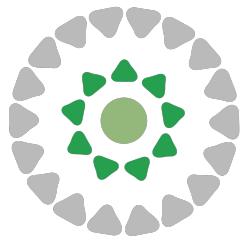


ThoughtWorks[®]



Sensible Conversations about Security

Lessons learned encouraging security thinking in software development teams

Motivation



OBJECTIVE

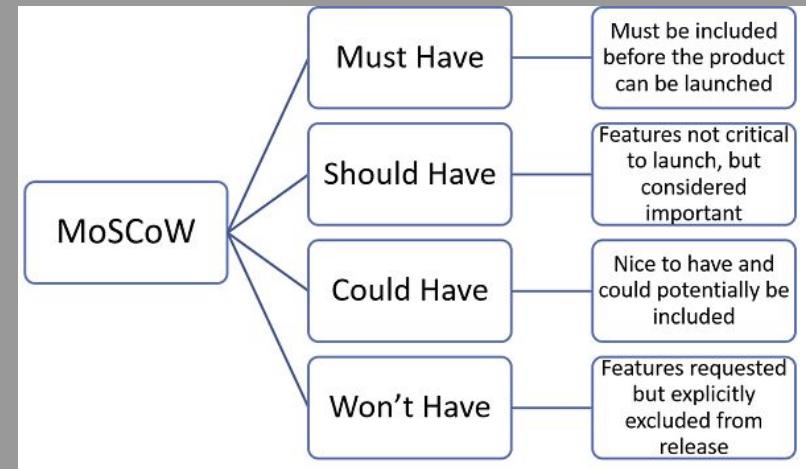
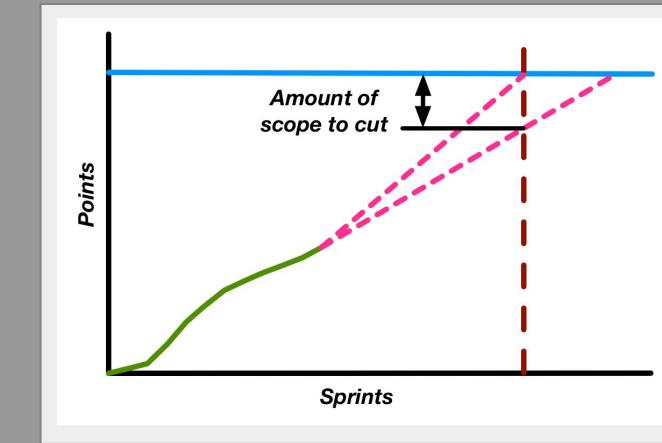
We need software teams
to 'build security
in'





OBJECTIVE

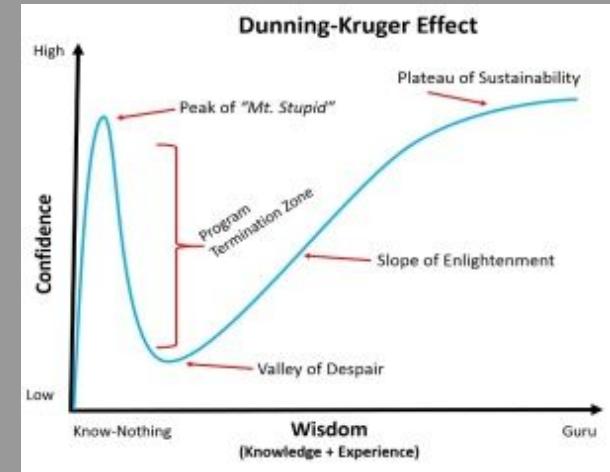
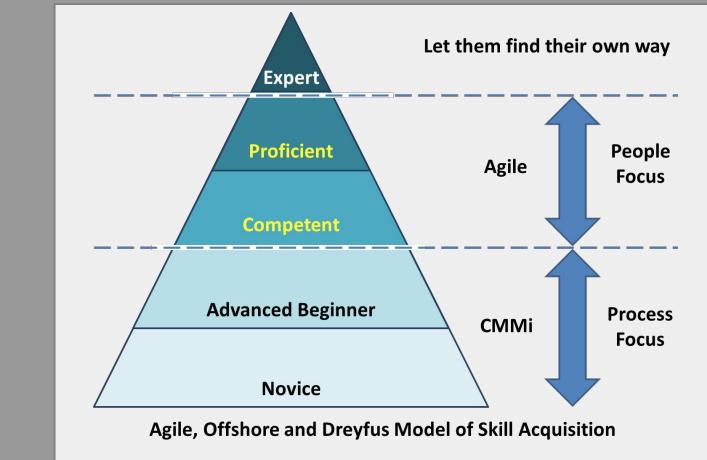
We need to prioritise the highest value security work





OBJECTIVE

We need to build security awareness and capability in every role in the delivery team

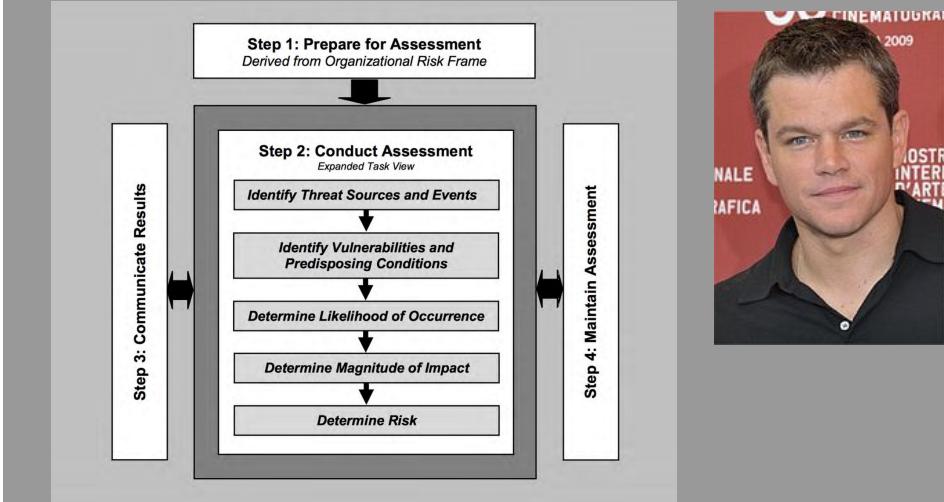




OBJECTIVE

Threat modelling
and risk
assessment are
complicated,
specialised and
hard!

A more comprehensive application threat modeling process might also include a preliminary risk analysis of the application, the threat agents, the threat libraries used to identify likelihood and impacts to the assets, attack tree analysis of the different channels and assets that can be attacked, correlation of threats to existing vulnerabilities identified in the application, determination of technical and business risk, determination of security measures and prioritization of these based on a risk strategy whose objective is to maximize protection by minimizing cost to the business.



- **Asset:** What we're trying to protect.
- **Actor:** Who we're protecting an asset from.
- **Threat:** What we're trying to protect an asset from.
- **Vulnerability:** Weakness or gap in our protection efforts.
- **Exploit:** Vulnerability that has been triggered by a threat.
- **Risk:** Event at the intersection of assets, threats, and vulnerabilities.
- **Vector:** How an actor is getting to the asset.
- **Payload:** What an actor is getting to the asset with.



GOAL

To make threat
modelling simple





WORKSHOP

Sensible Conversations Objectives

Gather cross functional group and share understanding of:

- What needs protecting and why
- What the real threats are
- What and where there might be technical exposure

In order to prioritise most valuable next steps



Step 1

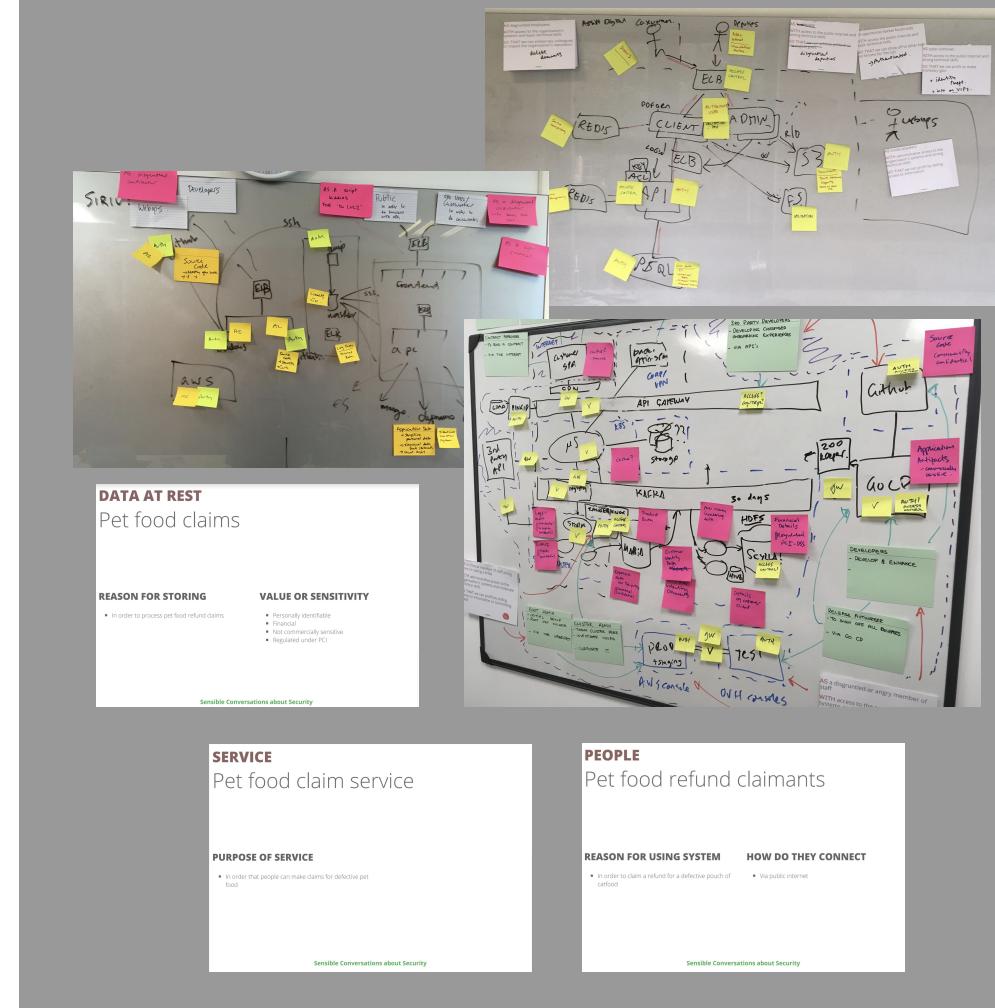
Gather cross functional group: delivery team, stakeholders, folks from security team





Step 2

Use component architecture diagram and 'asset' cards to identify scope





Step 3

Using threat cards as cues, explore impact and likelihood of threats and prioritise 3 for further discussion

Headline for high level 'threat'

THREAT
A cyber criminal or hacktivist group mount a denial of service attack on the system

LIKELIHOOD

- Could an attacker demand a ransom were your system unavailable?
- Is it in the interest of any group to impact your reputation by taking your system down?
- Are there knock on effect on third parties or clients which an attack could benefit from?

IMPACT

- What is the impact on revenue or operations if the system is down?
- How long can the system be down until it really hurt? 3 min? 1 hour? 1 week?

Sensible Conversations about Security

Questions for group discussion to help judge impact of threat

Questions for group discussion to help judge likelihood of threat

THREAT: Cyber criminal, hacktivist or nation state group try to steal data from the system

LIKELIHOOD

- Is it in the interest of any group to impact your reputation by taking your system down?
- Are there knock on effect on third parties or clients which an attack could benefit from?

IMPACT

- What is the impact on revenue or operations if the system is down?
- How long can the system be down until it really hurt? 3 min? 1 hour? 1 week?

THREAT: A developer or admin makes an error in configuring or securing the system

LIKELIHOOD

- Could an attacker demand a ransom were your system unavailable?
- Are there knock on effect on third parties or clients which an attack could benefit from?

IMPACT

- What is the impact on revenue or operations if the system is down?
- How long can the system be down until it really hurt? 3 min? 1 hour? 1 week?

THREAT: An internal user tries to access sensitive information out of curiosity

LIKELIHOOD

- Is it in the interest of any group to impact your reputation by taking your system down?
- Are there knock on effect on third parties or clients which an attack could benefit from?

IMPACT

- What is the impact on revenue or operations if the system is down?
- How long can the system be down until it really hurt? 3 min? 1 hour? 1 week?



Step 4

Have a nice break :)





Step 5

Mark areas of focus on technical architecture, based on threat 'playbook'





Step 6
Split into smaller groups and use exposure cards to explore areas to improve

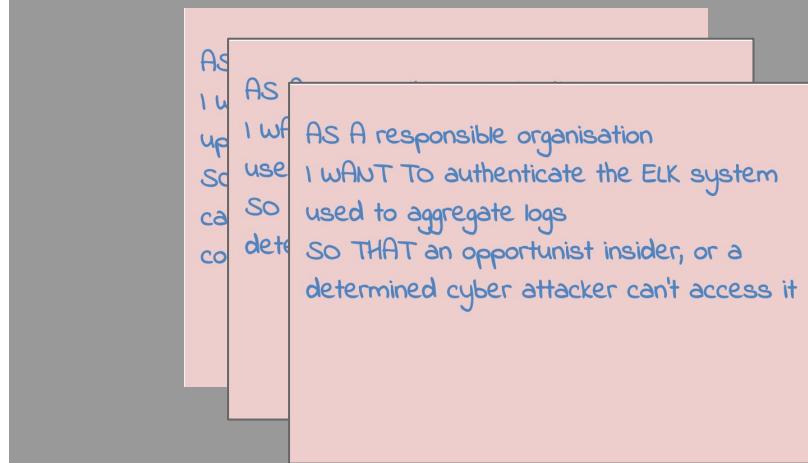
EXPOSURE	
Access to data or services	
FOR ASSET:	
VULNERABILITY	EXPOSURE?
Lack of access control, i.e. any form of authentication	<input type="checkbox"/>
Use of shared accounts and credentials	<input type="checkbox"/>
Reliance on a single factor for authentication	<input type="checkbox"/>
Failure to configure access controls	<input type="checkbox"/>
Lack of identity or entitlement management	<input type="checkbox"/>
Weakness in offline password storage	<input type="checkbox"/>
Lack of audit log showing access attempts	<input type="checkbox"/>
Lack access control to assets	<input type="checkbox"/>
Lack of awareness material	<input type="checkbox"/>
EXPOSURE	
Support for GDPR subject access rights	
FOR ASSET:	
VULNERABILITY	EXPOSURE?
Lack of means to purge personal data for a data subject in response to request	<input type="checkbox"/>
Lack of means to correct personal data	<input type="checkbox"/>
Lack of features to package personal data	<input type="checkbox"/>
Lack of data retention policy for personal data	<input type="checkbox"/>
Personal data is being stored indefinitely	<input type="checkbox"/>
EXPOSURE	
Server-side web implementation	
FOR ASSET:	
VULNERABILITY	EXPOSURE?
Fails to prevent stored or reflected Cross Site Scripting (XSS)	<input type="checkbox"/>
File upload feature fails to block malware	<input type="checkbox"/>
Fails to prevent SQL, XML, (XXE) or LDAP injection	<input type="checkbox"/>
Fails to prevent shell injection	<input type="checkbox"/>
Fails to prevent open redirects	<input type="checkbox"/>
Fails to prevent Cross-site request forgery (CSRF)	<input type="checkbox"/>
It is possible for attacker to tamper with cookies	<input type="checkbox"/>
Framework support for mass binding can be exploited	<input type="checkbox"/>
Alternate character encodings can be used to circumvent protections	<input type="checkbox"/>
User forms can be completed in a scripted manner	<input type="checkbox"/>
Lack of rate limiting allows 'scraping' or 'spidering' of valuable data	<input type="checkbox"/>
URL paths can be manipulated to access system files or load remote files	<input type="checkbox"/>
URL paths can be manipulated to access unauthorised resources	<input type="checkbox"/>
Developers have disabled framework security protections	<input type="checkbox"/>
Application is sensitive to application layer denial of service	<input type="checkbox"/>
Triggering an exception leaks unnecessary information that can assist attacker	<input type="checkbox"/>





Step 7

Playback findings and agree 3 valuable next steps. Wrap up



Delivery team outcomes from threat modelling

What outcomes are we trying to effect within the delivery team?

CONFIDENCE

ACTION

INSIGHT

AWARENESS

4. Team able to continuously identify and deliver highest value defensive work

3. Team are working on the high value defensive building work

2. Team start to see where they have exposure and what needs improvement

1. Team aware what they are protecting, from what and what defenses they have

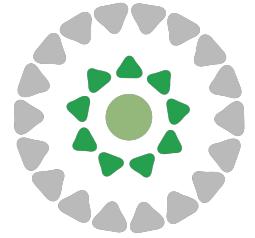
Continuous practice



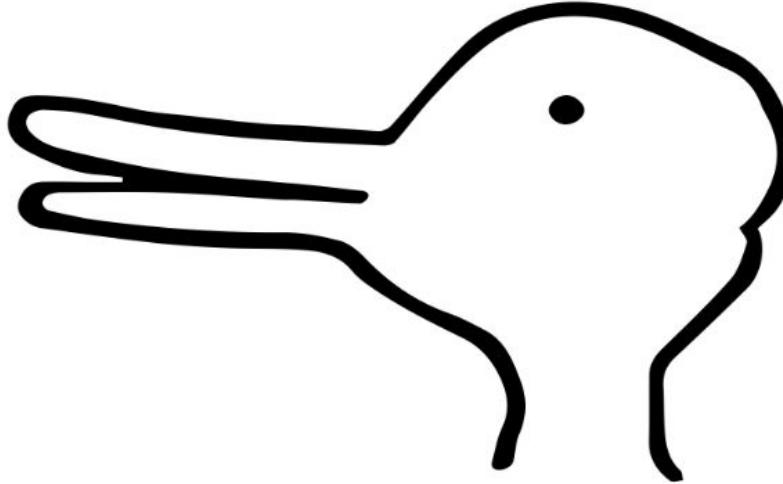
Next steps

Summary and conclusions

- Valuable security next steps discovered every time!
- Great way to connect security teams and delivery teams
- Still refining and simplifying approach
- 'Train the trainer' model for other facilitators
- Open source the materials!
- Want more feedback! Keep in growing approach



Jim Gumbley
@jgumbley 



Thanks!

THOUGHT BEHIND SENSIBLE CONVERSATIONS

What was some of the thinking which motivated the work?

