Fast product development in digital banking without sacrificing security

DEVOPS ENTERPRISE SUMMIT LAS VEGAS - VIRTUAL 2020

fluid attacks
we hack your software

Camilo Piedrahita

IT MANAGER

BANCOLOMBIA

DevSecOps, reactive programming, functional programming and best practices of software development

Camilo Piedrahita Macias

@Camilo9229

capiedra@bancolombia.com.co

Rafael Alvarez

CTO & CO-FOUNDER

FLUID ATTACKS

Red team operations and product development focused on fast exploitation and vulnerability disclosure

Rafael Alvarez

ralvarez@fluidattacks.com

fluid attacks
we hack your software

FAST PRODUCT DEVELOPMENT IN DIGITAL BANKING WITHOUT SACRIFICING SECURITY

Bancolombia

+8.3
Billion Transactions

87%
Digital Transactions

+4k
Servers

+3k
Engineers in IT VP

+25k
Working Stations

+5.090
ATMs

fluid attacks
we hack your software

2%
False Positive Rate

4%
False Negative Rate

240M
Lines of Code Tested

28M
Secured Deployments

35
Languages Tested

50%
Apps with high or critical vulnerabilities

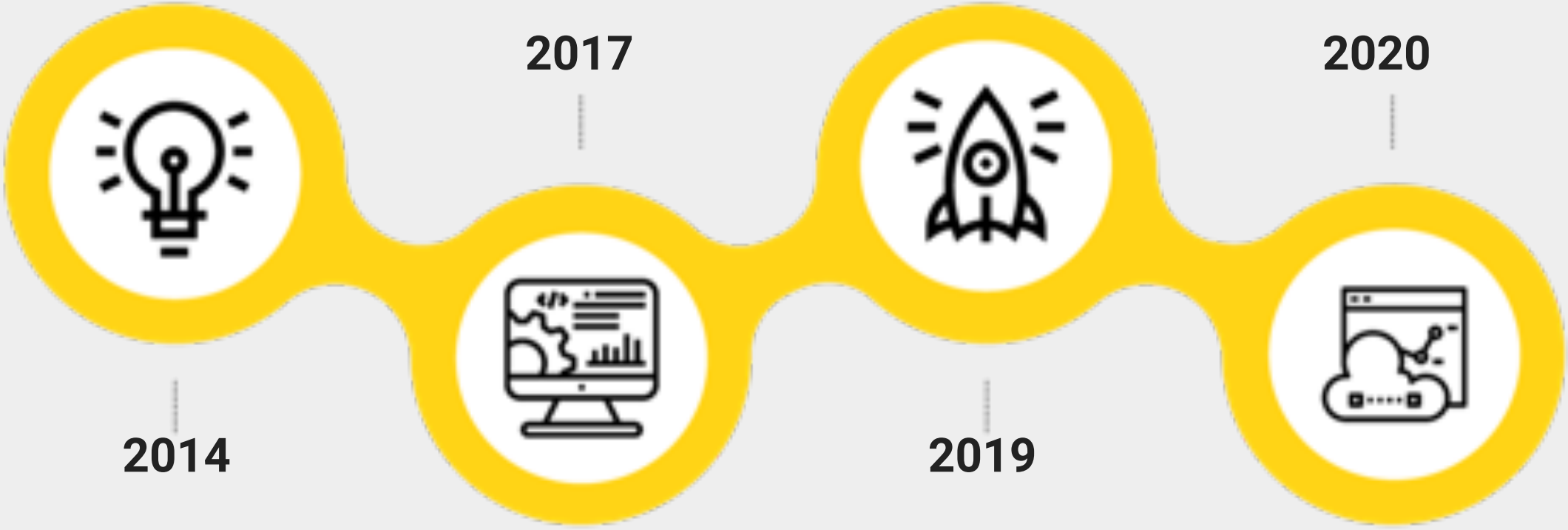
Fintech Context in LATAM

Giants

Pay

pay

Journey


2014
100% Agile
100% DevOps
2017
2019
DevSecOps
100% Cloud
Open First
2020

FAST PRODUCT DEVELOPMENT IN DIGITAL BANKING WITHOUT SACRIFICING SECURITY

Strategy

BASE CAMP

- Referral Journey
- Sherpas: define tools, change processes and define sessions
- Advanced Squad: early adapters to accelerate cultural change
- Guides: introduce change in each team
- Expedition Leader

NORTH CAMP

- From DevOps to DevSecOps
- DevOps for Databases and Mainframes
- Measure 4 key metrics
- Unify tester + developer role

SUMMIT

- 100% Cloud
- Open First
- Extend DevOps for Databases
- Daily Releases

Referral Journey

Sherpas

Advanced Squad

Guides

Expedition Leader

Inspired by Nationwide DevOps Journey 2017

Why Fast?

Bancolombia APP

Before

54 days

Today

23 days

Transactional Site

Before

32 days

Today

5 days

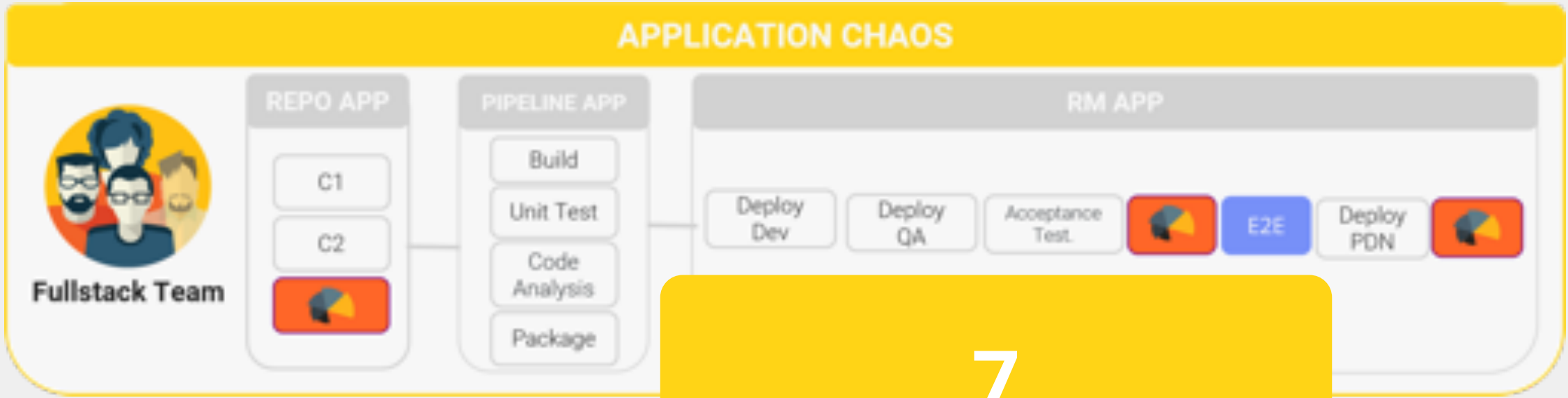
Bancolombia on Hand

Before

Today

7 releases/day

How?



Continuous chaos

7
Deliveries per day

E2E Tests on ATMs

How to involve robotics to accelerate processes?

Hygieia - Open First

Better Governance – DOES17

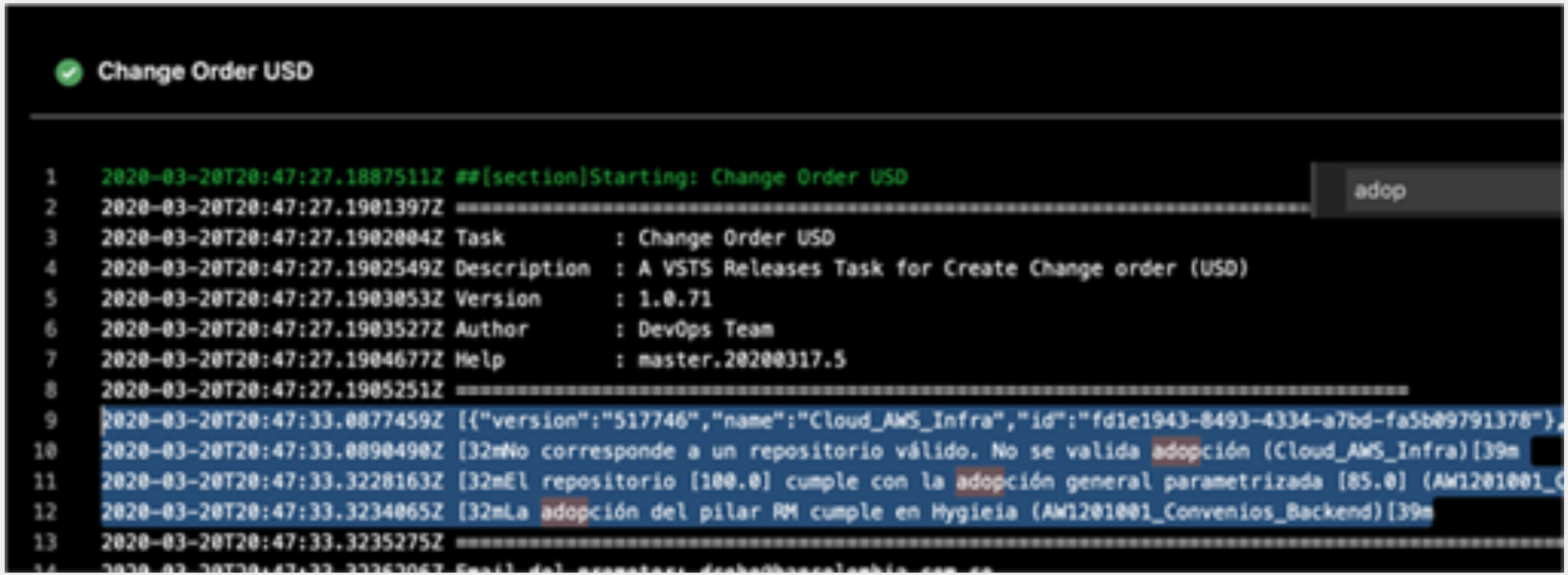
“Ensure that a single developer can not make changes to production bypassing all controls.”

Tapabrata Pal & Jennifer B

~~**Compliance**~~ **Governance**

Automation Compliance

Adoption validators

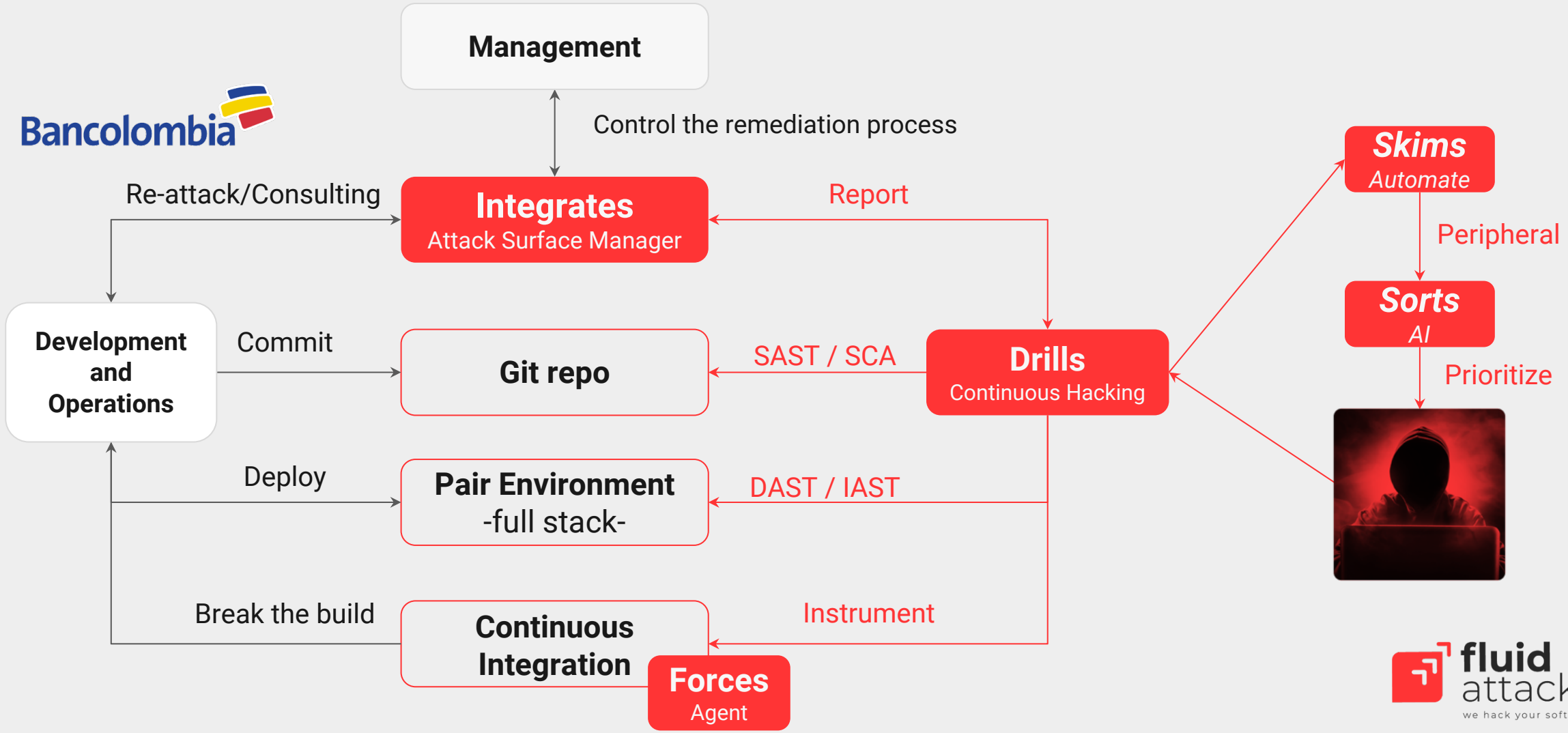


Where is Security?

Automation is not Enough

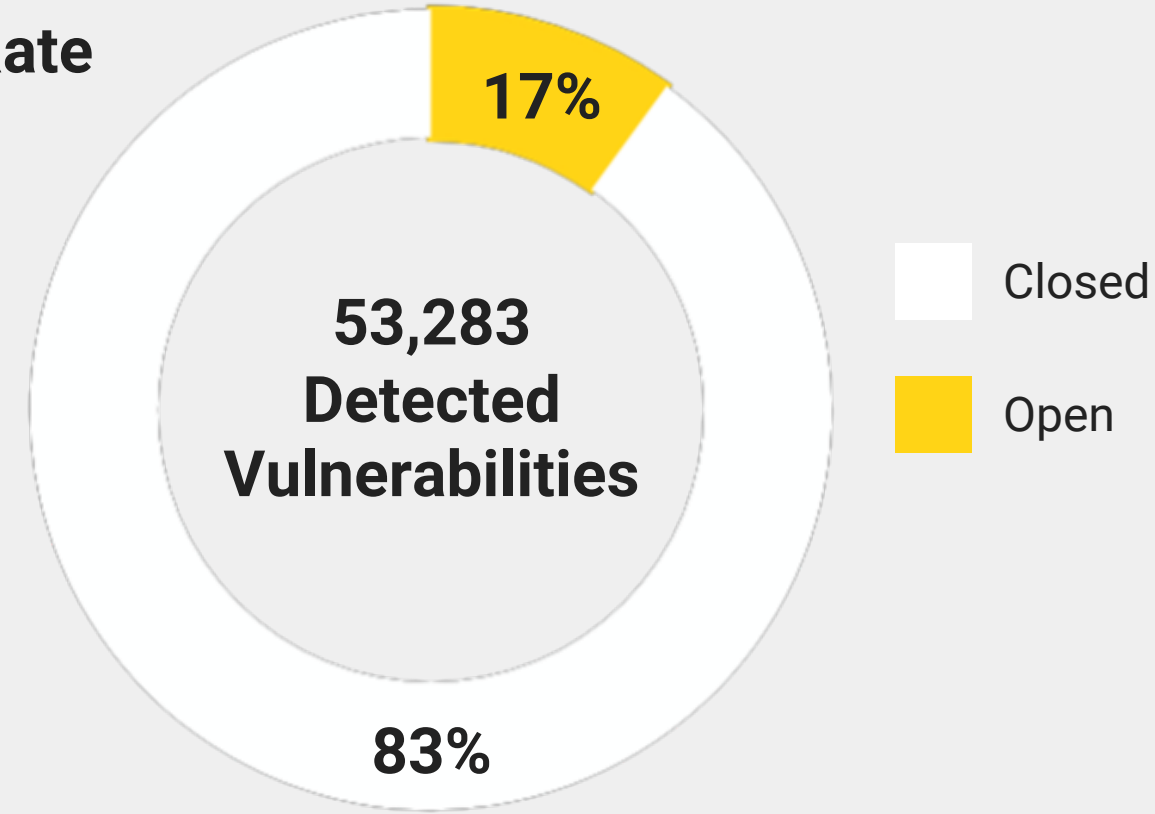
3 million vulnerabilities

Our Approach: Hackers at the Center + Prioritization by AI



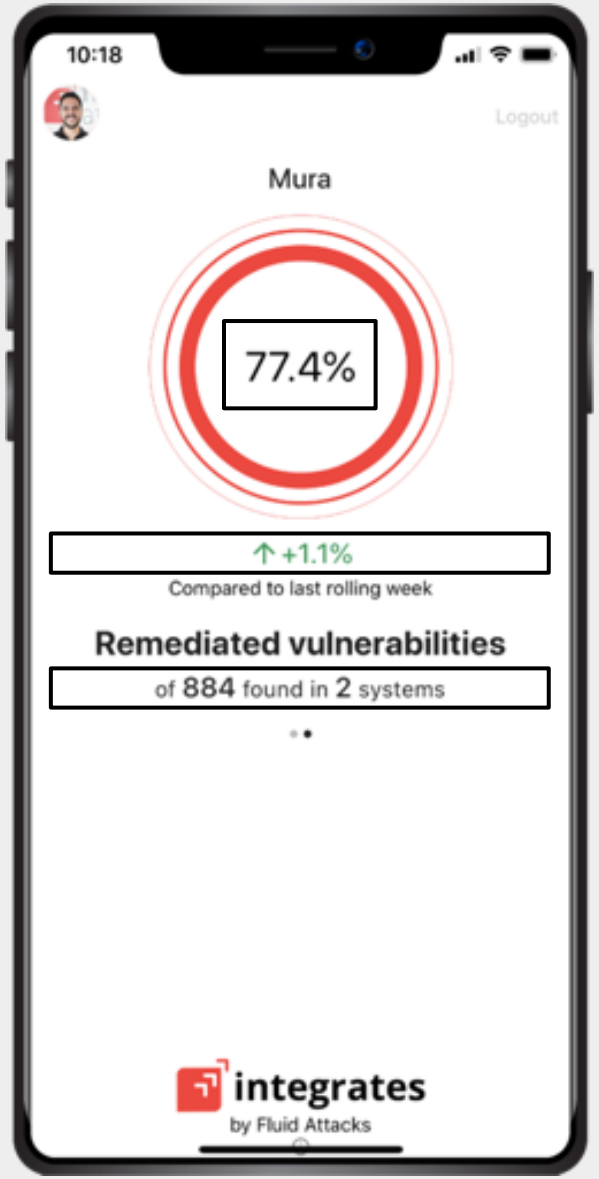
Vulnerabilities

Closing Rate



Integrates (web): Controlling the Remediation Process

Integrates (mobile): One Indicator for Top Management



Lessons Learned

1. **Architecture matters, it matters a lot**
   - You don’t have the same speed in mainframe
2. **Governance ! = Compliance**
   - Lean process == lean pipeline
3. **Federal DevOps**
   - Centralized DevOps is another silo
4. **Continuous hacking is key**

Takeaways: Don't Go Too Fast; You Could Crash or Go in the Wrong Direction

1. **Hackers at the center**
   - To remove false negatives (omissions)
2. **Discard vulnerabilities**
   - To remove false positives (lies)
3. **Use Artificial Intelligence**
   - To increase hackers' speed, not to remove them from the equation
4. **Break the build**
   - To force DevOps teams to remediate
5. **Top management visibility**
   - One indicator on the CEO's mobile guarantees resources for a full remediation

Bancolombia

Due to the formality level of this approach, the application's team prefers remediation rather than signing off on the acceptance of the risk associated with a vulnerability.