accu
2022

THE HIP APPROACH TO SAFEGUARDING YOUR USERS

CHARLES WEIR

PETRAS

Safeguarding

- Safeguarding?
- Thinking up what could go wrong
- Where to start?
- How do we go about fixing it?
- How to get the effort and money required?

What Security- Examples?

WhatsApp

Phoenix Project

A Novel About IT, DevOps, and Helping Your Business Win

REVISED WITH NEW RESOURCE GUIDE

Gene Kim, Kevin Behr, and George Spafford

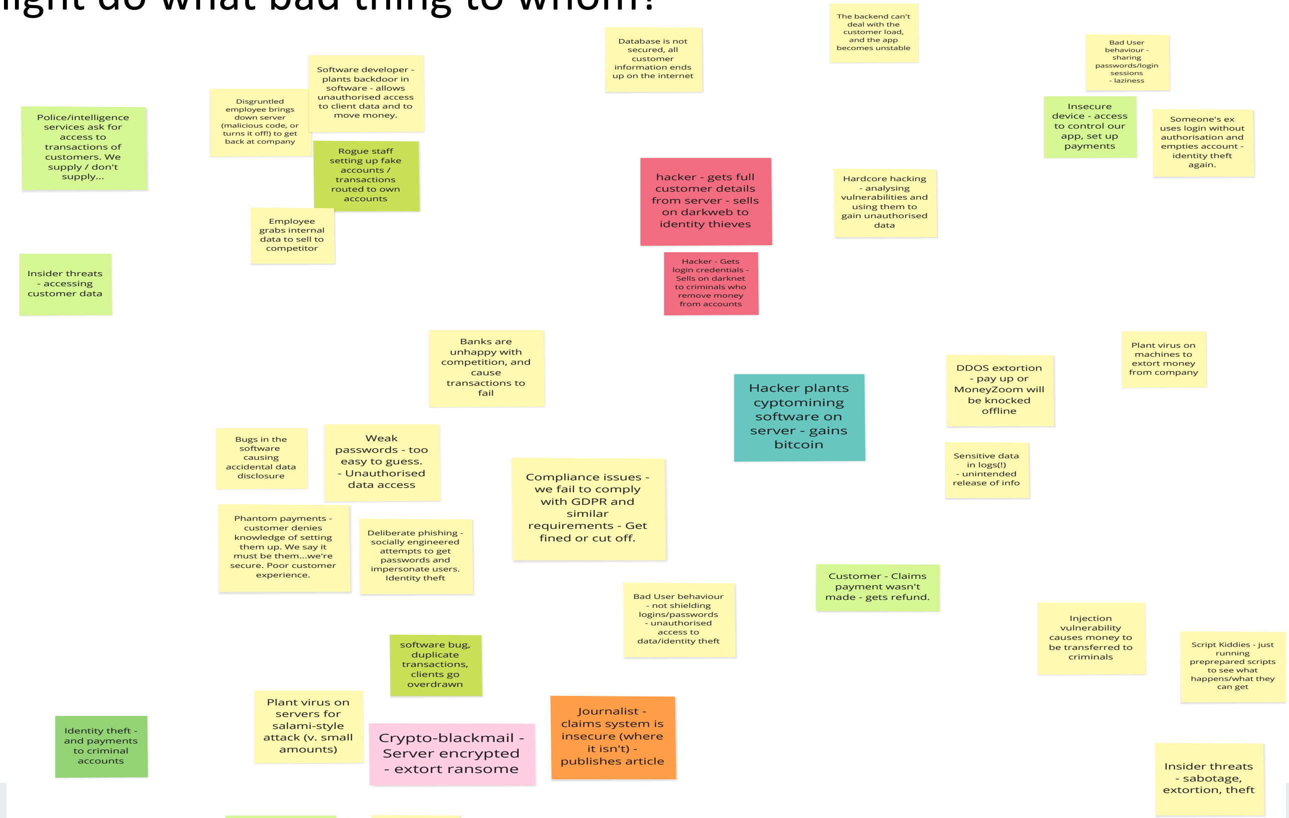
What could possibly go wrong?

One Solution – Workshops

C.f. Training from the back of the room - Sharon Bowman

Threat assessment…

Who might do what bad thing to whom?



Police/intelligence services ask for access to transactions of customers. We supply / don't supply…

Insider threats - accessing customer data

Disgruntled employee brings down server (malicious code, or turns it off!) to get back at company

Software developer - plants backdoor in software - allows unauthorised access to client data and to move money.

Rogue staff setting up fake accounts / transactions routed to own accounts

Employee grabs internal data to sell to competitor

Database is not secured, all customer information ends up on the internet

hacker - gets full customer details from server - sells on darkweb to identity thieves

Hacker - Gets login credentials - Sells on darknet to criminals who remove money from accounts

The backend can't deal with the customer load, and the app becomes unstable

Hardcore hacking - analysing vulnerabilities and using them to gain unauthorised data

Bad User behaviour - sharing passwords/login sessions - laziness

Insecure device - access to control our app, set up payments

Someone's ex uses login without authorisation and empties account - identity theft again.

Banks are unhappy with competition, and cause transactions to fail

Hacker plants cyptomining software on server - gains bitcoin

DDOS extortion - pay up or MoneyZoom will be knocked offline

Plant virus on machines to extort money from company

Sensitive data in logs(!) - unintended release of info

Bugs in the software causing accidental data disclosure

Weak passwords - too easy to guess. - Unauthorised data access

Compliance issues - we fail to comply with GDPR and similar requirements - Get fined or cut off.

Phantom payments - customer denies knowledge of setting them up. We say it must be them...we're secure. Poor customer experience.

Deliberate phishing - socially engineered attempts to get passwords and impersonate users. Identity theft

Bad User behaviour - not shielding logins/passwords - unauthorised access to data/identity theft

Customer - Claims payment wasn't made - gets refund.

Injection vulnerability causes money to be transferred to criminals

Script Kiddies - just running preprepared scripts to see what happens/what they can get

software bug, duplicate transactions, clients go overdrawn

Identity theft - and payments to criminal accounts

Plant virus on servers for salami-style attack (v. small amounts)

Crypto-blackmail - Server encrypted - extort ransome

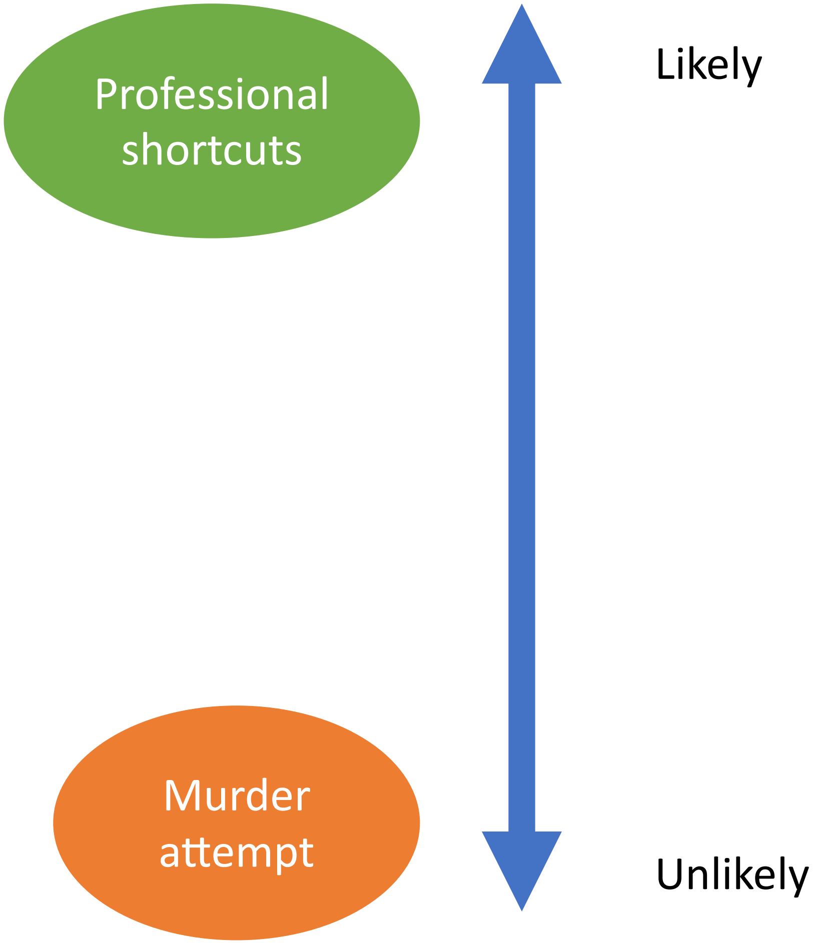
Journalist - claims system is insecure (where it isn't) - publishes article

Insider threats - sabotage, extortion, theft

Where do we start?

Risk-Impact Grid

	Low Impact	Medium Impact	High Impact
Likely	Bad User behaviour - not shielding logins/passwords - unauthorised access to data/identity theft Customer - Claims payment wasn't made - gets refund. Sensitive data in logs(!) - unintended release of info		Bugs in the software causing accidental data disclosure Weak passwords - too easy to guess. - Unauthorised data access Compliance issues - we fail to comply with GDPR and similar requirements - Get fined or cut off. Phantom payments - customer denies knowledge of setting them up. We say it must be them...we're secure. Poor customer experience. Deliberate phishing - socially engineered attempts to get passwords and impersonate users. Identity theft
Fairly unlikely		Injection vulnerability causes money to be transferred to criminals Script Kiddies - just running preprepared scripts to see what happens/what they can get Identity theft - and payments to criminal accounts	software bug, duplicate transactions, clients go overdrawn Plant virus on servers for salami-style attack (v. small amounts) Crypto-blackmail - Server encrypted - extort ransome Journalist - claims system is insecure (where it isn't) - publishes article
Unlikely		Insider threats - sabotage, extortion, theft	Our server hosts fail for 24 hours. Inaccessibility to data/funds. Accidental release - someone leaves a USB with usernames & passwords on the train



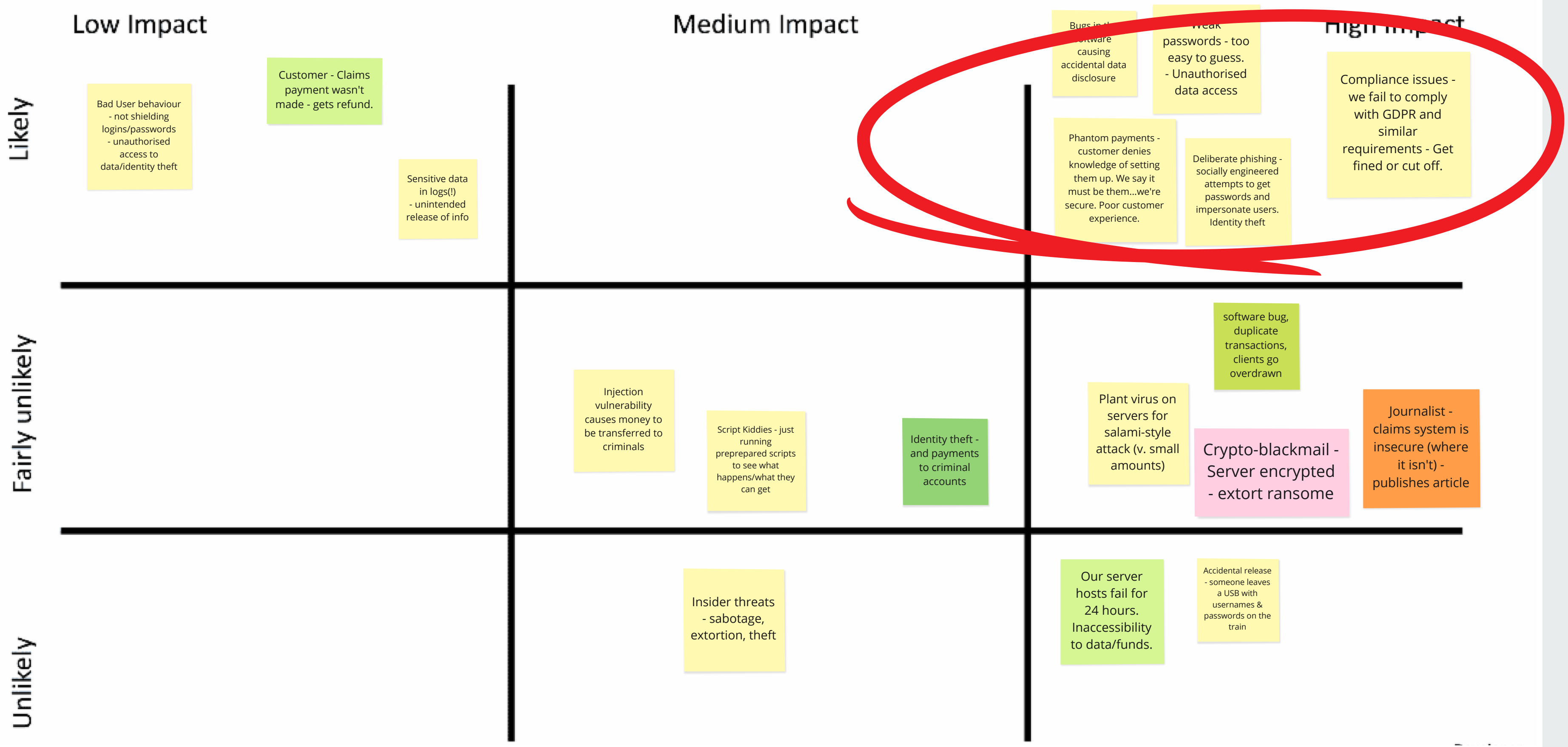
Professional shortcuts

Likely

Murder attempt

Unlikely

Risk-Impact Grid



	Low Impact	Medium Impact	High Impact
Likely	Bad User behaviour - not shielding logins/passwords - unauthorised access to data/identity theft Customer - Claims payment wasn't made - gets refund. Sensitive data in logs(!) - unintended release of info		Bugs in the software causing accidental data disclosure Weak passwords - too easy to guess. - Unauthorised data access Compliance issues - we fail to comply with GDPR and similar requirements - Get fined or cut off. Phantom payments - customer denies knowledge of setting them up. We say it must be them...we're secure. Poor customer experience. Deliberate phishing - socially engineered attempts to get passwords and impersonate users. Identity theft
Fairly unlikely		Injection vulnerability causes money to be transferred to criminals Script Kiddies - just running preprepared scripts to see what happens/what they can get Identity theft - and payments to criminal accounts	software bug, duplicate transactions, clients go overdrawn Plant virus on servers for salami-style attack (v. small amounts) Crypto-blackmail - Server encrypted - extort ransome Journalist - claims system is insecure (where it isn't) - publishes article
Unlikely		Insider threats - sabotage, extortion, theft	Our server hosts fail for 24 hours. Inaccessibility to data/funds. Accidental release - someone leaves a USB with usernames & passwords on the train

How do we go about fixing things?

Functionality changes and fixes

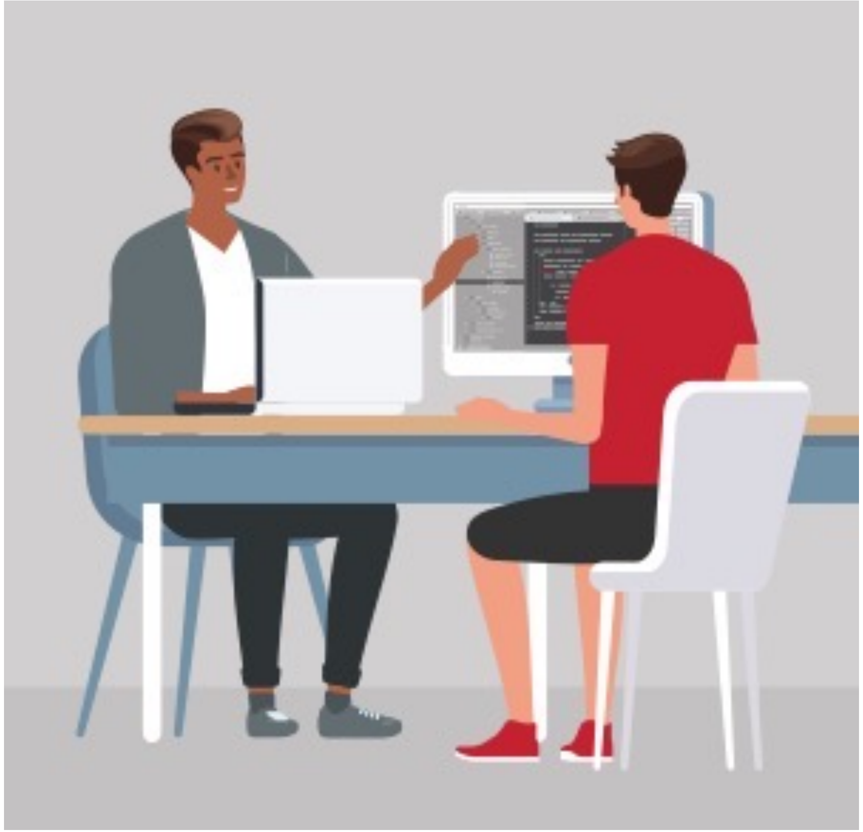
Configuration Review

Choosing secure components and frameworks, and keeping them up to date

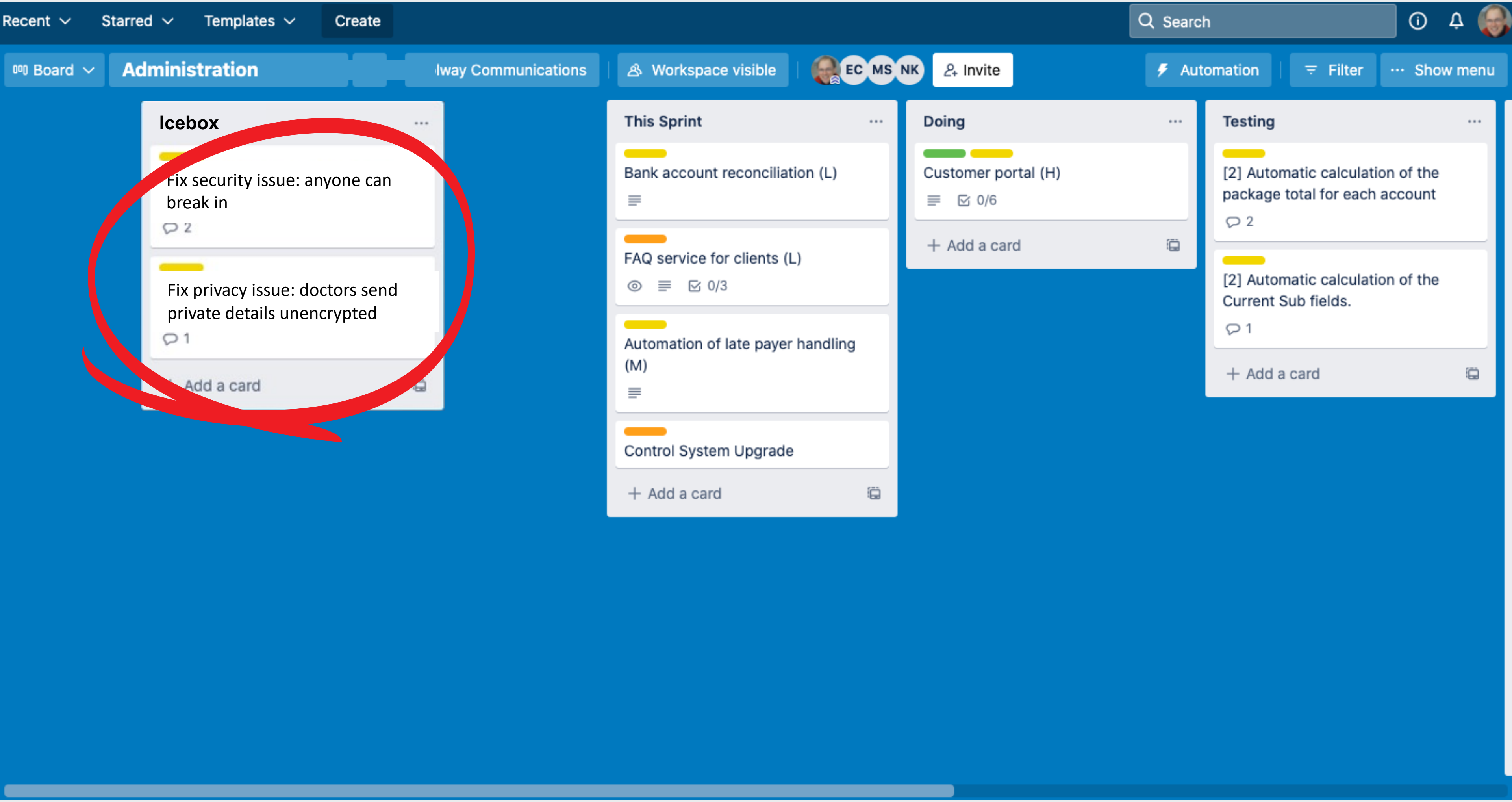
Automated Static Analysis

Code Review

- Scheduled meetings, pull requests, or pair programming to analyse code for security defects



How to get the effort and money allocated?



Icebox

- Fix security issue: anyone can break in — 2
- Fix privacy issue: doctors send private details unencrypted — 1

This Sprint

- Bank account reconciliation (L)
- FAQ service for clients (L) — 0/3
- Automation of late payer handling (M)
- Control System Upgrade

Doing

- Customer portal (H) — 0/6

Testing

- [2] Automatic calculation of the package total for each account — 2
- [2] Automatic calculation of the Current Sub fields. — 1

How product owners think:

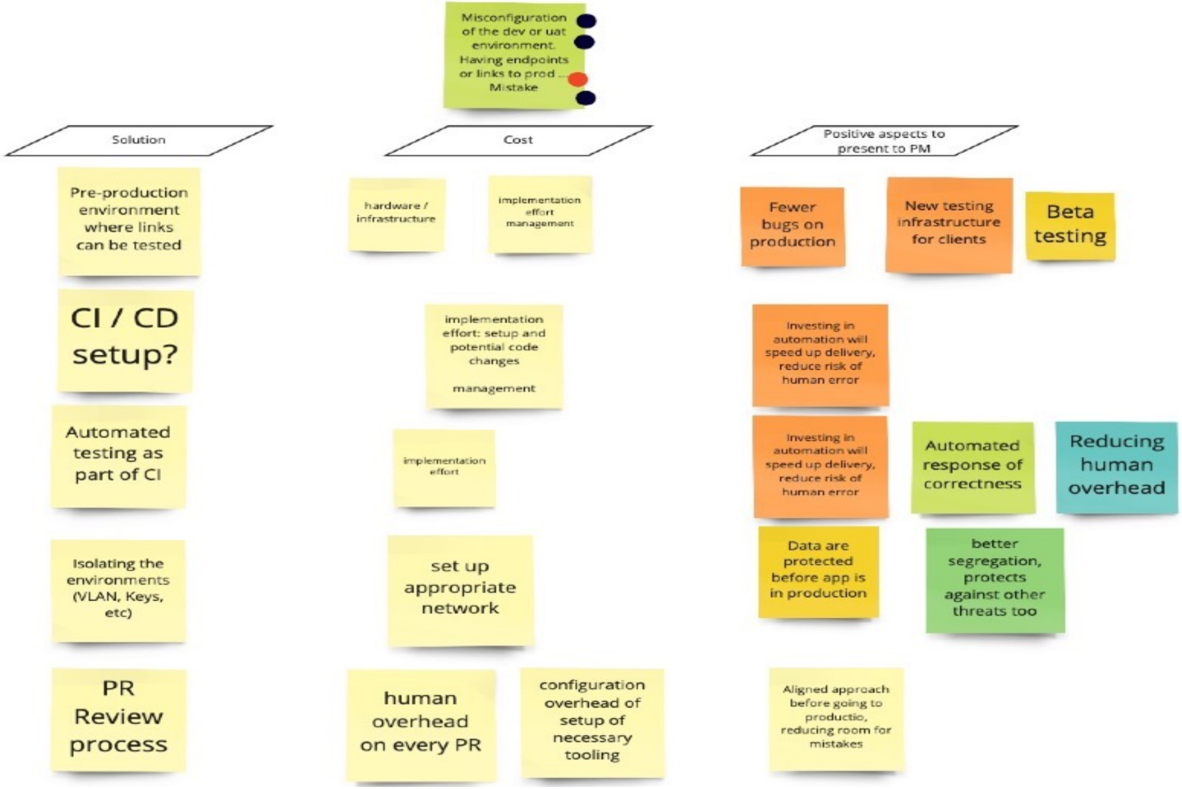
DESIRABILITY
somebody wants
this
FEASIBILITY
we can create
this
PROFITABILITY
they'll pay enough for
thi$$$$

Image © Richard Blandfield
https://medium.com/@freshtilledsoil/how-to-prioritize-product-features-and-improvements-8aea72c8bf27

	Desirability	Feasibility	Profitability
	somebody wants this	we can create this	they'll pay enough for thi$$$$
Security needs us to update many components	✗	✓	✗
We offer up-to-date industry-standard security…	✓	✓	✓

	Desirability	Feasibility	Profitability
	somebody wants this	we can create this	they'll pay enough for thi$$$$
Some customers need more effort on security…	✗	✓	✗
We offer Gold, Silver or Bronze security…	✓	✓	✓✓

Yes, Developers Can…



Misconfiguration of the dev or uat environment. Having endpoints or links to prod ... Mistake

Solution

Pre-production environment where links can be tested

CI / CD setup?

Automated testing as part of CI

Isolating the environments (VLAN, Keys, etc)

PR Review process

Cost

hardware / infrastructure

implementation effort management

implementation effort: setup and potential code changes

management

implementation effort

set up appropriate network

human overhead on every PR

configuration overhead of setup of necessary tooling

Positive aspects to present to PM

Fewer bugs on production

New testing infrastructure for clients

Beta testing

Investing in automation will speed up delivery, reduce risk of human error

Investing in automation will speed up delivery, reduce risk of human error

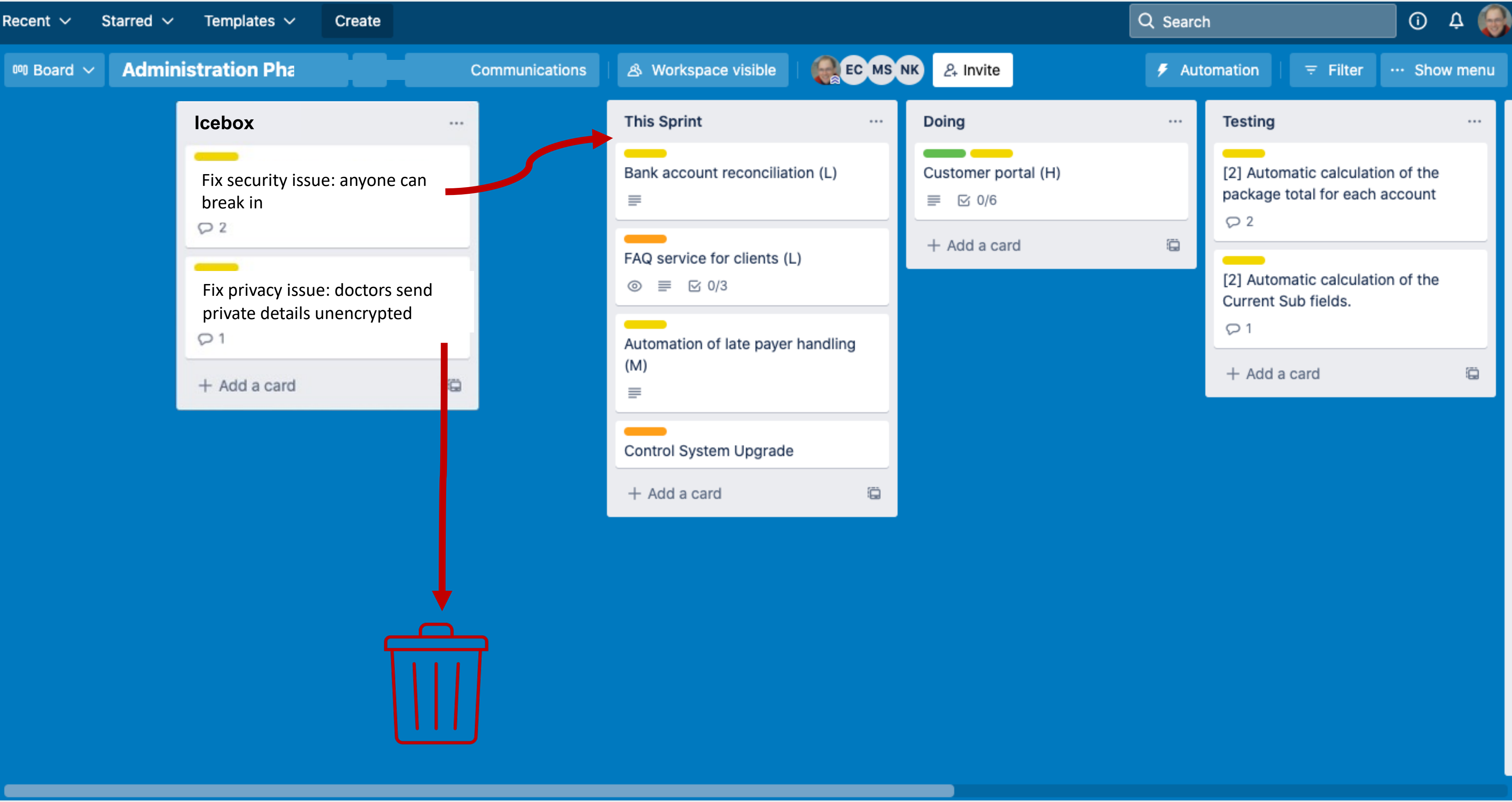
Automated response of correctness

Reducing human overhead

Data are protected before app is in production

better segregation, protects against other threats too

Aligned approach before going to productio, reducing room for mistakes



Icebox

- Fix security issue: anyone can break in — 2
- Fix privacy issue: doctors send private details unencrypted — 1

+ Add a card

This Sprint

- Bank account reconciliation (L)
- FAQ service for clients (L) — 0/3
- Automation of late payer handling (M)
- Control System Upgrade

+ Add a card

Doing

- Customer portal (H) — 0/6

+ Add a card

Testing

- [2] Automatic calculation of the package total for each account — 2
- [2] Automatic calculation of the Current Sub fields. — 1

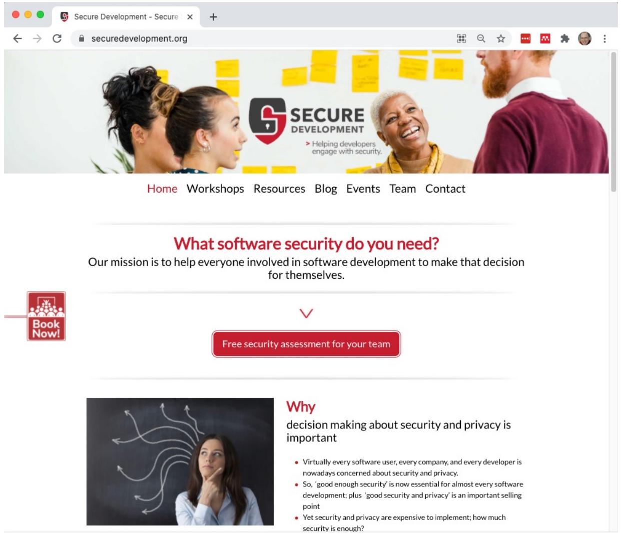
+ Add a card

Safeguarding

- Safeguarding?
- Thinking up what could go wrong
- Where to start?
- How do we go about fixing it?
- How to get the effort and money required?

Next steps

- Free! Hipster: Health IoT device support https://lancaster.ac.uk/hipster
- Free! Team security survey
- Free! Workshop materials to find the answers for your own projects.
- https://securedevelopment.org



Secure Development - Secure
securedevelopment.org
SECURE DEVELOPMENT
> Helping developers engage with security.
Home
Workshops
Resources
Blog
Events
Team
Contact
Book Now!
Free security assessment for your team

What software security do you need?

Our mission is to help everyone involved in software development to make that decision for themselves.

Why

decision making about security and privacy is important

- Virtually every software user, every company, and every developer is nowadays concerned about security and privacy.
- So, 'good enough security' is now essential for almost every software development; plus 'good security and privacy' is an important selling point
- Yet security and privacy are expensive to implement; how much security is enough?