A Technical Approach to Zero Trust Application Access

Gijs Van Laer

SecAppDev

About me

CTO at XFA, a cybersecurity company focused on device security

Previous

- Information Security Consultant
- CISO at DPG Media
- Software developer

Education

- PhD in Cryptography (advised by Matt Green), Johns Hopkins University
- Master of Science in Security Informatics, Johns Hopkins University
- Master of Science in Pure Mathematics, University of Antwerp

gijs.vanlaer@xfa.tech

SecAppDev

The audience (by show of hands)

- Who is (or considers themselves) a network security engineer?
- Who heard of the term Zero Trust?
- Who heard of the term Zero Trust Network Access?
- Who heard of the term Zero Trust Application Access? (before hearing the title of this lecture)

SecAppDev

What is Zero Trust?

“The term ‘zero trust’ is now used so much and so widely that it has almost lost its meaning,” - Steve Riley

What is Zero Trust?

Companies thought their network was a castle…

…but over the years it became more like a soap bubble

SecAppDev

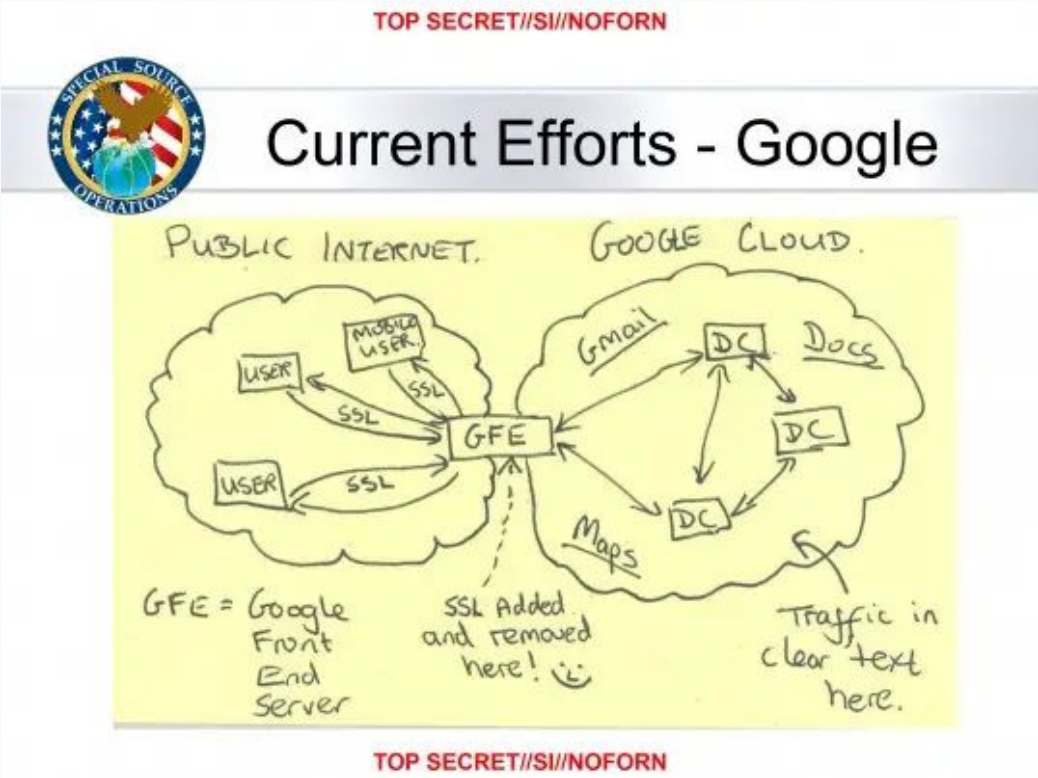
Connecting remotely, with any device

Classic approach: connecting remotely into a trusted network

SecAppDev

Connecting remotely, with any device

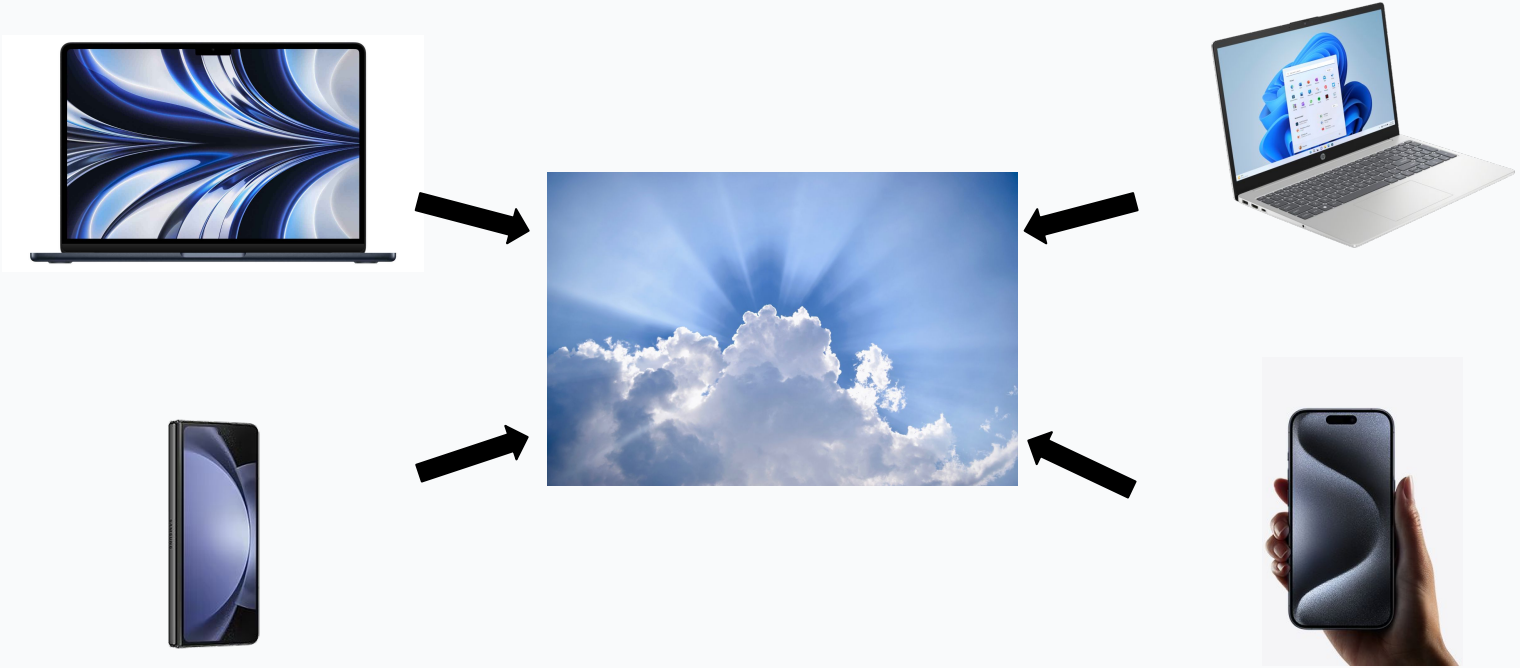
Classic approach: connecting remotely into a trusted network



SecAppDev

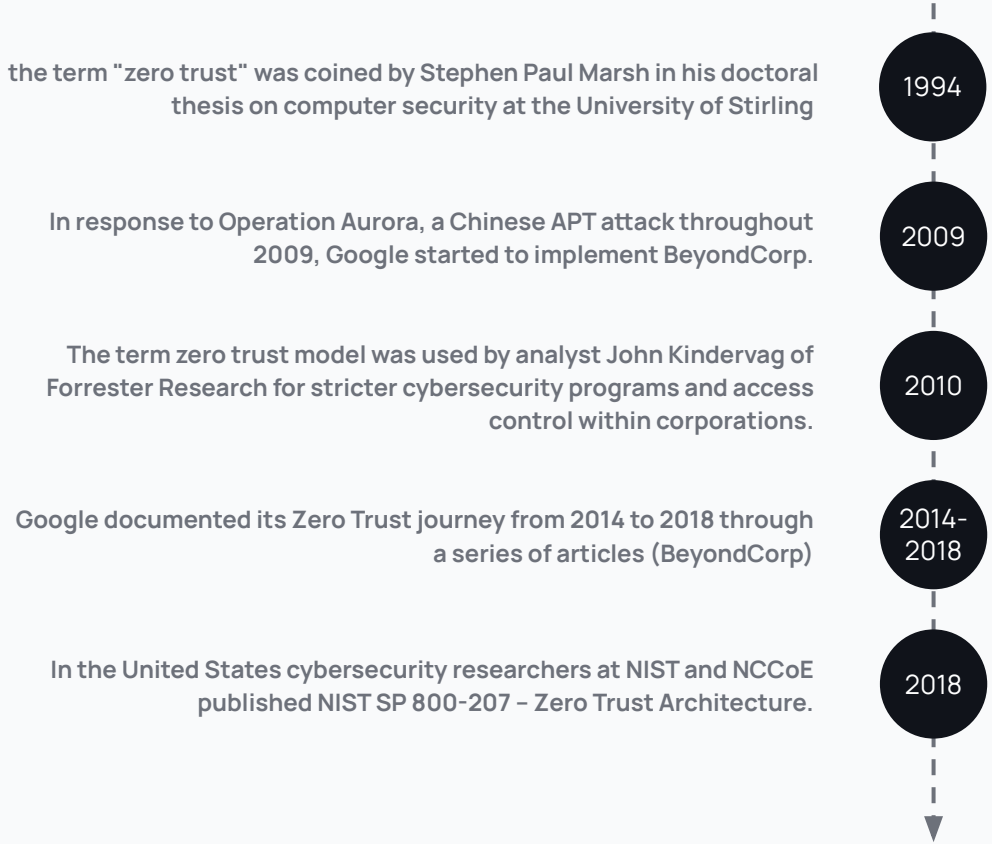
Embrace the new reality

Modern approach: authenticate to the cloud (SaaS applications)



SecAppDev

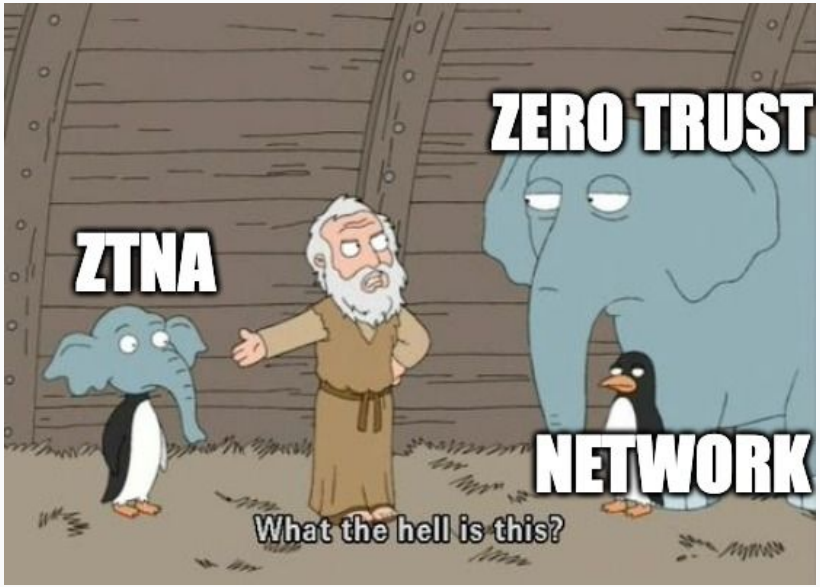
The history of Zero Trust?



SecAppDev

The mistake called ZTNA

- Zero Trust Network Access - coined by Steve Riley at Gartner in 2019
- Happily adopted by all network security vendors seeing their market disappearing.



SecAppDev

Towards ZTAA

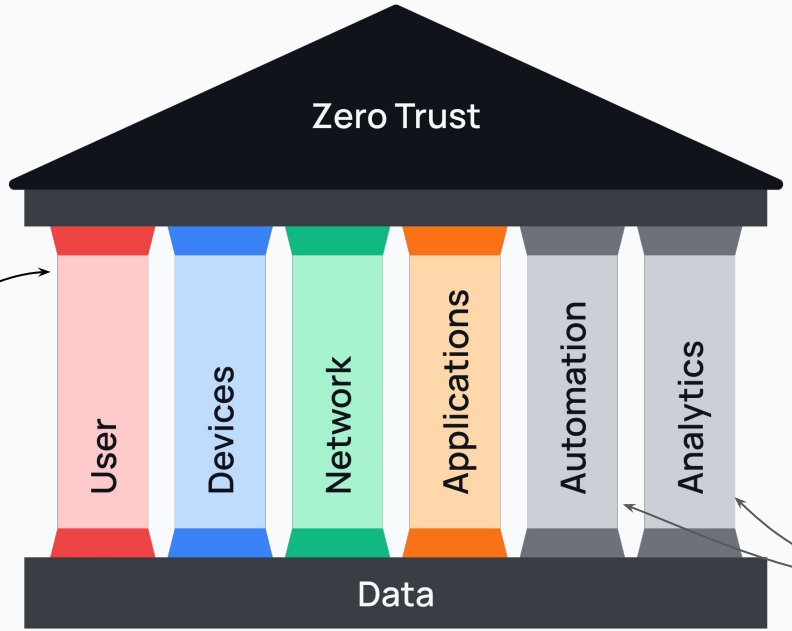
- Zero Trust Application Access
- We thought we came up with it, but Riley already said in an interview with *SecurityWeek* in 2022 :

> “In fairness and retrospect, Riley wishes he had used the term zero trust application access (ZTAA), but now thinks it is too late to change.”

Do not trust the network

And build around what you control

start with 4 first pillars



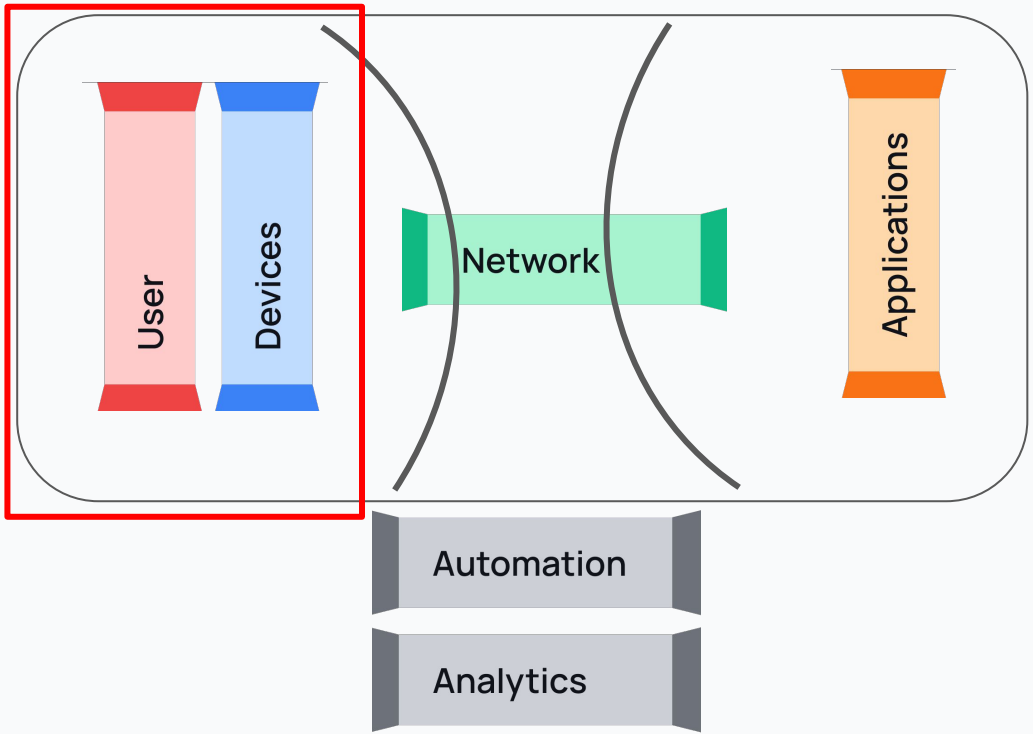
The only way to scale

Six Pillars of a Zero Trust Security Model

SecAppDev

Do not trust the network

My mental model



SecAppDev

Zero Trust - building blocks

Pillar: Users

Objectives:

- Secure identity

Tools:

- Identity provider (if possible move to single-sign-on)
- Multi-factor authentication
- Password Manager

SecAppDev

Zero Trust - building blocks

Pillar: Devices

Objectives:

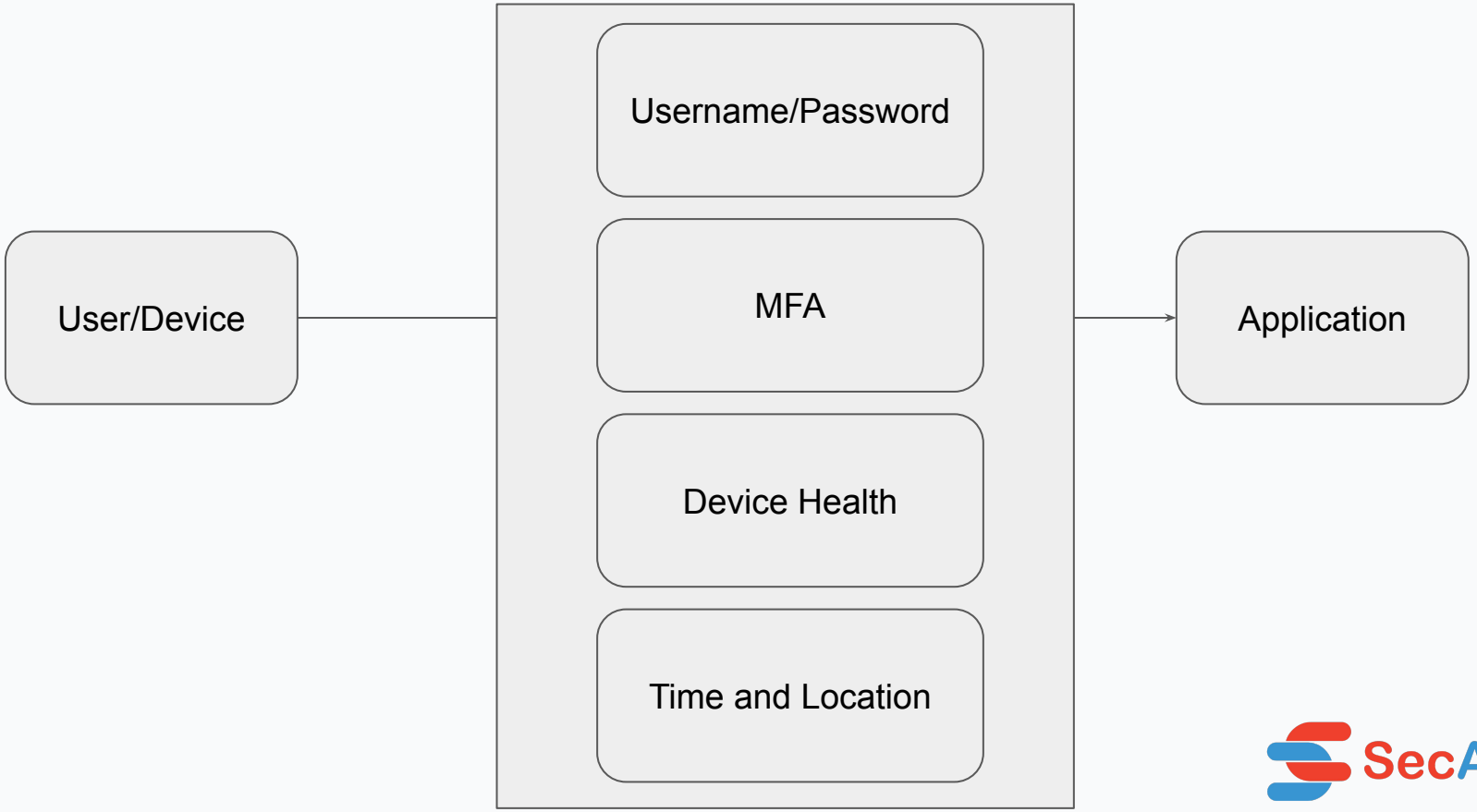
- Up to date devices
- Up to date browsers
- Disk encryption
- Backups

Tools:

- Enforced checks on endpoints
- Device management
- Keep data in the cloud

SecAppDev

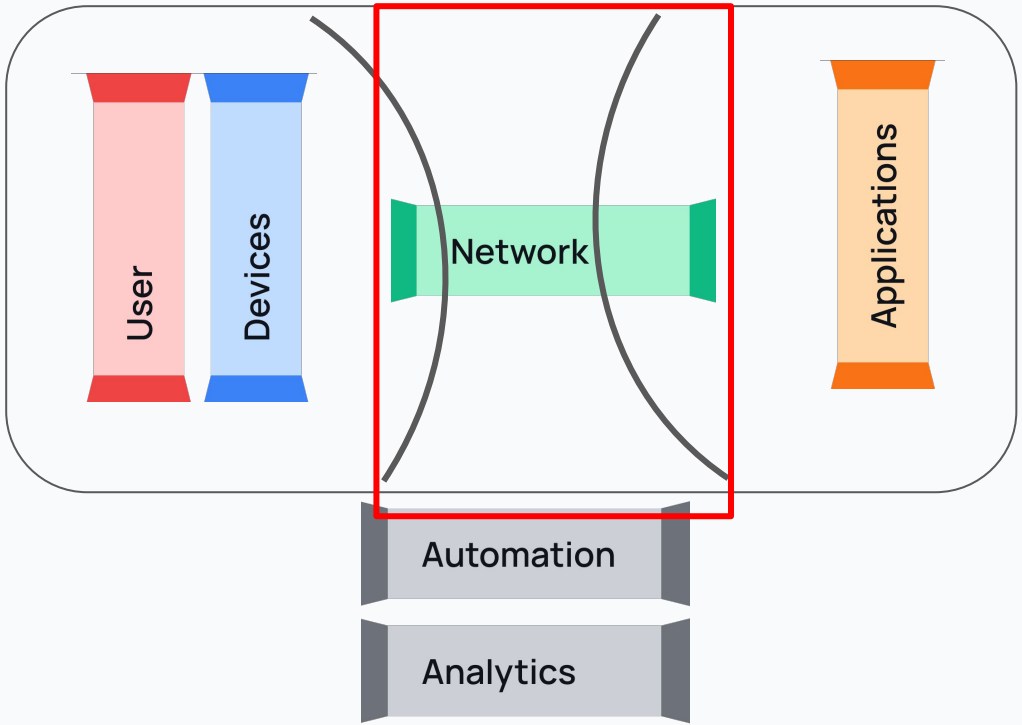
Context Aware Access



SecAppDev

Do not trust the network

My mental model



SecAppDev

Zero Trust - building blocks

Pillar: Network

Objectives:

- All network traffic encrypted

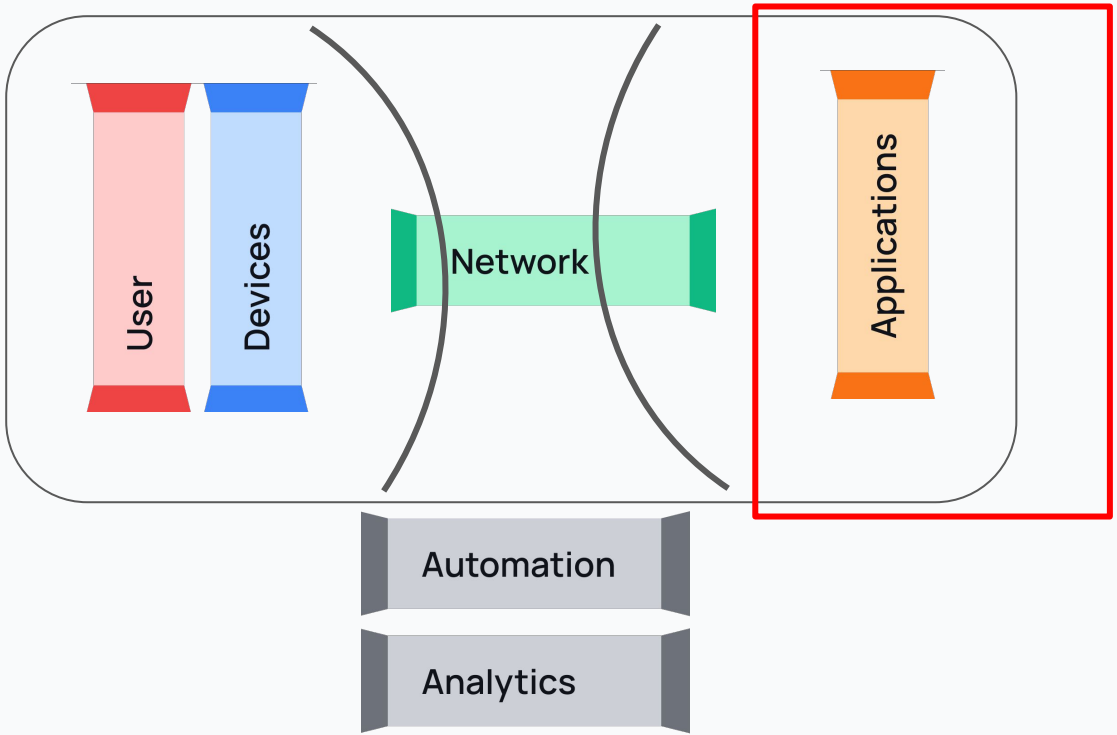
Tools:

- HTTPS Everywhere
- DNS-over-HTTPS

SecAppDev

Do not trust the network

My mental model



SecAppDev

Zero Trust - building blocks

Pillar: Applications

Objectives:

- Isolation between applications
- Secure vendors - secure versions of applications

Tools:

- Default isolation with SaaS applications
- Review your vendors
- Keep used software up to date
- When building software yourself:
  - Secure Development Lifecycle
  - Use OWASP as the best resource for secure development
  - Keep used libraries up to date

SecAppDev

Shift to the left & DevSecOps

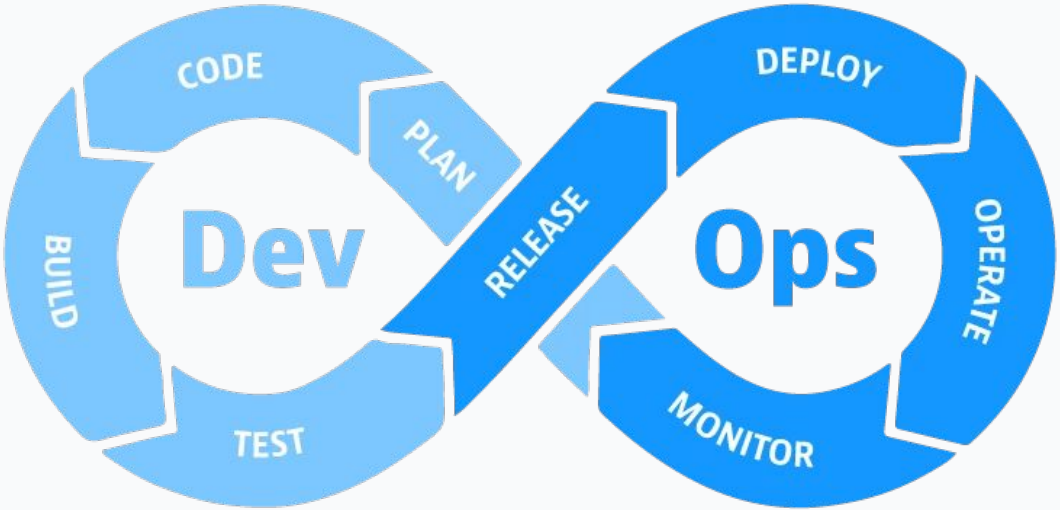


Image source: dynatrace

SecAppDev

Shift to the left & DevSecOps

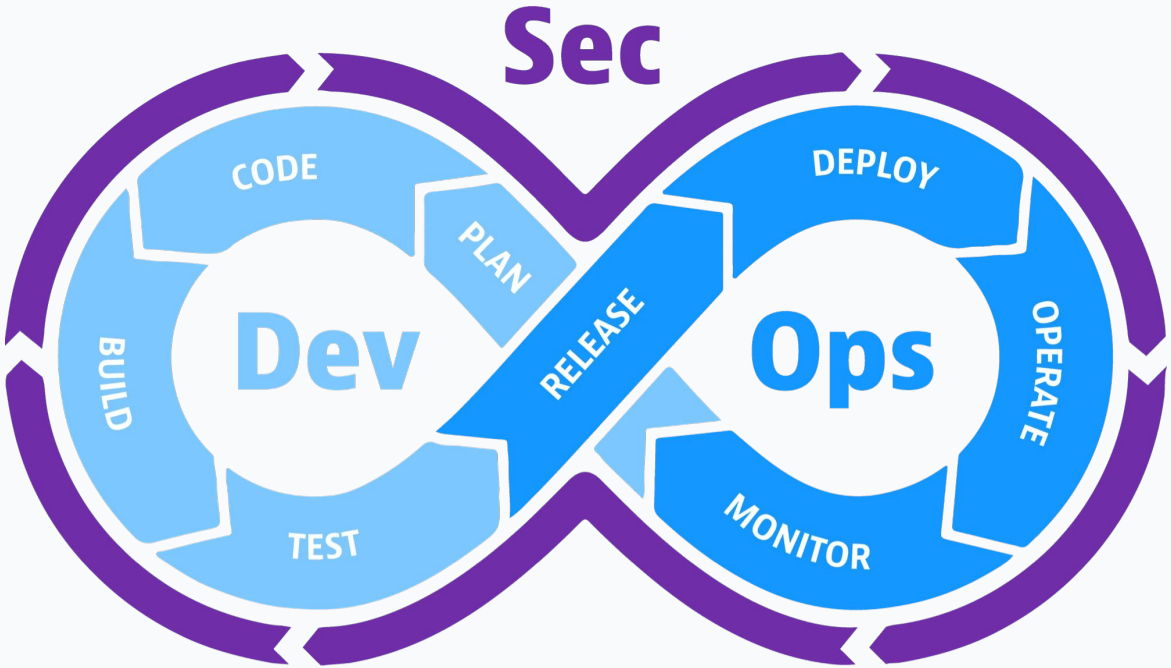
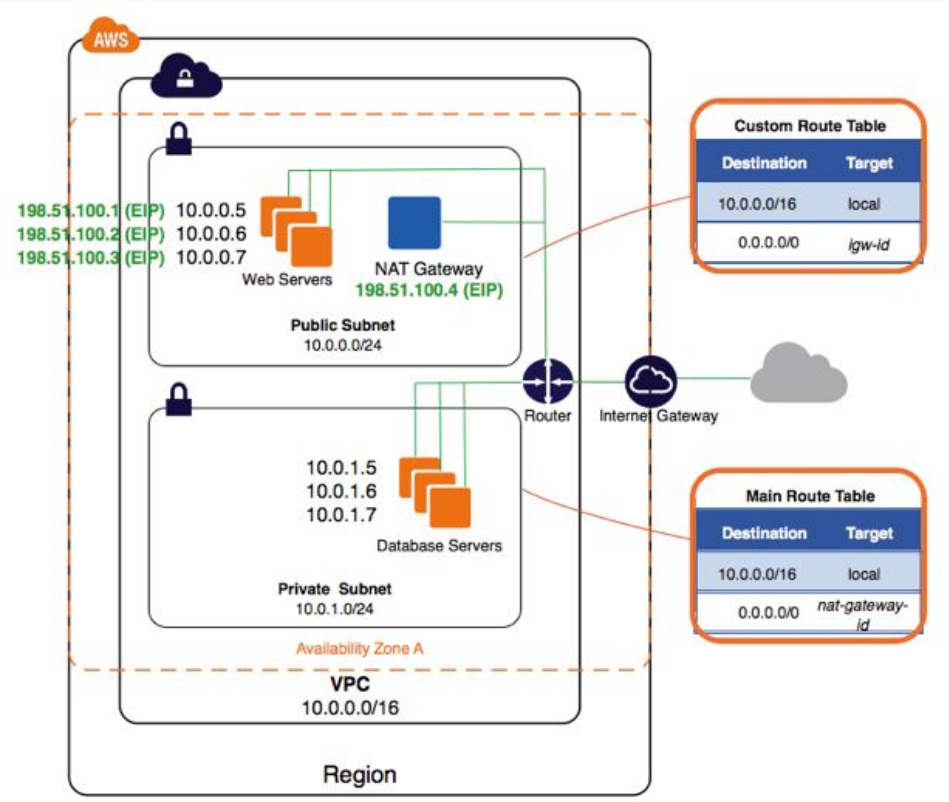


Image source: dynatrace

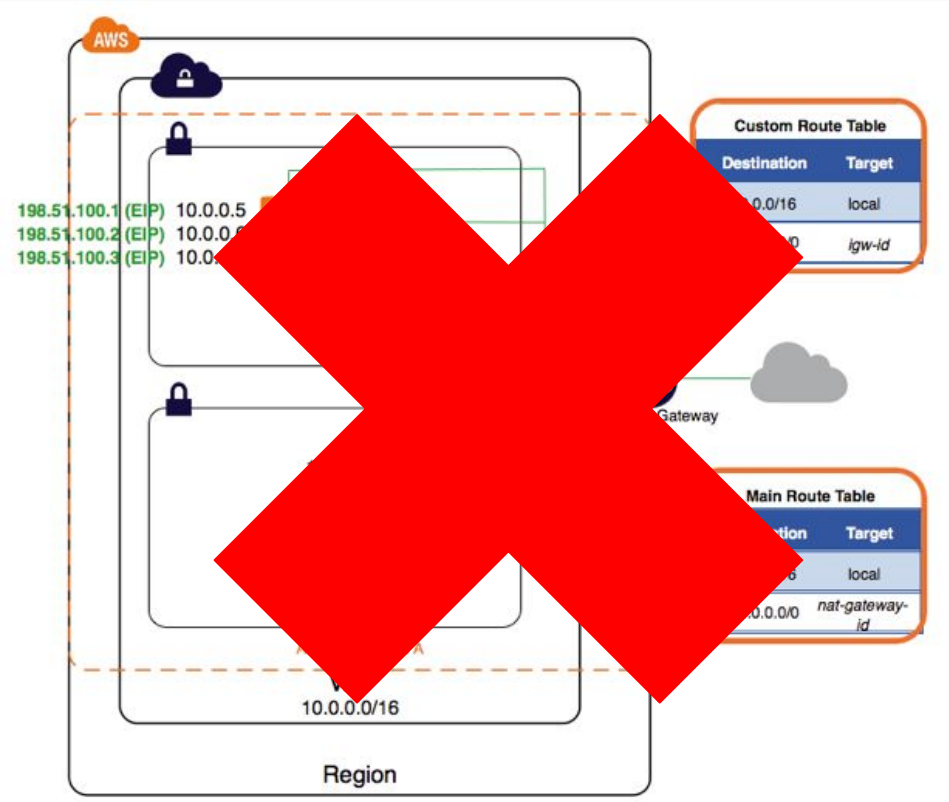
SecAppDev

Extreme isolation



SecAppDev

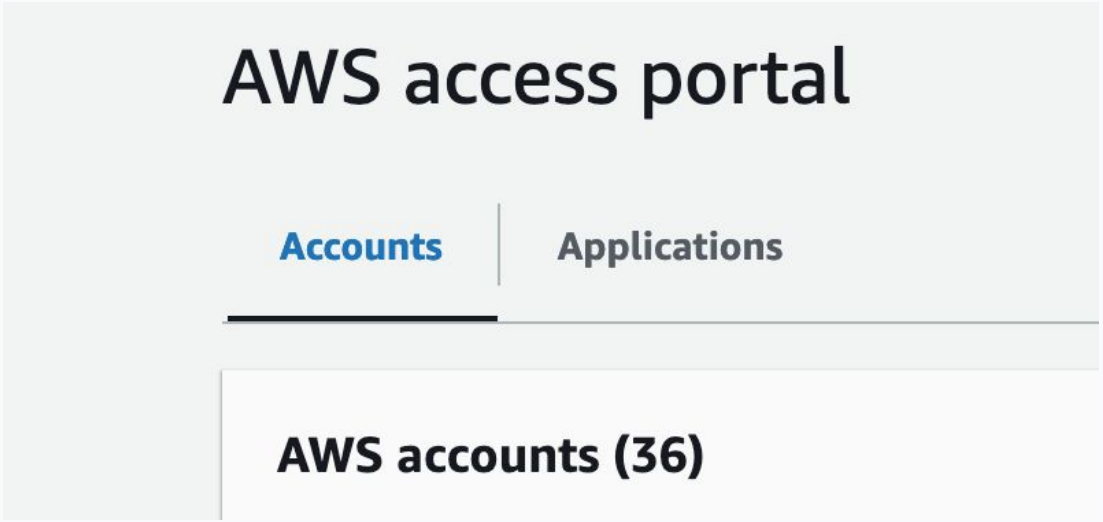
Extreme isolation



SecAppDev

Extreme isolation

- Application-based cloud accounts



SecAppDev

Keeping libraries up to date

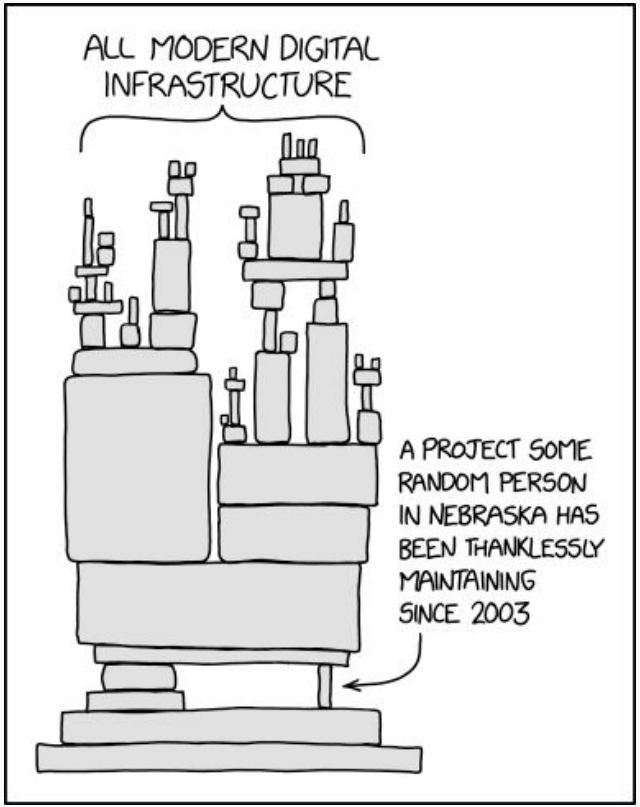
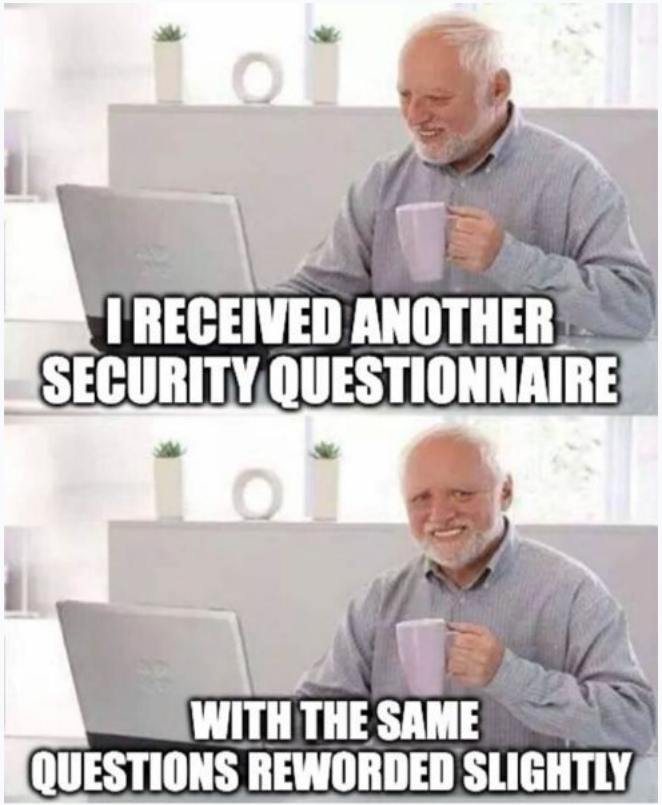


Image source: https://xkcd.com/2347/

SecAppDev

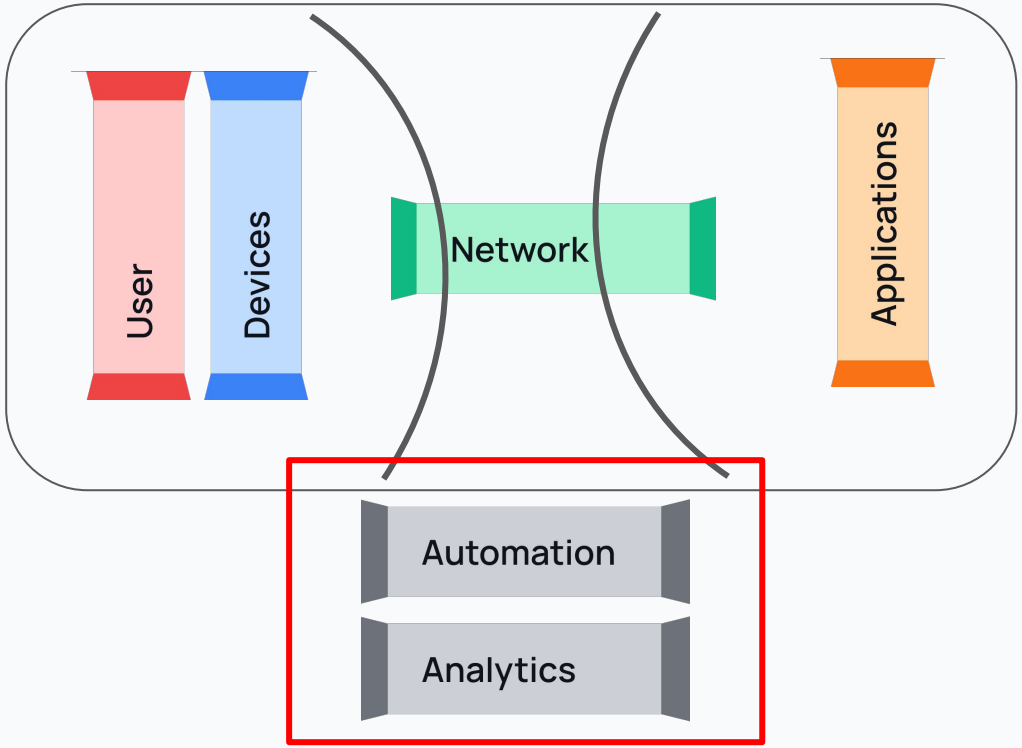
Third-party management



SecAppDev

Do not trust the network

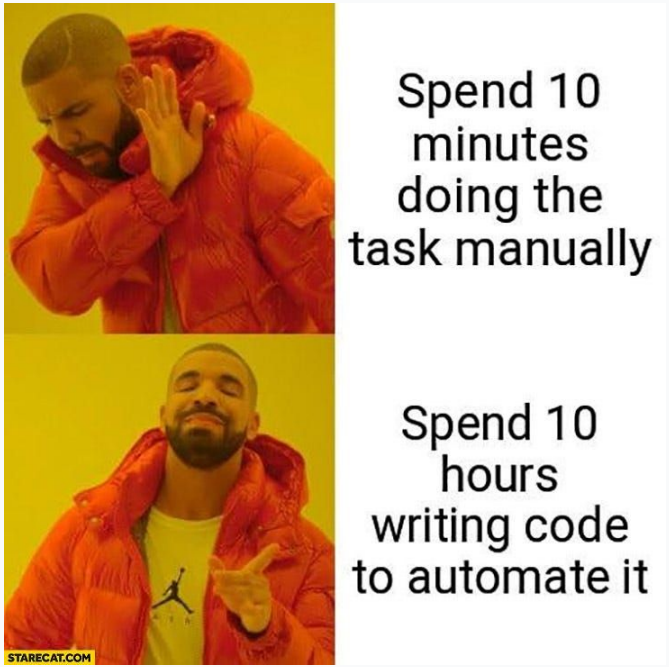
My mental model



SecAppDev

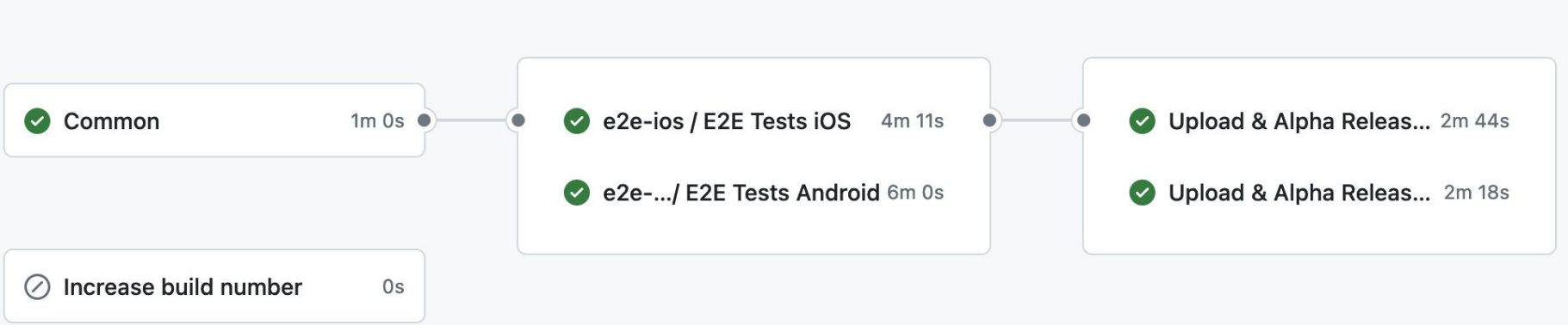
We've already covered Automation and Analytics

- Without automation, this concept doesn't scale at all



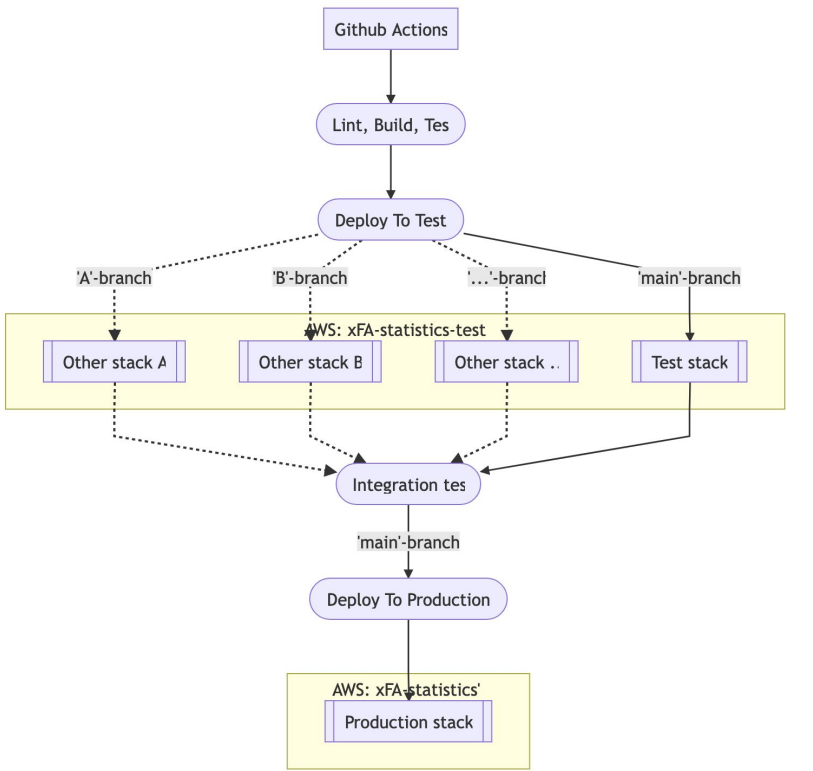
SecAppDev

We've already covered Automation and Analytics



SecAppDev

We've already covered Automation and Analytics

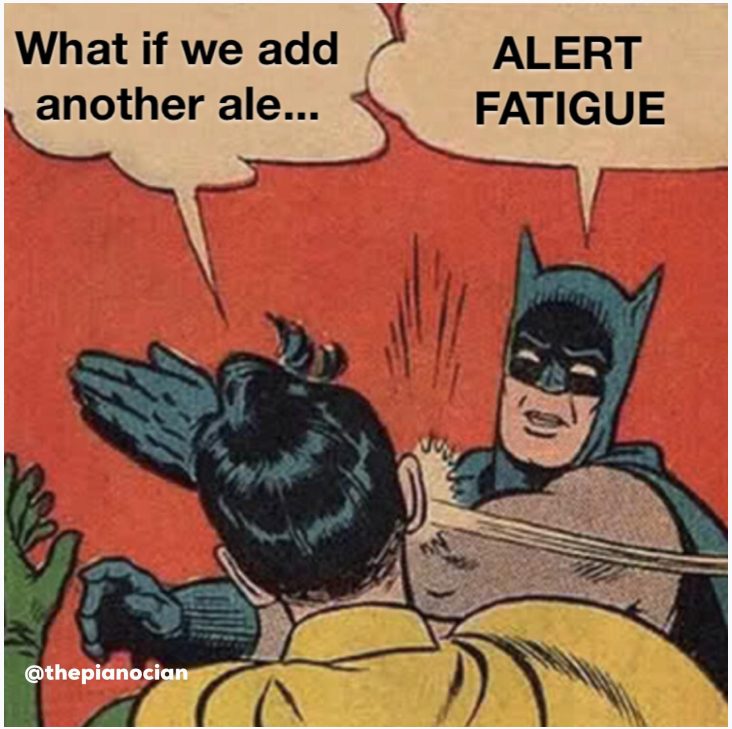


SecAppDev

We've already covered Automation and Analytics

SecAppDev

We've already covered Automation and Analytics



SecAppDev

Thank you

gijs.vanlaer@xfa.tech

SecAppDev