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

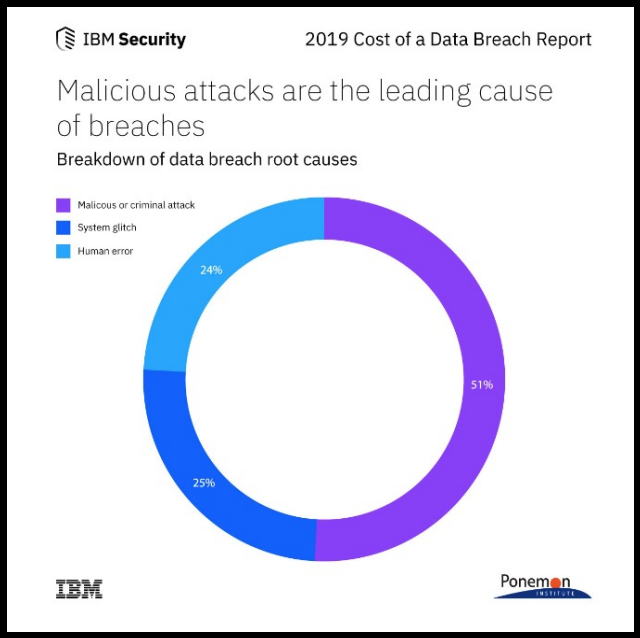
WHY WE AREN'T HERE

- I won't solve all your security problems
- Neither will the person sitting(?) next to you
- 2016 - Université du Luxembourg
  - 29% → 43.5%

3

WHY ARE WE HERE

- 3 rules of SDLC
  - Security is not an Afterthought!
  - Vulns (and breaches) are real
  - Not if..
- And..
  - Companies spent $150B on Security "stuff" in 2021
    - Breaches and Incidents continue to rise



4

THREATS

- In Simplest Terms
  - Network
  - Host
  - Application
- But what is Threat Modeling?

.. is the practice of identifying and prioritizing potential threats and security mitigations to protect something of value

5

TRADITION

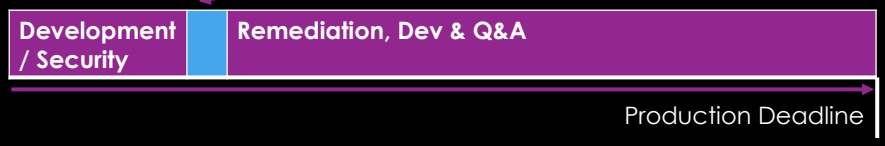
- How it has been

6

A BETTER WAY

- How it should be

Threat Modeling & Security Review
9 vulns



Teamwork!

YAY!!

7

THE THREE STAGES

- Threat Modeling - 3 high level stages
  - Decompose application
  - Determine and rank threats
  - Determine mitigations

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

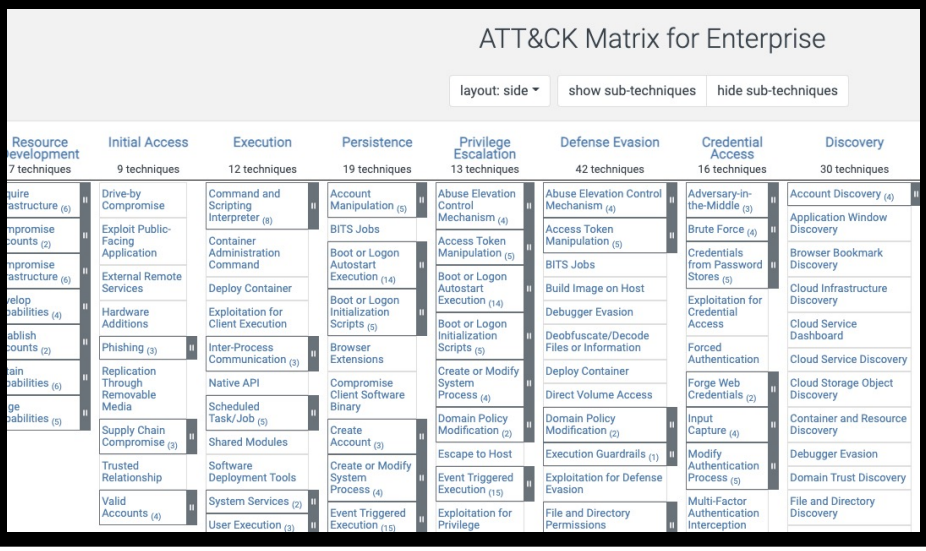
OR IDENTIFY THREATS (2)

- 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..

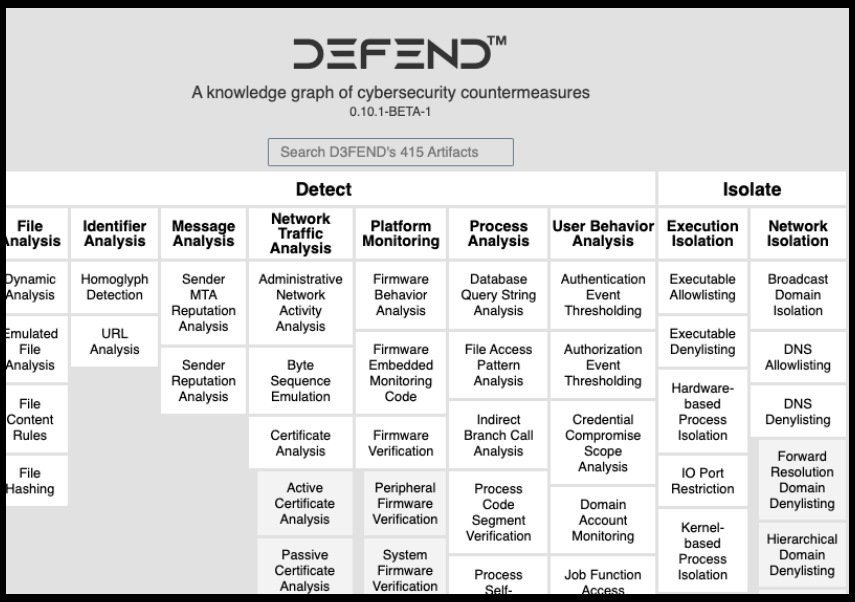
https://attack.mitre.org/



16

AND THEN..

- https://d3fend.mitre.org/



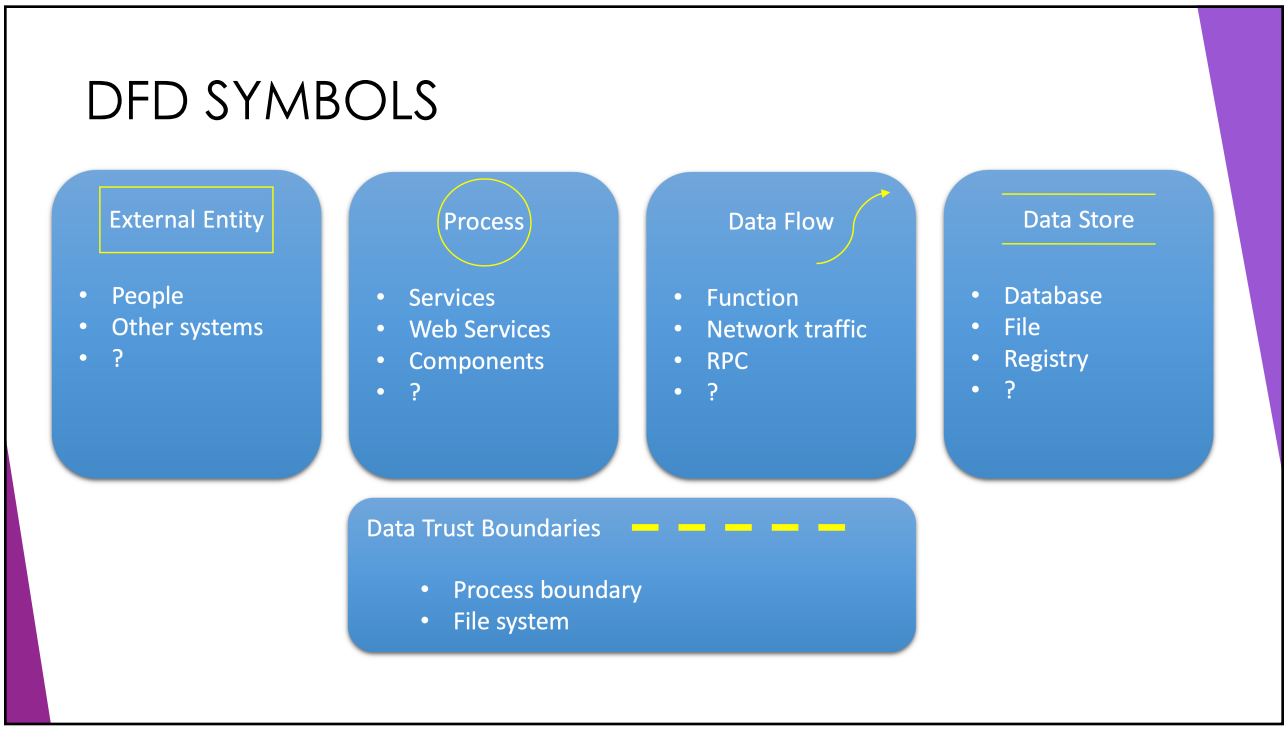
17

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

20

THREAT MODEL THIS

Women's Leather RFID Blocking Small Wallet

21

THREAT MODEL THIS

22

DFD CHECKLIST

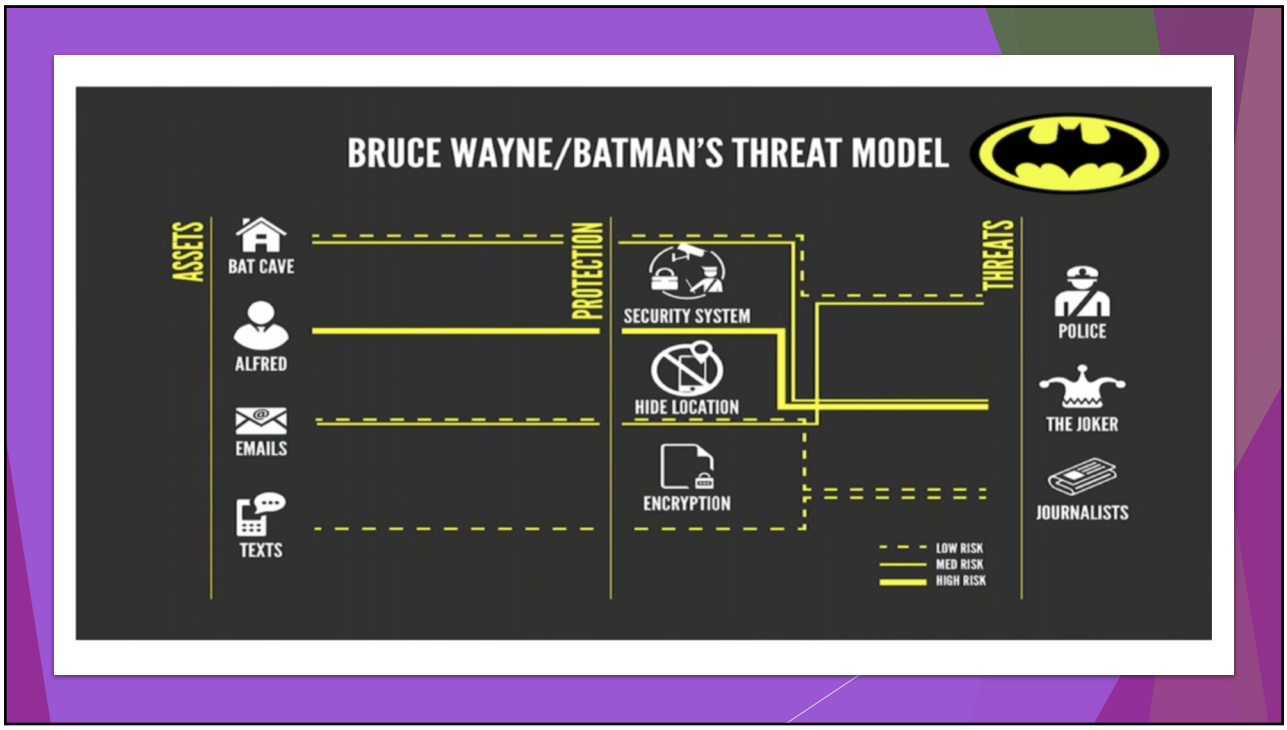
- Define Scope
- Break down, identify all the assets
- Start your diagram
  - Context (L0)
  - Just keep ~~swimming~~ layering
  - Add dataflows (not a flowchart)
- Add where important data:
  - lives
  - transits
  - transforms

23

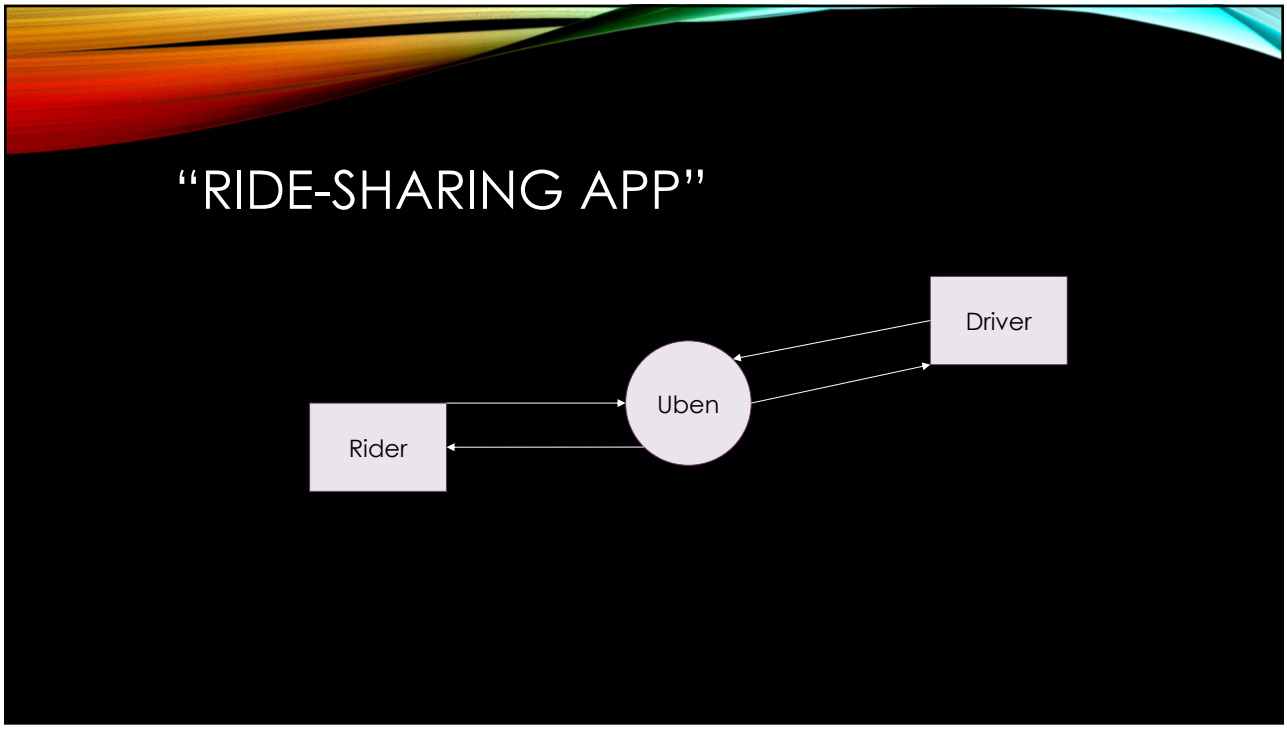
DFD CHECKLIST (2)

- 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


BRUCE WAYNE/BATMAN'S THREAT MODEL
ASSETS
BAT CAVE
ALFRED
EMAILS
TEXTS
PROTECTION
SECURITY SYSTEM
HIDE LOCATION
ENCRYPTION
THREATS
POLICE
THE JOKER
JOURNALISTS
LOW RISK
MED RISK
HIGH RISK

25

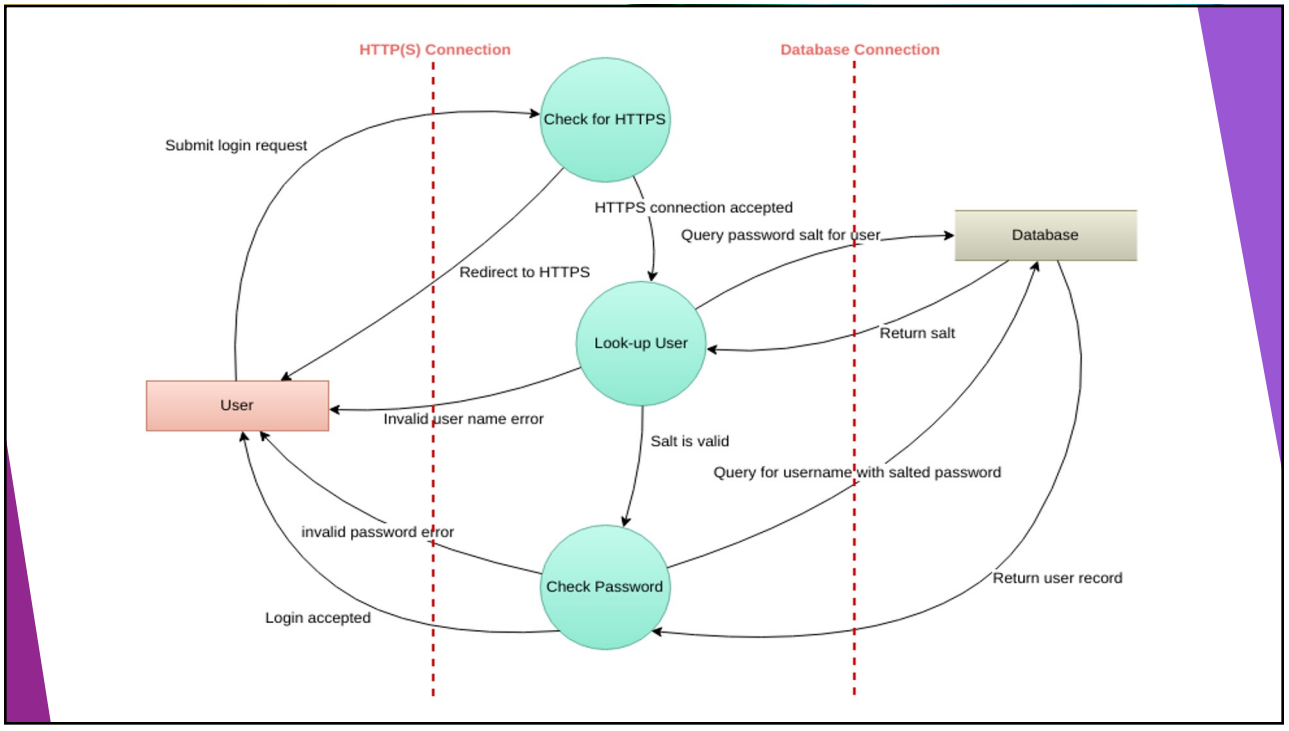

"RIDE-SHARING APP"
Driver
Uben
Rider

26

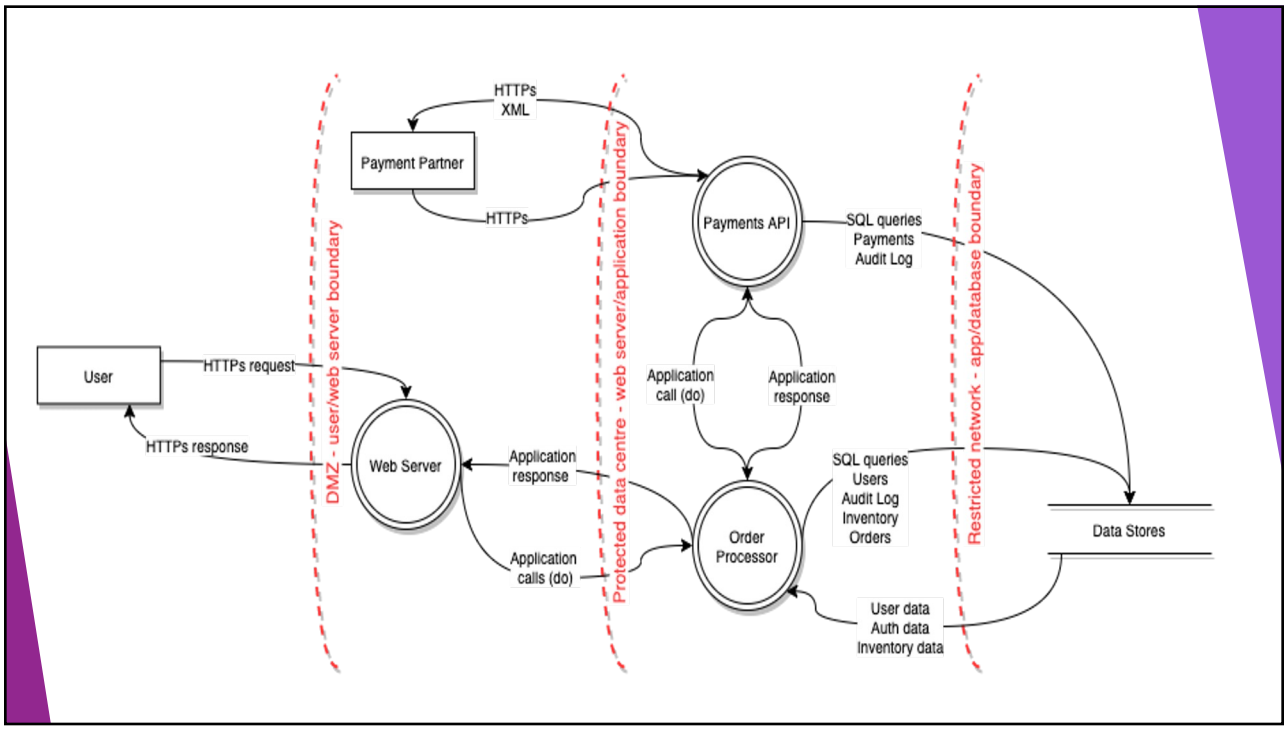
DFD 1

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

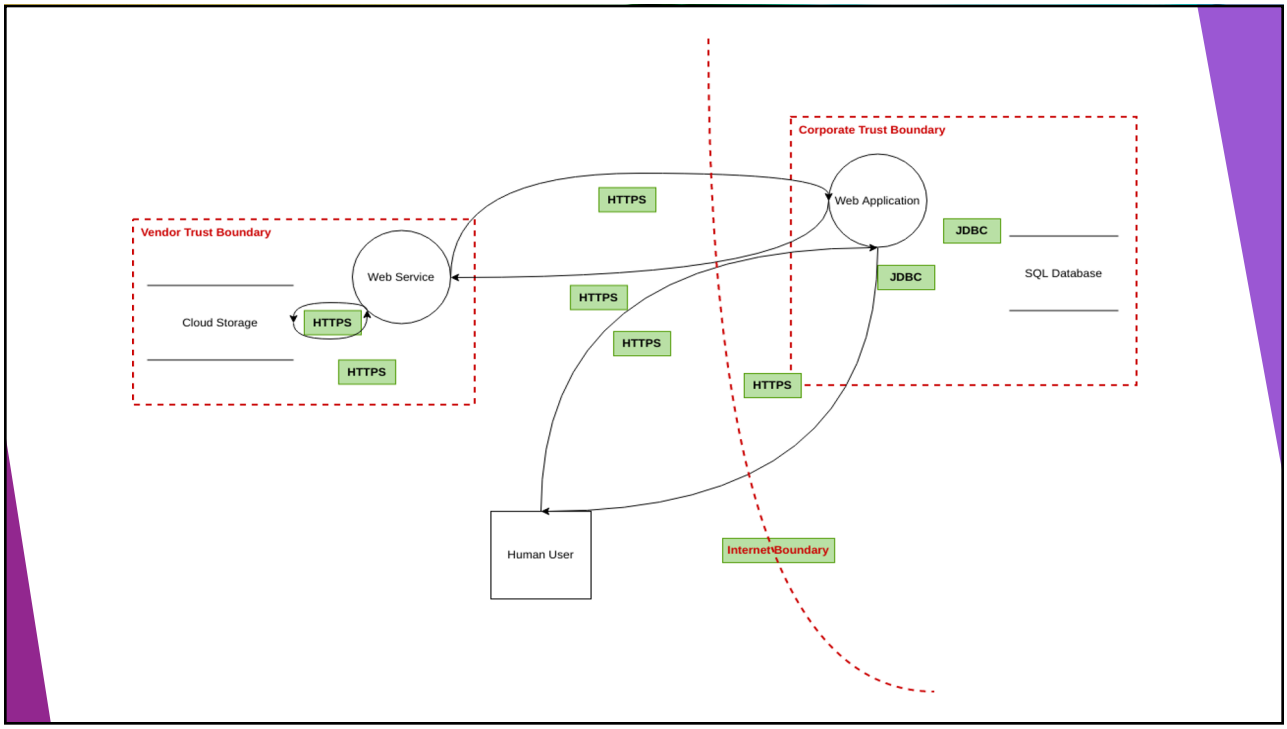
27



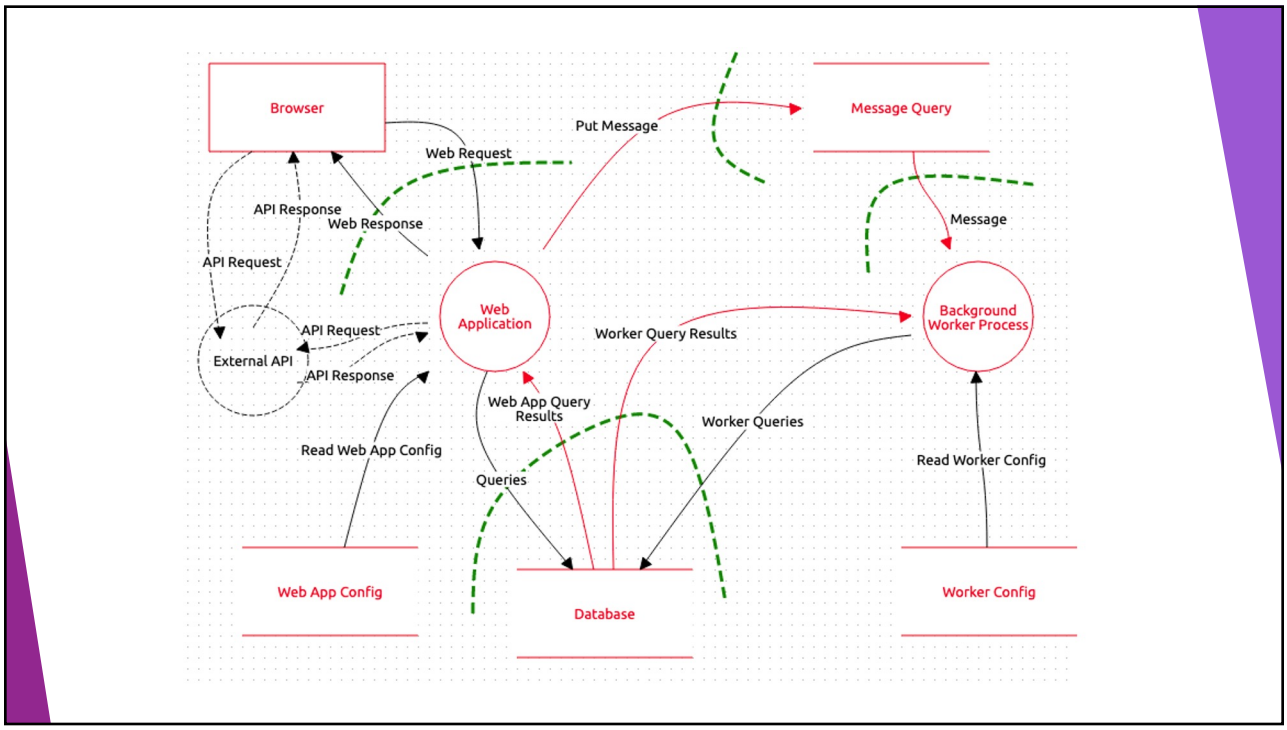
28


HTTPs
XML
Payment Partner
HTTPs
Payments API
SQL queries
Payments
Audit Log
DMZ - user/web server boundary
Protected data centre - web server/application boundary
Restricted network - app/database boundary
User
HTTPs request
HTTPs response
Web Server
Application
response
Application
calls (do)
Application
call (do)
Application
response
Order
Processor
SQL queries
Users
Audit Log
Inventory
Orders
Data Stores
User data
Auth data
Inventory data

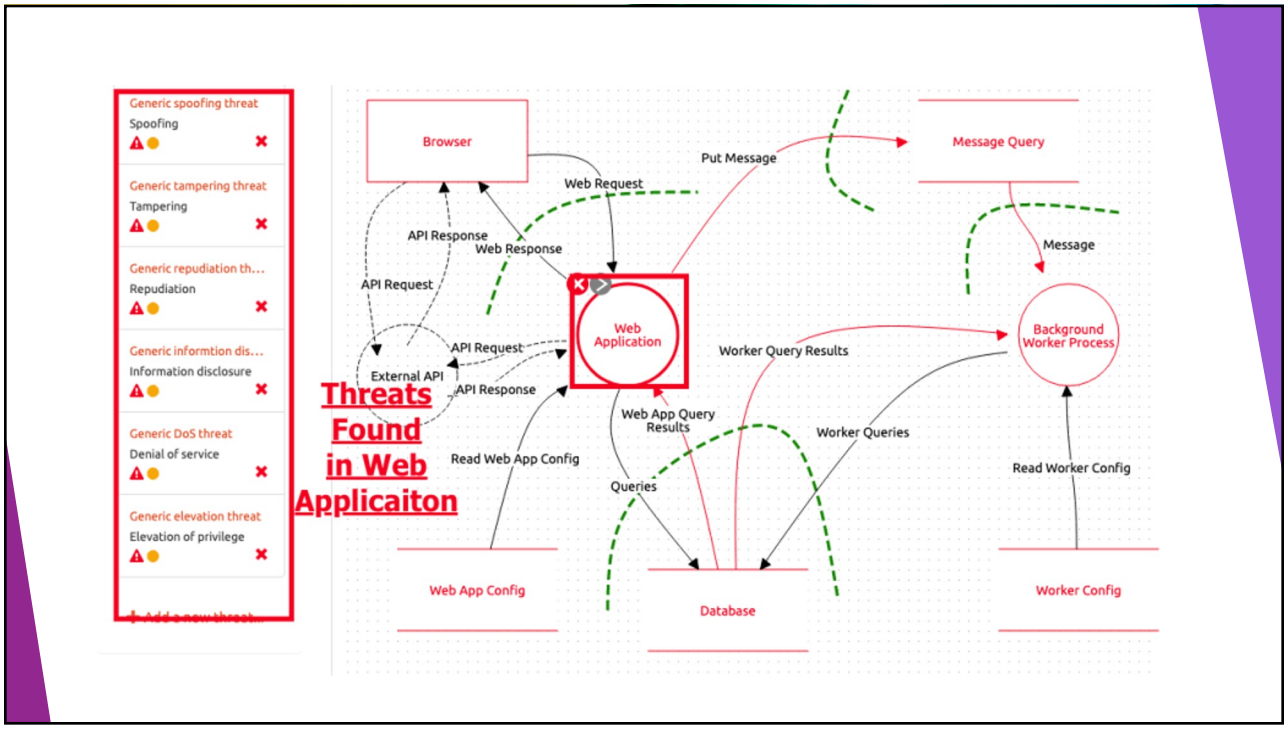
29


Corporate Trust Boundary
Vendor Trust Boundary
Web Application
Web Service
Cloud Storage
HTTPS
JDBC
SQL Database
Human User
Internet Boundary

30


Browser
Message Query
Put Message
Web Request
API Response
Web Response
API Request
Message
Web Application
Background Worker Process
Worker Query Results
API Request
External API
API Response
Web App Query Results
Worker Queries
Read Web App Config
Read Worker Config
Queries
Web App Config
Database
Worker Config

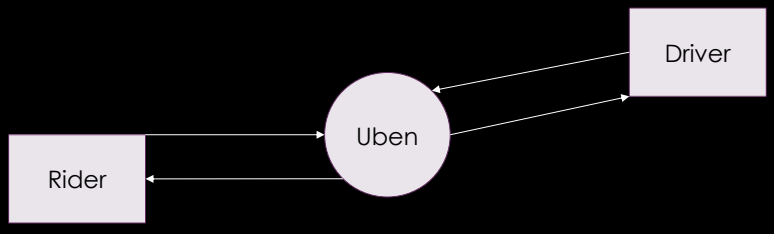
31


Generic spoofing threat
Spoofing
Generic tampering threat
Tampering
Generic repudiation th...
Repudiation
Generic informtion dis...
Information disclosure
Generic DoS threat
Denial of service
Generic elevation threat
Elevation of privilege
Threats Found in Web Applicaiton
Browser
Message Query
Put Message
Web Request
API Response
Web Response
API Request
Message
Web Application
Background Worker Process
Worker Query Results
API Request
External API
API Response
Web App Query Results
Worker Queries
Read Web App Config
Read Worker Config
Queries
Web App Config
Database
Worker Config

32

"RIDE-SHARING APP"

GIVE IT A TRY



33

TAKEAWAYS

- Identify Assets
- Detailed DFD
- Trust Boundaries are Critical
- Are threats enumerated?
  - STRIDE
- Define Done(?)
  - CTM – Continuous Threat Modeling

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 (Foreseeti)

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