APISEC
Secure APIs for fintech companies

DistriNet

AGENTSCHAP INNOVEREN & ONDERNEMEN

TSUNDOKU VENTURES

API Security Afternoon! #learn #share #meet

AGENDA

12:00	Welcome & lunch
13:00	Introduction
13:15	API Security Architecture (Philippe De Ryck)
14:00	– break –
14:15	Peer learning: share insights from your use cases (all)
14:45	Using the OAuch tool (Pieter Philippaerts)
15:15	– break –
15:30	Offensive API Security (Philippe De Ryck)
16:10	Closing remarks and next steps
16:30	Networking drink
17:30	End

Introduction

COOCK: “Secure APIs for fintech companies”

- “Collectief Onderzoek en Ontwikkeling en Collectieve Kennisdeling”
- Why we started this project? Why fintech?
  - With the uptake of the API Economy, it became clear that APIs were quickly gaining in importance, and their security was often very weak
  - There is a big systemic “ripple effect” risk in API vulnerabilities
  - The first big and very hyped use case was Payment Services Directive 2 (PSD2)
  - “*Regulation aiming to increase pan-European competition and participation in the payments industry also from non-banks, and to provide for a level playing field by harmonizing consumer protection and the rights and obligations for payment providers and users.*”
    Frontrunners, early adopters: APIs security is non-negotiable in this use case.

PSD2… well, it's complicated

Learning from the Failure of the EU Payment Services Directive (PSD2): When Imposed Innovation Does Not Change the Status Quo

Amir Bahman Radnejad
State University of New York, Brockport

Oleksiy Osiyevskyy
University of Calgary

Olivia Scheibel
Technical University of Munich

Corporate Innovation/Opinion/

Dear banks: this is why you're still losing out to fintechs

Covid changed everything about banking, but the big banks still haven't noticed

BY LEON GAUHMAN AND ALESSANDRO HATAMI
TUESDAY 23 NOVEMBER 2021

Covid-19 reshaped how customers interact with their banks forever — but has anyone told the banks? At recent banking innovation events including Money 2020 and the Paris Fintech Forum, we found banks still focused mainly on improving the present, not creating the future. Like a carriages conference in 1895, everyone was thinking about making the horses faster and not how to use cars.

PSD2 and open banking dangled the prospect of increased consumer choice, improved service and greater control over finances. Yet despite glossy ads promising banks are "By Your Side" and "Making Money Work for You", the banking sector still hasn't stepped up to the challenge of solving customer problems in a way that is genuinely customer focused.

The banking sector's survival pivots on flawless customer experience while also holding on tight to the relationships

Starling CEO says open banking a flop: Other fintech chiefs beg to differ

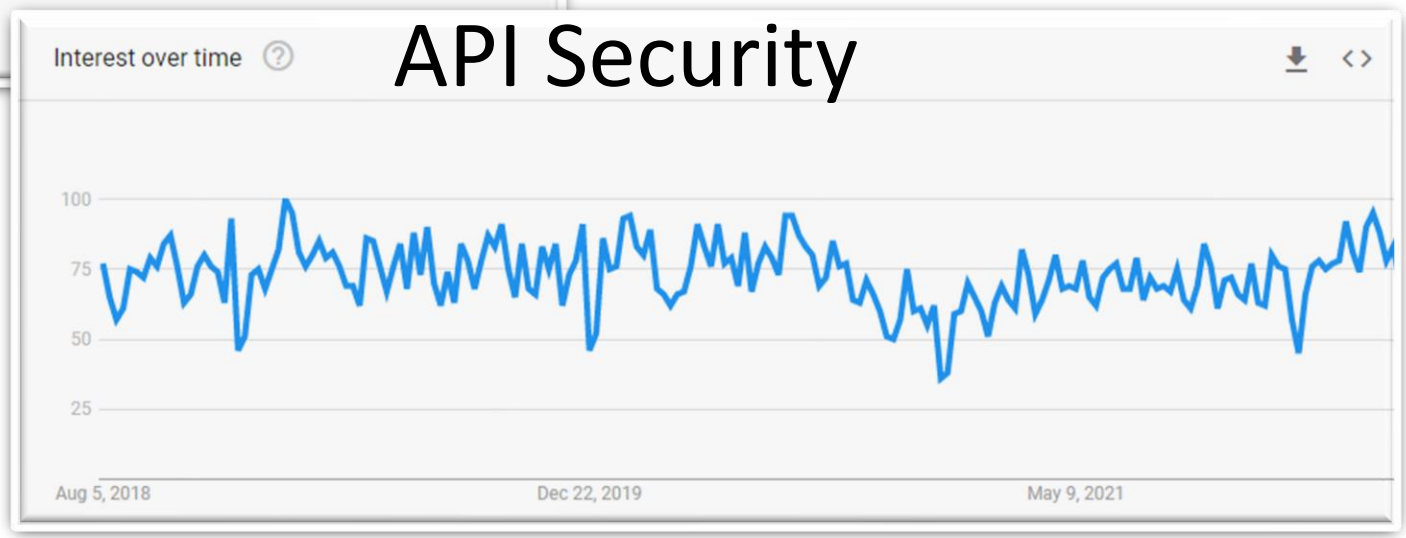
By Eric Johansson

DistriNet

AGENTSCHAP INNOVEREN & ONDERNEMEN

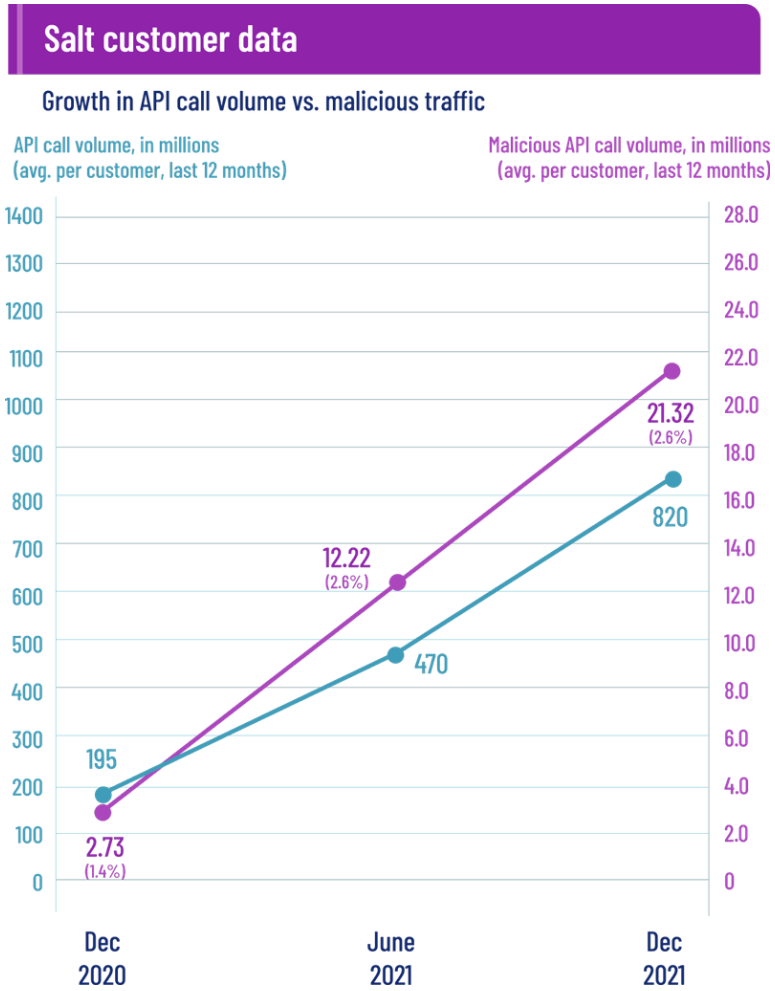
TSUNDOKU VENTURES

PSD2 went, API Security stayed



(Google trends)

Sharp increase of API attacks



(State of API Security report 2022, Salt)

API attacks rose 681% in the last year (2021), compared to a 321% increase in overall API traffic

Sharp increase of API attacks

95% of respondents suffered an API security incident in 2021

(State of API Security report 2022, Salt)

Sharp increase of API attacks

Lack of expertise is the #1 obstacle for companies to properly secure their APIs

(State of API Security report 2022, Salt)

Conclusions

The initial business driver of our project (PSD2) has faded a bit, although still very relevant for fintech companies

The use of APIs has exploded (Gartner predict every company will become an API consumer)

API Security is becoming ever more important as attacks surge at a much higher pace than API adoption

Sharing knowledge and expertise is the #1 enabler for safer API adoption in companies

Conclusions

By jointly researching best practices and new frameworks and tools, and collectively sharing insights and experience, we're tackling the #1 reason why companies suffer API security incidents and breaches.

#APISEC

API Security Afternoon! #learn #share #meet

AGENDA

12:00	Welcome & lunch
13:00	Introduction
13:15	**API Security Architecture (Philippe De Ryck)**
14:00	– break –
14:15	Peer learning: share insights from your use cases (all)
14:45	Using the OAuch tool (Pieter Philippaerts)
15:15	– break –
15:30	Offensive API Security (Philippe De Ryck)
16:10	Closing remarks and next steps
16:30	Networking drink
17:30	End

DistriNet

AGENTSCHAP INNOVEREN & ONDERNEMEN

TSUNDOKU VENTURES

API Security Afternoon! #learn #share #meet

AGENDA

12:00	Welcome & lunch
13:00	Introduction
13:15	API Security Architecture (Philippe De Ryck)
14:00	– break –
14:15	**Peer learning: share insights from your use cases (all)**
14:45	Using the OAuch tool (Pieter Philippaerts)
15:15	– break –
15:30	Offensive API Security (Philippe De Ryck)
16:10	Closing remarks and next steps
16:30	Networking drink
17:30	End

Peer learning: share insights from your use cases

GOAL: to share an insight, a tip or an experience regarding your own use case that can help others

FLOW: every COOCK participant, one at a time, 30 minutes total

1. Briefly mention the **topic** from the COOCK you have focused most on
2. Share something you learned during implementation, something practical, something useful, **share an insight** you wish you would have learned sooner.
3. Mention one topic or **question** that you still struggle with or would like to discuss with one of your peers.
4. AUDIENCE: if this topic is something you can help with, shout your name

API Security Afternoon! #learn #share #meet

AGENDA

12:00	Welcome & lunch
13:00	Introduction
13:15	API Security Architecture (Philippe De Ryck)
14:00	– break –
14:15	Peer learning: share insights from your use cases (all)
14:45	**Using the OAuch tool (Pieter Philippaerts)**
15:15	– break –
15:30	Offensive API Security (Philippe De Ryck)
16:10	Closing remarks and next steps
16:30	Networking drink
17:30	End

DistriNet

AGENTSCHAP INNOVEREN & ONDERNEMEN

TSUNDOKU VENTURES

API Security Afternoon! #learn #share #meet

AGENDA

12:00	Welcome & lunch
13:00	Introduction
13:15	API Security Architecture (Philippe De Ryck)
14:00	– break –
14:15	Peer learning: share insights from your use cases (all)
14:45	Using the OAuch tool (Pieter Philippaerts)
15:15	– break –
15:30	Offensive API Security (Philippe De Ryck)
16:10	**Closing remarks and next steps**
16:30	Networking drink
17:30	End

Closing remarks

As a result of this COOCK project, so far:

- Participants were able to **learn about state-of-the-art API Security** techniques and best practices, and learn from each other;
- Participants were able to make very important architectural and technology choices, much quicker, better, **reducing their time to market**;
- Participants were able to move *upmarket* quicker due to their much increased internal cybersecurity maturity, which helped to **increase the TRUST and RESILIENCE of their companies**;
- We were able to create **re-usable knowledge, demonstrators**, which will remain online and publicly available for a broad audience.

Closing remarks

What we've focussed on:

- Common API vulnerabilities, OWASP, PoV from a hacker;
- API architecture best practices, authentication flows;
- Oauth 2.0, OpenID Connect, the OAuch tool;
- Typical vulnerabilities identified by intigriti bug bounty platform;
- JSON Web Tokens;
- Access control for multi-tenant cloud applications;
- Authorization, limiting data exposure;
- Normalization;
- API Security testing

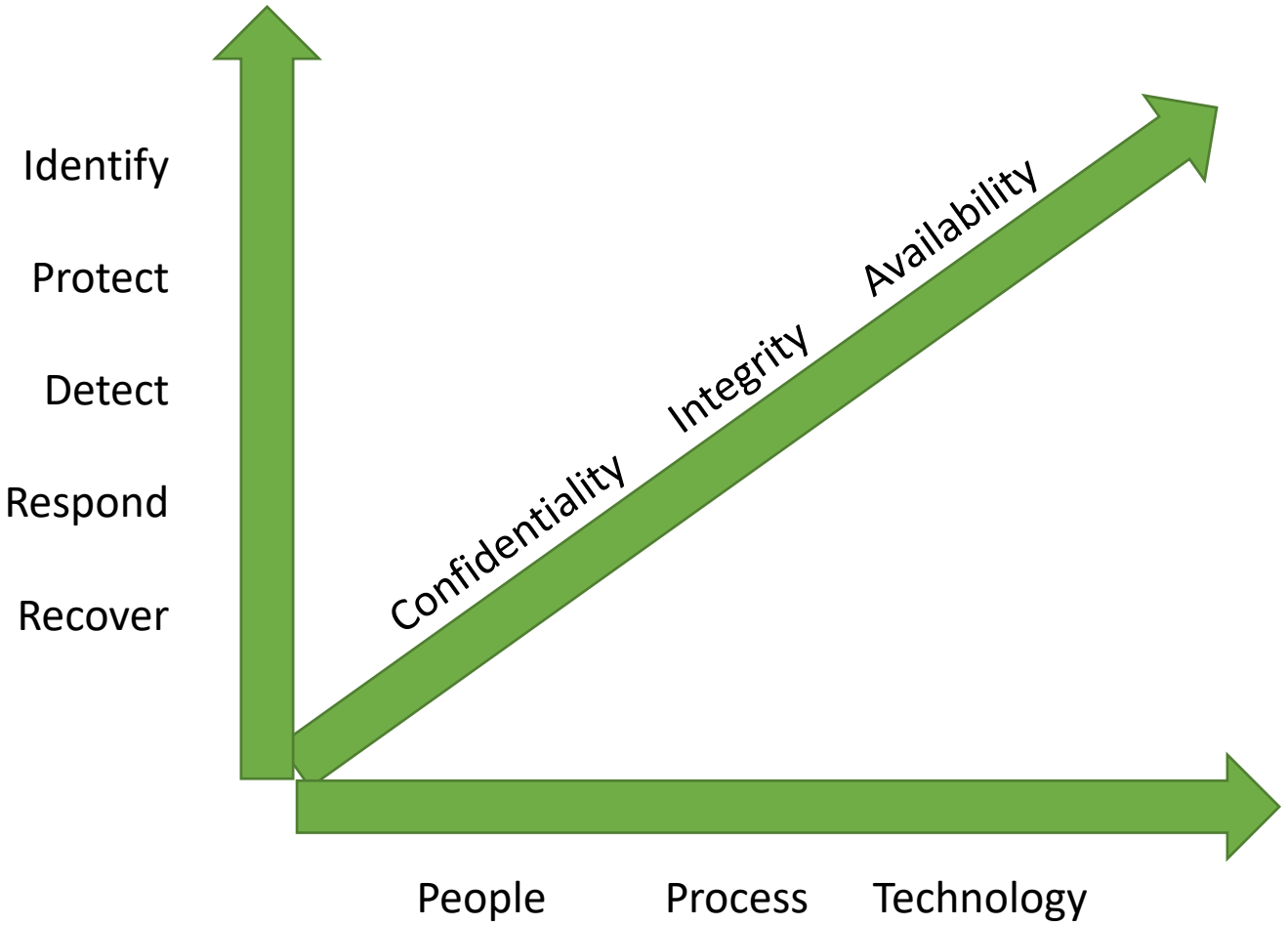
Closing remarks

One last thing: a reminder…

(anecdote from my cybersecurity fundamentals training)

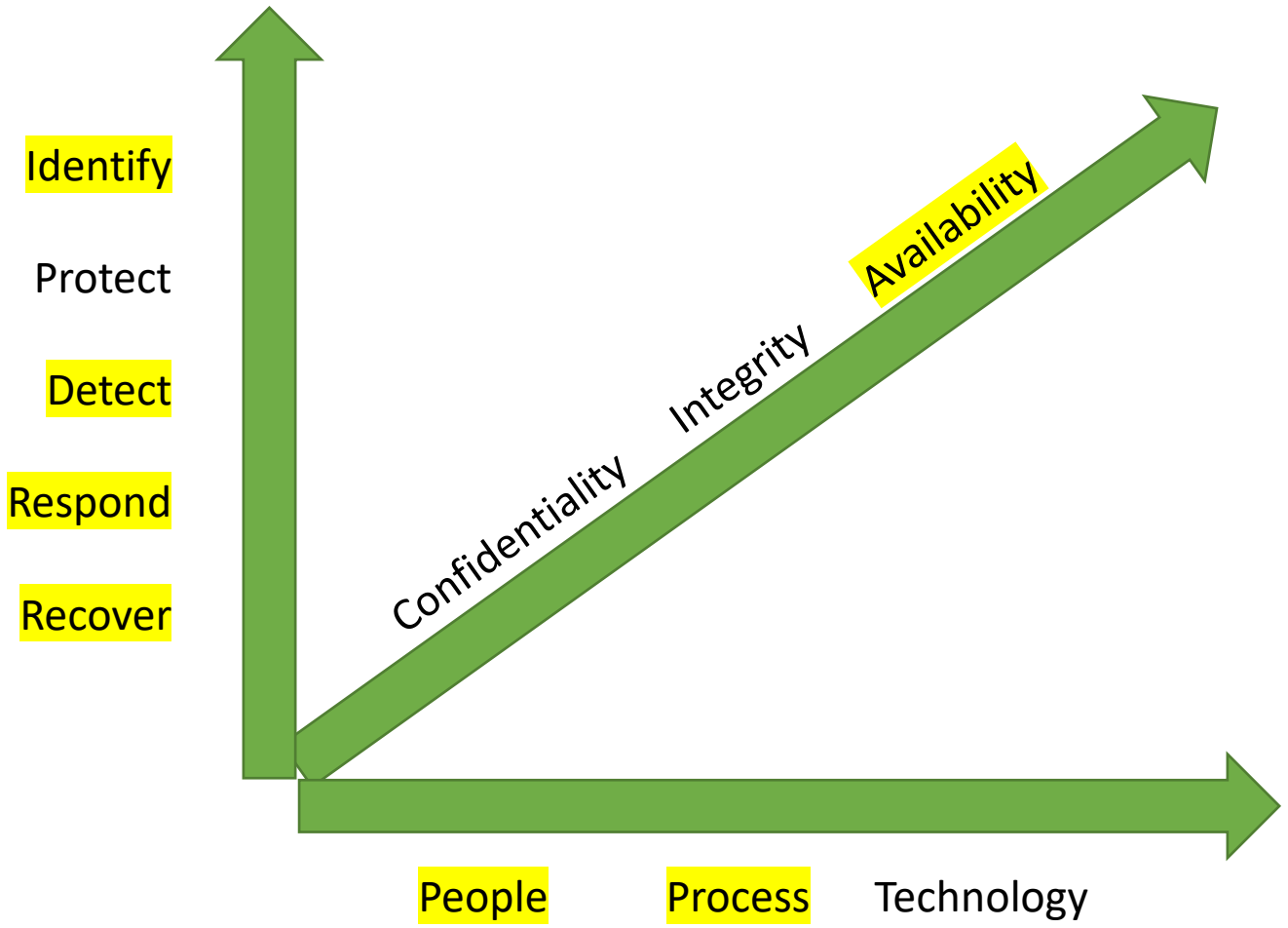
Assignment: make sure Joanna can work safely (scope: cybersecurity) while she is working remotely

3 dimensional matrix of cybersecurity



(Technology, Protect, Confidentiality)

3 dimensional matrix of cybersecurity



TAKEWAYS:

Don't forget about the other aspects of cybersecurity

Never stop learning

Don't compete on the domain of cybersecurity, but collaborate

You can never tick ALL the boxes: use a risk-based approach, BIA, Risk & Vuln. Ass't, Threat model, …

Being an advocate for cybersecurity you increase the TRUST your stakeholders have in your company.

OUR ASK – YOUR OPPORTUNITY

1. To discuss (additional) cases in detail
   ➔ speak to KU Leuven staff or myself
2. Give quotes, success story, an interview
   ➔ speak to Hans Hermans, journalist for VLAIO
3. To speak with VLAIO about how you can receive subsidies for your next leap into secure APIs, and cybersecurity in general
   ➔ speak to Patrick Hauspie, VLAIO
4. Share best practices, dare to ask questions or discuss challenges
   ➔ speak to each other ☺
5. Look for partnerships, collaboration, synergies between companies
   ➔ speak to each other ☺

THANK YOU!!

- https://apisec.be

DistriNet

AGENTSCHAP INNOVEREN & ONDERNEMEN

TSUNDOKU VENTURES