OWASP

TM

Gamification of Agile

Threat Modelling

Using OWASP Cornucopia

grant @ securedelivery . io
grant . ongers @ owasp . org
@rewtd

Community Focused

- OWASP Global Board of Directors (https://owasp.org/)
- DEF CON Goon (https://www.defcon.org/)
- BlackHat Staff (USA, EU) (https://www.blackhat.com/)
- BSides Staff (CPT, LND, LAS) (http://www.securitybsides.com/)
- 0xC0FFEE (CPT, LND) (https://twitter.com/0xc0ffeeL)
- DC2721 (https://dc2721.co.za/)

Seen things and done stuff; years of both seeing and doing

- 10+ in Dev (Managed Service Providers, Telecommunications, Banking);
- 20+ in Ops (European Agencies, Utilities Providers); and
- 30+ in Sec (mostly white hat)

Firm believer that there's no such thing as DevSecOps

- it’s “just” DevOps done right.

Co-founder (and CTO) of Secure Delivery (https://securedelivery.io/)

Advancing AppSec

We have deep expertise across product delivery and security in demanding, regulated business environments with global operations

We are closely involved with OWASP, the world's foremost not-for-profit application security organisation, at both global board level and at project level defining the curriculum for application security education in industry and academia

We've distilled our experience into a world-class, predictable programme of capability improvement delivered remotely for organisations at any stage of growth

HSBC

HM Revenue & Customs

rbi reed business information

O2

SECURE DELIVERY

ASSESS | ADVISE | ADVANCE

Improving AppSec

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software through:

150+ projects - covering everything from documentation, code to tools including tools like OWASP Juice Shop, OWASP ZAP, and documentation projects like the OWASP ASVS, SAMM and the Top 10(s)

Community driven 200+ chapters in 50 countries

https://www.meetup.com/owasp

OWASP

(GAMIFICATION OF AGILE)

Threat Modelling

Security work as part of development planning.

THREAT MODELLING

Five second overview: What it is & why do we do it.

NOW AT PACE

The issues with traditional threat modelling and the causes.

CORNUCOPIA

Introducing the game for developers to do TM at pace

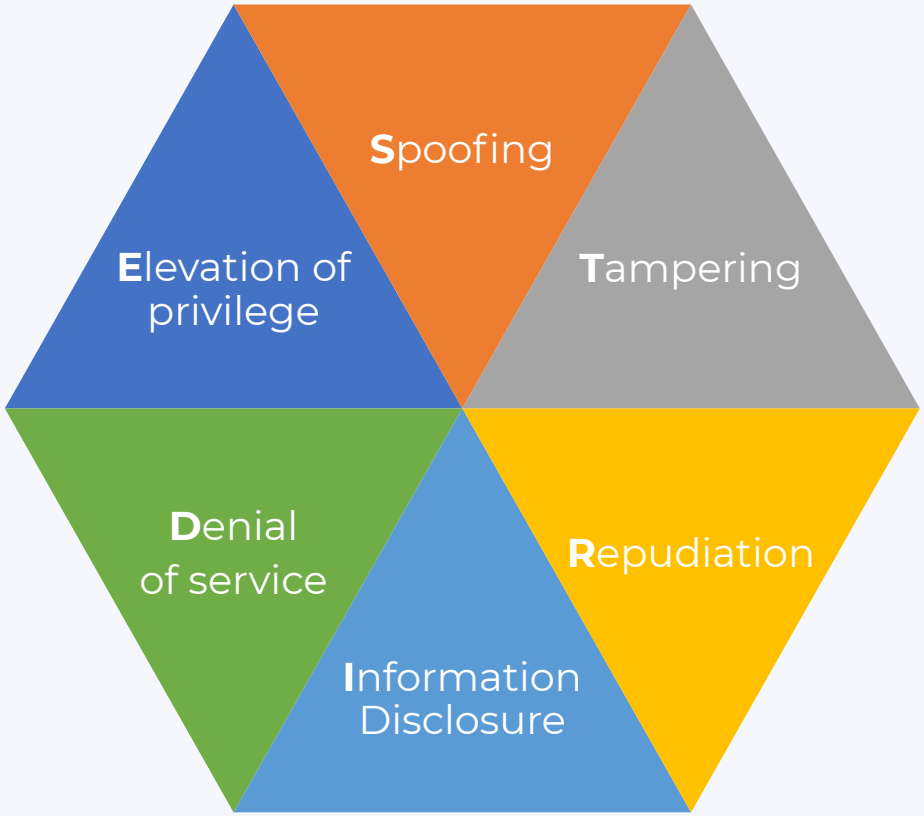
TWEAKING IT

Has this been done? How can you work it to do it with your teams?

THREAT MODELLING USING

STRIDE

The purpose of threat modelling is to understand security possible issues before discovering them in your product. Threat models give you pressure points to focus on There are other methodologies in use (DREAD, Attack Trees, P.A.S.T.A, and VAST for example). DREAD is the most popular, most thorough and the one most experts mostly tell you to mostly use. For the most part.



Spoofing

Pretending to be something other than what you are. The inverse characteristic we want to ensure is **Authenticity**.

Tampering

Modifying or manipulation of data within the application the way to ensure this can happen is testing **Integrity**.

Repudiation

A threat or a design feature? It's a security issue that we may not know who performed what action so **Non-repudiation** is desirable.

Information disclosure

The primary threat of any system that has data of value. The required feature, **Confidentiality**, is part of the core CIA triad.

Denial of service

Another major threat and one often employed against systems. Again the required characteristic is in the triad, **Availability**.

Elevation of privilege

This threat covers being able to do more than you should and at the core of access control, **Authorisation** is the desired state.

LET'S START WITH WHAT IT WAS

WATERFALL

Development methodology that preceded Agile and that is still practised where Agile is not (for whatever reason).

STEP ONE

Gather the requirements of the solution ensuring you don't miss any...

STEP TWO

Design a working solution and ensure that it covers all everything ... security too.

STEP THREE

Build the solution and make sure that during that process we take security seriously.

STEP FOUR

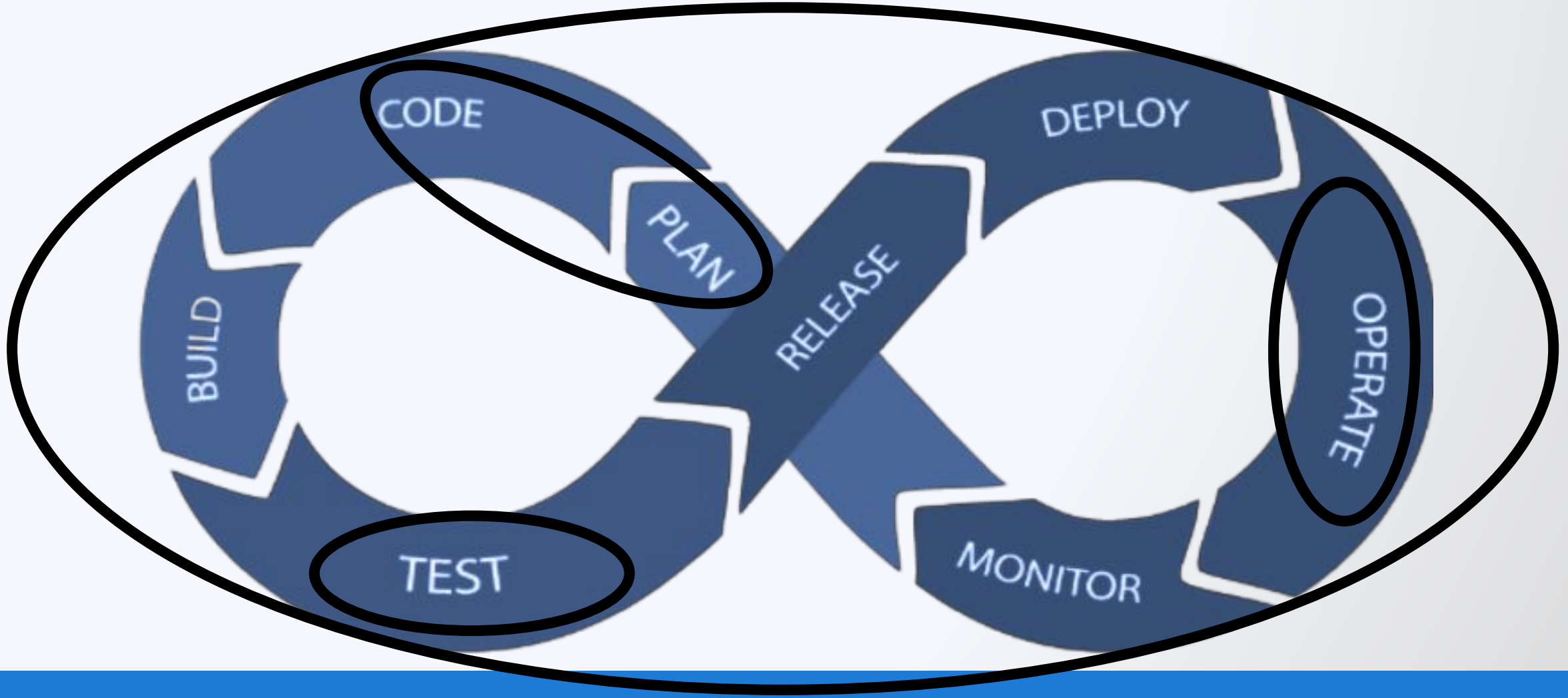
Comprehensively test the solution. That it functionally does as designed ... securely.

STEP FIVE

Deploy the solution. Securely, of course. And hope that it still meets the requirements.

SO WHAT IS IT NOW?

AGILE



THREAT MODELLING + AGILE

DESIGN TIME

TAKES TIME

CHANGES IN TIME

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.

THIS LEADS TO TROUBLE

DESIGN TIME

TAKES TIME

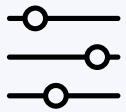
CHANGES IN TIME

MODELLED TOO LATE

Threat modelling is generally done by security professionals. And they are usually invited to look at designs ... completed designs

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.



“Threat modeling: the sooner the better, but never too late.”

Steven Wierckx
Avi Douglen
(OWASP Threat Modelling Project)

THIS LEADS TO TROUBLE

DESIGN TIME

MODELLED TOO LATE

Threat modelling is generally done by security professionals. And they are usually invited to look at designs ... completed designs

TAKES TIME

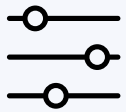
TOO MUCH TIME

Doing threat modelling with a large part of a design leads to a large number of threats being found ... often too many to deal with

CHANGES IN TIME

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.



“… you probably want to find too many threats, rather than too few…”

Adam Shostack

https://adam.shostack.org/blog/2017/08/magical-approaches-to-threat-modeling/

THIS LEADS TO TROUBLE

DESIGN TIME

MODELLED TOO LATE

Threat modelling is generally done by security professionals. And they are usually invited to look at designs ... completed designs

TAKES TIME

TOO MUCH TIME

Doing threat modelling with a large part of a design leads to a large number of threats being found ... often too many to deal with

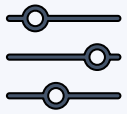
CHANGES IN TIME

INACCURATE MODELS

Upfront designs change as products evolve. If your threat modelling doesn't also evolve then you have nothing at all

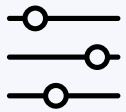
IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.



“All models are wrong, but some models are useful…”

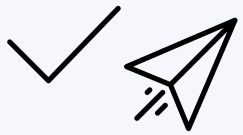
George Box



“… the question is, is the model good enough for this particular application?”

George Box

https://en.wikipedia.org/wiki/All_models_are_wrong/



TO FIX THESE ISSUES THEN

DESIGN TIME

MODELLED TOO LATE

AS EARLY AS POSSIBLE

TAKES TIME

TOO MUCH TIME

USING THE TIME WE HAVE

CHANGES IN TIME

INACCURATE MODELS

GOOD ENOUGH MODEL

IT'S ABOUT TIME: WHEN, AMOUNT & HOW OFTEN

At design time, when the use cases are understood but before building starts. It's in that special point in time that you can design for security. It takes time to do. The larger the piece of design work the more time you need to spend on it. And as we start to build, that's when you realise that more threat modelling needs to be done.

TO FIX THESE ISSUES THEN

DESIGN TIME

MODELLED TOO LATE

AS EARLY AS POSSIBLE

Story Scrubbing
or
Backlog Grooming

TAKES TIME

TOO MUCH TIME

USING THE TIME WE HAVE

This is timeboxed
combined
with NRF & acceptance

CHANGES IN TIME

INACCURATE MODELS

GOOD ENOUGH MODEL

We stop
when we are just about
“close … enough”

Gamification using OWASP Cornucopia

There are a couple of other gamification of Threat Modelling tools out there (for example the Microsoft / OWASP Elevation of Privilege that Adam designed) but there are (in my opinion) none quite as well designed for developers or as well connected as Cornucopia.

The game combines several excellent projects:

- OWASP ASVS
- OWASP SCP
- OWASP AppSensor
- SAFECODE / CAPEC

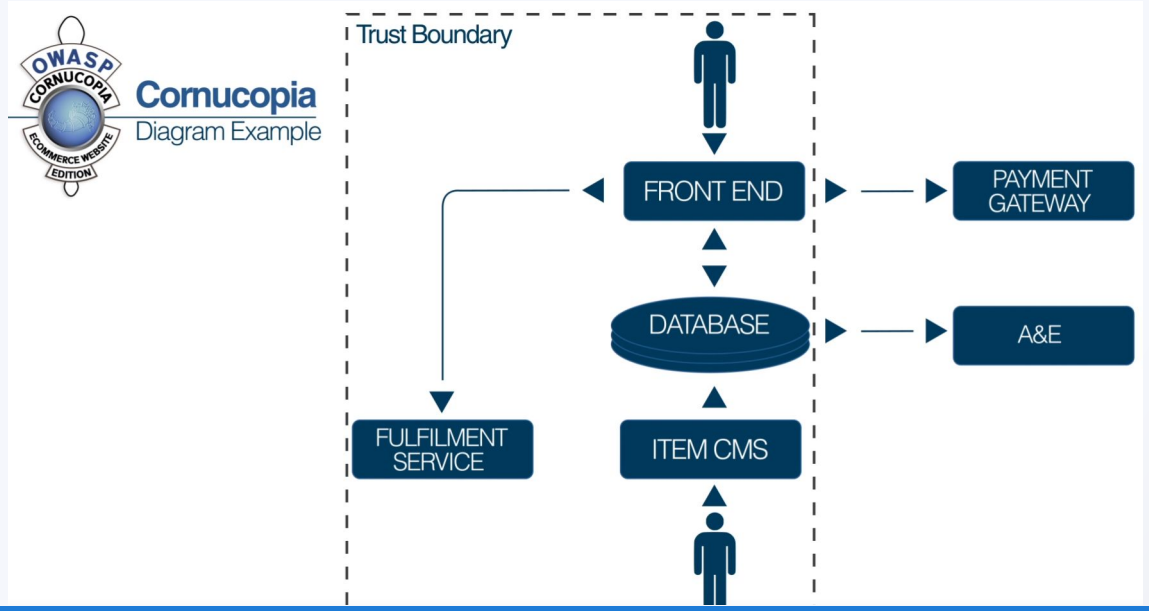
WHAT DO YOU NEED TO START?

Most importantly you need the people building the features to discuss the security impact on and of those features.

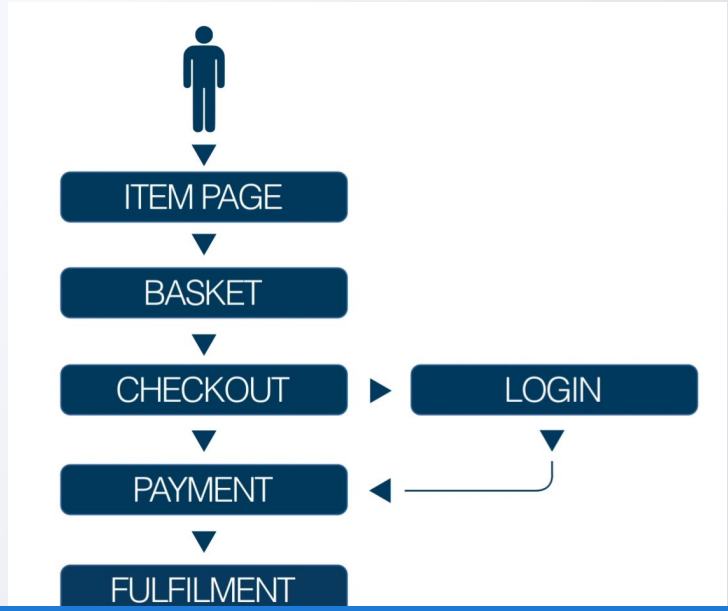
Diagrams that describe the functioning of the application, if available, otherwise draw just what you need. How data flows through that system provides insights into potential attacks.

Architectural designs are valuable to this process. They help us understand the systems in play. But again you can draw the parts involved as you discuss them.

Architectural Designs



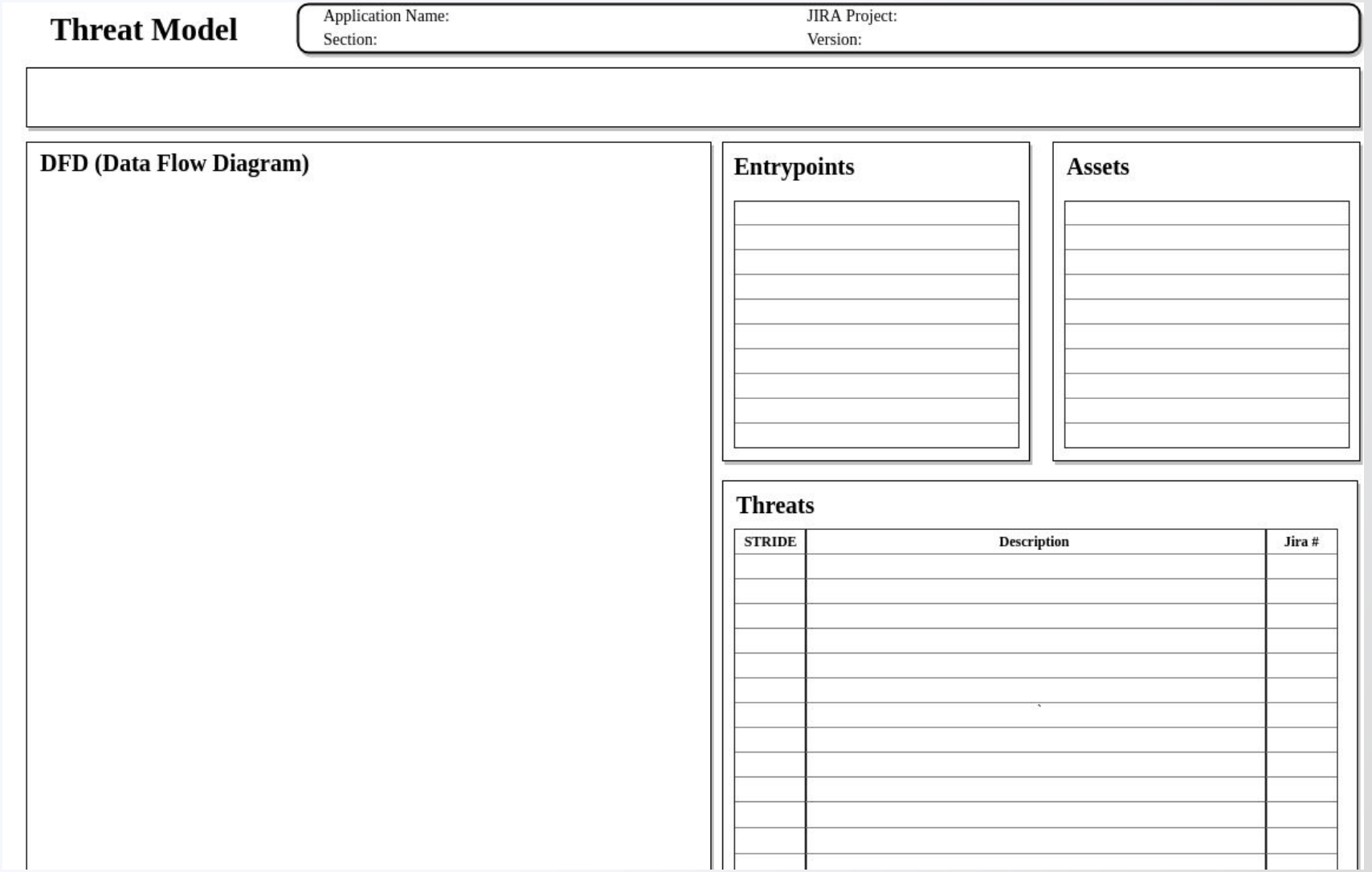
Dataflow Diagrams



WHAT ARE THE OUTPUTS?

Traditional Threat Modelling:

- Threats
- System Insights (what, where)
- Data flows



Threat Model

Application Name: JIRA Project:
Section: Version:

DFD (Data Flow Diagram)

Entrypoints

Assets

Threats

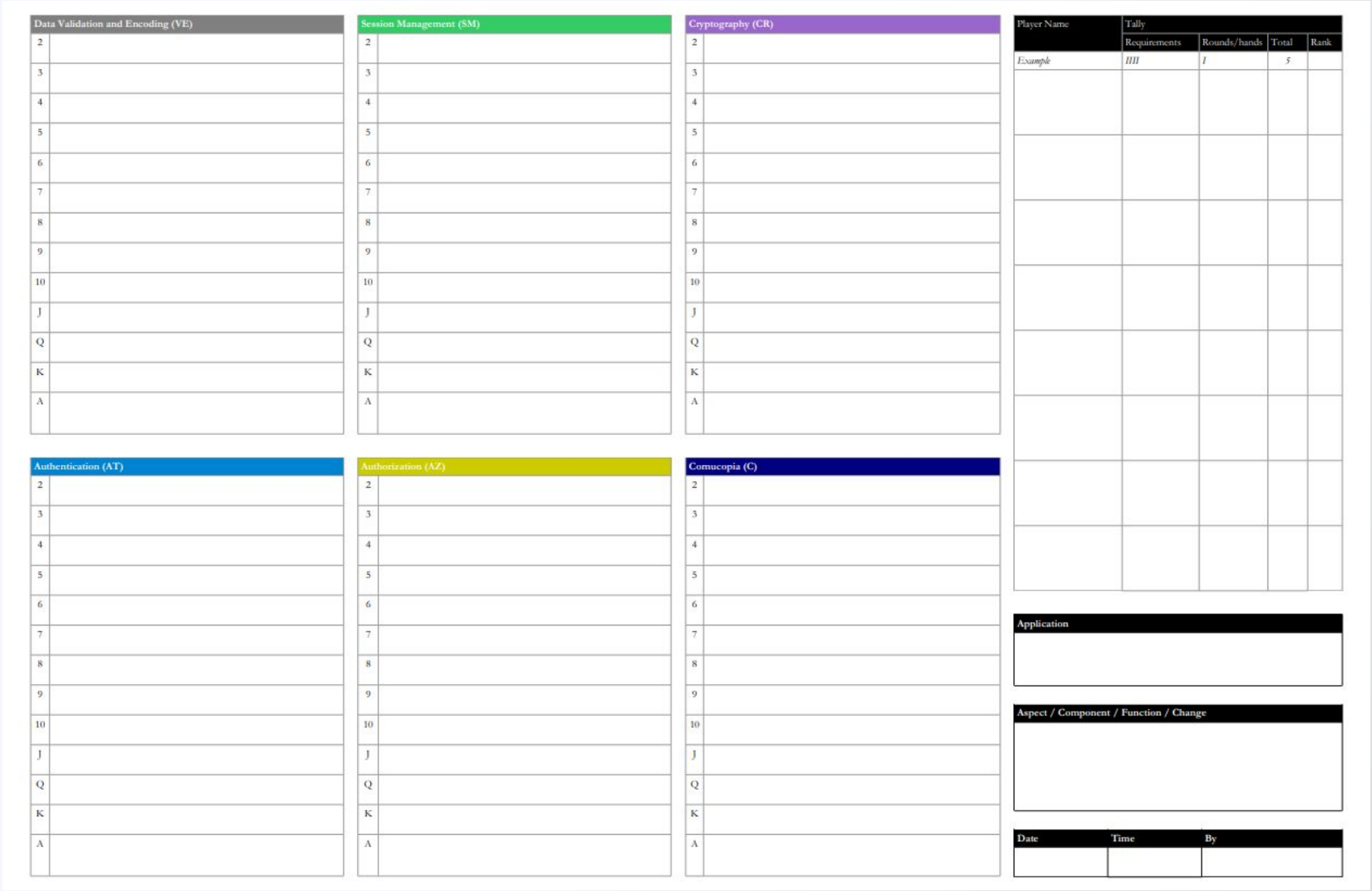
STRIDE	Description	Jira #

OWASP Threat Model Cookbook: https://github.com/OWASP/threat-model-cookbook/blob/master/INDEX.md

WHAT ARE THE ***AGILE*** OUTPUTS?

Agile Threat Modelling:

- Acceptance Criteria for Stories
- Security / story context
- Updated diagrams (perhaps)



Data Validation and Encoding (VE)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Session Management (SM)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Cryptography (CR)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Player Name	Tally			
	Requirements	Rounds/hands	Total	Rank
Example	*IIII*	*1*	*5*	

Application

Aspect / Component / Function / Change

Date	Time	By

Authentication (AT)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Authorization (AZ)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

Cornucopia (C)	
2	
3	
4	
5	
6	
7	
8	
9	
10	
J	
Q	
K	
A	

OWASP Cornucopia Score Sheet: https://wiki.owasp.org/images/6/69/Cornucopia-scoresheet.pdf

WHAT ARE THE ***REAL*** OUTCOMES?

Security:

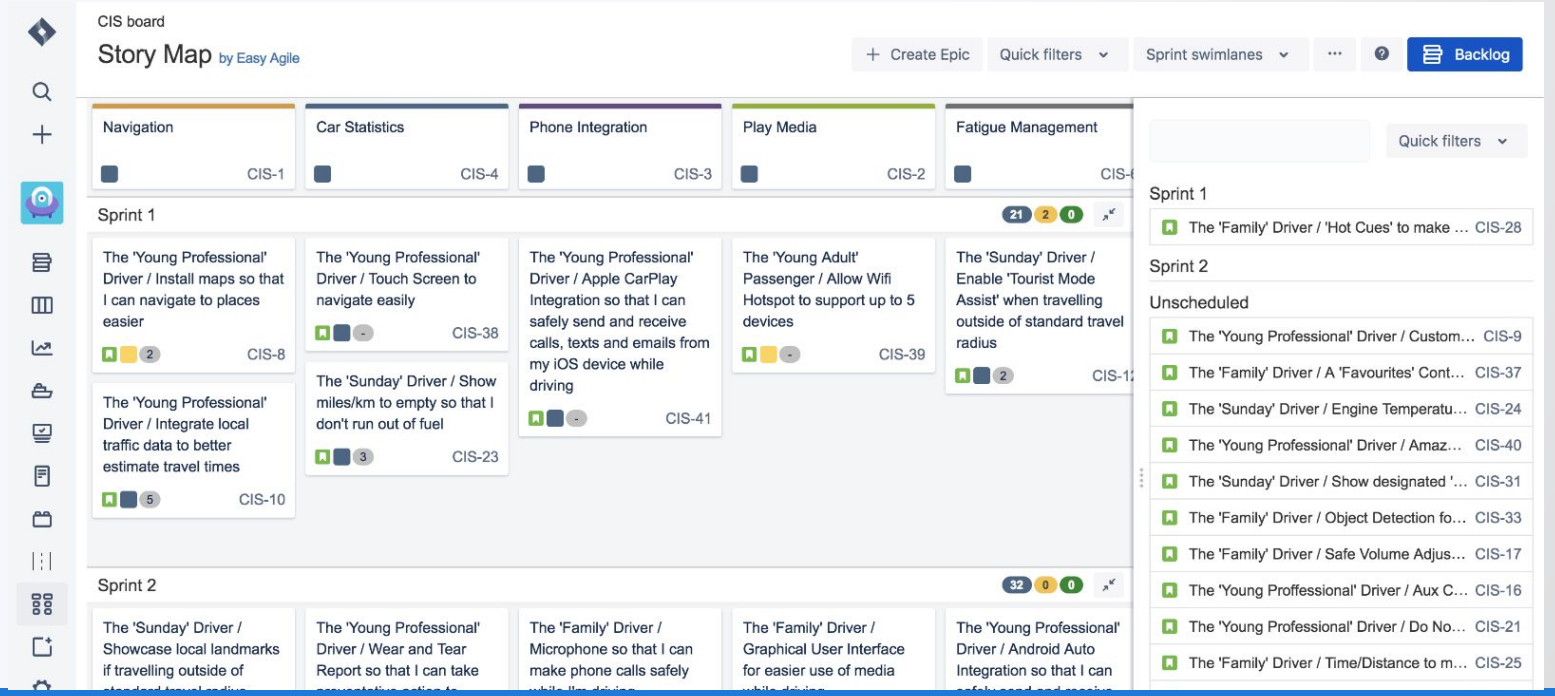
User stories are created from the cards successfully played. Those stories lead to design features or investigations that secure the product when they are implemented.

Compliance:

Doing Threat Modelling is a requirement of many organisation, especially those following SAMM or that are regulated. While Security and Compliance are not the same thing they can be complementary.

Additionally you will find that you see an improvement in general good practices like:

- More accurate design docs;
- Better knowledge sharing; and
- Less hidden tech-debt




OWASP
CORNUCOPIA
ECOMMERCE WEBSITE
EDITION

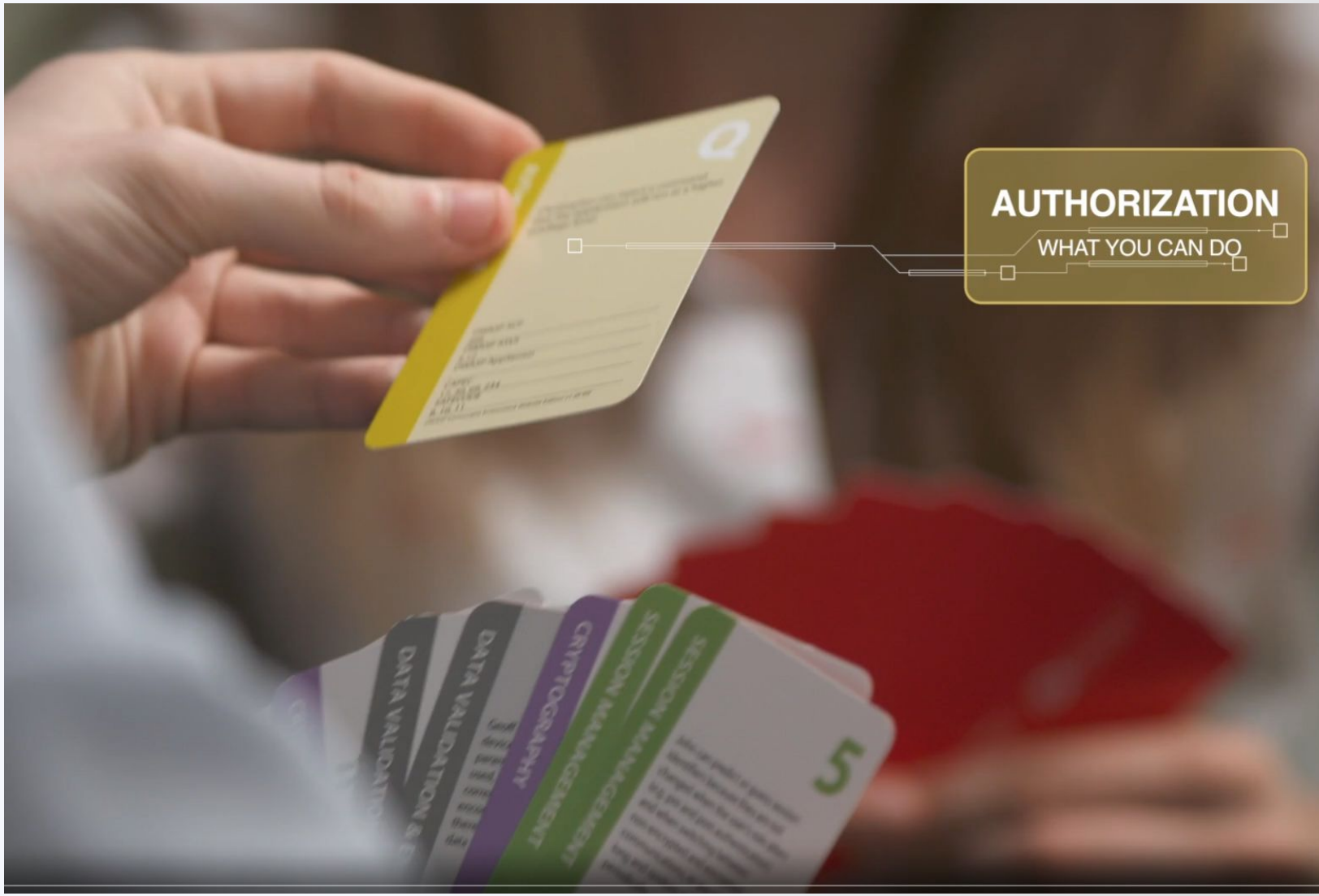
AUTHENTICATION

Verifying you are who who say you are, this is the basis of any auth system and the part that's most often attacked.

SPOOFING / REPUDIATION

AUTHORISATION

Verifying that you can do what you are attempting to do, this covers the realm of privilege escalation discussed earlier.



ELEVATION OF PRIVILEGE

SESSION MGT

Checking the previous two happens regularly. Not every moment, not every action but often enough. The balance being all important.

DENIAL OF SERVICE

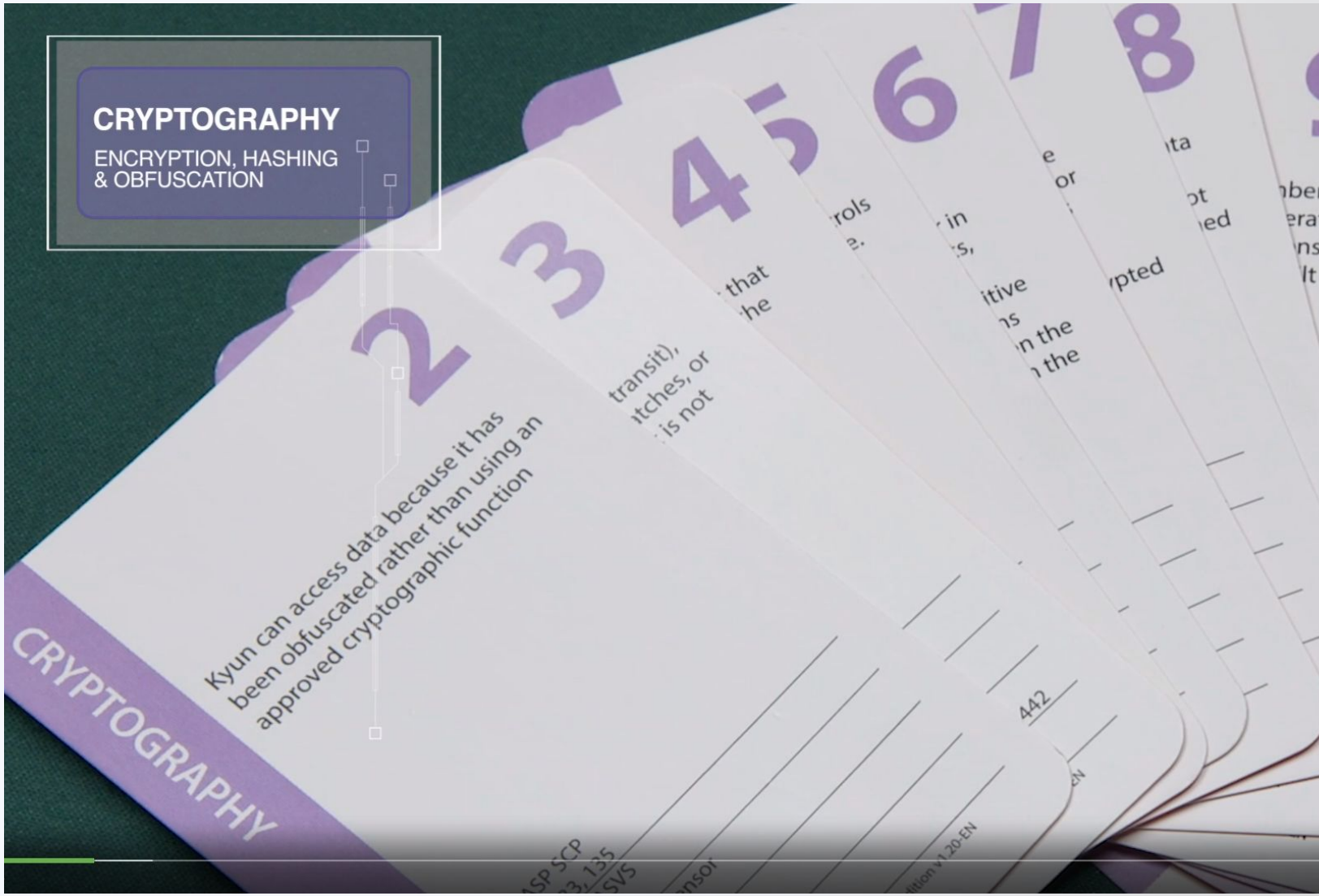
DATA VALIDATION

Validating inputs and encoding outputs. This basic hygiene when it comes to allowing users to interface with your application.

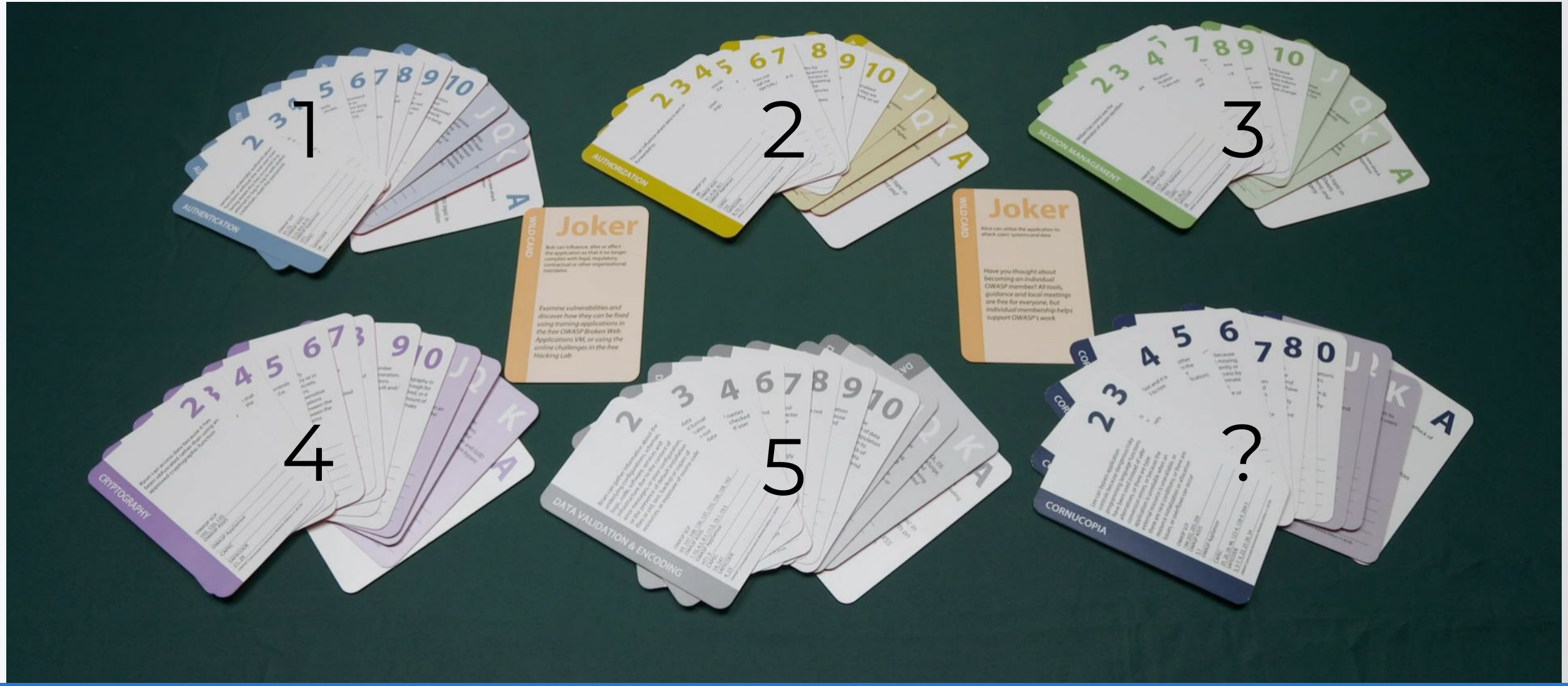
TAMPERING

CRYPTOGRAPHY

Whether this is encryption, or hashing. Whether it's on the wire, or on disk, this is about protecting secrets.



INFORMATION DISCLOSURE


1
2
3
4
5
?
Joker
Joker
AUTHENTICATION
AUTHORIZATION
SESSION MANAGEMENT
CRYPTOGRAPHY
DATA VALIDATION & ENCODING
CORNUCOPIA

CORNUCOPIA

The trump suite that contains all of the general nasties you can imagine.

ALL OF THE THINGS

HOW TO PLAY

THE GAME

The game is a simple one to play. Each of the suites consists of cards with faces from the standard deck: 2 through ten and Jack, Queen, King and Ace. Aces are high and each card describes an attack.

1

PRE-SORT

Sometimes you only want some cards from the deck

2

DEAL

All the cards, to all the players equally

3

PLAY

Look at the app, look at your hand. Select a card

4

DESCRIBE

Using the tools Cornucopia provides, describe the attack

5

CONVINCE

Your fellow players may not be convinced by your play

6

SCORE

1 point for a valid attack, 1 for the highest valid card played

7

FOLLOW SUIT

The next player follows the suit played originally

8

AWARD

Winner has the most points, there should be a prize

9

FOLLOW UP

Each valid item should be noted and added to the backlog

RBI

RBI (Reed Business Information) is a division of RELX (Reed, Elsevier, Lexisnexis, and Reed eXhibitions) which is a FTSE #10 company who have customers in more than 198 countries and offices in about 50 cities, and employs over 15,000 people.

SCALE

15,000

Employees and 1,500 developers. Building products for 7 markets

COMPLEX

HARD PROBLEMS

Massive data sets, hugely time sensitive, critical in nature and requiring complex calculations.

REGULATED

FS-ISAC

Building software for banking puts RBI in the domain of the FS-ISAC (Financial Services Information Sharing and Analysis Center).

AGILE

MOVING FAST

Building software to meet the customer's ever growing requirements.

K E Y O U T P U T S

WHY DO WE DO THIS

What advantages does Cornucopia have for customers that implement it over other methods:

close	smart	effective	addictive
DEVELOPERS DO IT	EDUCATIONAL	THINGS GET SEEN AND FIXED	BECOMES NATURAL

“… Cornucopia empowers … (engineers) to move fast more securely”

Jeff Jenkins
(CISO at Reed Business Information)

HOW DO WE MAKE IT WORK?

USE THE DECKS

Physical decks are awesome, table-top gaming is great when it is real. Not always doable but there are options.

CHANGE UP THE GAME

Not all features hit all the five (six) areas. Use the parts that make sense for the features you are building. Not all features need you to work them through this. Not all features need threat modelling...

USE THE SYSTEMS YOU HAVE AVAILABLE

We live in a world where gaming together may not be a thing for a while. It can still work. Make it work

https://agilestationery.co.uk/
https://croupier.agilestationery.co.uk/

QUESTIONS?

SECURE DELIVERY

ASSESS | ADVISE | ADVANCE

grant @ securedelivery . io
grant . ongers @ owasp . org
@rewtd

LINKS

RBI Video Walk-Through:
https://youtu.be/BZVoQurTEMc

Adam's 20 Years of STRIDE article:
https://www.darkreading.com/20-years-of-stride-looking-back-looking-forward/a/d-id/1334275

OWASP Cheatsheets
https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

OWASP Threat Modelling Cookbook
https://owasp.org/www-project-threat-model-cookbook/

Agile Stationary's Croupier / Cards:
https://croupier.agilestationery.co.uk/
https://agilestationery.co.uk/products/owasp-cornucopia-card-deck-ecommerce-website-edition
use code (OWASP20)