RSAConference2022
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

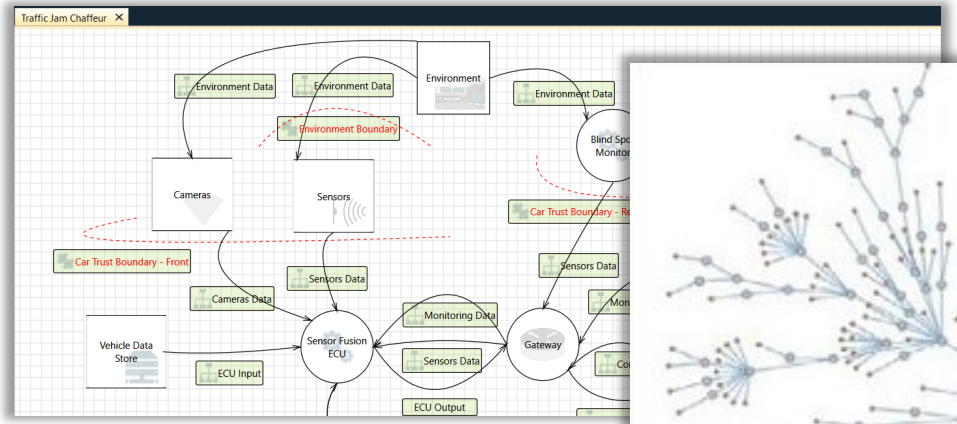
Disclaimer

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.

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.

Alyssa MILLER
www.alyssasec.com



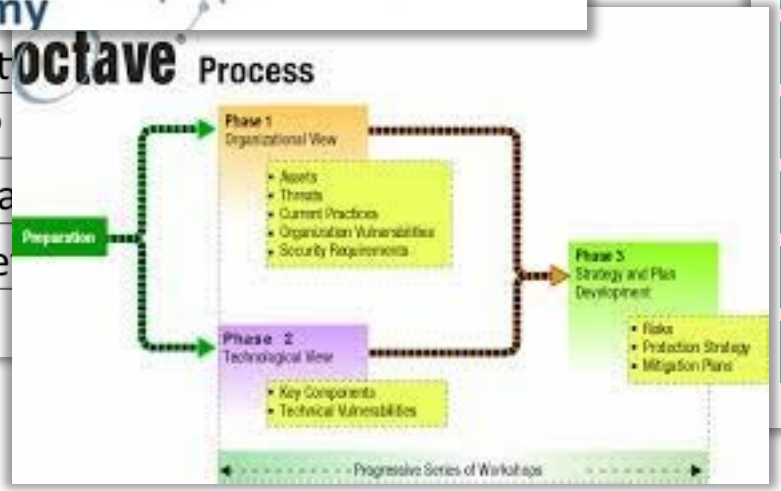
STRIDE

ition	Property	Example
nd to be someone else.	Authentication	Hack victim's email and use to send messages in name of the victim.
ge data or code.	Integrity	Software executive file is tampered by hackers.
ing not to do a ular action.	Non-repudiation	"I have not sent an email to Alice".
ge of sensitive nation.	Confidentiality	Credit card information available on the internet.
vailability of servi		
o perform unauth		

DREAD+D

Damage	How bad would
Reproducability	How easy to re
Exploitability	How easy to launch the at
Affected Users	How many are impacted?
Discoverability	How easy to discover for a
Detection	How hard to detect for de

ConFoo Vancouver 2016

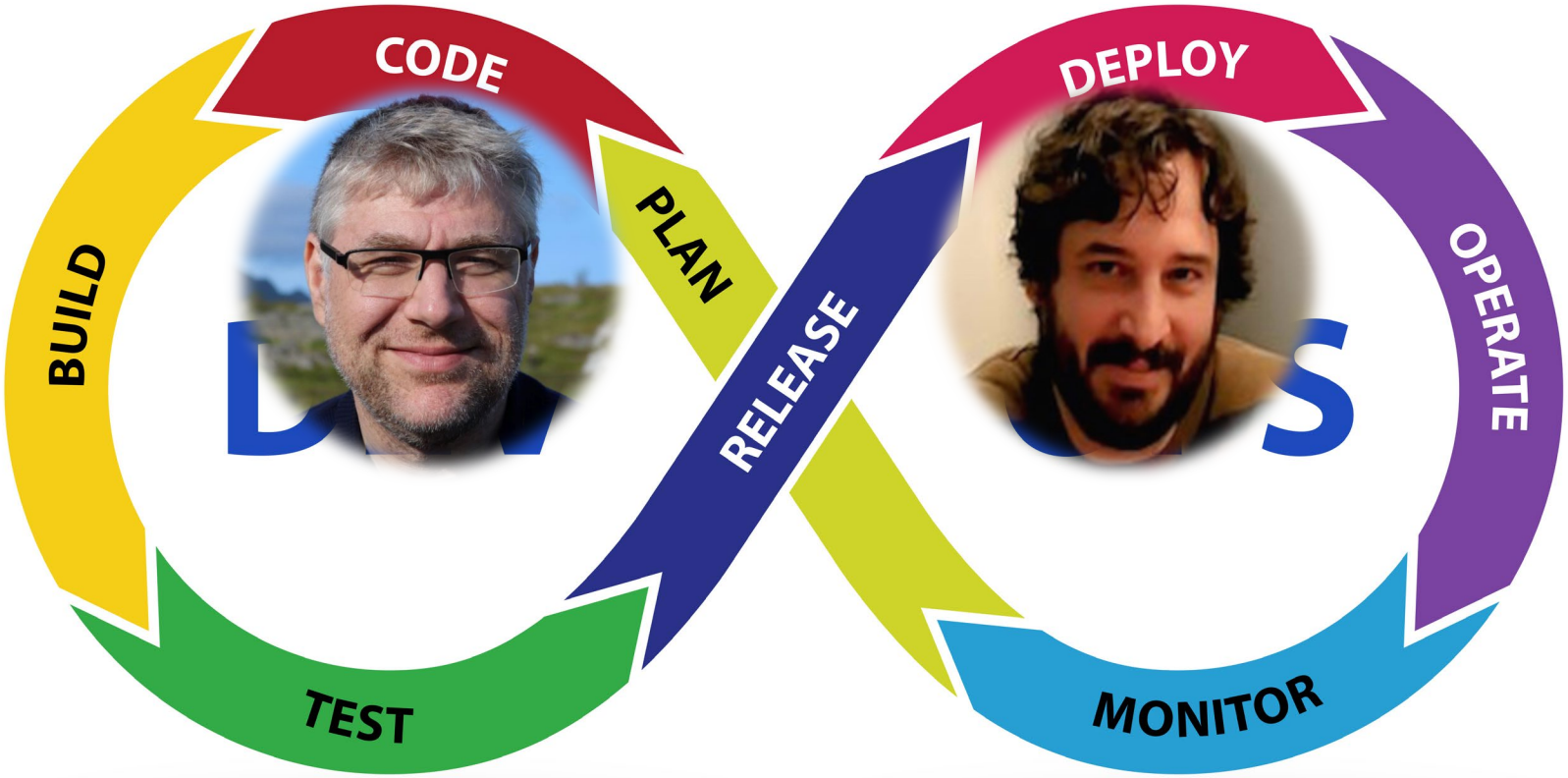


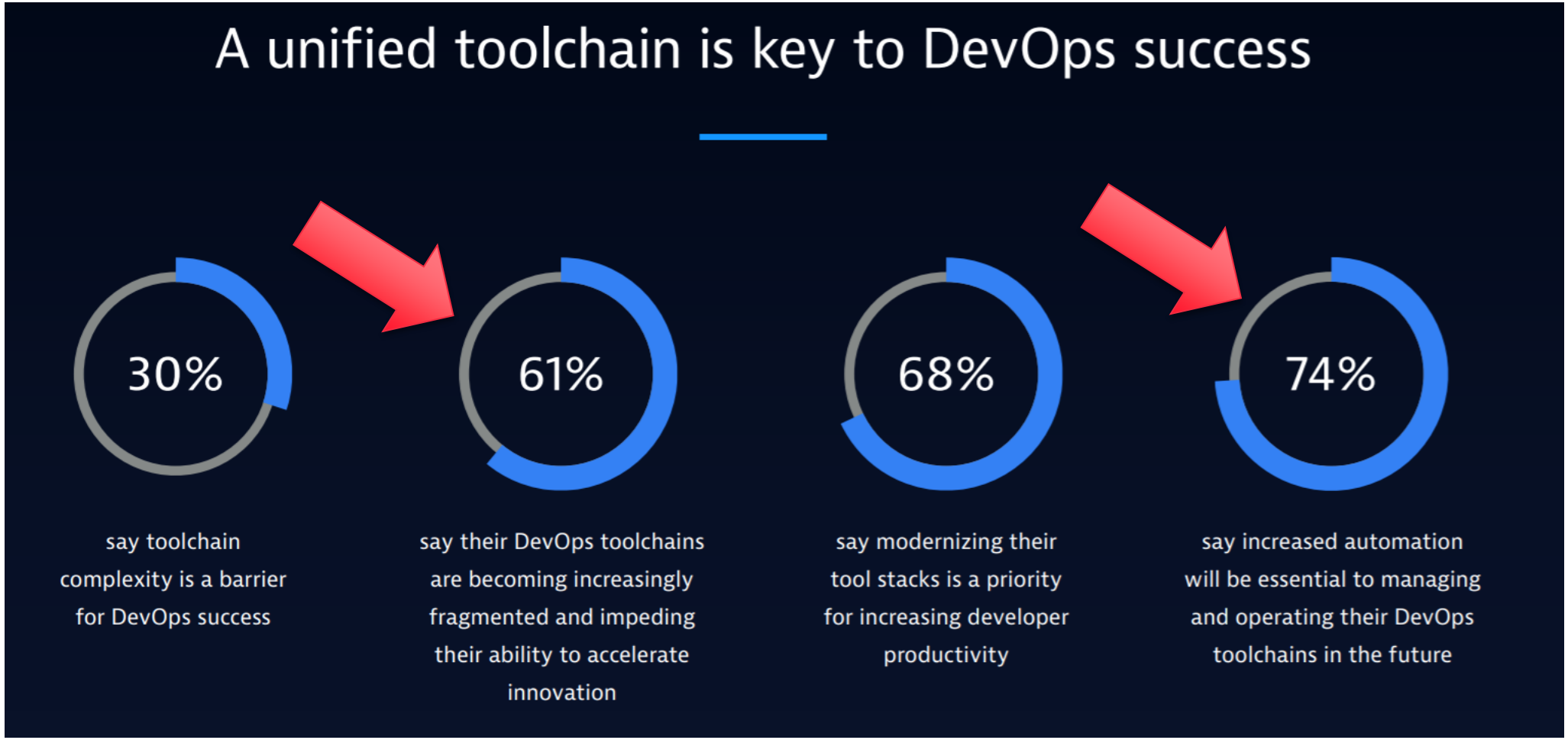
PASTA Methodolgy

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

DICEUS

Meanwhile, in 2008…





Dynatrace 2021 DevOps Report
https://www.dynatrace.com/monitoring/solutions/devops-report

What is Threat Modeling?

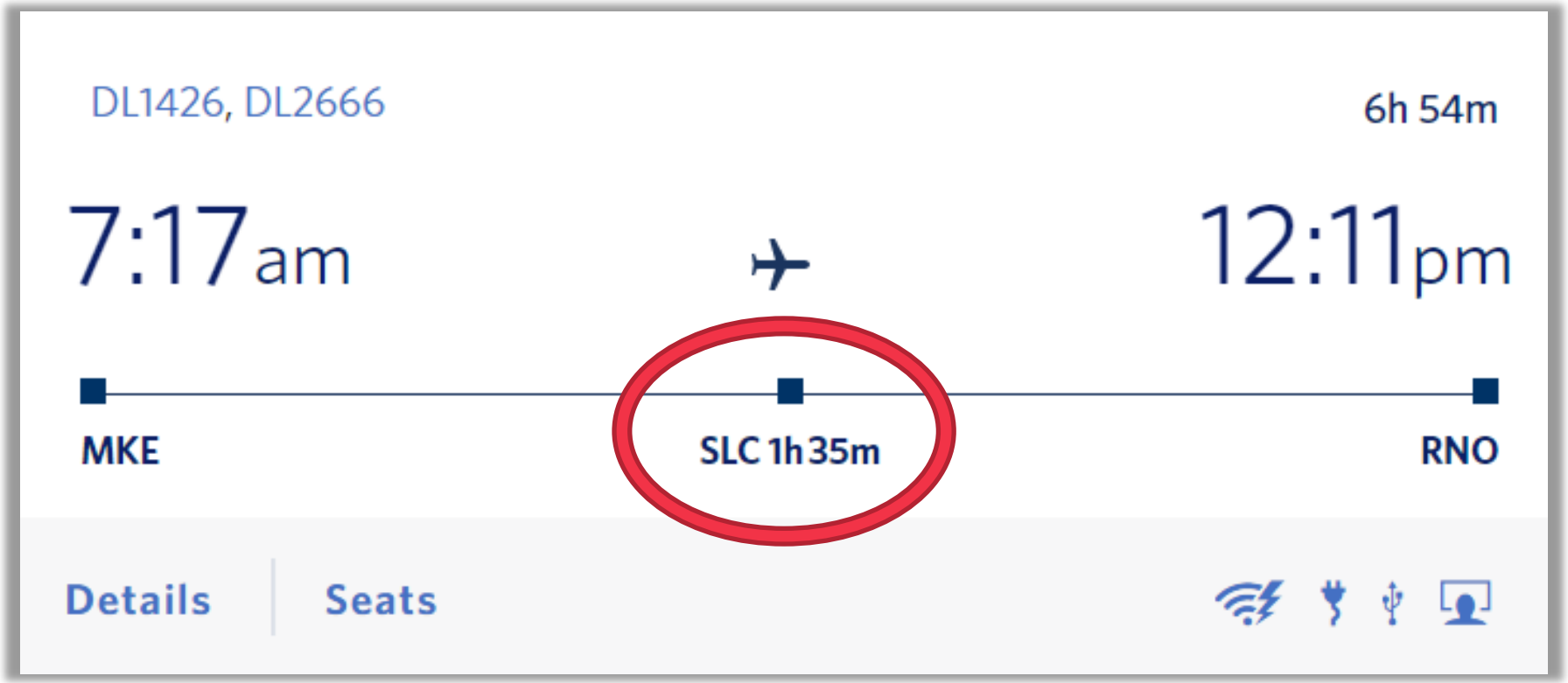
Why do we Threat Model?

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.”

https://www.threatmodelingmanifesto.org/

"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/

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

https://www.threatmodelingmanifesto.org/

RSAConference2022

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…

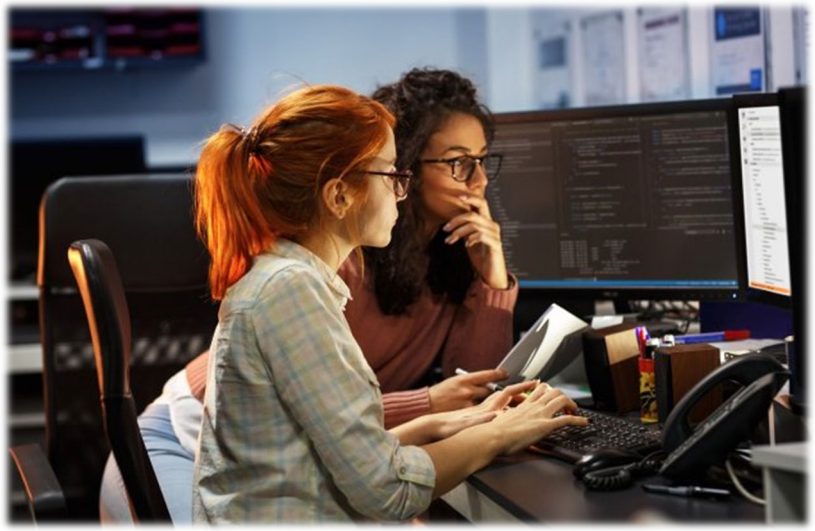
…over a single delivery

RSAConference2022

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

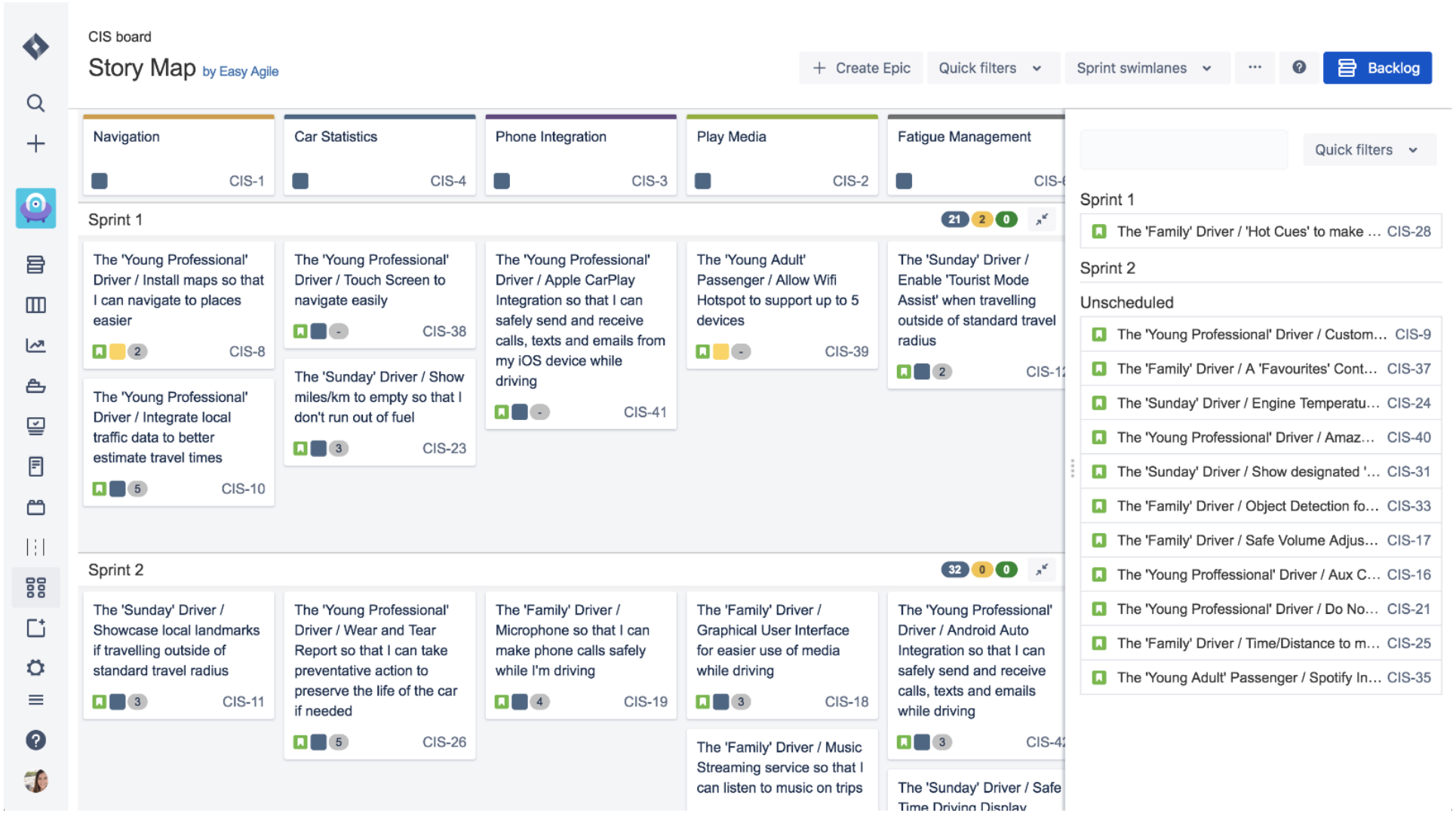
RSAConference2022

Building a Methodology in DevSecOps

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

The DevOps Pipeline

Build a security empowered culture



Alyssa MILLER
www.alyssasec.com

As a Car driver

I want to Enter a destination name

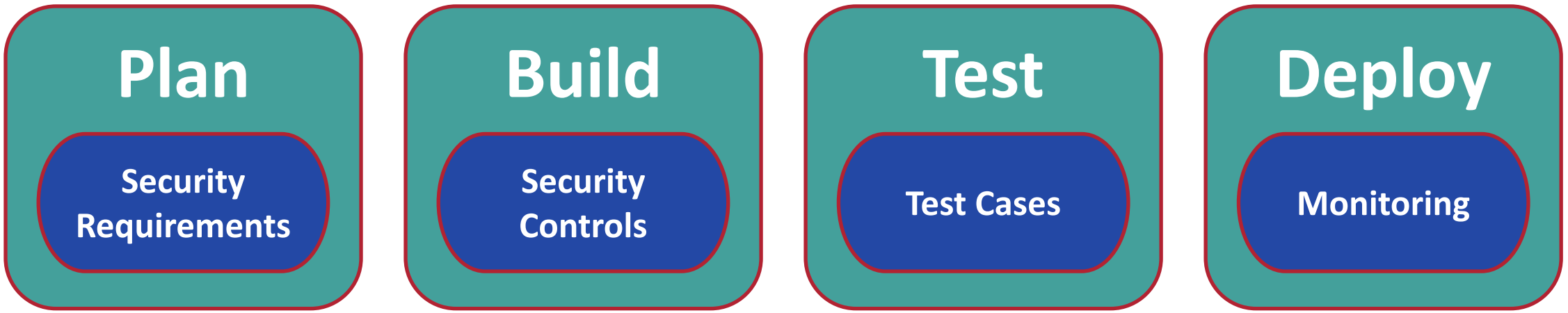
So that I can navigate w/o an address

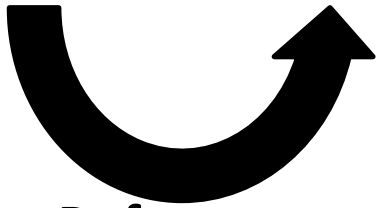
** I want you to:

Protect My search history

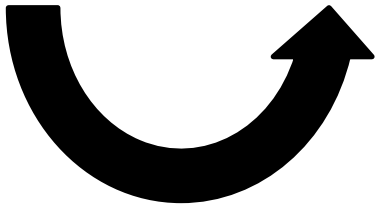
From Being accessed by attackers

Asset & Threat Information

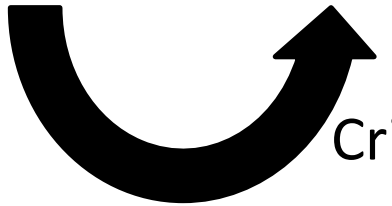




Reference Architectures



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]
```

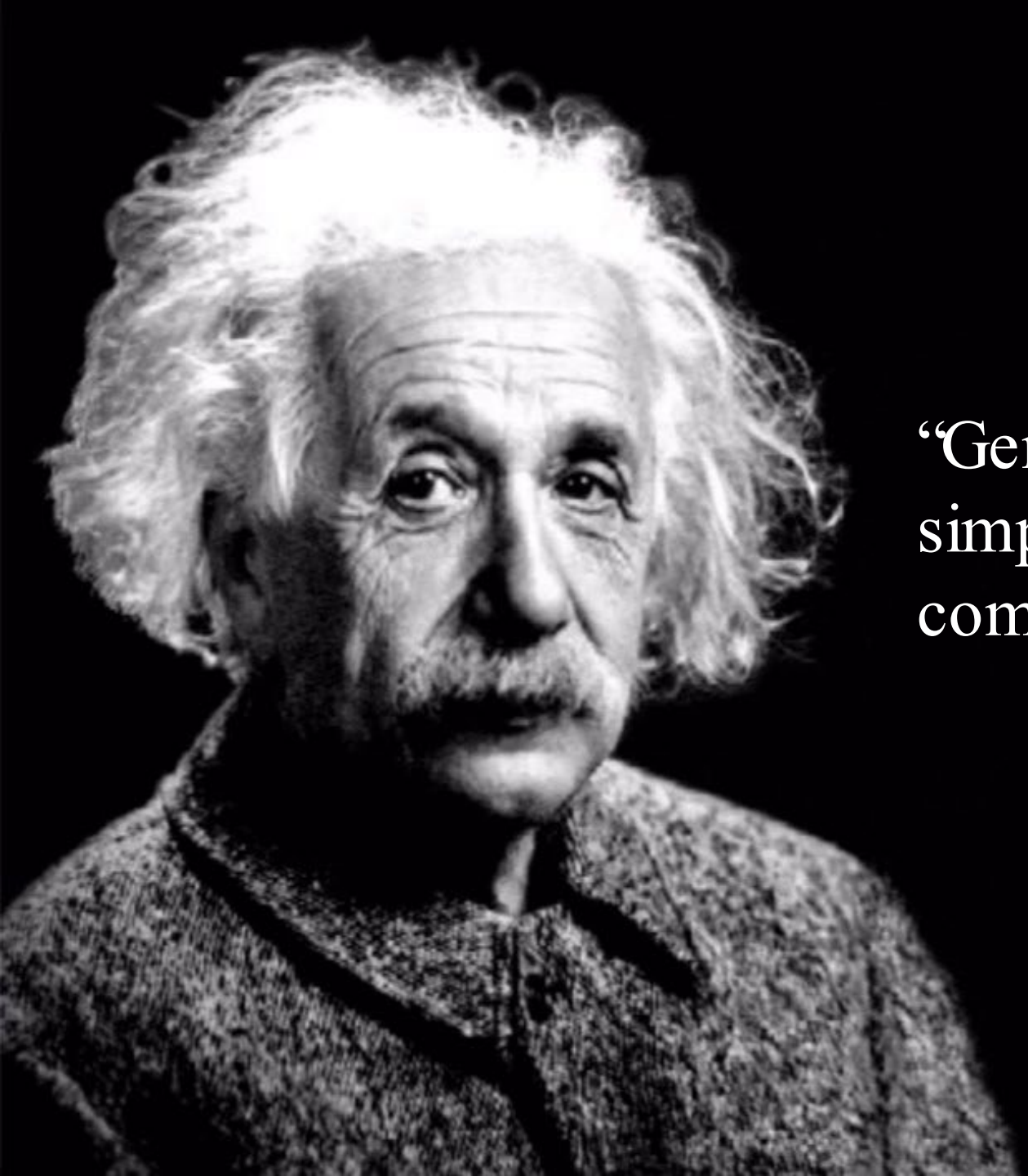
```
steps:
-task: myRepo.tstExtensionId.contribId.FuzzSessTkn@0
  inputs:
    tokenName: ‘jzsession'
    format: ‘base64’
  target:<hostname>
- task: parseTestResults@1
  inputs:
    testResultsFiles: "**/tstFuzzResults-*.xml"
  condition: succeededOrFailed()
```

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



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

– Albert Einstein