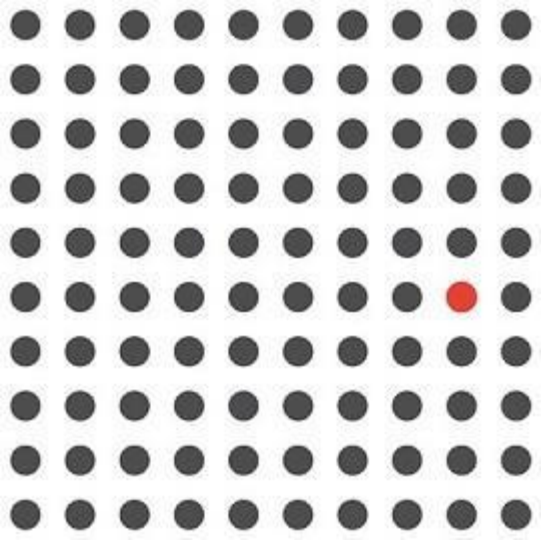
ADDO

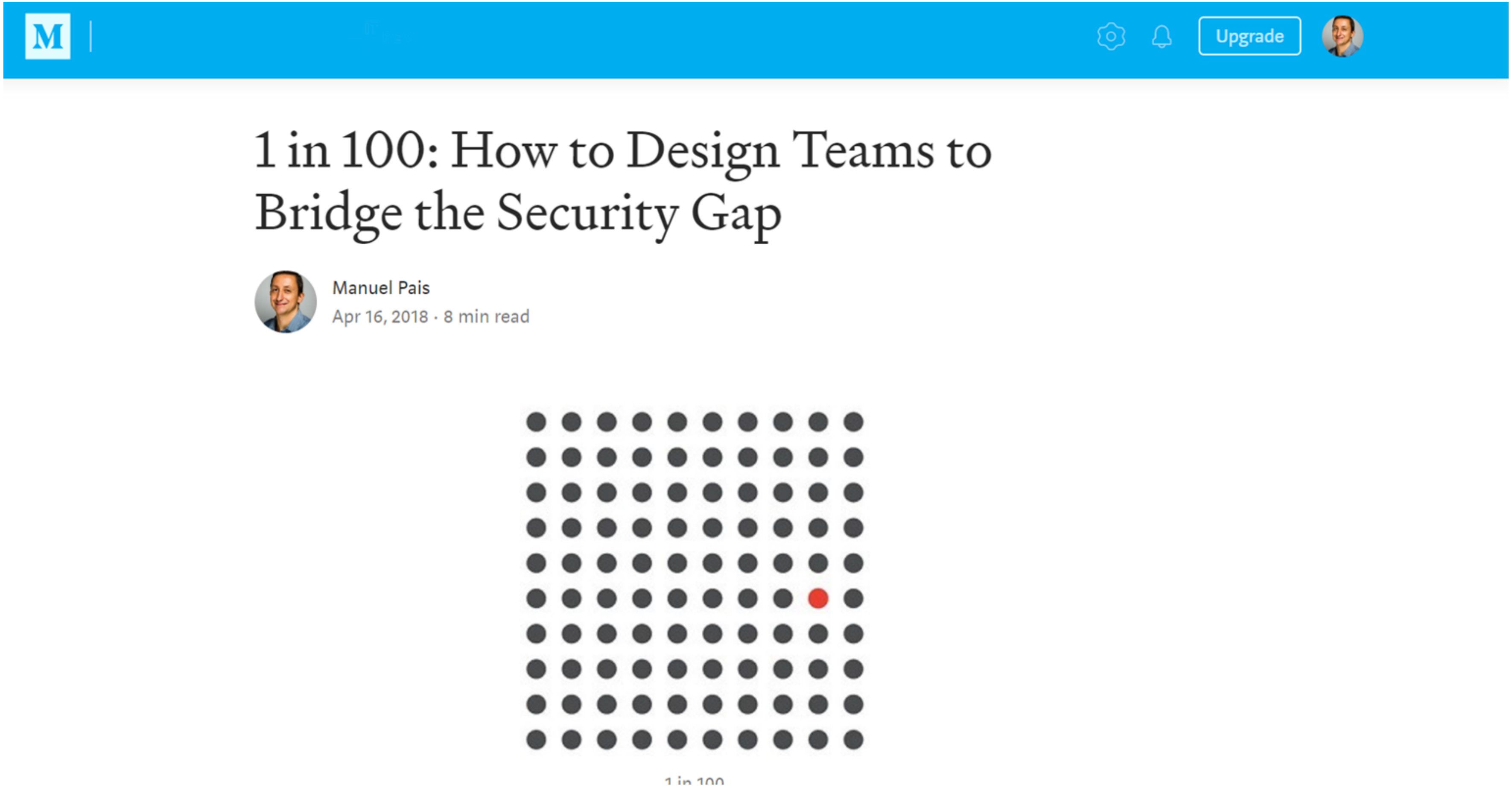
ALL DAY DEVOPS

NOVEMBER 6, 2019

Manuel Pais, Team Topologies

Beating the 1:100 Odds with Team Design for Security





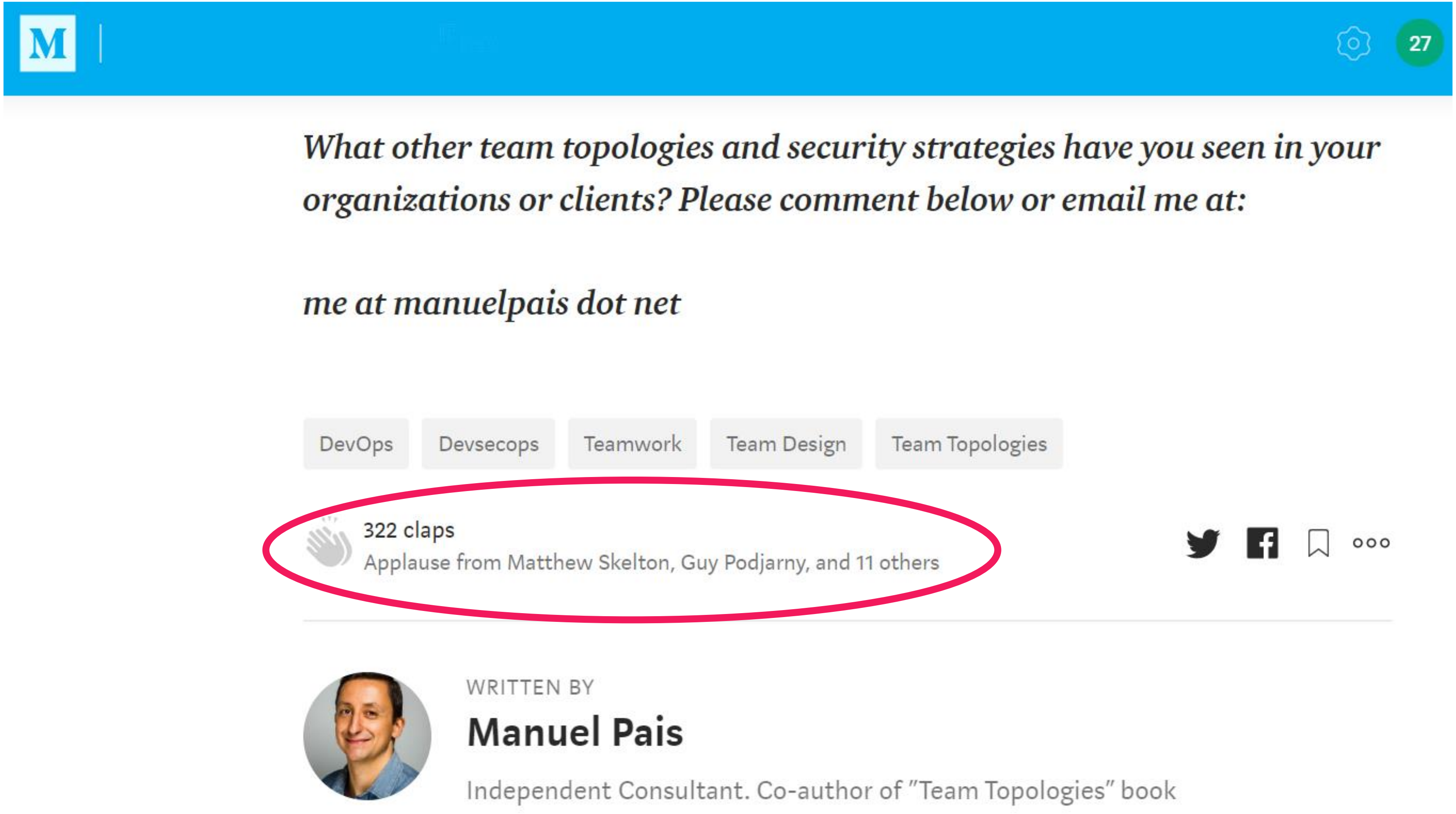
1 in 100: How to Design Teams to Bridge the Security Gap

Manuel Pais

Apr 16, 2018 · 8 min read

1 in 100

Source: https://medium.com/itrevolution/1-in-100-how-to-design-teams-to-bridge-the-security-gap-985f17ebb5cc

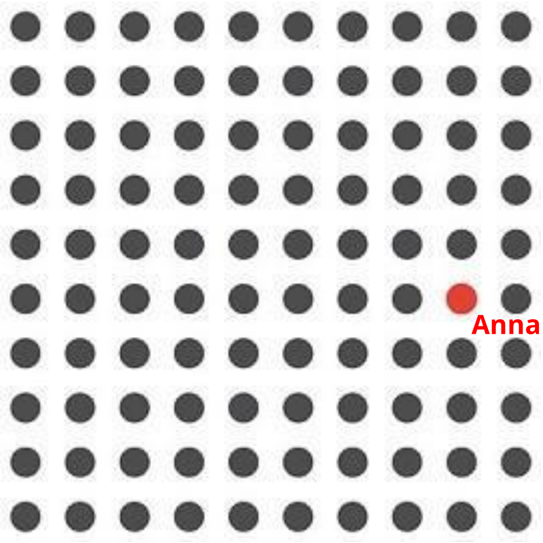


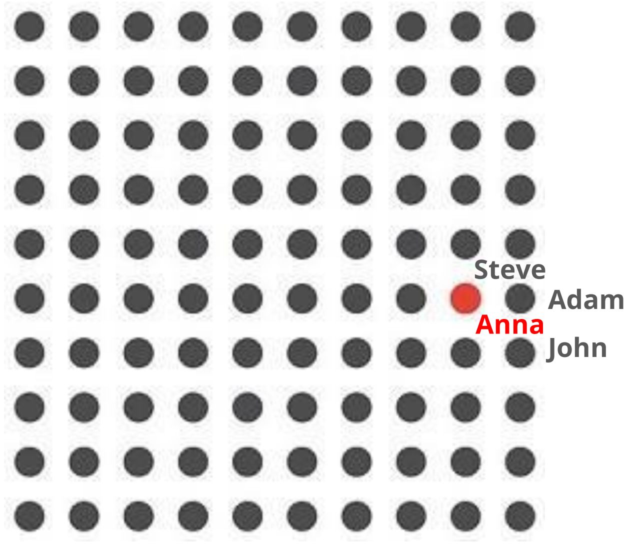
What other team topologies and security strategies have you seen in your organizations or clients? Please comment below or email me at:

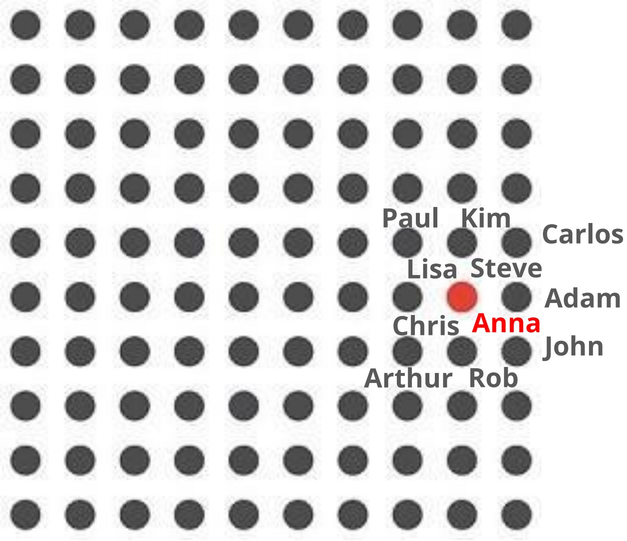
me at manuelpais dot net

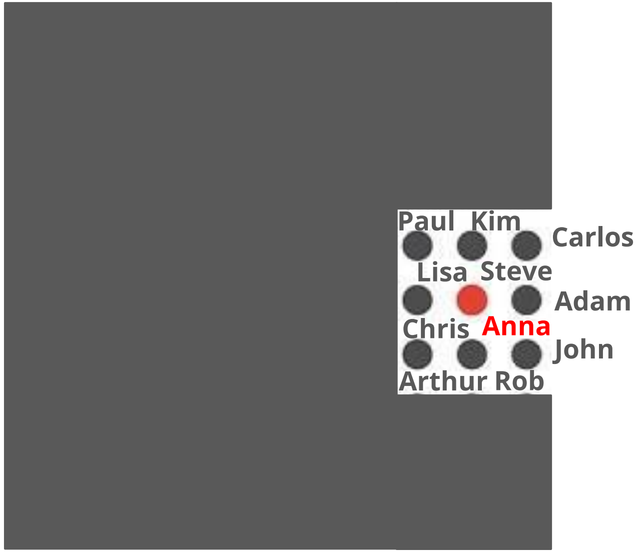
322 claps
Applause from Matthew Skelton, Guy Podjarny, and 11 others

WRITTEN BY
Manuel Pais
Independent Consultant. Co-author of "Team Topologies" book


Anna


Steve
Adam
Anna
John


Paul
Kim
Carlos
Lisa
Steve
Adam
Chris
Anna
John
Arthur
Rob


Paul
Kim
Carlos
Lisa
Steve
Adam
Chris
Anna
John
Arthur
Rob

Security team

Source: https://www.ona.ca/blog/cyber-security-insurance-ottawa/#.XcAZODNKhPY

Security team

Source: https://www.ona.ca/blog/cyber-security-insurance-ottawa/#.XcAZODNKhPY

Product team

Security team

VULNERABILITY CHECKING

SECURE CODE ANALYSIS

SCAN ARTIFACTS

CLOSED PORTS

AUTHENTICATION & AUTHORIZATION

SECRETS MANAGEMENT

Product team

Security team

Team Topologies

VULNERABILITY CHECKING

SECURE CODE ANALYSIS

SCAN ARTIFACTS

CLOSED PORTS

AUTHENTICATION & AUTHORIZATION

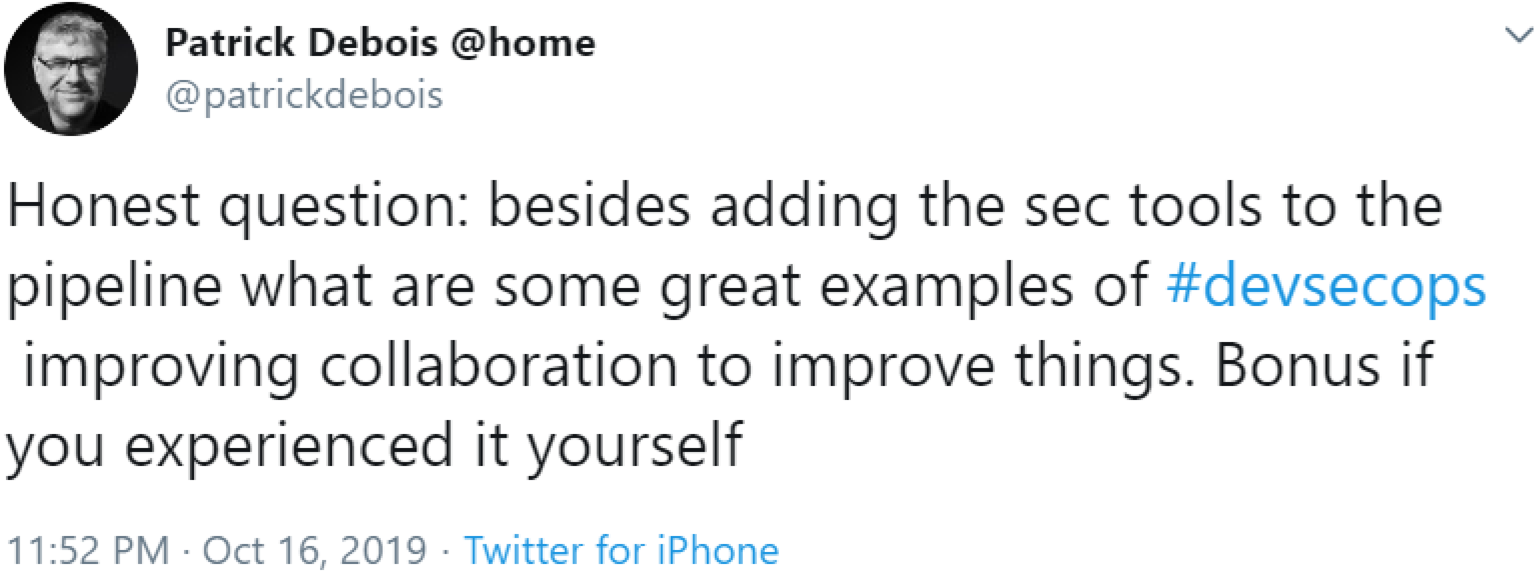
SECRETS MANAGEMENT

OWASP TOP 10

Product team

Security team

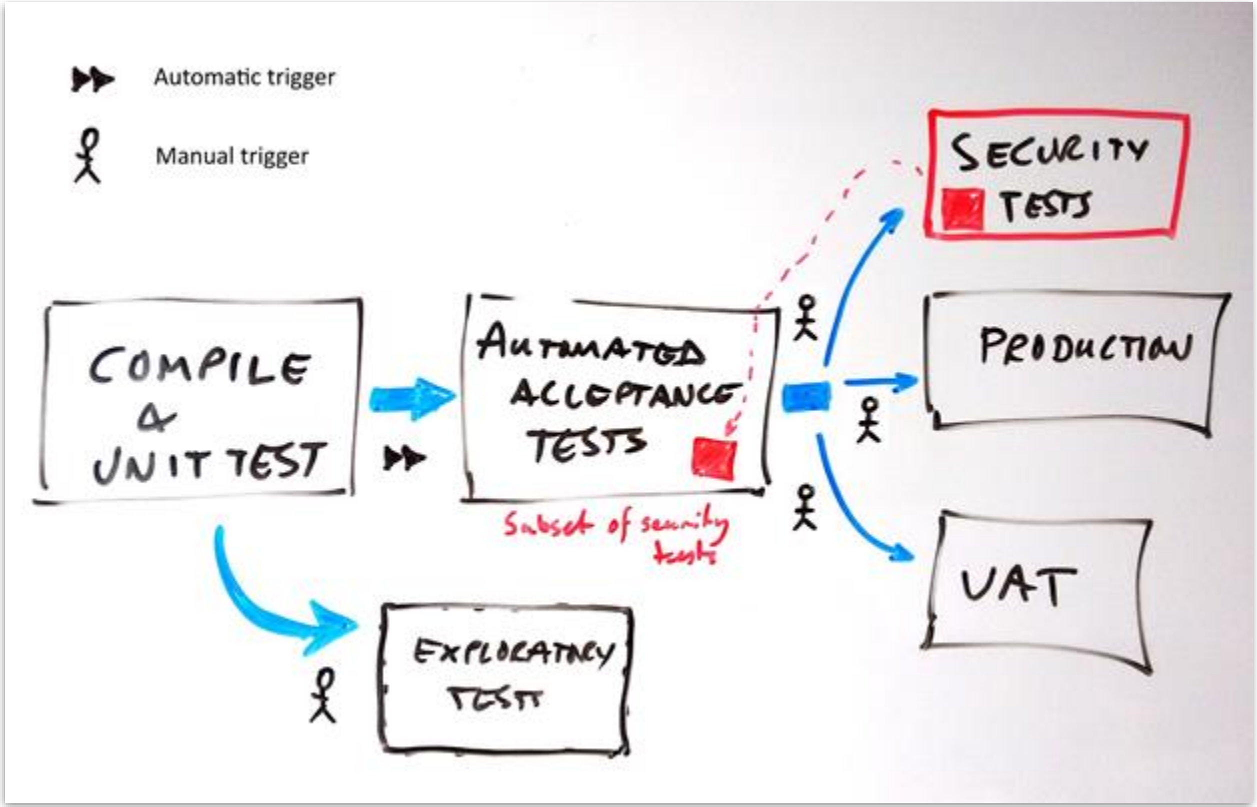
Team Topologies



Patrick Debois @home
@patrickdebois

Honest question: besides adding the sec tools to the pipeline what are some great examples of #devsecops improving collaboration to improve things. Bonus if you experienced it yourself

11:52 PM · Oct 16, 2019 · Twitter for iPhone



Automatic trigger
Manual trigger
COMPILE & UNIT TEST
AUTOMATED ACCEPTANCE TESTS
Subset of security tests
EXPLORATORY TESTS
SECURITY TESTS
PRODUCTION
UAT

Securing a Continuous Delivery Pipeline

BY MATTHEW SKELTON & MANUEL PAIS

Team Topologies

QUICK VIEW

01
With a collaborative mindset, security officers, developers, and testers can come together and help each other with their respective gaps in knowledge and experience.

02
At an early stage it might be advisable to keep manual security controls in the delivery pipeline.

03
Tools and practices alone don't lead to more secure systems; we also need frequent and open communication, feedback, and empathy for other people.

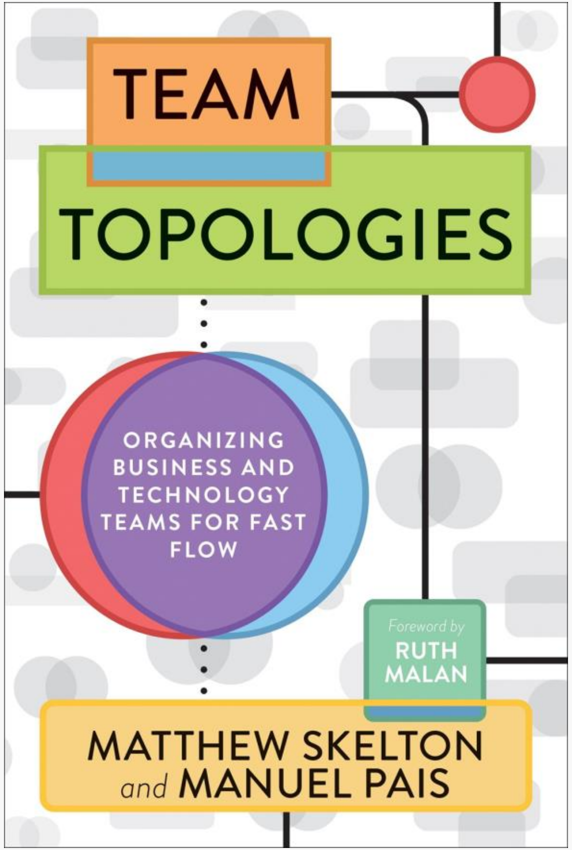
Team Topologies

Organizing business and technology teams for fast flow

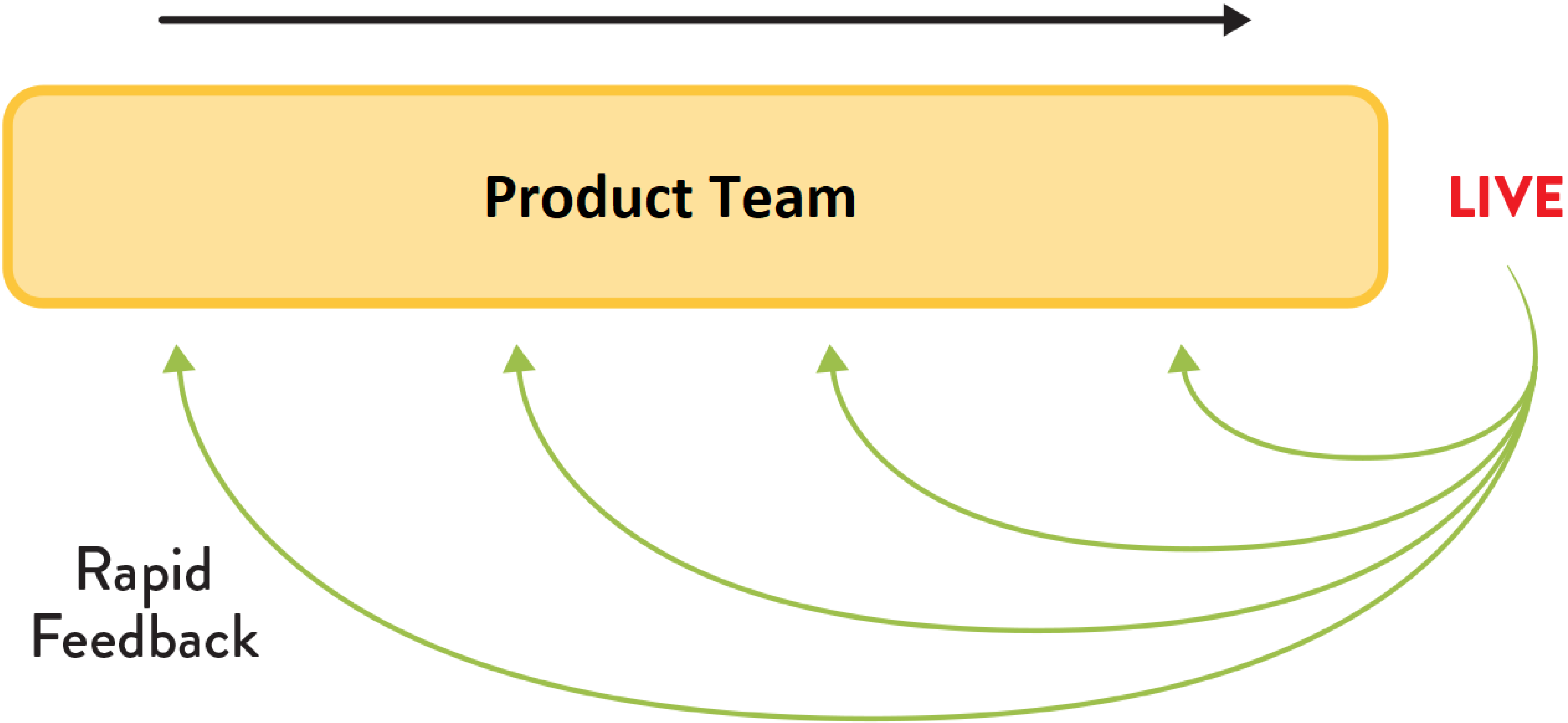
Matthew Skelton & Manuel Pais

IT Revolution Press (2019)

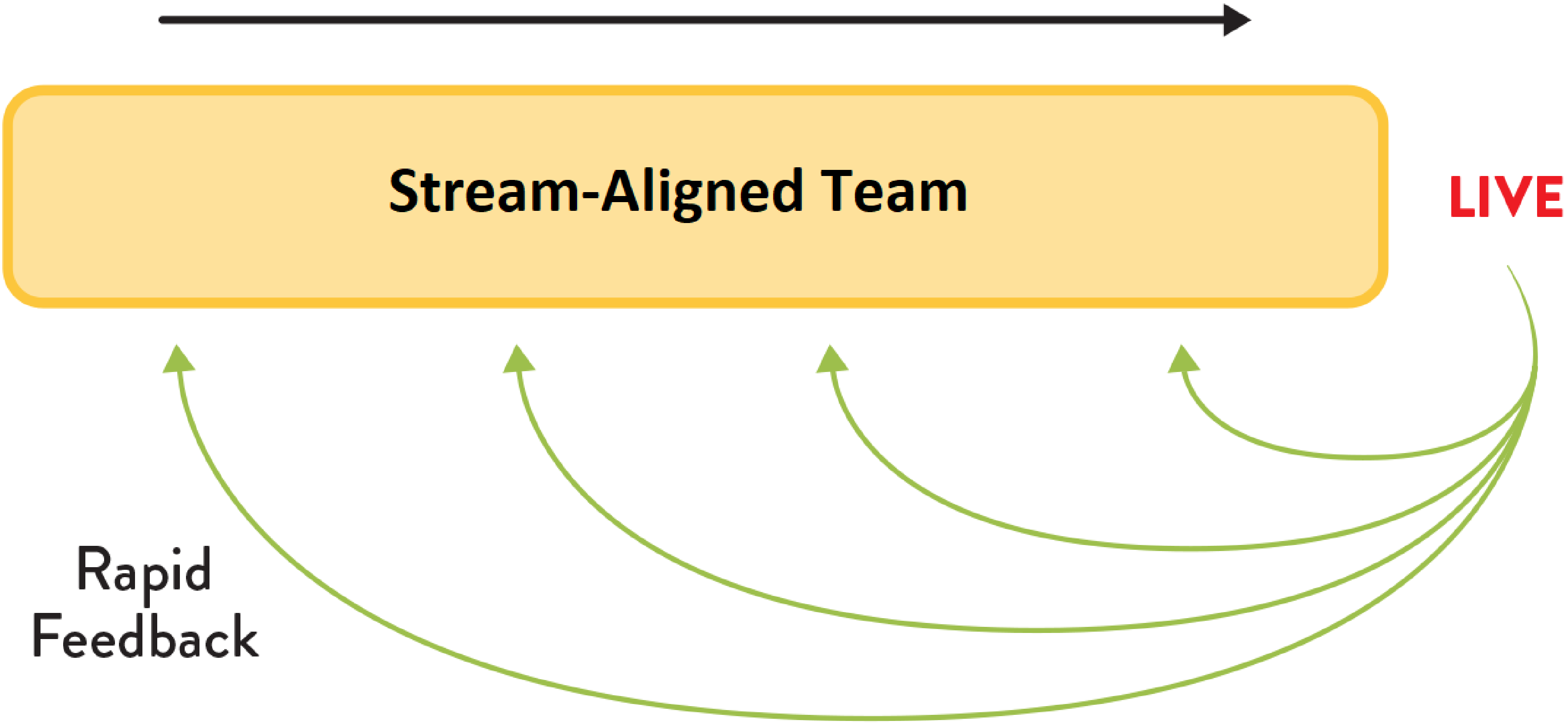
https://teamtopologies.com



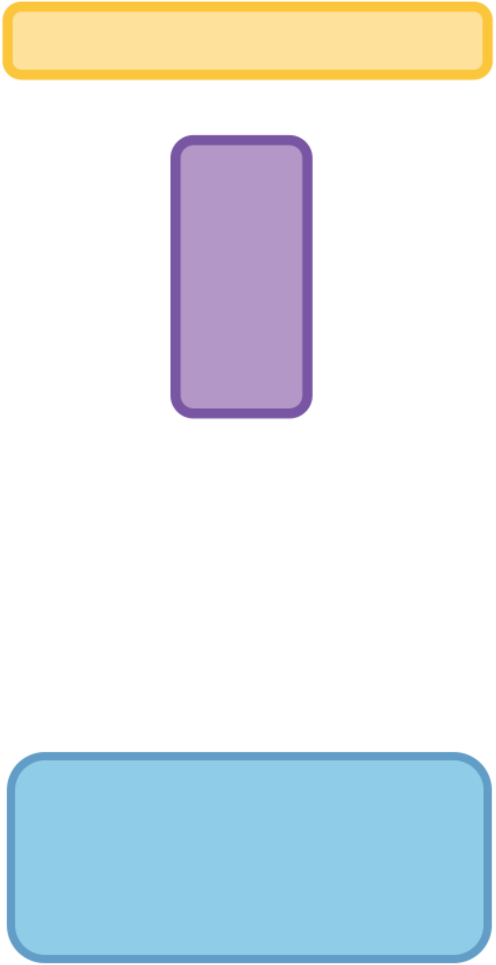
Team Topologies



Rapid Feedback



Team Topologies



Stream-aligned team

Enabling team

Platform team

Image by Dimitris Vetsikas from Pixabay

Enabling Purpose

orbit around stream-aligned teams

Enabling Purpose

team of **security** experts to detect and help bridge gaps

Enabling Purpose

reduce dependencies on **security** experts by teaching rather than doing the work

Enabling Behaviors

regular checkpoints
with stream-aligned team

jointly agree when more
collaboration is needed

Enabling Behaviors

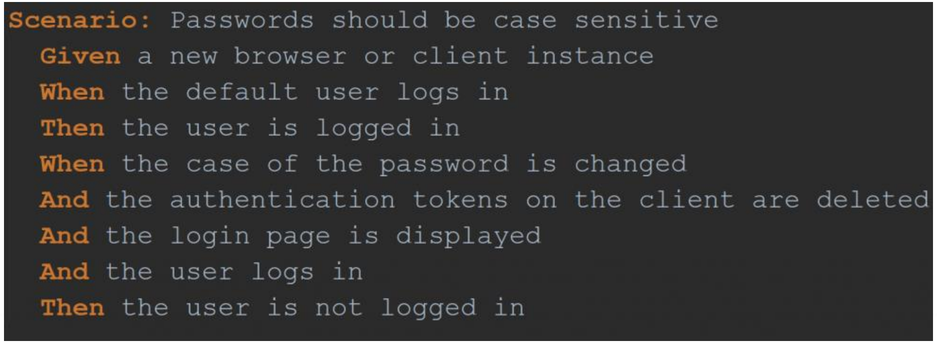
stay on top of new security

- strategies
- practices
- tools
- frameworks
- threats / behaviors

GAUNTLT

BE MEAN TO YOUR CODE AND LIKE IT

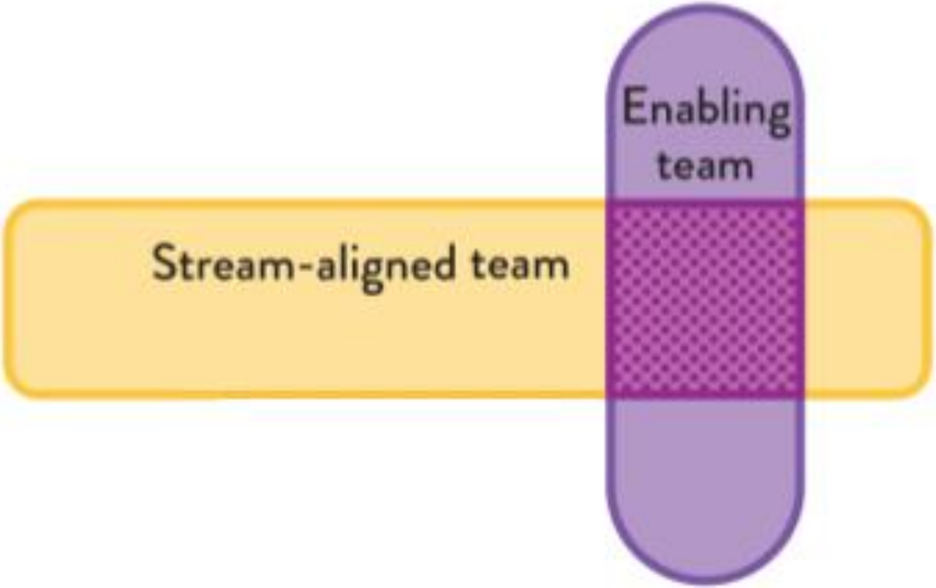
```
Scenario: Check standard web ports
  When I launch an "nmap" attack with:
    """
    nmap -F <hostname>
    """
  Then the output should match /80.tcp\s+open/
  Then the output should not match:
    """
    25\/tcp\s+open
    """
```

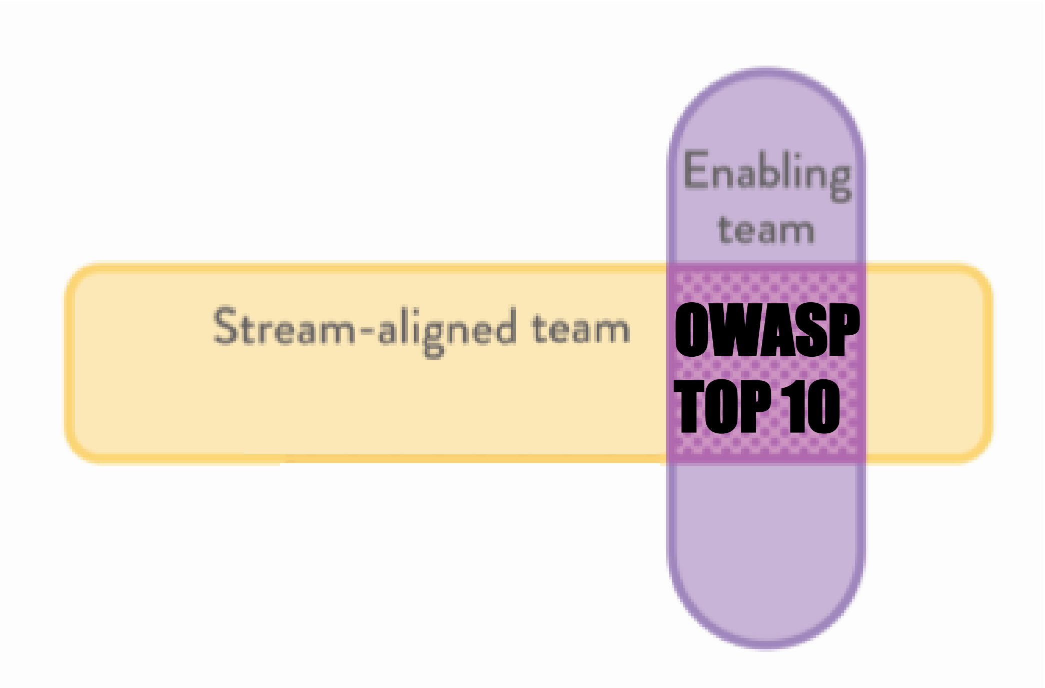


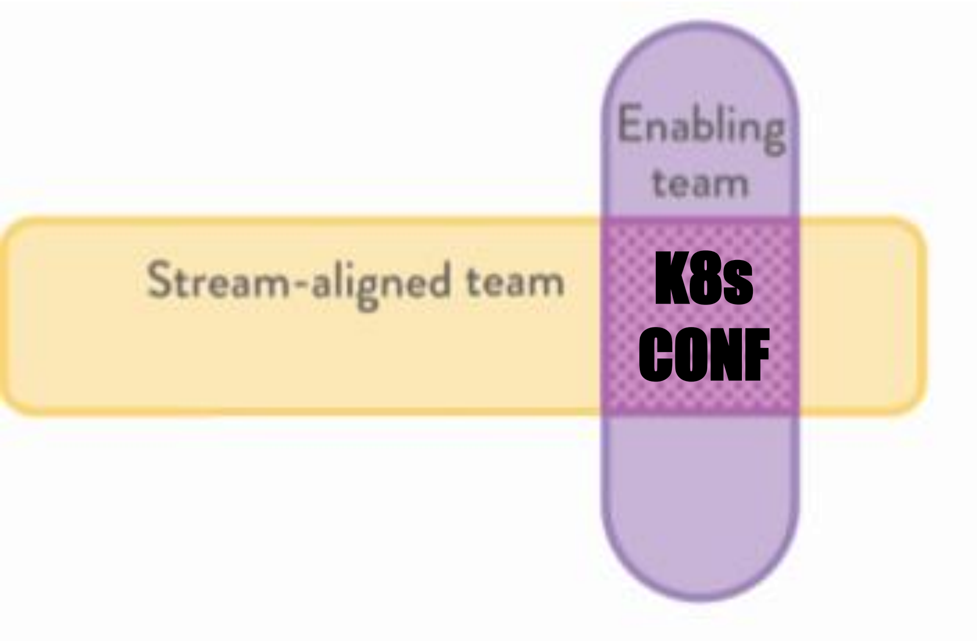
```
Scenario: Passwords should be case sensitive
  Given a new browser or client instance
  When the default user logs in
  Then the user is logged in
  When the case of the password is changed
  And the authentication tokens on the client are deleted
  And the login page is displayed
  And the user logs in
  Then the user is not logged in
```

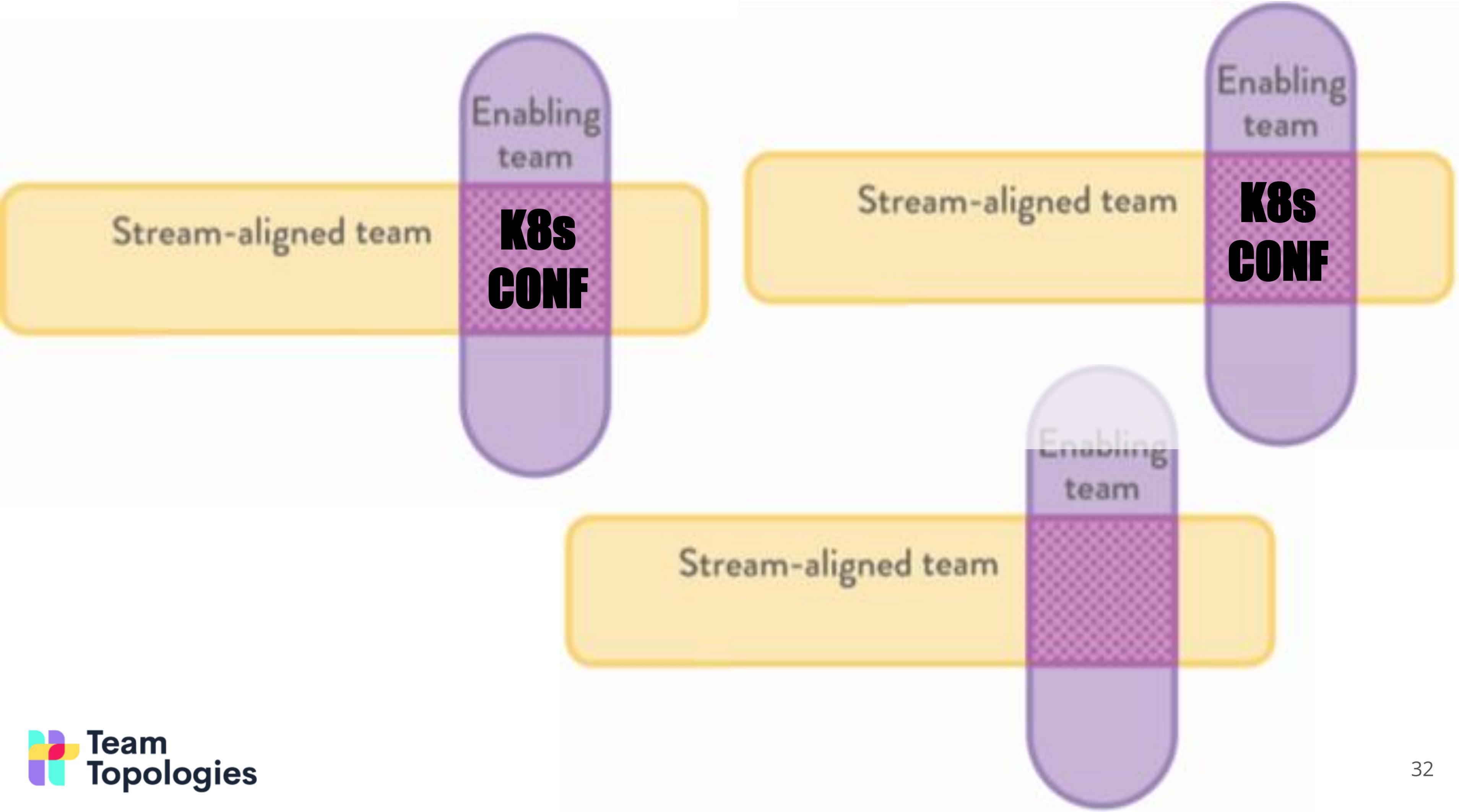
BDD-security

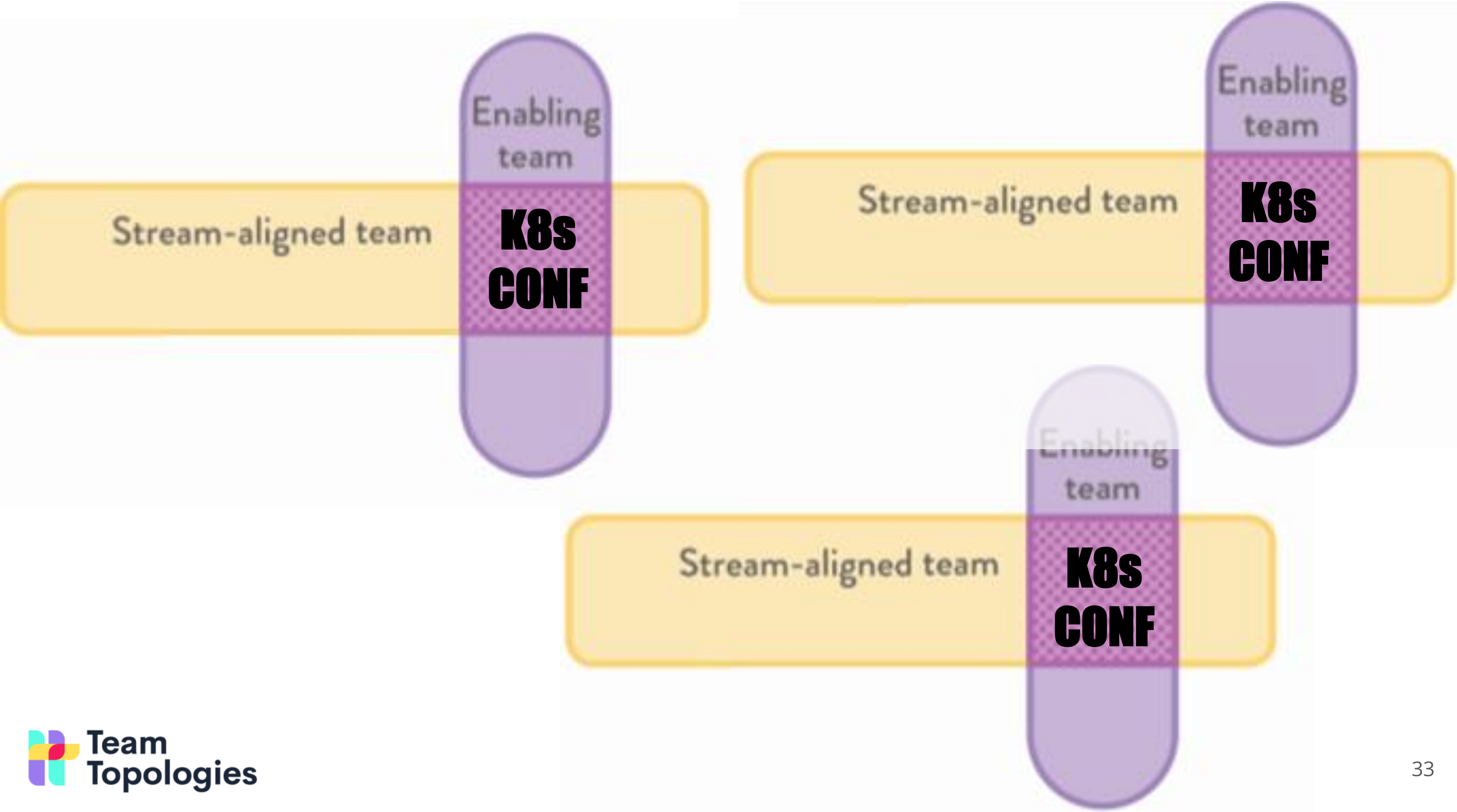
Team Topologies

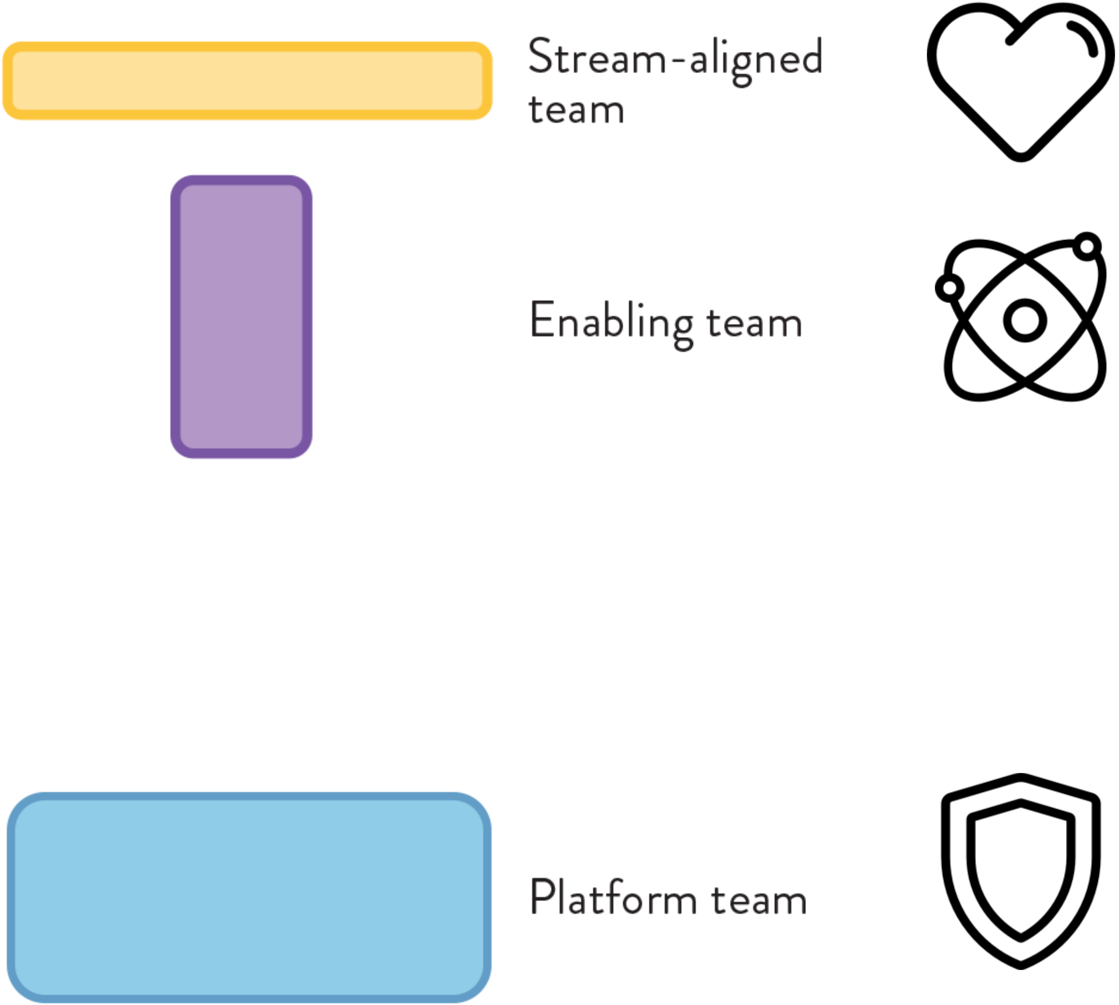

Enabling team
Stream-aligned team


Enabling team
Stream-aligned team
OWASP TOP 10


Enabling team
Stream-aligned team
K8s CONF


Enabling team
Stream-aligned team
K8s CONF
Enabling team
Stream-aligned team
K8s CONF
Enabling team
Stream-aligned team


Enabling team
Stream-aligned team
K8s CONF
Enabling team
Stream-aligned team
K8s CONF
Enabling team
Stream-aligned team
K8s CONF

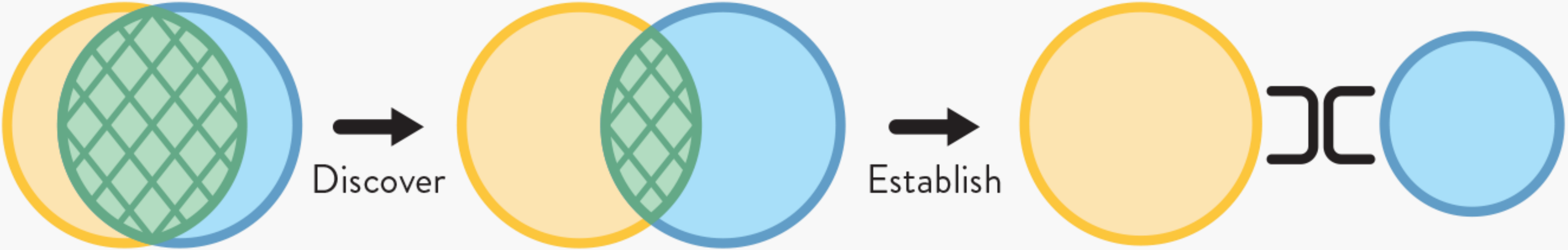


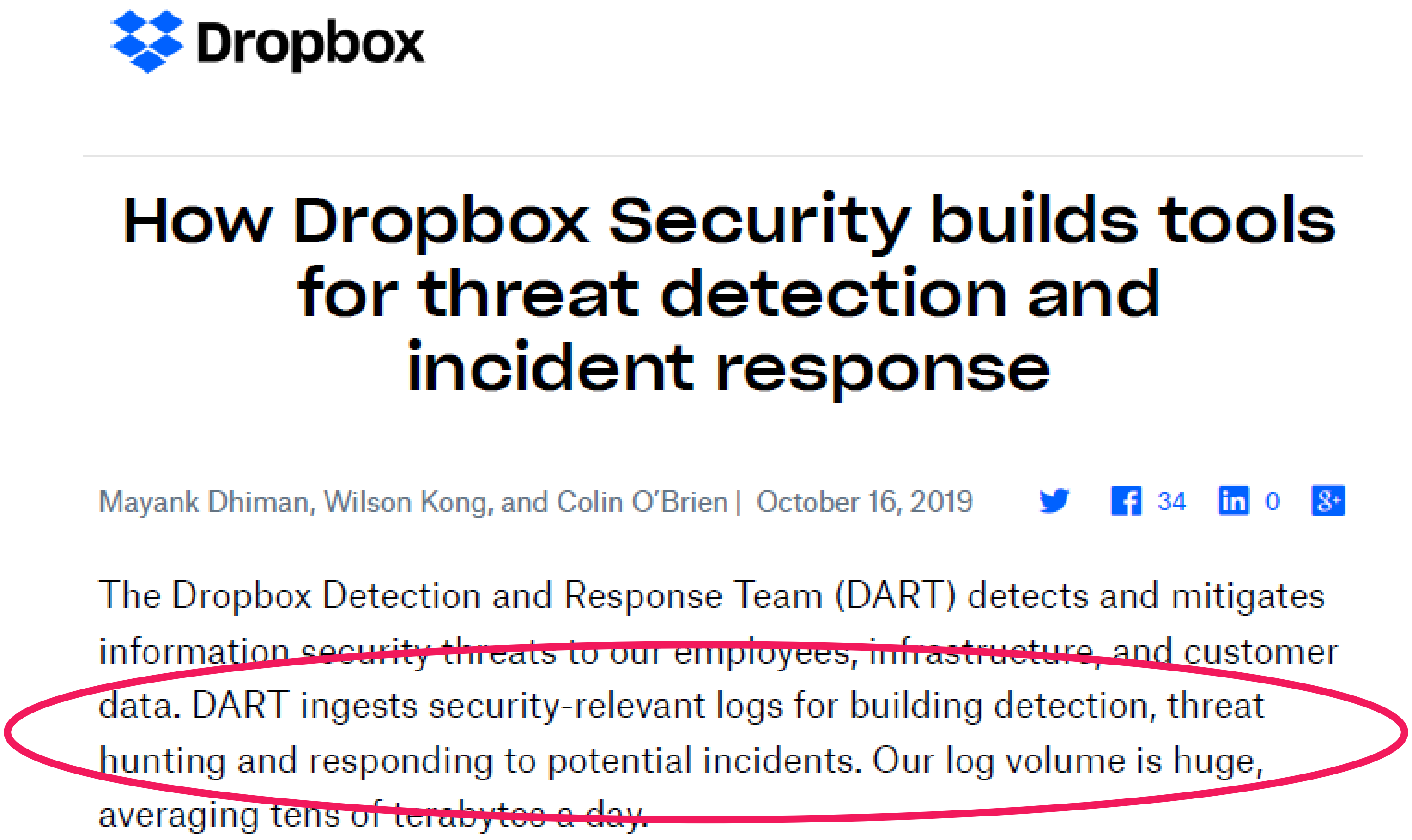
Stream-aligned team

Enabling team

Platform team

Discover useful patterns then push to platform (sensing for evolution)


Discover
Establish

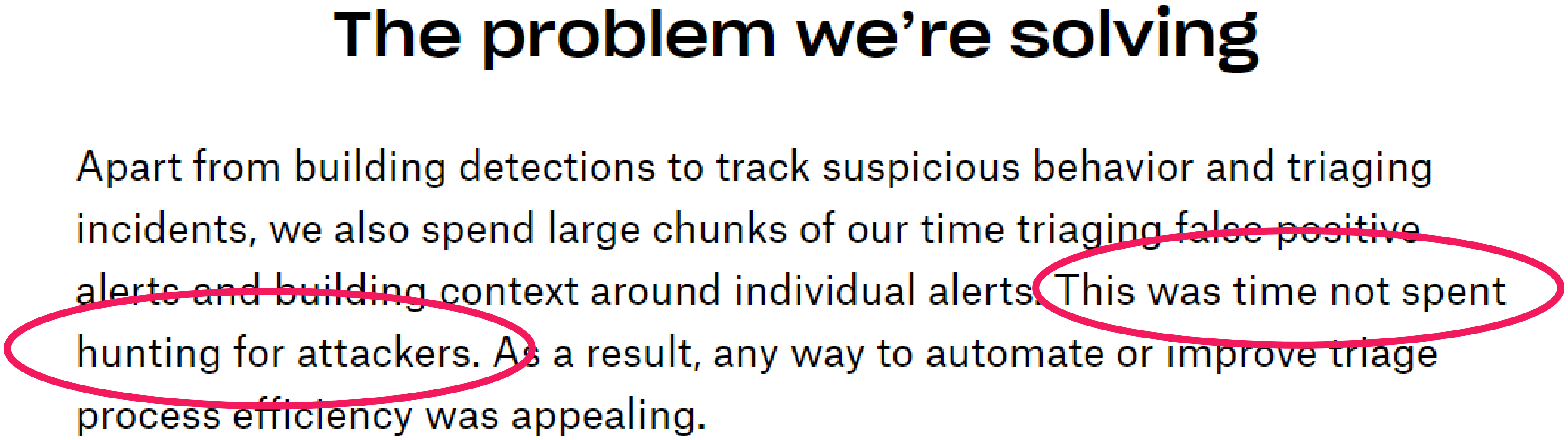


How Dropbox Security builds tools for threat detection and incident response

Mayank Dhiman, Wilson Kong, and Colin O'Brien | October 16, 2019

The Dropbox Detection and Response Team (DART) detects and mitigates information security threats to our employees, infrastructure, and customer data. DART ingests security-relevant logs for building detection, threat hunting and responding to potential incidents. Our log volume is huge, averaging tens of terabytes a day.

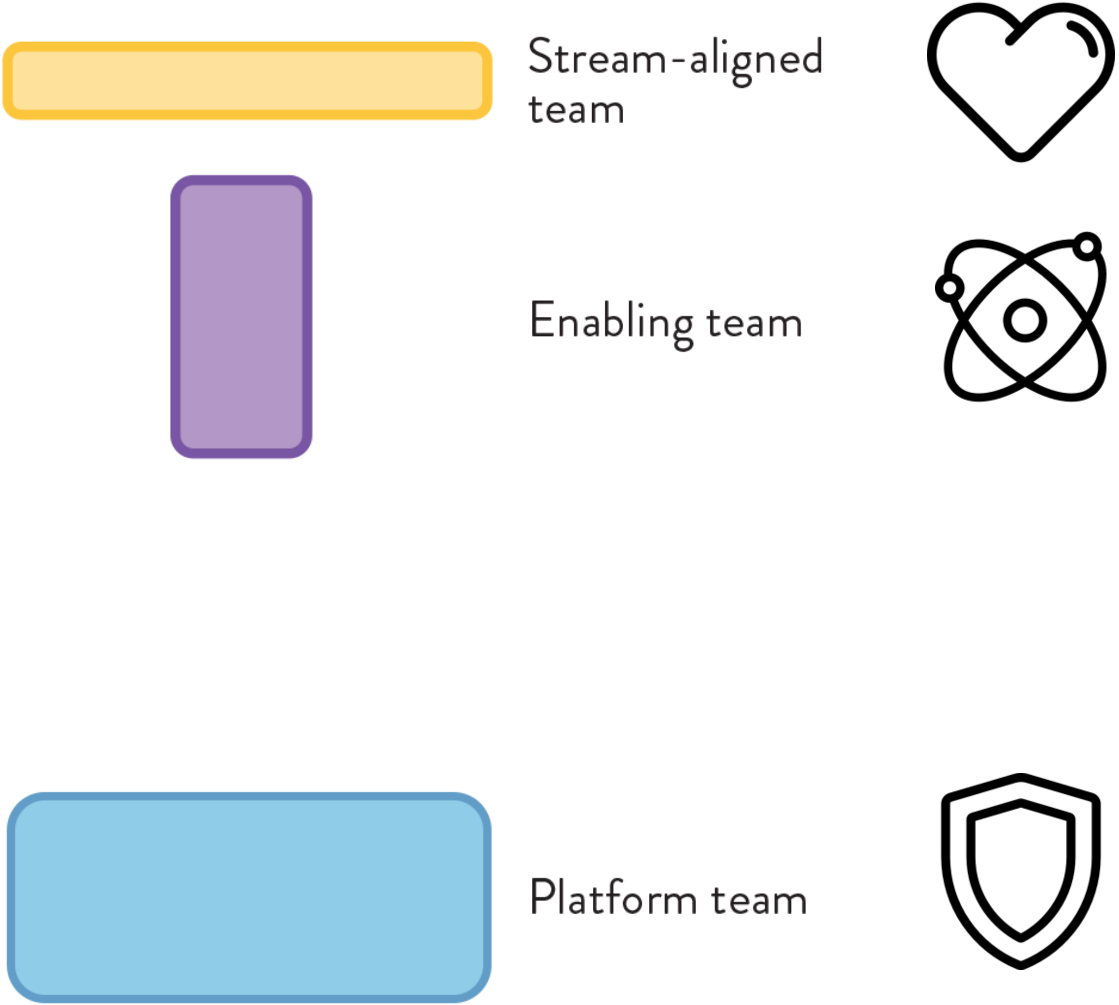
Source: https://blogs.dropbox.com/tech/2019/10/how-dropbox-security-builds-better-tools-for-threat-detection-and-incident-response/



The problem we're solving

Apart from building detections to track suspicious behavior and triaging incidents, we also spend large chunks of our time triaging false positive alerts and building context around individual alerts. This was time not spent hunting for attackers. As a result, any way to automate or improve triage process efficiency was appealing.

Source: https://blogs.dropbox.com/tech/2019/10/how-dropbox-security-builds-better-tools-for-threat-detection-and-incident-response/

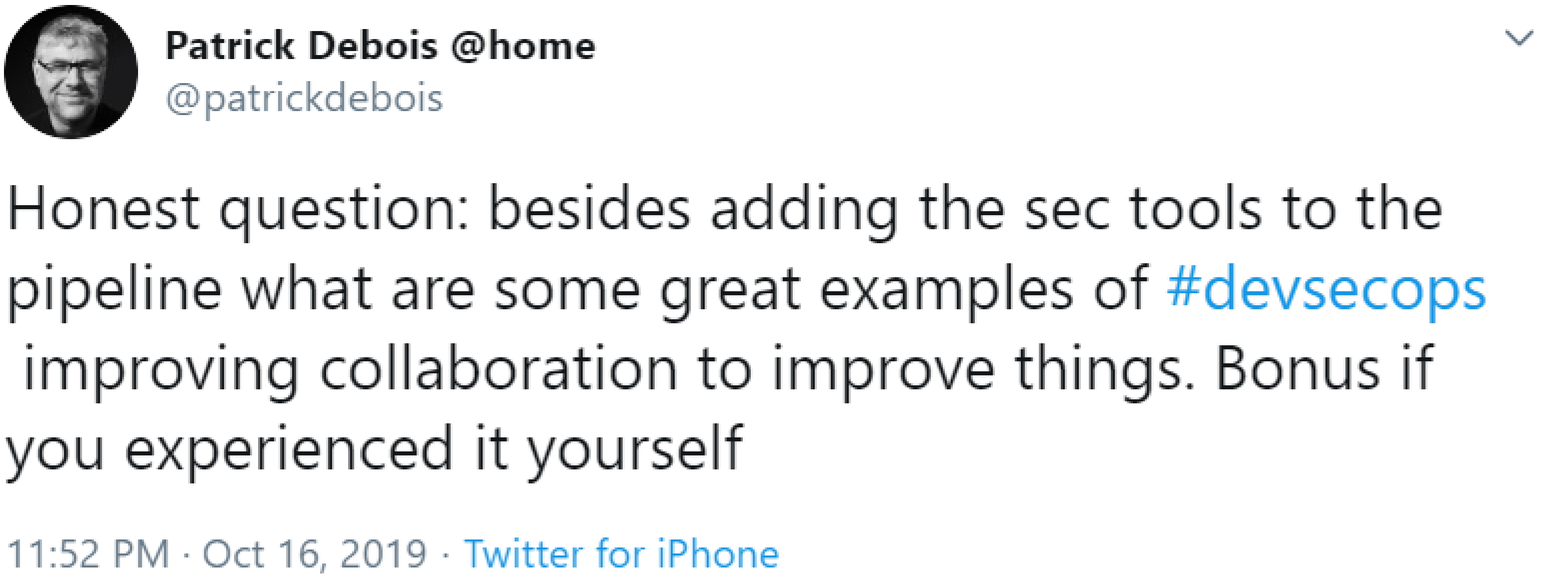


Stream-aligned team

Enabling team

Platform team

https://twitter.com/patrickdebois/status/1184587947607314433



Patrick Debois @home
@patrickdebois

Honest question: besides adding the sec tools to the pipeline what are some great examples of #devsecops improving collaboration to improve things. Bonus if you experienced it yourself

11:52 PM · Oct 16, 2019 · Twitter for iPhone

Security team

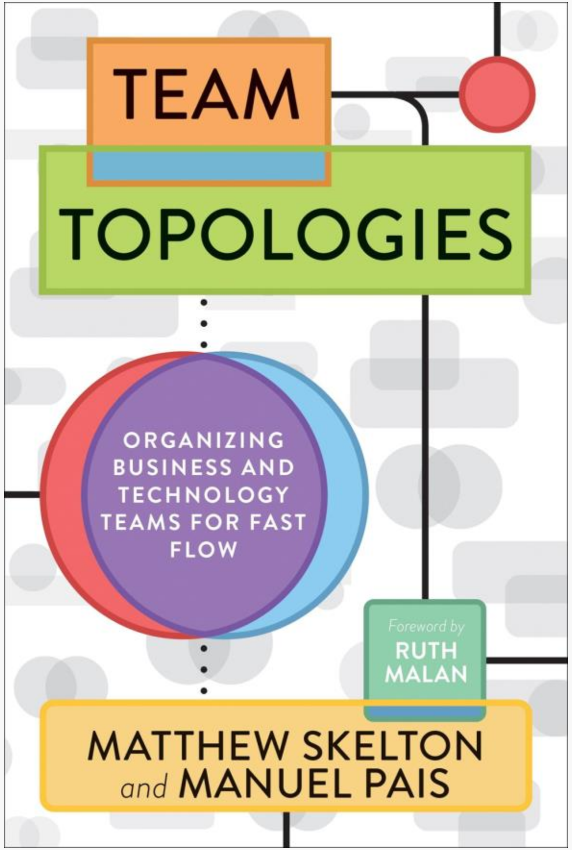
Team Topologies

Organizing business and technology teams for fast flow

Matthew Skelton & Manuel Pais

IT Revolution Press (2019)

https://teamtopologies.com



Team Topologies

Training

1-day training

Team Topologies

FUNDAMENTALS

1-day advanced training

Team Topologies

DEEP DIVE

1-day advanced workshop

Team Topologies

APPLYING IN CONTEXT

Day 1
Fundamentals

Day 2
Deep Dive

Day 3
Applying in Context

teamtopologies.com/training

Thank you!

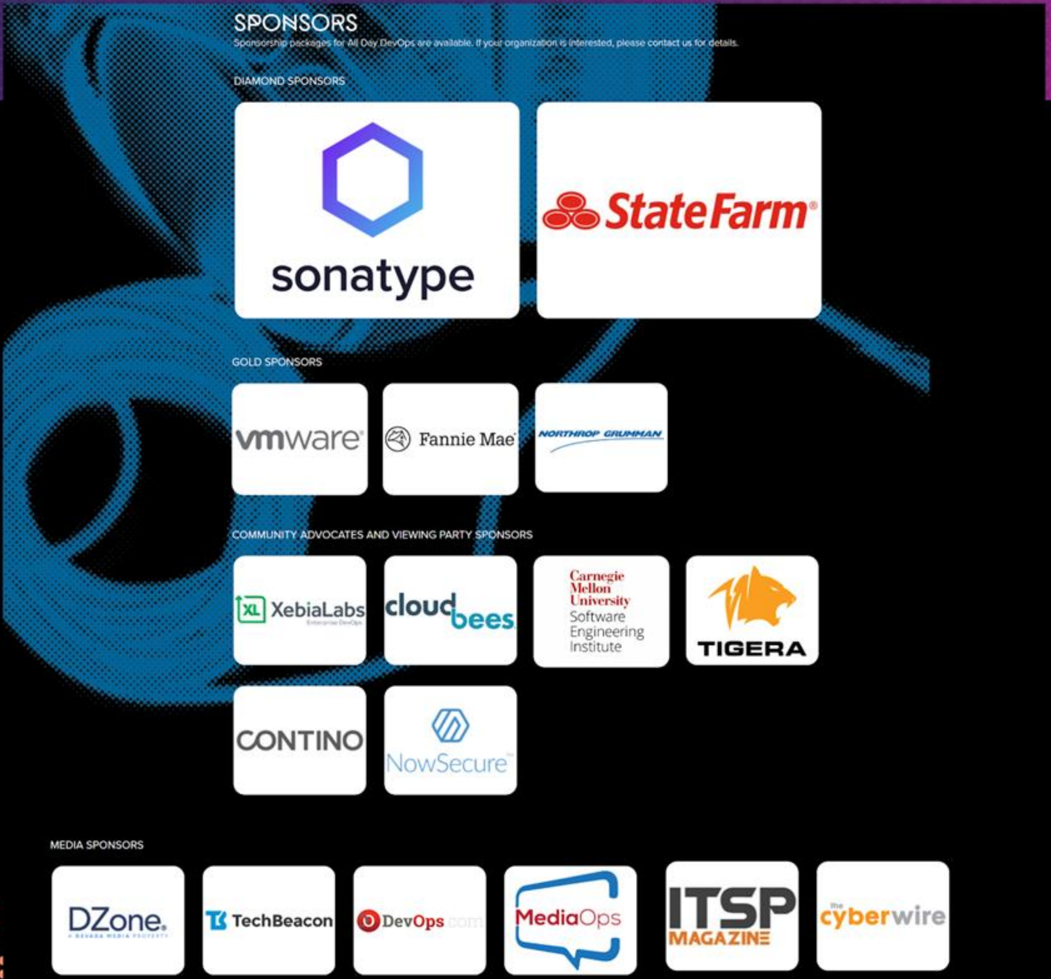
teamtopologies.com

Matthew Skelton, Conflux
@matthewpskelton

Manuel Pais, Independent
@manupaisable

Team Topologies

Icons made by Freepick from www.flaticon.com - used under license



SPONSORS

Sponsorship packages for All Day DevOps are available. If your organization is interested, please contact us for details.

DIAMOND SPONSORS

sonatype

State Farm®

GOLD SPONSORS

vmware®

Fannie Mae

NORTHROP GRUMMAN

COMMUNITY ADVOCATES AND VIEWING PARTY SPONSORS

XL XebiaLabs
Enterprise DevOps

cloudbees

Carnegie Mellon University
Software Engineering Institute

TIGERA

CONTINO

NowSecure™

MEDIA SPONSORS

DZone.
A DEVADA MEDIA PROPERTY

TechBeacon

DevOps.com

MediaOps

ITSP MAGAZINE

the cyberwire