



Security through Transparency


Scaling your Customer Trust Program

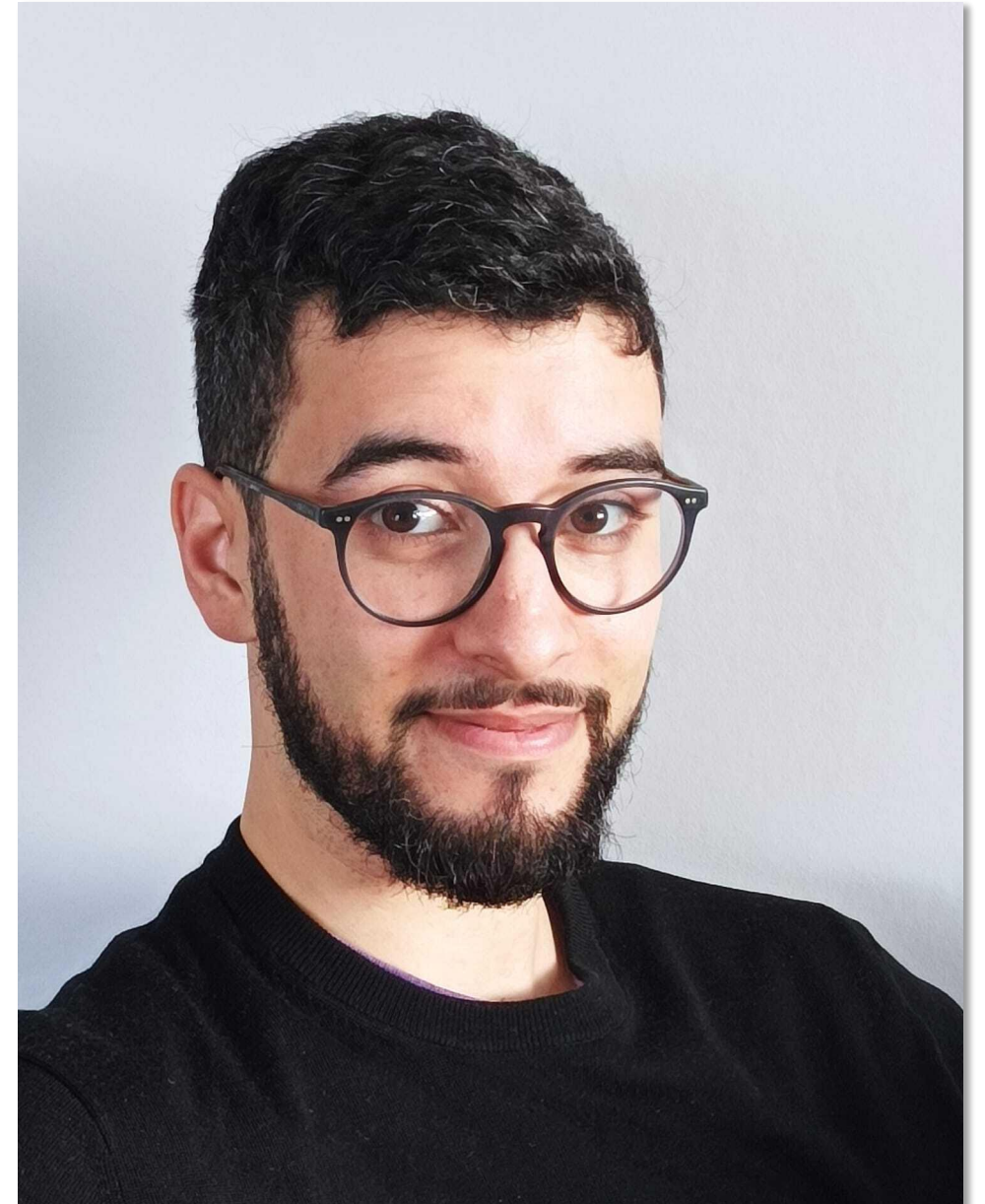
Ayoub Fandi - BlackHat Europe 2023 - 12/06/2023

#BHEU @BlackHatEvents



WHOAMI

- Ayoub Fandi, working in Customer Trust at GitLab 
- Been working in the GRC vertical for about 5 years
- LinkedIn Learning course on GRC for the Cloud-Native Revolution
- awesome-security-GRC GitHub repo
- GRC Engineering Podcast
- I like GRC 



Why should you care about transparency...



A story about Sales, security and hyperlinks



Because it makes sense

- Transparency = good
- Transparency = trust
- Trust = good



Effortless scaling

- Self service
- Can focus on high-leverage work





Transparent with the public



**yes, we have the same
security policies!**

Sharing is caring

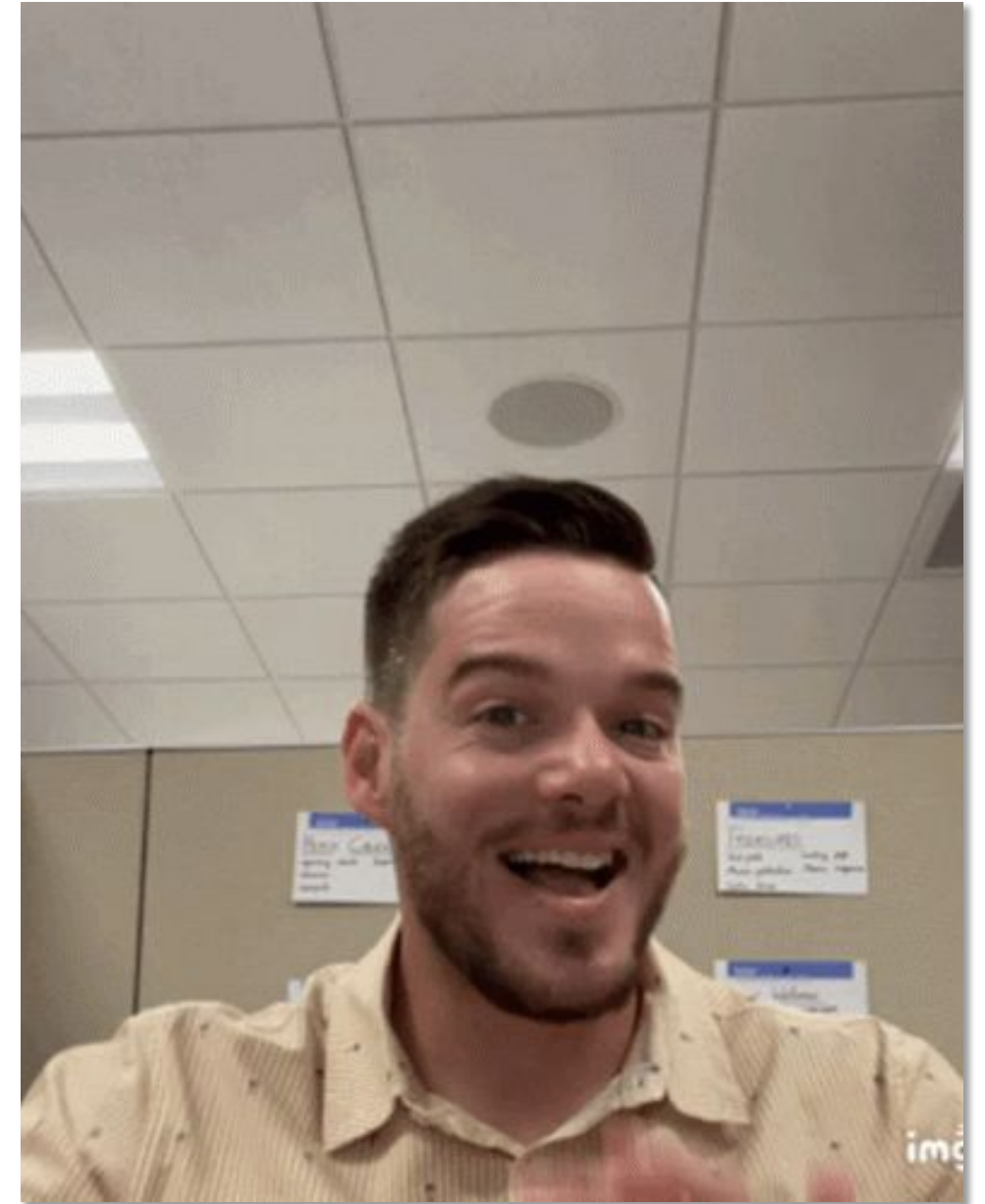
- Leveraged by others to build their programs
- Receive feedback to improve your own





Open sourcing security

- Improving everyone's security
- Influencing the industry





Getting started:

Public-facing security wiki

Share externally anything that wouldn't have additional value to an attacker if public.

Everyone knows you use AWS anyway.

The Handbook

The Handbook

Introduction

The GitLab team handbook is the central repository for how we run. It consists of over [2,000 pages of text](#). As part of our value of being [open to the world](#), and we welcome feedback. Please make a [merge request](#) for improvements or add clarifications. Please use [issues](#) to ask questions.

For a very specific set of [internal](#) information we also maintain an [internal handbook](#).

Handbook Contents

Company

- [Company](#) 
 - [About GitLab](#) 
 - [History](#)
 - [Values](#)
 - [Mission](#)
 - [Vision](#)



Transparent with your customers

Have you ever heard of security questionnaires?



Increased exposure (not that type)

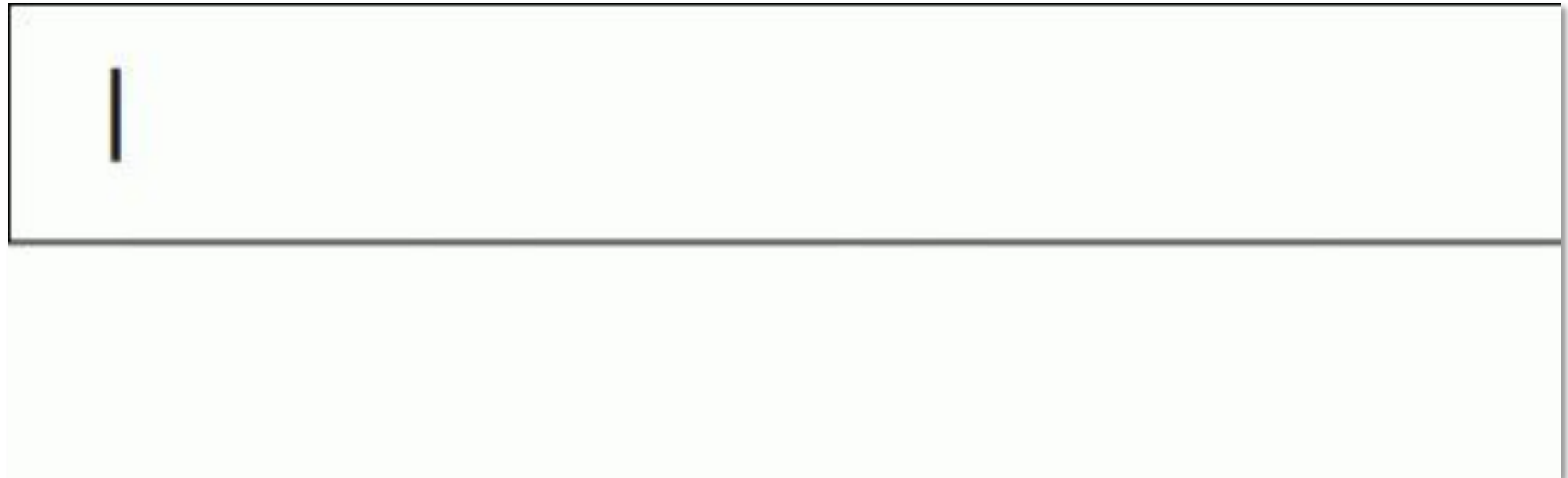
- Better reputation for your security team
- I can find your policies on Google





Empowering with the right resources

- They have all the info they need
- Maybe they'll fill it themselves?





zendesk Security

Getting started:

Sharing your security docs

Compliance Center
Member groups

We're committed to Information Security

GitLab Trust Center

It's our mission to be the leading example in security, innovation, and transparency.

Google Cloud Trust Center

How we focus on security, compliance, and privacy to earn the position of your most trusted cloud.

Explore security products

Contact us



Responsible AI—learn more about our commitment to the advancement of AI driven by



CONTACT SALES

BUY NOW

TRY FOR FREE

Overview

Cloud Status

Security

Data Protection and Privacy

Cloud Delivery Options

Compliance

Overview

Alerts

Compliance

Legal

Privacy

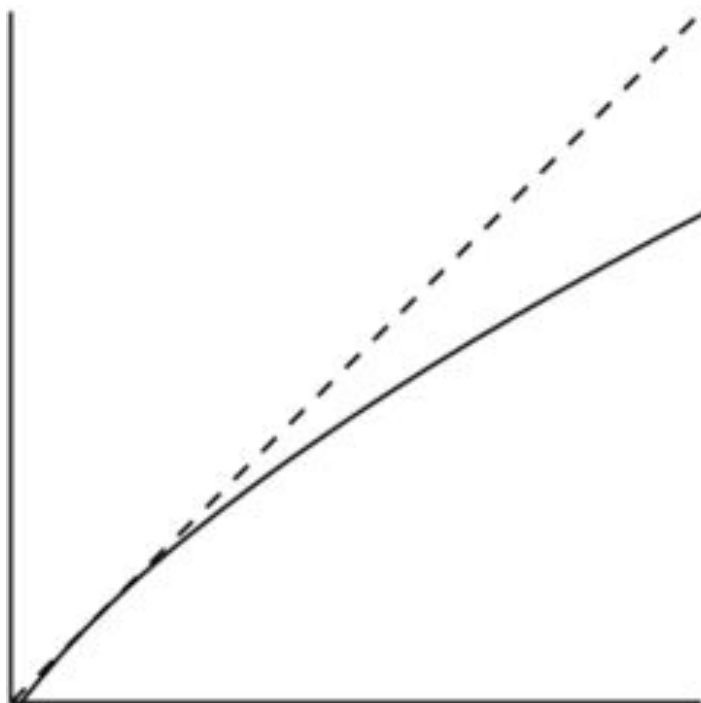
Security

System Status

Trust Portal



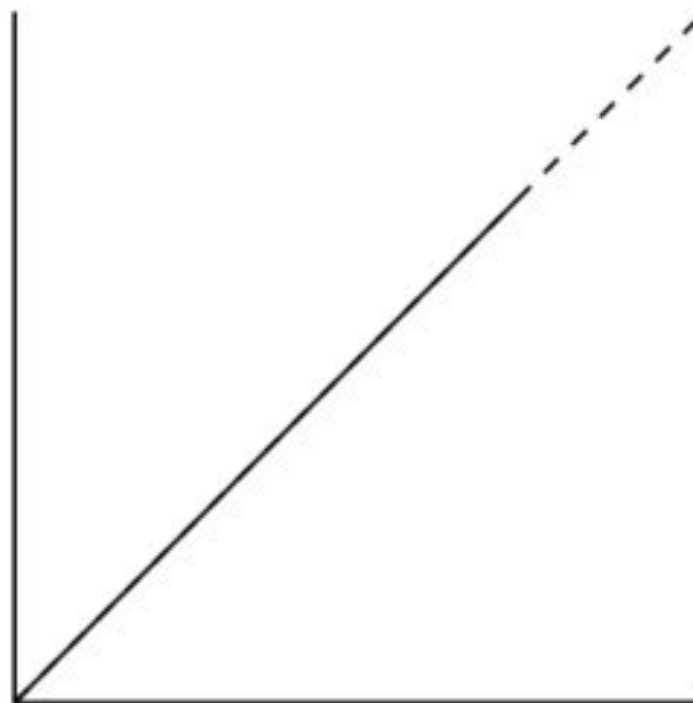
Transparent with Sales



sublinear

(a)

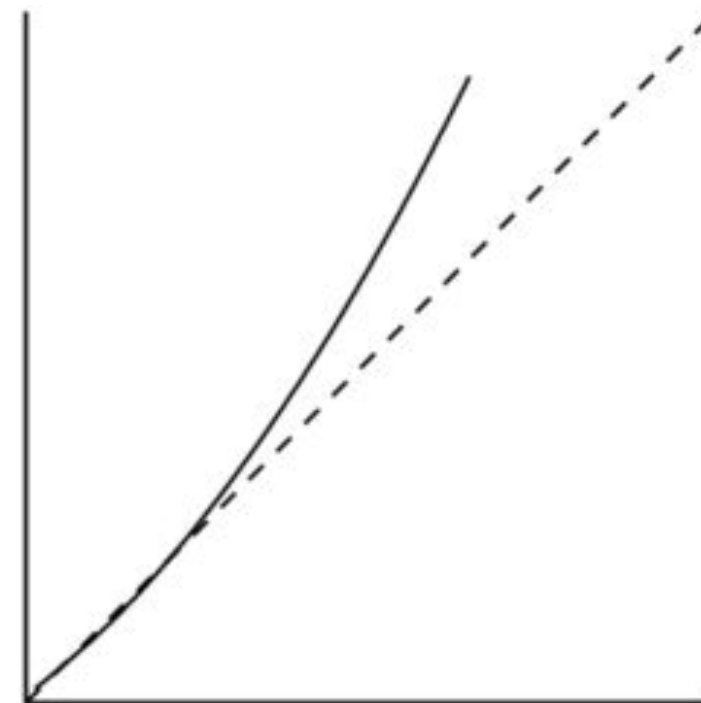
This is us



linear

(b)

This is a chart



superlinear

(c)

This is sales



Selling is hard, don't make it worse

- Let's be friends
- Let's work together (free training)



Smoothing out the cycle

- FASTER
- Less back-and-forths
- Sometimes we're not even involved





Getting started:

Database of security Q&As

- Are you secure?
 - Yes
- Can you prove it?
 - Yes
- Prove it then
 - I have ISO

... within the organisation?	Contact Details
... database to identify Information Security risks and	Evidence of inform
... into consideration risks posed by the organisation	
... use of a standardised Anti-Virus solution?	Advice which AV p
... network security appliance(s) to filter threats from	Network Security d
... led Threat Management features (IPS/IDS, Anti-Virus,	Description of imp
... ously monitor its infrastructure and services for	Please provide any
... ile process for handling security incidents?	IS incident respon
... is that impact ser...	Process for respon
... ced any significant	Reporting detaili
... made any informati	Information securi
... sation is stored?	Details of inform
... stored?	
... is ability to recover	Evidence of
... from personally ident	
... s any data for purpo	
... rest?	Encryption standa
... t data in transit and if so, how?	Encryption standa
... dicy enforced by the organisation?	Password policy d
... utilised where appropriate?	Brief explanation o
... prevent unauthorised access to information?	Brief explanation o
... ion to detect unauthorised access to systems and/or	Brief explanation
... tam admin / super user) restricted to those who have	Brief explanation
... process for managing updates to its devices and	Process / procedu





Common objections



I read “insecure by design”

Everyone can get
better at reading

Looks like an impersonal way to sell

The goal isn't to sell, it's to help sales. They are already doing the selling.

**How can I keep all of this
up to date?**

You need to Git it
right the first time.



AI

Abstract geometric patterns in shades of blue and white, resembling a complex network or data visualization, located in the top right corner of the slide.

**You should try it.
Let me know how it goes.**



Any questions?

Feel free to reach out on LinkedIn (yes, I know, I don't use Twitter) if you have any questions or need guidance on having a more transparent security program