



The Diana INITIATIVE

Threat Modeling in 600 seconds
(ok, I lied, more like 2,400)

Kat Fitzgerald
@rnbwkat evilkat@rnbwmail.com

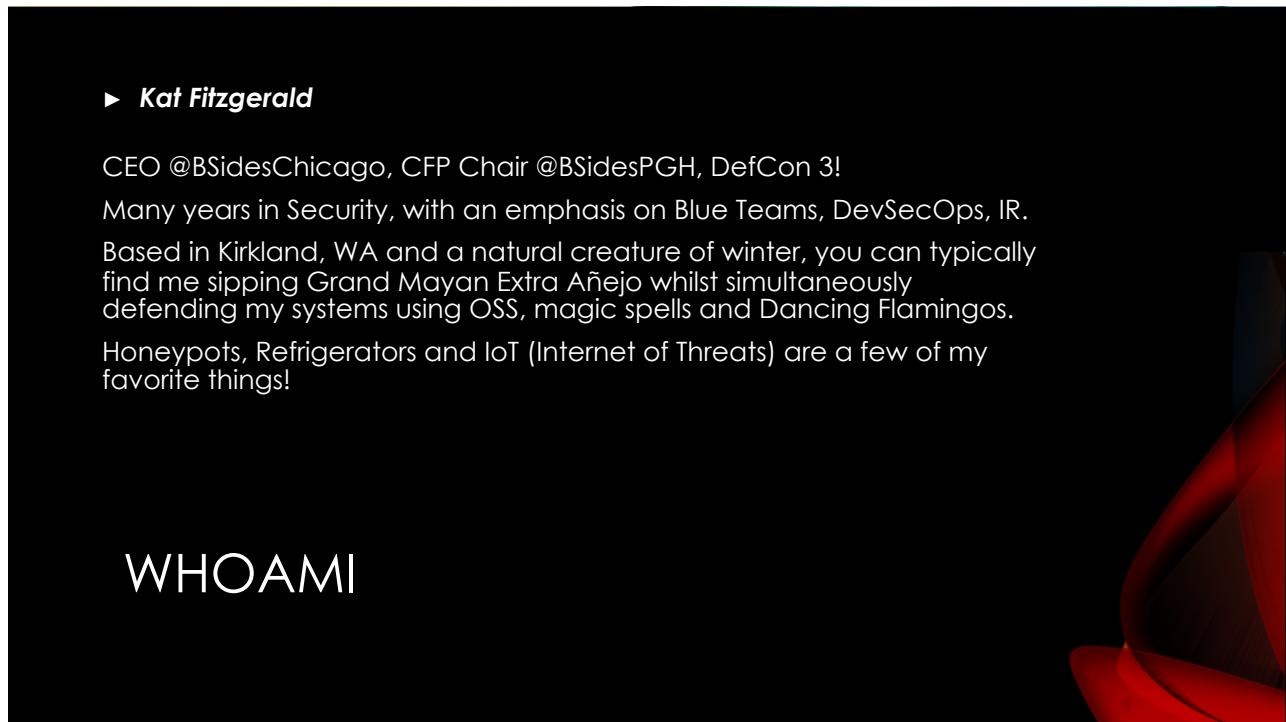
Virtual Conference JULY 16, 2022 *Las Vegas Conference AUGUST 10-11, 2022*

TAKE The INITIATIVE *DianaInitiative.org*





1

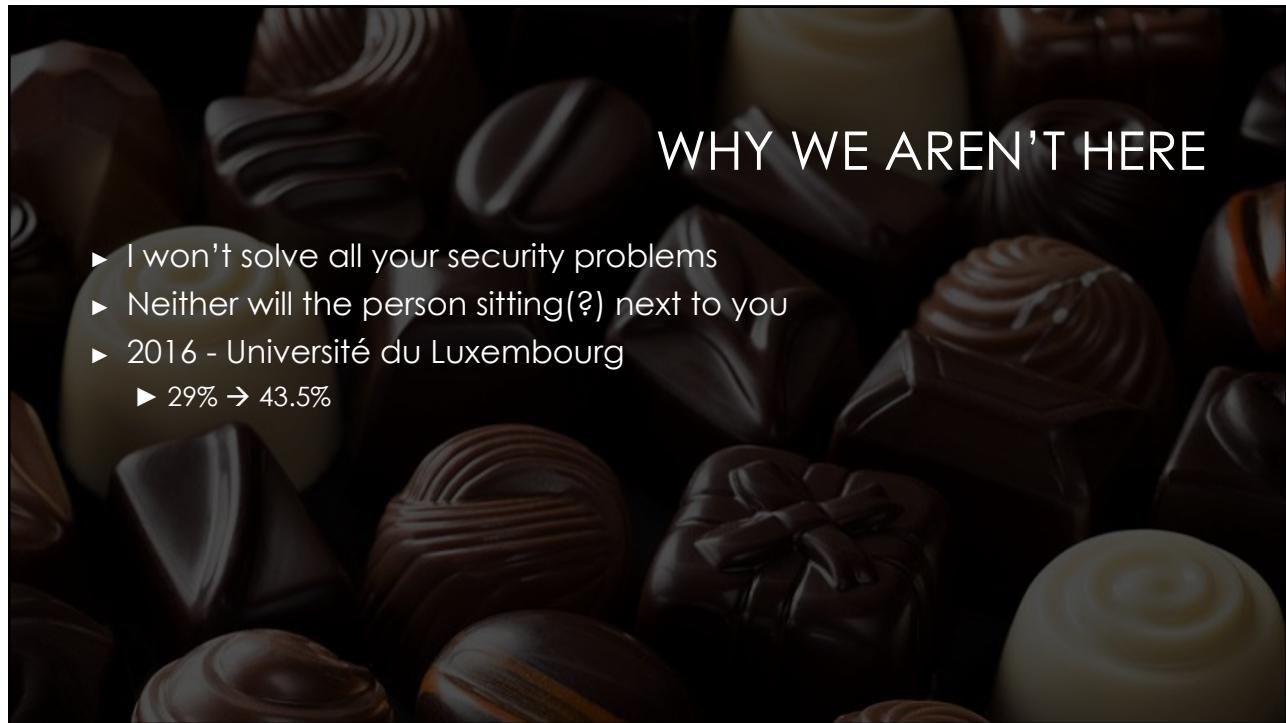


► **Kat Fitzgerald**

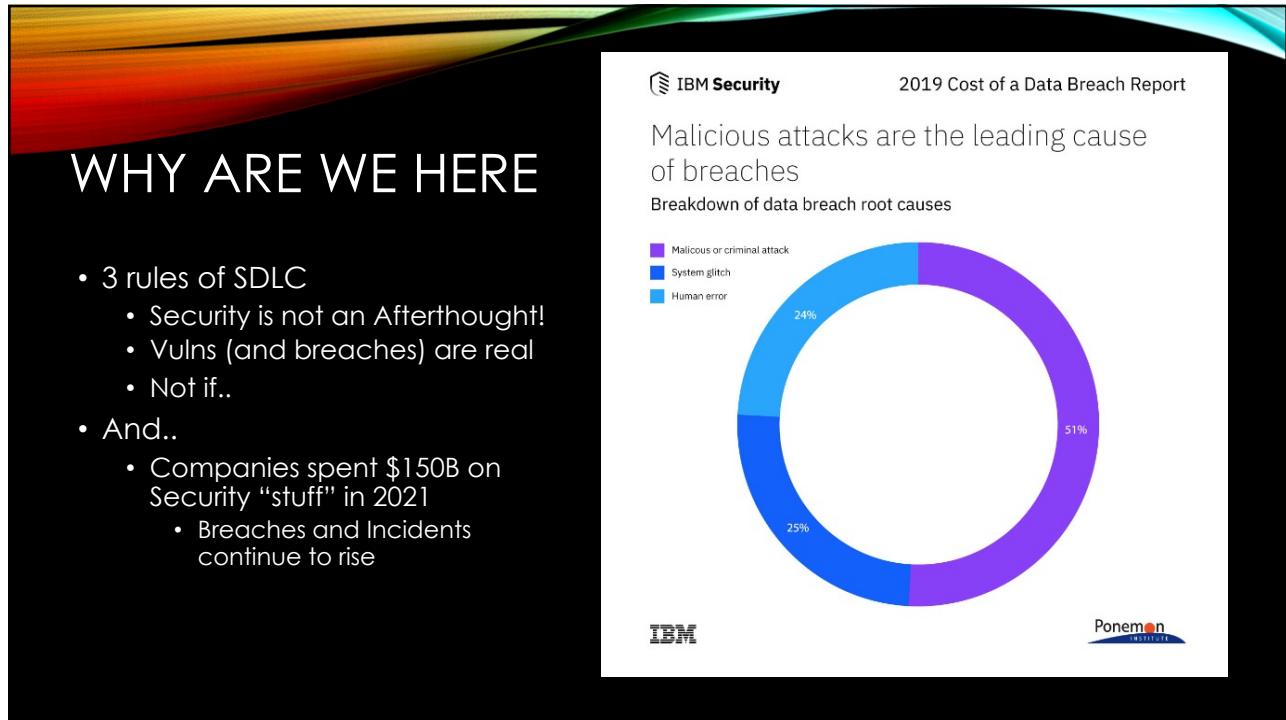
CEO @BSidesChicago, CFP Chair @BSidesPGH, DefCon 3!
Many years in Security, with an emphasis on Blue Teams, DevSecOps, IR.
Based in Kirkland, WA and a natural creature of winter, you can typically
find me sipping Grand Mayan Extra Añejo whilst simultaneously
defending my systems using OSS, magic spells and Dancing Flamingos.
Honeypots, Refrigerators and IoT (Internet of Threats) are a few of my
favorite things!

WHOAMI

2



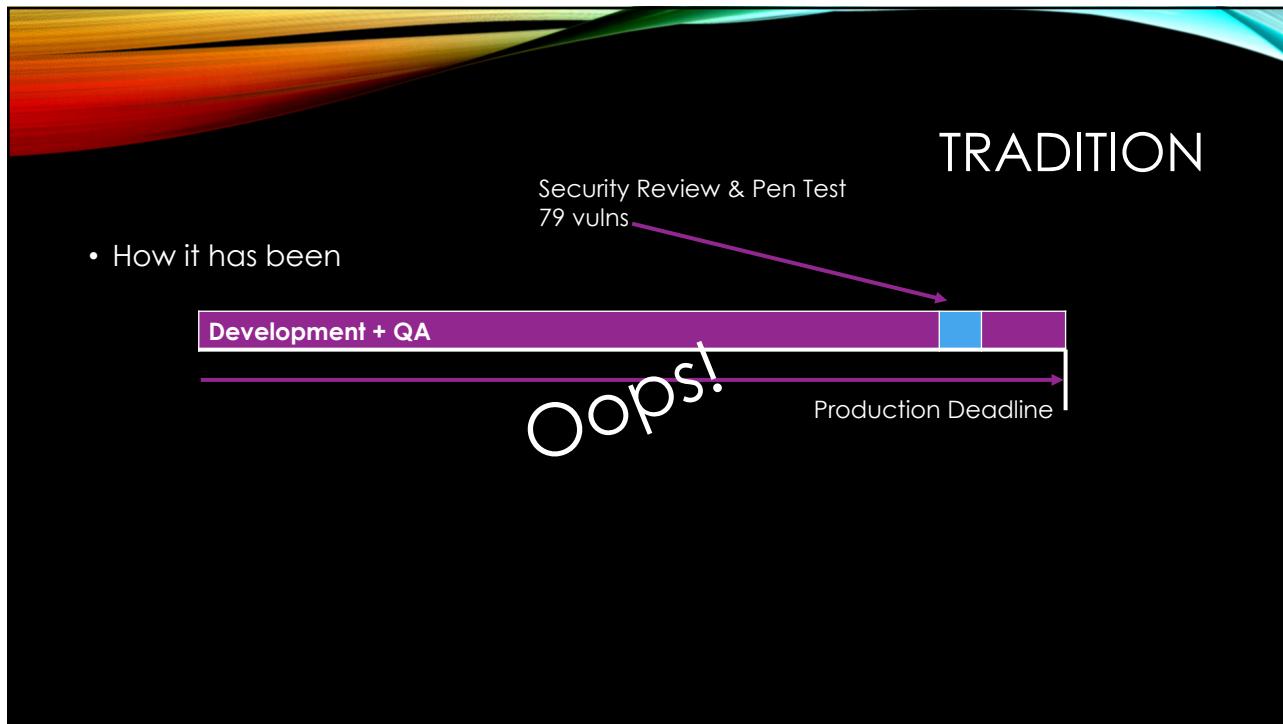
3



4



5



6



7



8

IDENTIFY, ENUMERATE, PRIORITIZE

Diagram

- What are we building?
- What/where are high-value targets?
- Pictures really are worth 1000 words!

Identify Threats

- What can go wrong?
- Where are attack vectors?

Mitigate

- How do we fix all the things?

Validate!

Attacks keep getting better!

9

IDENTIFY ASSETS

- ▶ What are you protecting
 - ▶ High level Always ←
 - ▶ Break it down as you go
- ▶ Other "assets"
 - ▶ CIA
 - ▶ Confidentiality
 - ▶ Integrity
 - ▶ Availability

10

DOCUMENT THE ARCHITECTURE

Define WHAT it does and HOW

Who does it?

Diagram the Application <- FTW!!

- List Assets
- Show Data Flow
- Show Encryption
 - *(include protocols/ciphers where possible)*

11

DECOMPOSE

- ▶ Refine the Architecture
 - ▶ Show AAA
 - ▶ Don't forget the third "A"?
 - ▶ Trust Boundaries
 - ▶ Show Technologies
 - ▶ Ingress/Egress points



12

WHY?

- ▶ Most Vulnerabilities are introduced during *design phase*
- ▶ Architecture Flaws are hard to change
- ▶ Secure By Design!
- ▶ Attackers Think Differently



13

IDENTIFY THREATS

- STRIDE
 - Spoofing
 - Access using false identity
 - Tampering
 - Modify data
 - Repudiation
 - Prove who did it
 - Information Disclosure
 - Access the data
 - Denial of Service
 - Still counts!
 - Elevation of Privilege
 - Assume priv user

14

OR IDENTIFY THREATS (2)

- DREAD
 - Damage Potential
 - Reproducibility
 - Exploitability
 - Affected Users
 - Difficult to define importance of each population
 - Discoverability
 - (?)
- PASTA
 - Process of Attack Simulation and Threat Analysis

15

WHAT ABOUT..

<https://attack.mitre.org/>

ATT&CK Matrix for Enterprise							
Resource Development 7 techniques		Initial Access 9 techniques		Execution 12 techniques		Persistence 19 techniques	
Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	BITS Jobs	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)
Impersonate Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Access Token Manipulation (5)	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Impersonate Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	BITS Jobs	BITS Jobs	BITS Jobs	Credentials from Password Stores (5)
Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Debugger Evasion
Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Create or Modify System Process (4)	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Maintain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Domain Policy Modification (2)	Domain Policy Modification (2)	Deploy Container
Change Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Shared Modules	Escape to Host	Event Triggered Execution (15)	Event Triggered Execution (15)	Direct Volume Access
	Trusted Relationship	Software Deployment Tools	Create or Modify System Process (4)	Event Triggered Execution (15)	Exploit Guardrails (1)	Exploit Guardrails (1)	Forge Web Credentials (2)
	Valid Accounts (4)	System Services (2)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Input Capture (4)	Input Capture (4)
		User Execution (3)		Exploitation for Privilege	File and Directory Permissions	Modify Authentication Process (5)	Modify Authentication Process (5)
						Multi-Factor Authentication Interception	Multi-Factor Authentication Interception
						File and Directory Discovery	File and Directory Discovery
						Domain Trust Discovery	Domain Trust Discovery
						Debugger Evasion	Debugger Evasion
						Container and Resource Discovery	Container and Resource Discovery
						Cloud Storage Object Discovery	Cloud Storage Object Discovery
						Cloud Service Dashboard	Cloud Service Dashboard
						Cloud Service Discovery	Cloud Service Discovery
						Cloud Infrastructure Discovery	Cloud Infrastructure Discovery
						Browser Bookmark Discovery	Browser Bookmark Discovery
						Application Window Discovery	Application Window Discovery
						Account Discovery (4)	Account Discovery (4)

16

AND THEN..

- <https://d3fend.mitre.org/>

The DEFEND knowledge graph displays a grid of 415 artifacts categorized into two main sections: Detect and Isolate. The Detect section includes File Analysis, Identifier Analysis, Message Analysis, Network Traffic Analysis, Platform Monitoring, Process Analysis, and User Behavior Analysis. The Isolate section includes Execution Isolation and Network Isolation. The grid is organized into rows and columns corresponding to specific analysis types like Homoglyph Detection, URL Analysis, and File Hashing.

Detect							Isolate	
File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation
Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Firmware Behavior Analysis	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation
Emulated File Analysis	URL Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Embedded Monitoring Code	File Access Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting
File Content Rules			Certificate Analysis	Firmware Verification	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Hardware-based Process Isolation	DNS Denylisting
File Hashing			Active Certificate Analysis	Peripheral Firmware Verification	Process Code Segment Verification	Domain Account Monitoring	IO Port Restriction	Forward Resolution Domain Denylisting
			Passive Certificate Analysis	System Firmware Verification	Process Self-	Job Function Access	Kernel-based Process Isolation	Hierarchical Domain Denylisting

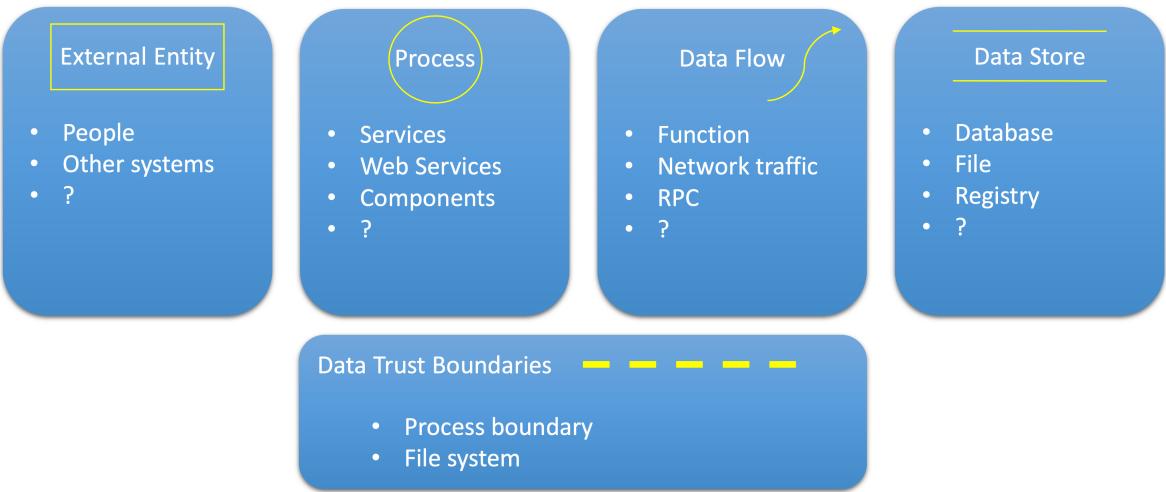
17

DFD – DATA FLOW DIAGRAM

- ▶ DFD = A graphical representation of the “flow” of data
 - ▶ Not the flow of control - that’s a flow chart
- ▶ Processes can run in parallel
- ▶ Simple Steps
 - ▶ Start at High level (see, I told you)
 - ▶ This is the “Context Level” - entities & processes
 - ▶ Level 0 - Subprocesses
 - ▶ Level 1-n - Data flows, data stores and boundaries

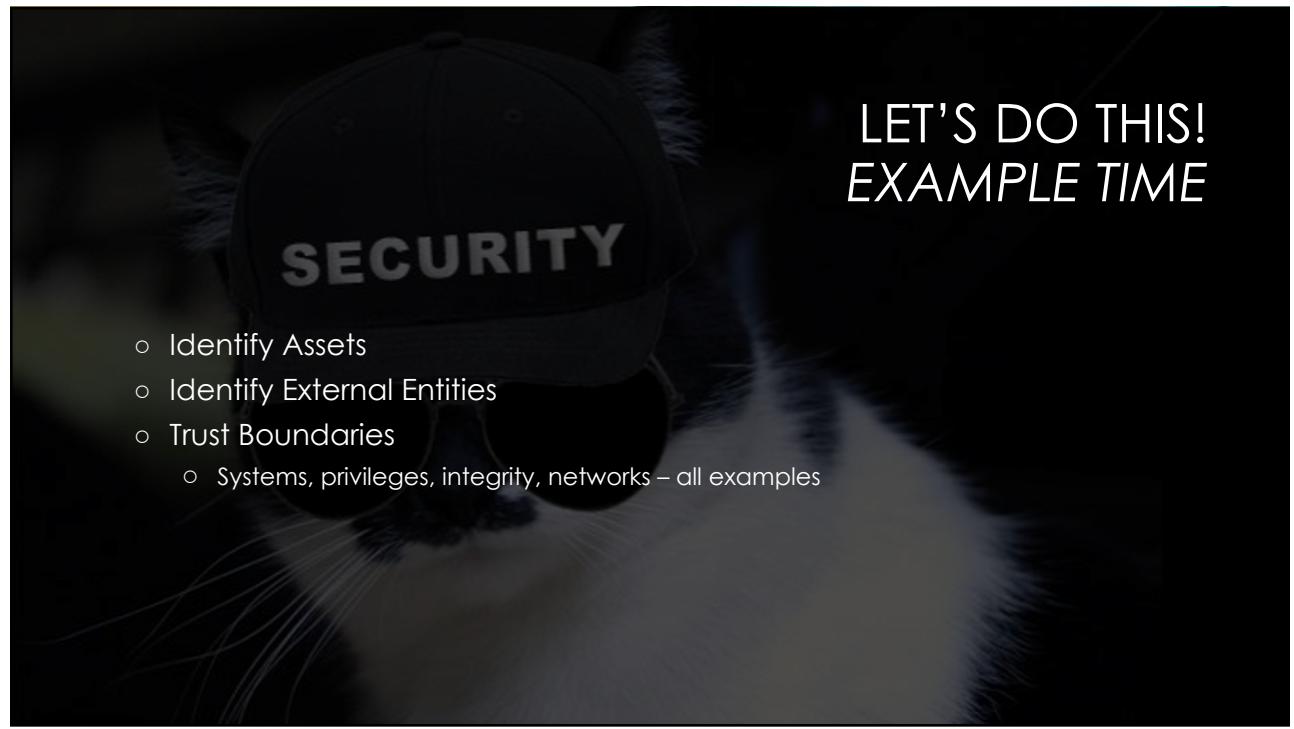
18

DFD SYMBOLS



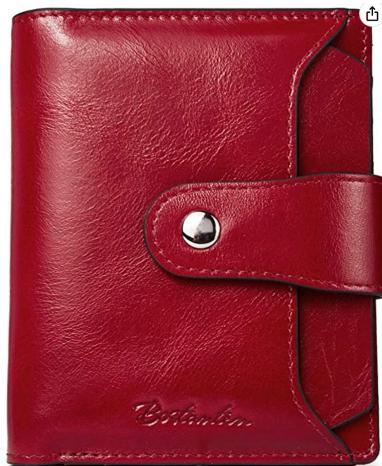
19

LET'S DO THIS!
EXAMPLE TIME

- 
- SECURITY
- Identify Assets
 - Identify External Entities
 - Trust Boundaries
 - Systems, privileges, integrity, networks – all examples

20

THREAT MODEL THIS

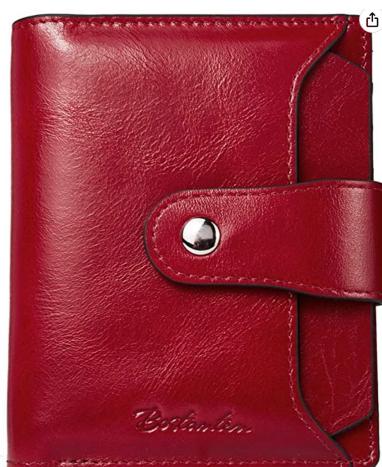


Women's Leather RFID
Blocking Small Wallet



21

THREAT MODEL THIS



22

DFD CHECKLIST

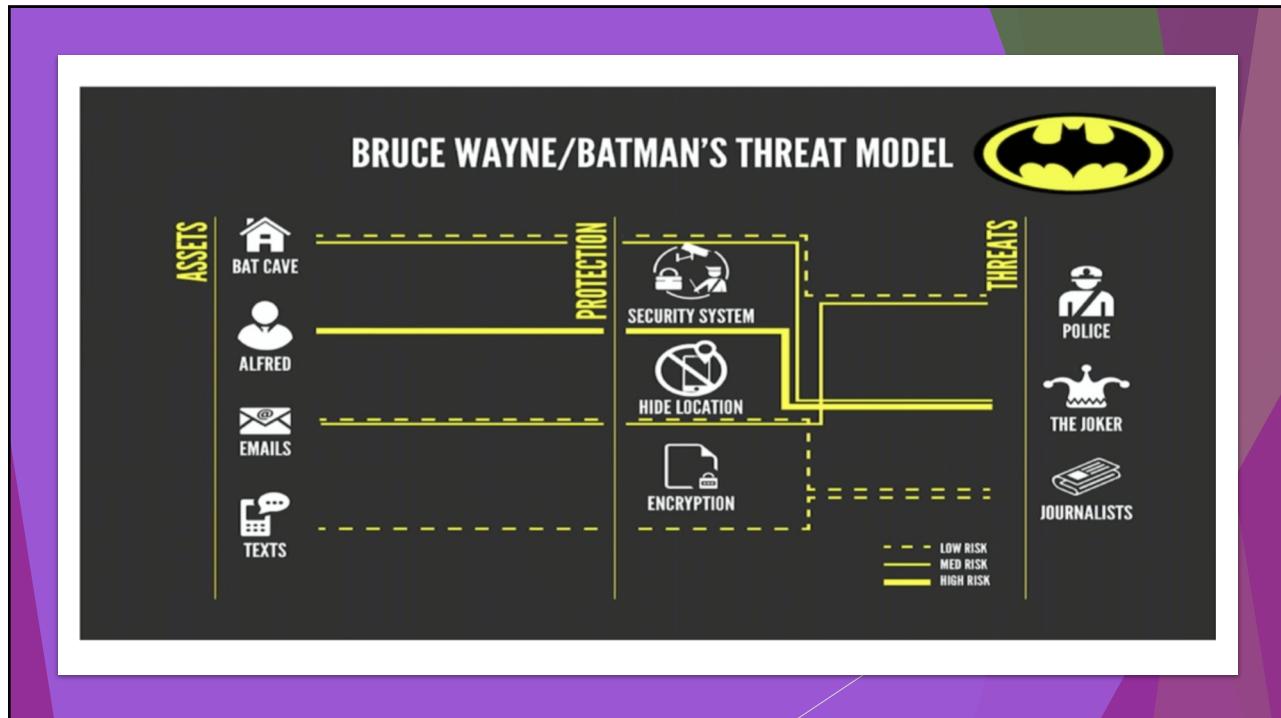
- Define Scope
- Break down, identify all the assets
- Start your diagram
 - Context (L0)
 - Just keep swimming layering
 - Add dataflows (not a flowchart)
- Add where important data:
 - lives
 - transits
 - transforms

23

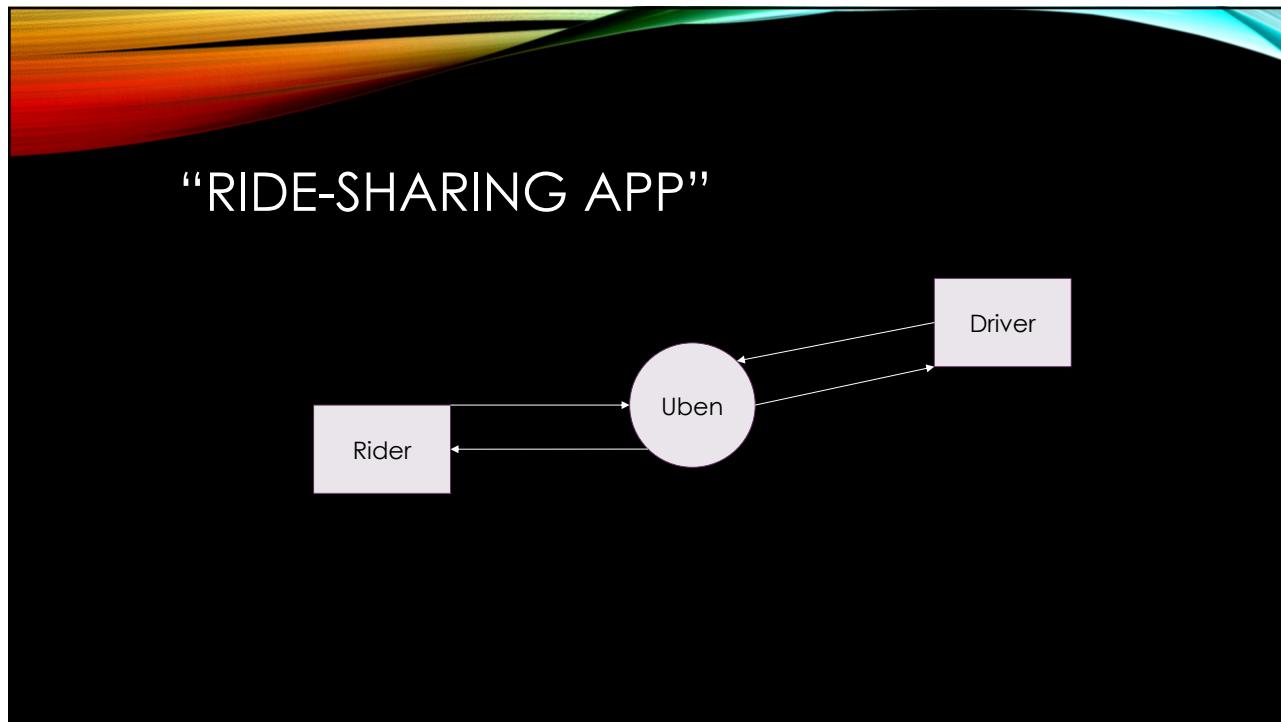
DFD CHECKLIST (2)

- Start with DFD 0 – Context
 - Label all assets
- Add “flows” including directions
 - Label main action on each flow
 - Don’t forget protocols
- Add Trust Boundaries (and networks)
- Label “types” of data and flow
- Add ppl and types
- Label each Authentication process
- Label each Authorization process
- Add order of all the actions
- Identify “Crown Jewels”
 - Data Classification
 - Transit/Rest

24



25



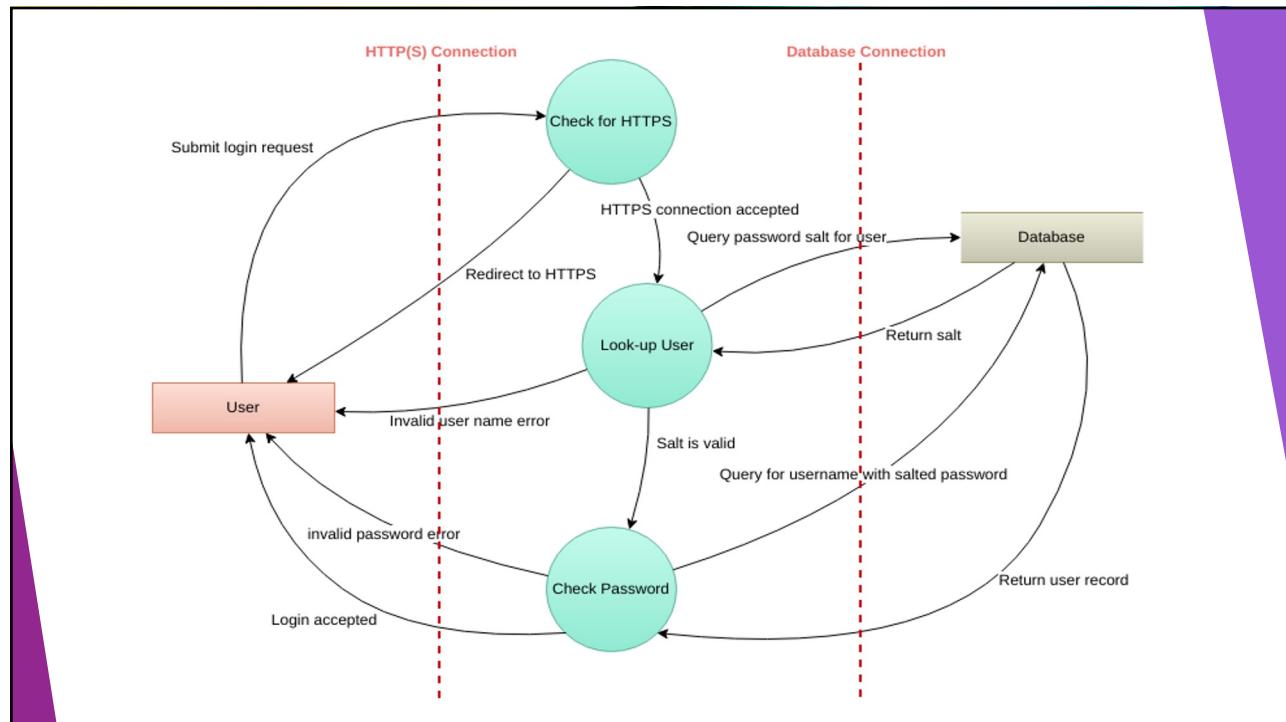
26

DFD 1

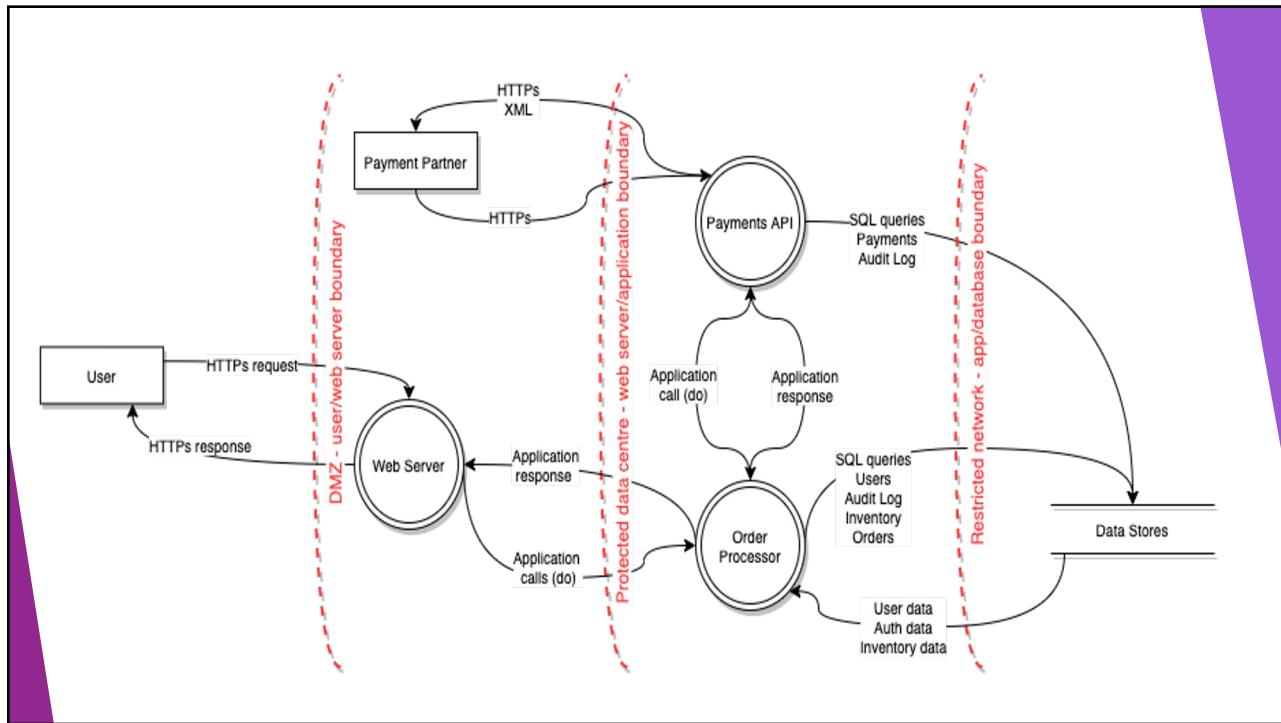
- ▶ And remember ..
- ▶ Defining Threats
 - ▶ Describe the Attack
 - ▶ Describe the Context
 - ▶ Describe the Impact



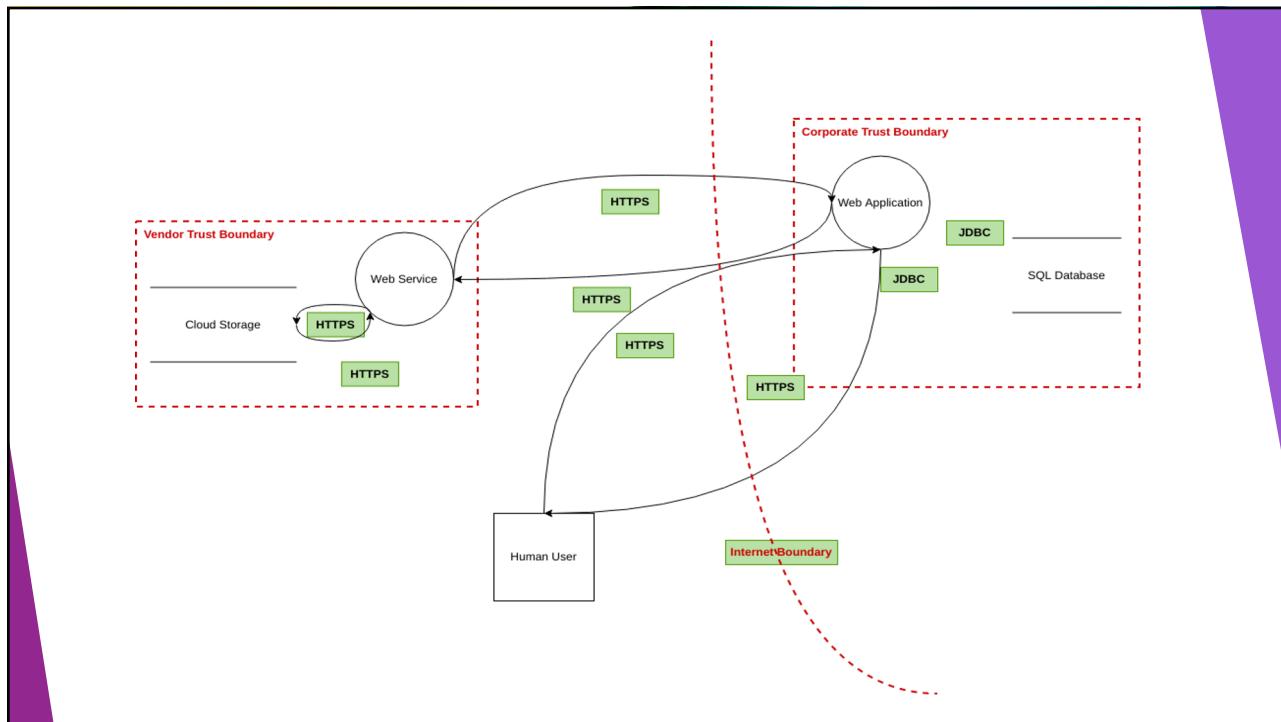
27



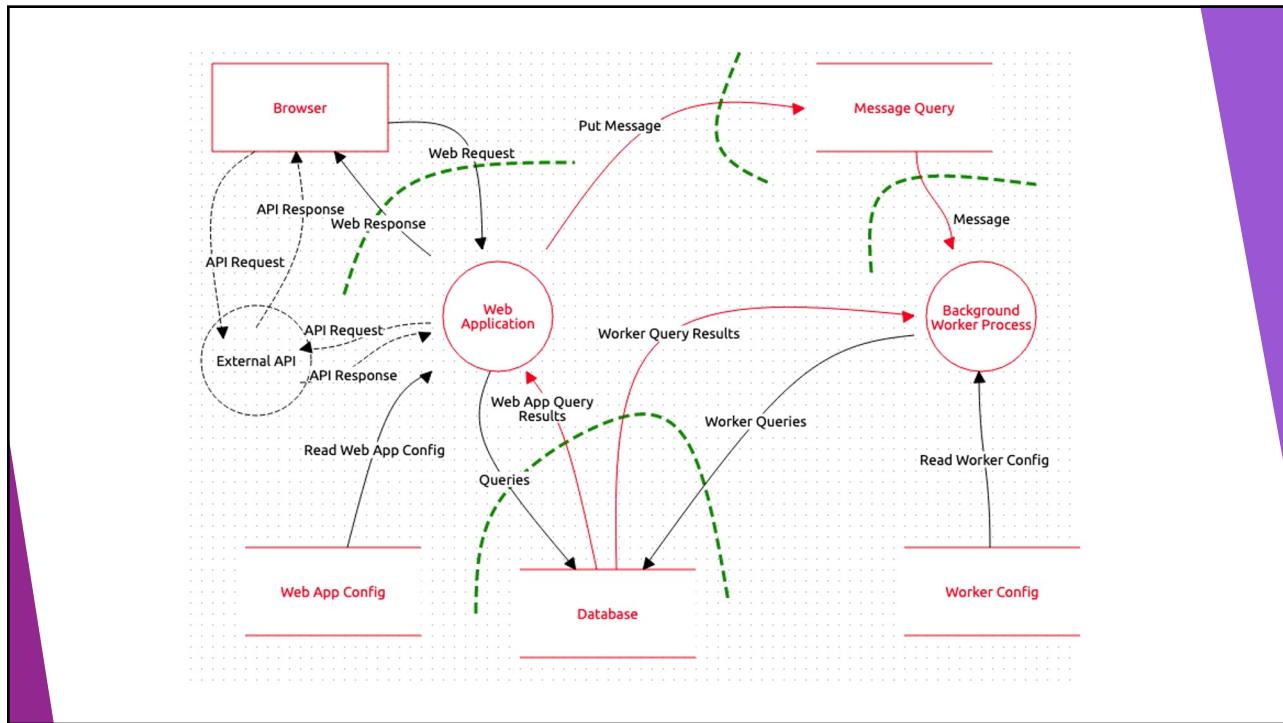
28



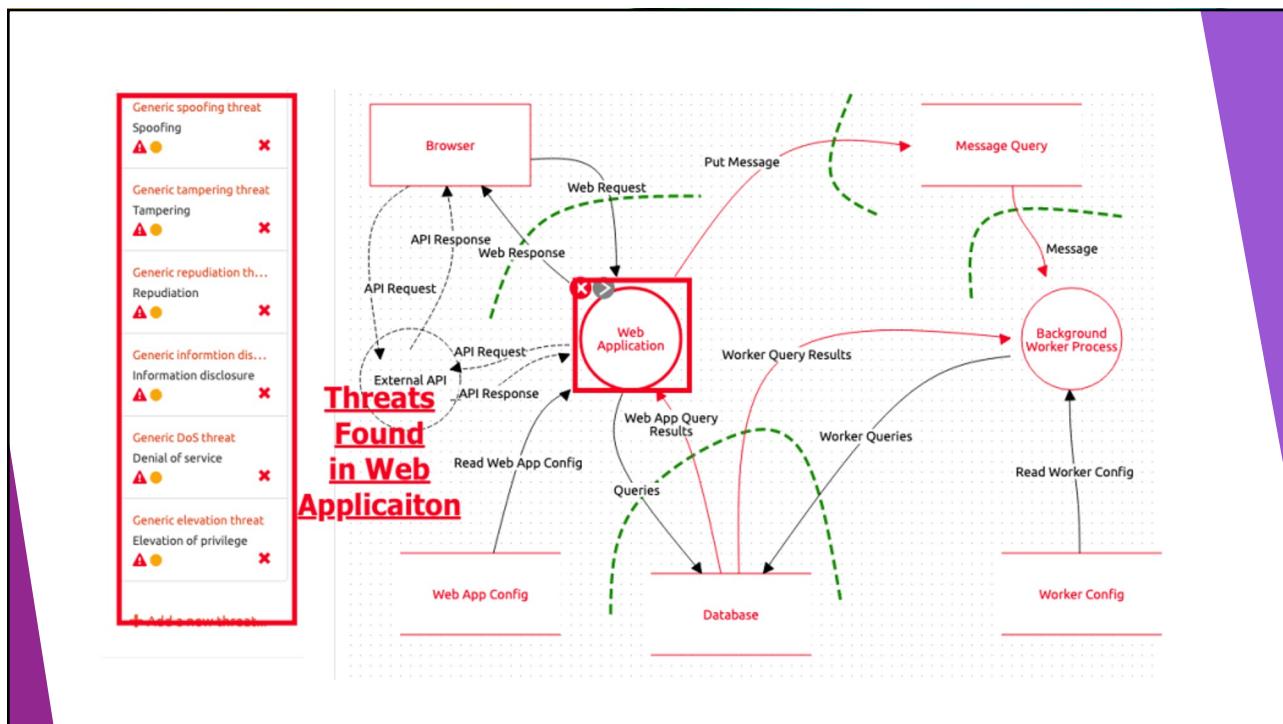
29



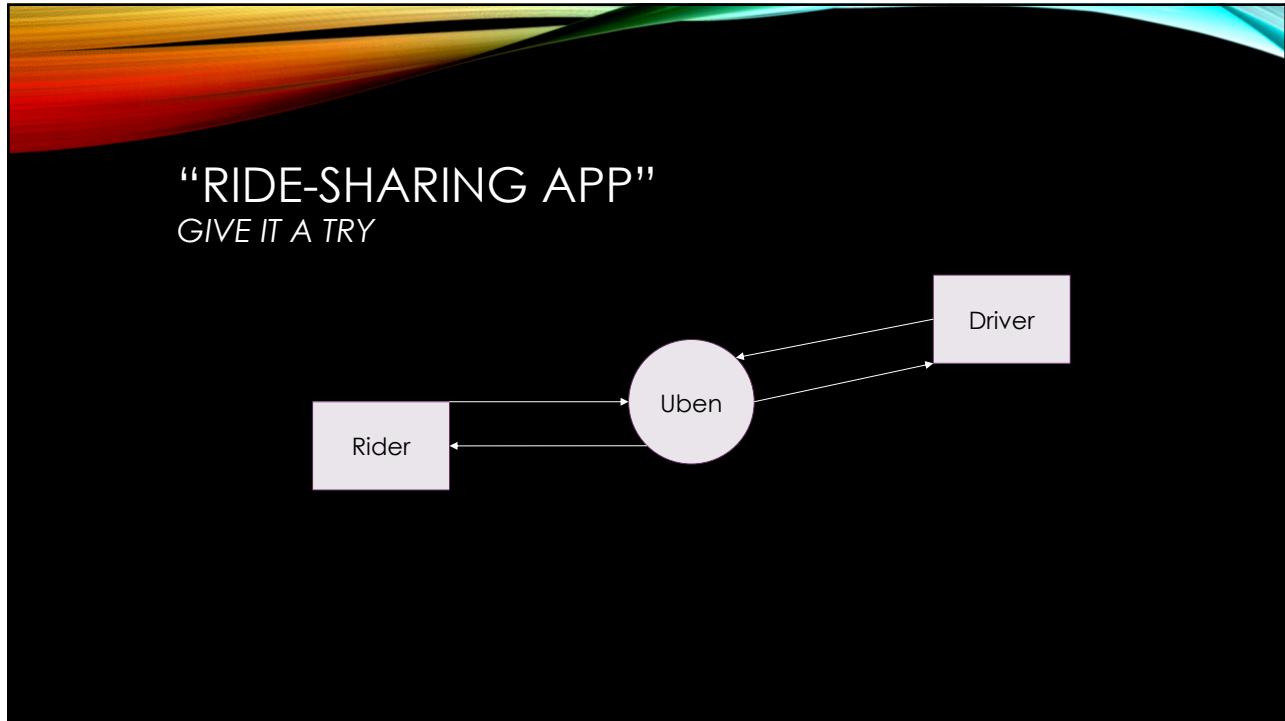
30



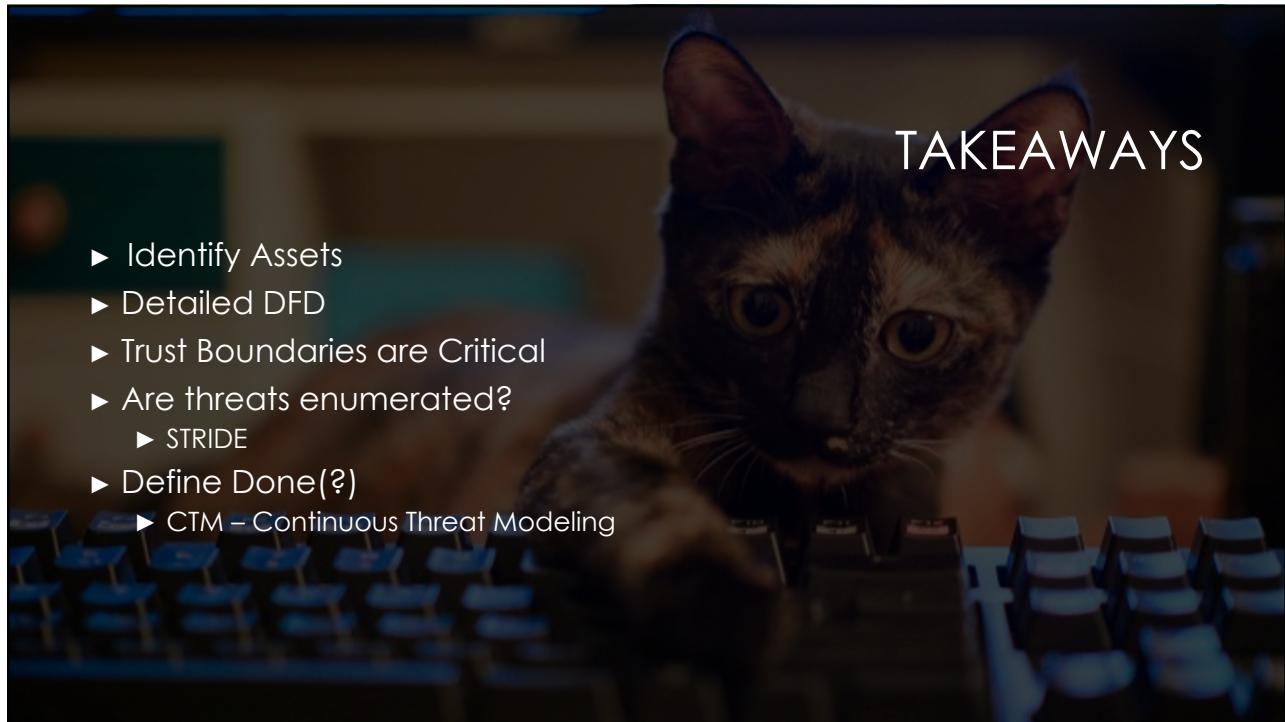
31



32



33



34

TAKEAWAYS (PT 2)

- ▶ Secure by Design
 - ▶ Not by Incident!
- ▶ Threat Actors have all the time in the world
 - ▶ You don't
- ▶ Diagraming!
 - ▶ Trust Boundaries are Critical!
- ▶ Spend time Exploring ATT&CK and D3FEND

And finally –

Threat Modeling can model ANYTHING, not just software.

35

TOOLS / RESOURCES

- [Threat Modeling w/Terraform](#)
- [IriusRisk](#) Community & Commercial
- [Cairis](#)
- [SecuriCAD](#) (Foreseeiti)

I'll tweet these!

36

AND SOME MORE

- ▶ [Threat modeling by DDSec](#)
- ▶ [STRIDE](#)
- ▶ [Threat Modeling Manifesto](#)
- ▶ [OWASP Threat Dragon](#)
- ▶ [OWASP Threat Model Project](#)



37

Thank You!!

@rnbwkat
evilkat@rnbwmail.com



38