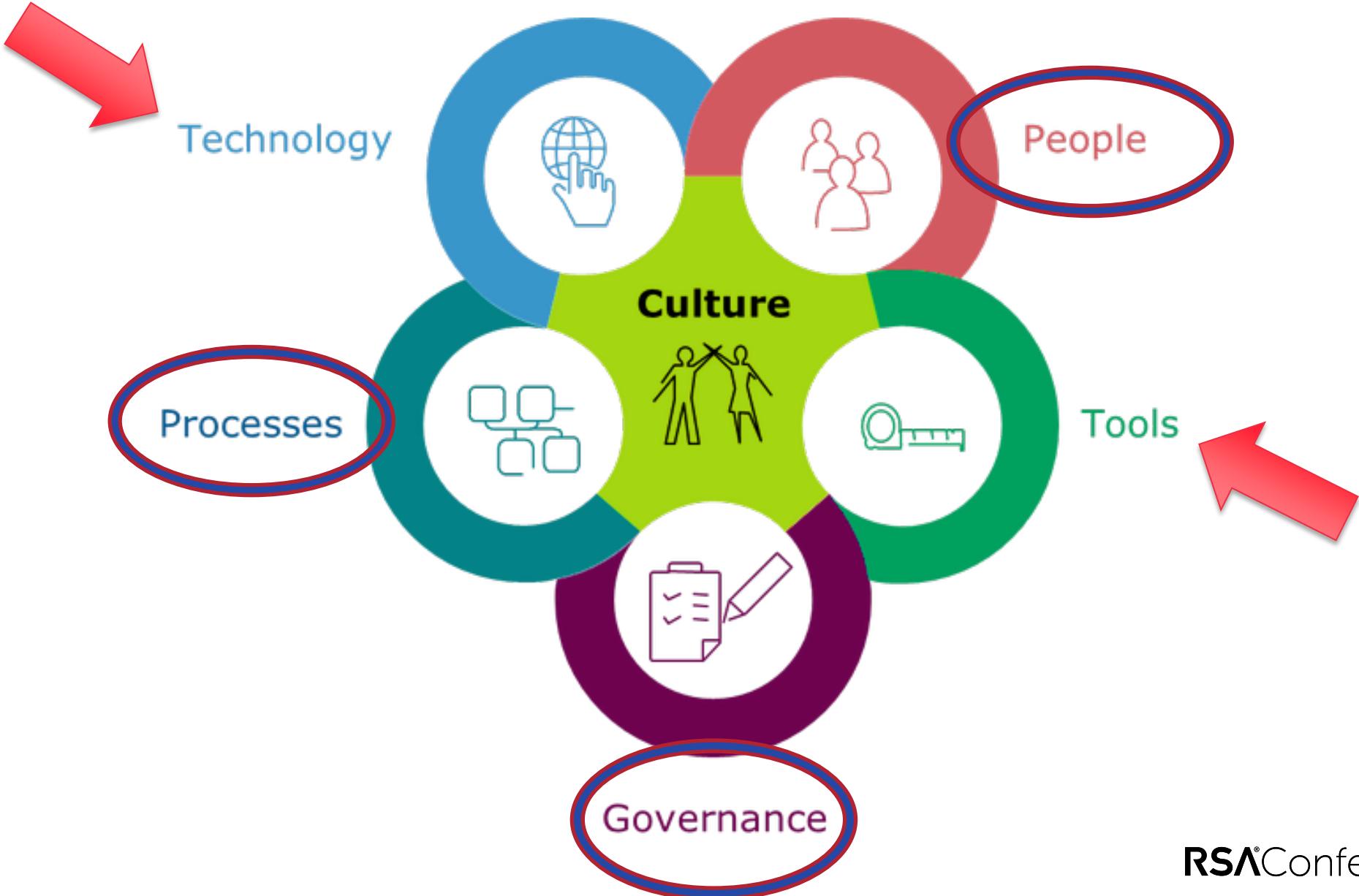
The DevOps Pipeline



Accelerate Right

PUSH LEFT!!!!!!

Build a security empowered culture



CIS board

Story Map by Easy Agile

+ Create Epic Quick filters Sprint swimlanes ... ? Backlog

Navigation	Car Statistics	Phone Integration	Play Media	Fatigue Management
CIS-1	CIS-4	CIS-3	CIS-2	CIS-6

Sprint 1

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 CIS-12
The 'Young Professional' Driver / Integrate local traffic data to better estimate travel times CIS-10				

Sprint 2

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 'Young Professional' Driver / Android Auto Integration so that I can safely send and receive calls, texts and emails while driving CIS-42
				The 'Sunday' Driver / Safe Time Driving Display

Quick filters

Sprint 1

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

Sprint 2

- 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 Professional' 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

Unscheduled

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

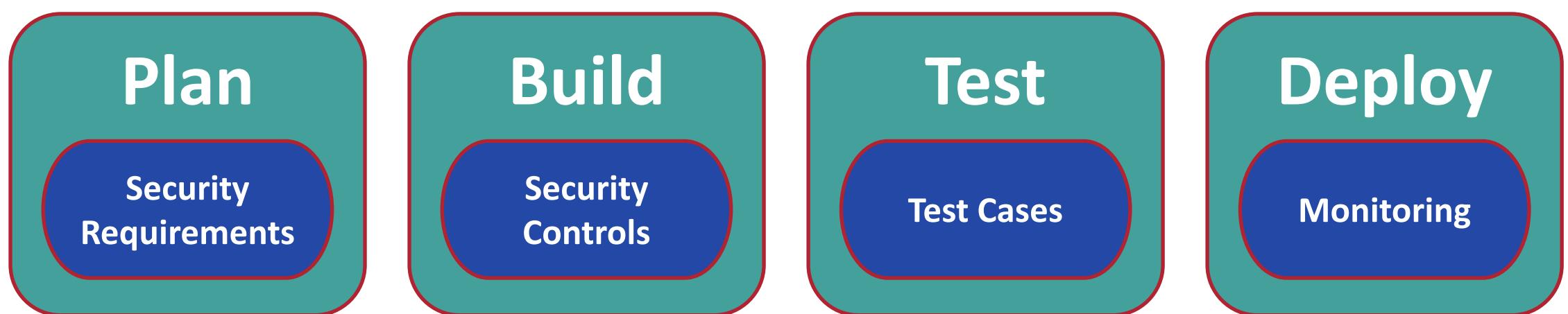
From Being accessed by attackers

Critical Asset

Threat



Asset & Threat Information



Reference
Architectures

Assets & Controls
(YAML)

Critical Functions

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]

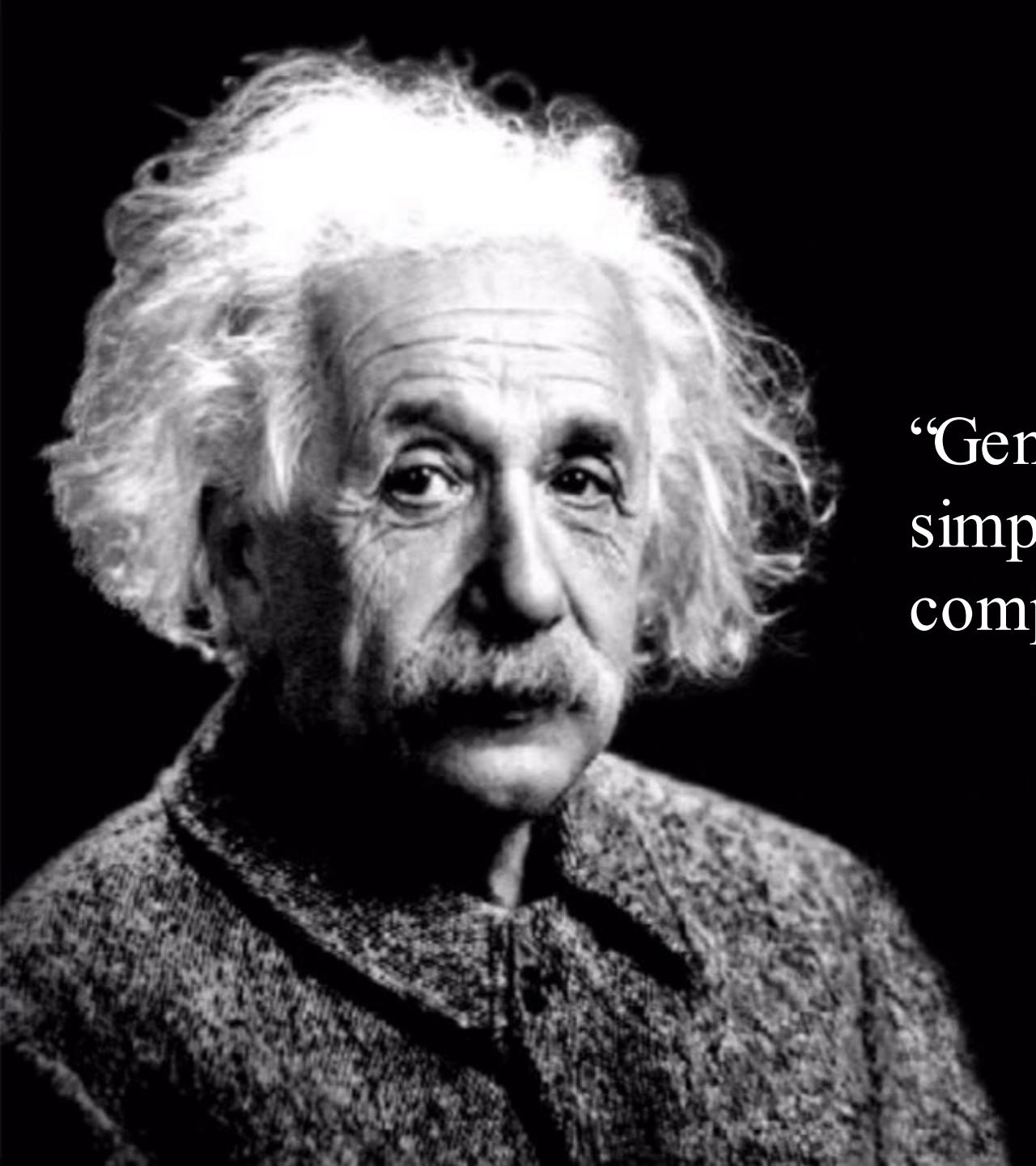
```
steps:  
- task: myRepo.tstExtensionId.contribId.FuzzSessTkn@0  
  inputs:  
    tokenName: 'jzsession'  
    format: 'base64'  
    target:<hostname>  
- task: parseTestResults@1  
  inputs:  
    testResultsFiles: "**/tstFuzzResults-*.*xml"  
    condition: succeededOrFailed()
```

Takeaways

- Threat modeling is just asking what can possibly go wrong
- Use the five values and four principles found in the Threat Modeling Manifesto to guide your methodology
- Take threat modeling out of the hands of security teams, make it a cultural collaboration activity
- Threat modeling can feed all phases of the DevOps pipeline and actually accelerate it
- Meet them where they live, bring threat modeling into existing tooling

Applying this to your organization

- This Month:
 - Identify value proposition for your organization
 - Connect with product & engineering leaders to link value prop to objectives
- This Quarter:
 - Define an initial methodology following the values and principles
 - Define a plain-language threat taxonomy
 - Create new user story templates
- This Year:
 - Launch a beta iteration using small scope as a POC

A black and white portrait of Albert Einstein, showing him from the chest up. He has his characteristic wild, grey hair and a full, bushy beard. He is looking slightly to the right of the camera with a thoughtful expression. The background is dark and out of focus.

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

– Albert Einstein