The Three Faces of DevSecOps

Guy Podjarny (@guypod)

About Me

- CEO & Co-Founder at Snyk
  - Find & Fix vulnerabilities in open source dependencies!
- Founder @Blaze, CTO @Akamai
- Security work since 1997
- DevOps & Performance since 2010
- Speaker, writer, communicator

We all love **DevOps!**

… but why?

DevOps helps

deliver value and adapt to market needs faster and at scale

What does “Doing DevOps” mean?

1. DevOps Technologies
2. DevOps Methodologies
3. DevOps Shared Ownership

So… what does **DevSecOps** mean?

1. Securing DevOps Technologies
2. Security in DevOps Methodologies
3. Include Security in DevOps Shared Ownership

Securing
DevOps Technologies

DevOps created or drove use of **New Technologies**

Cloud

Containers

Serverless

Open Source Libraries

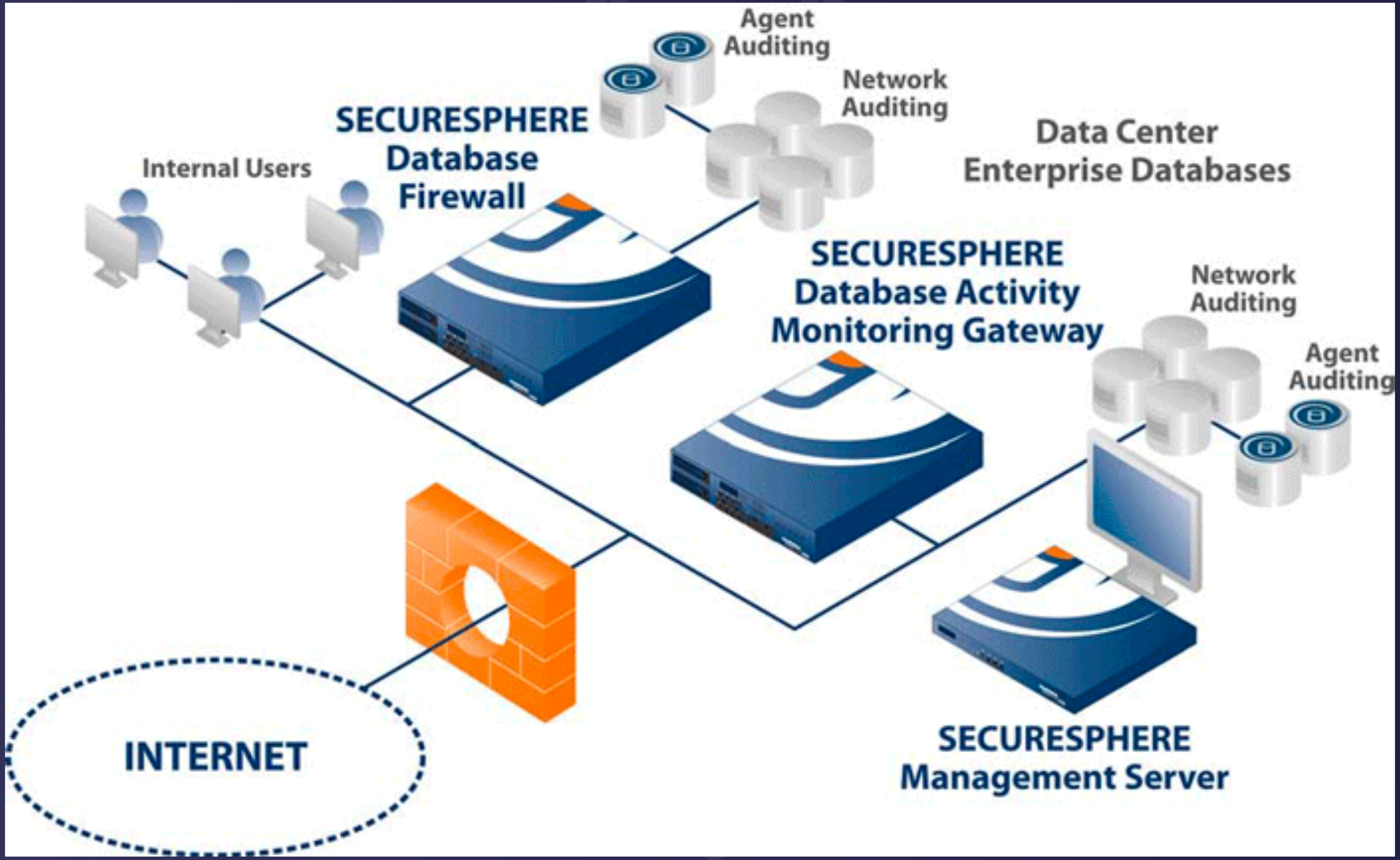
Creates
Two Types of Problems
for security

First, Security solutions

Often Don’t work

in the new surrounding

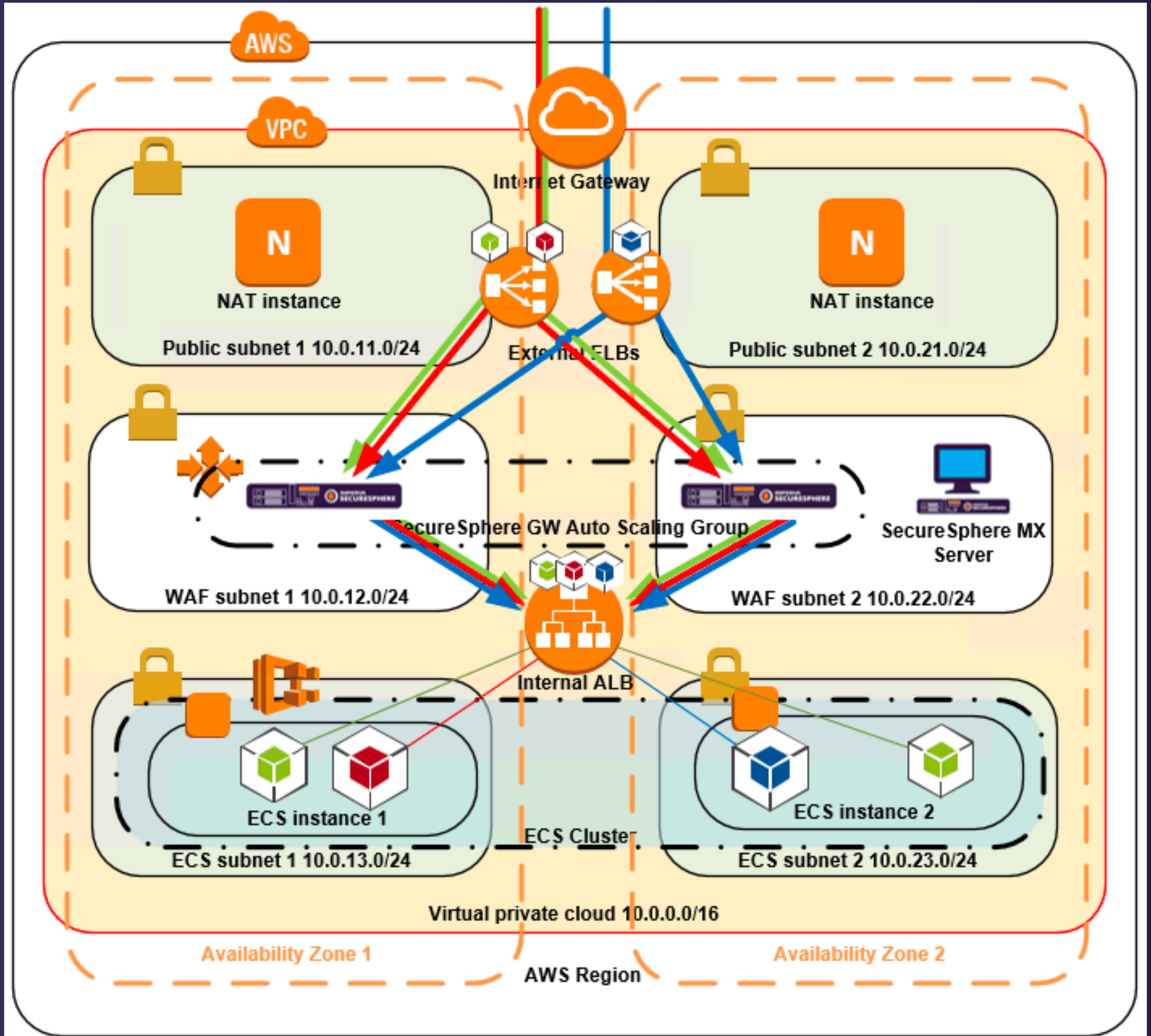
Web App Firewall


Agent Auditing
Network Auditing
SECURESPHERE Database Firewall
Internal Users
Data Center Enterprise Databases
SECURESPHERE Database Activity Monitoring Gateway
Network Auditing
Agent Auditing
INTERNET
SECURESPHERE Management Server

Traditionally an appliance

How do you use **block web attacks** when the applications you protect **auto-scale?**

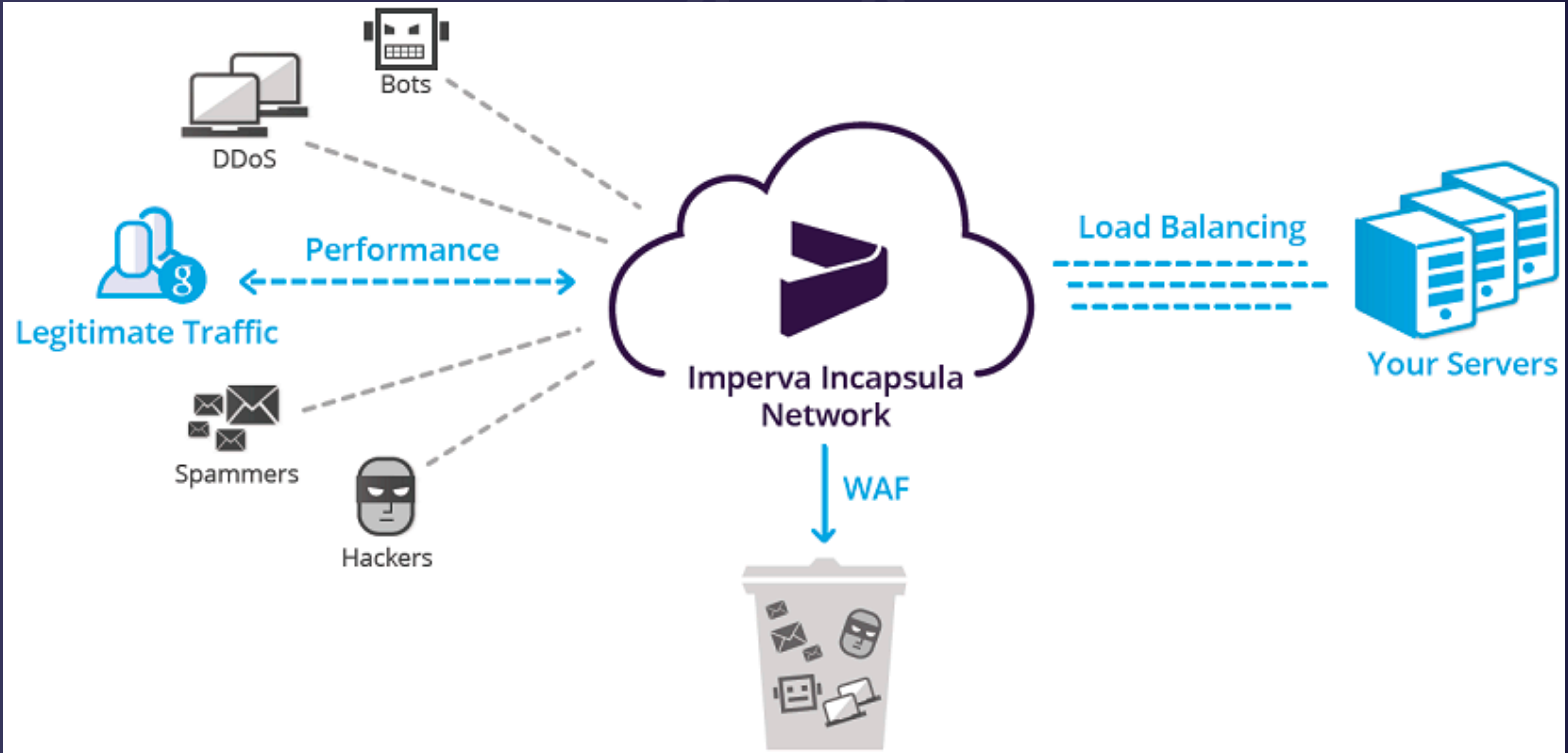
WAF that Auto-Scales


AWS
VPC
Internet Gateway
N
NAT instance
Public subnet 1 10.0.11.0/24
N
NAT instance
Public subnet 2 10.0.21.0/24
External ELBs
SecureSphere GW Auto Scaling Group
SecureSphere MX Server
WAF subnet 1 10.0.12.0/24
WAF subnet 2 10.0.22.0/24
Internal ALB
ECS instance 1
ECS instance 2
ECS Cluster
ECS subnet 1 10.0.13.0/24
ECS subnet 2 10.0.23.0/24
Virtual private cloud 10.0.0.0/16
Availability Zone 1
Availability Zone 2
AWS Region

@guypod

snyk

WAF as a Service

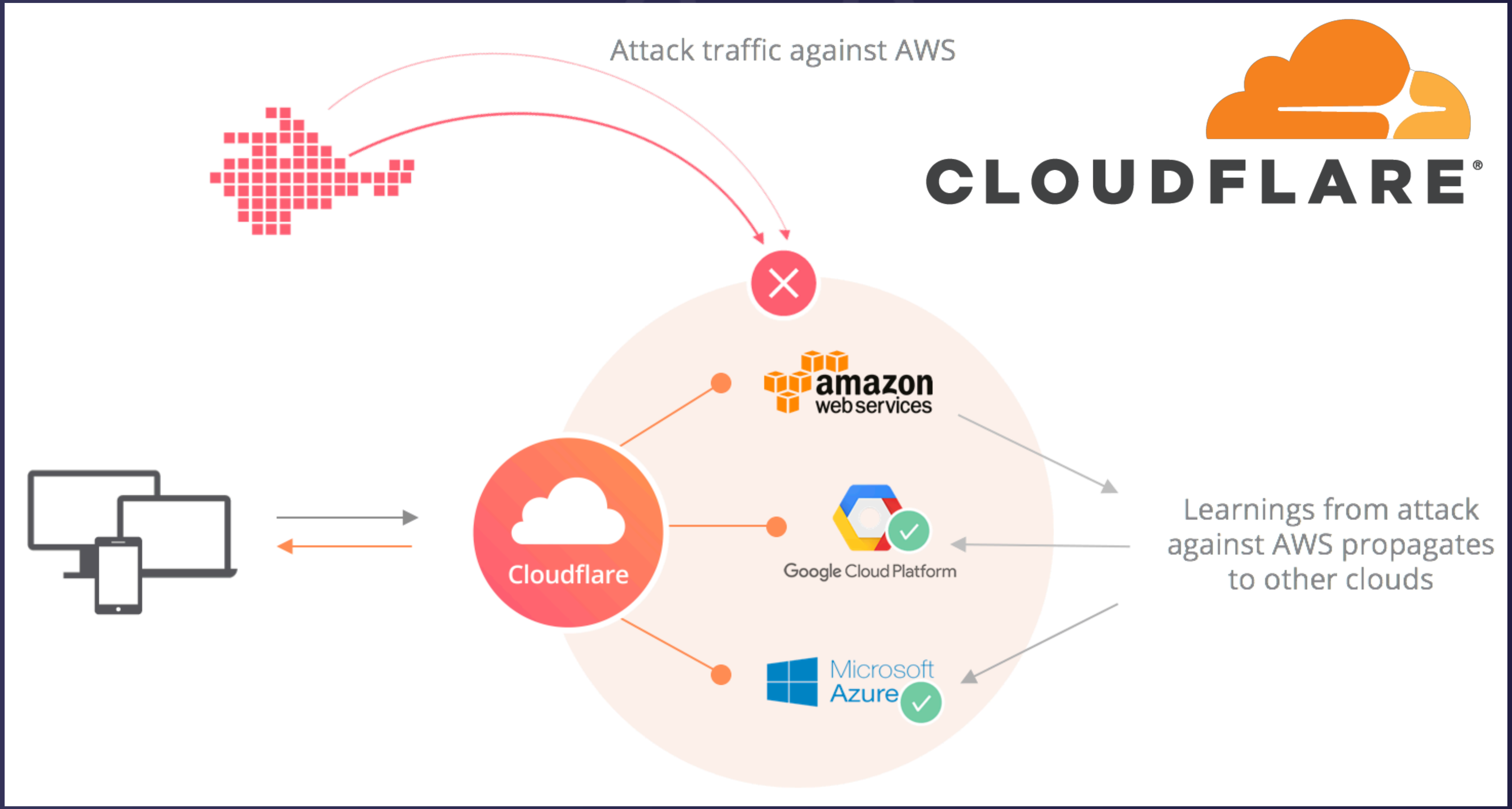


@guypod

snyk

The need to adapt is **an opportunity** for new players

WAF as *part of a* Service

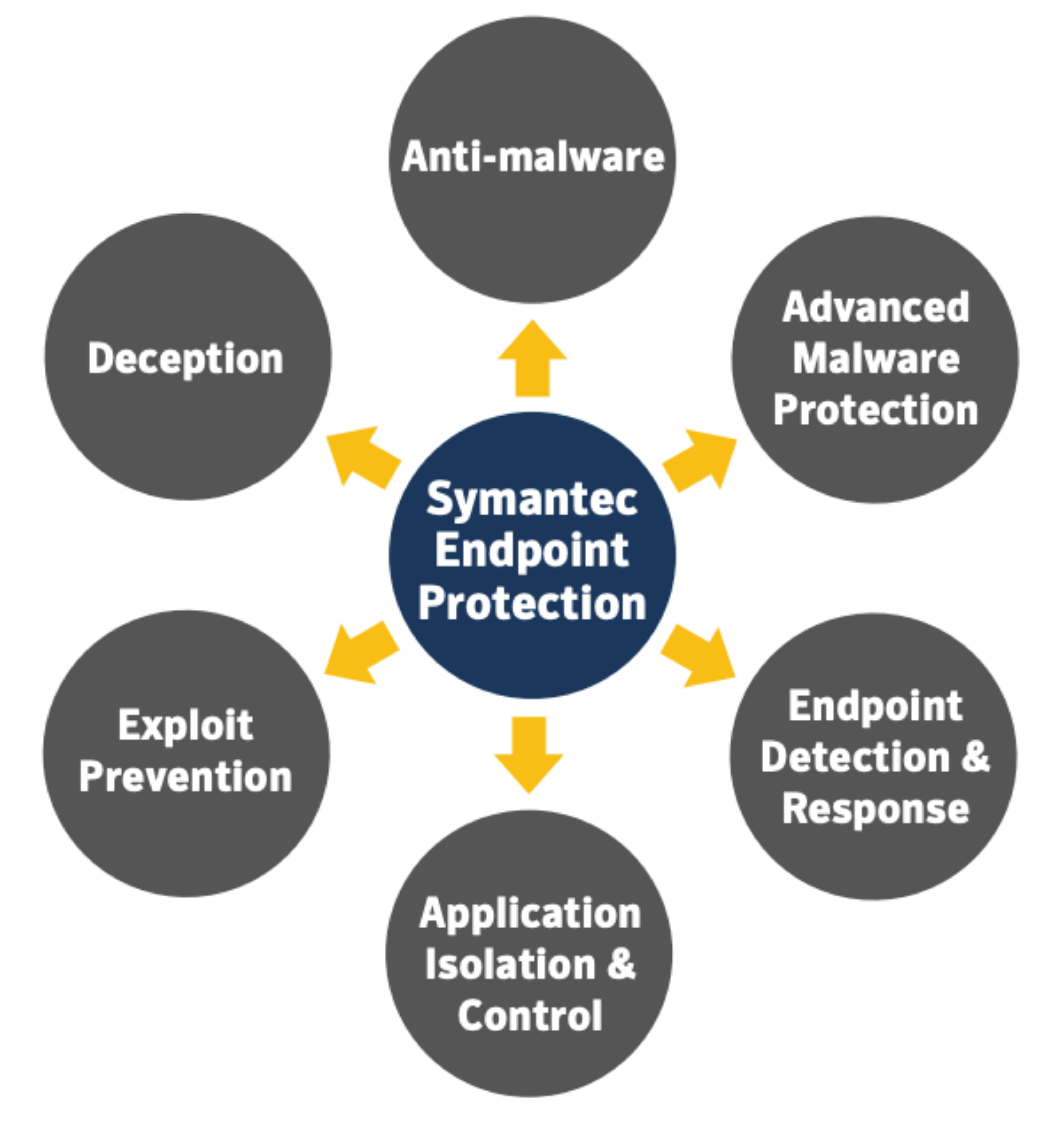

Attack traffic against AWS
CLOUDFLARE
Cloudflare
amazon web services
Google Cloud Platform
Microsoft Azure
Learnings from attack against AWS propagates to other clouds

@guypod

Another trouble maker:

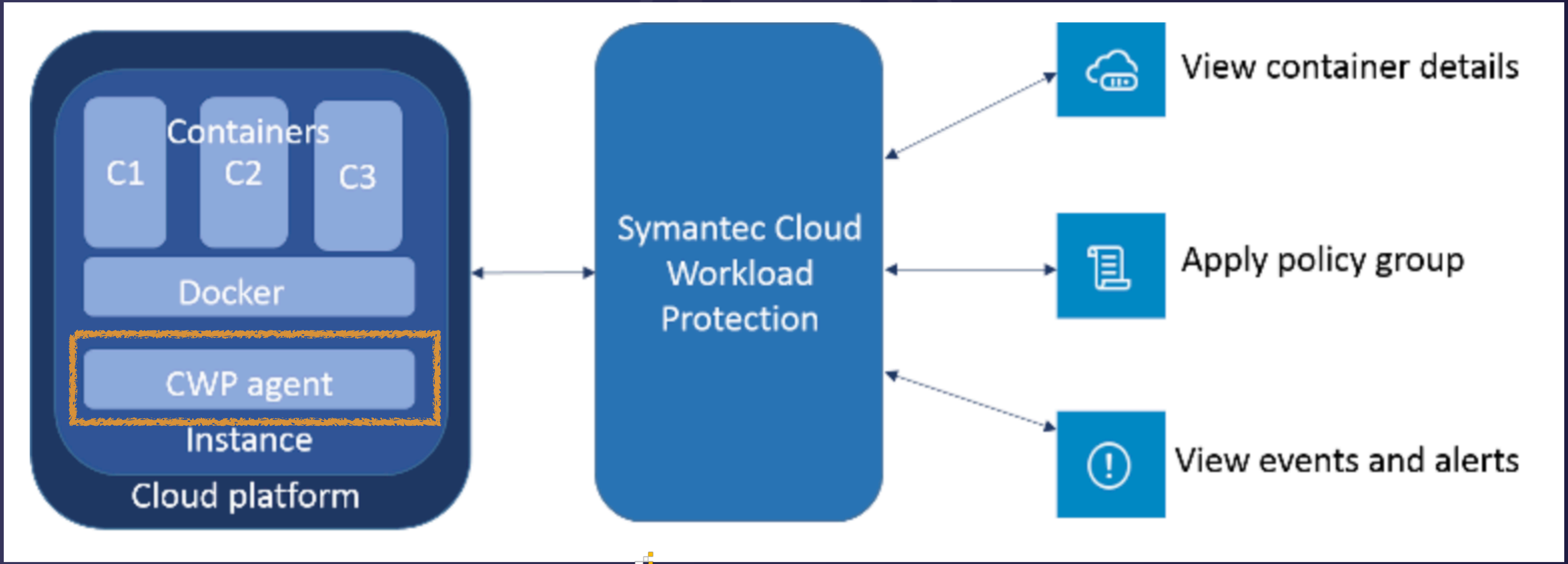
Containers!

End Point Protection


Anti-malware
Deception
Advanced Malware Protection
Symantec Endpoint Protection
Exploit Prevention
Endpoint Detection & Response
Application Isolation & Control

How do you identify malware or viruses **within a container?**

Endpoint Protection via Container Host



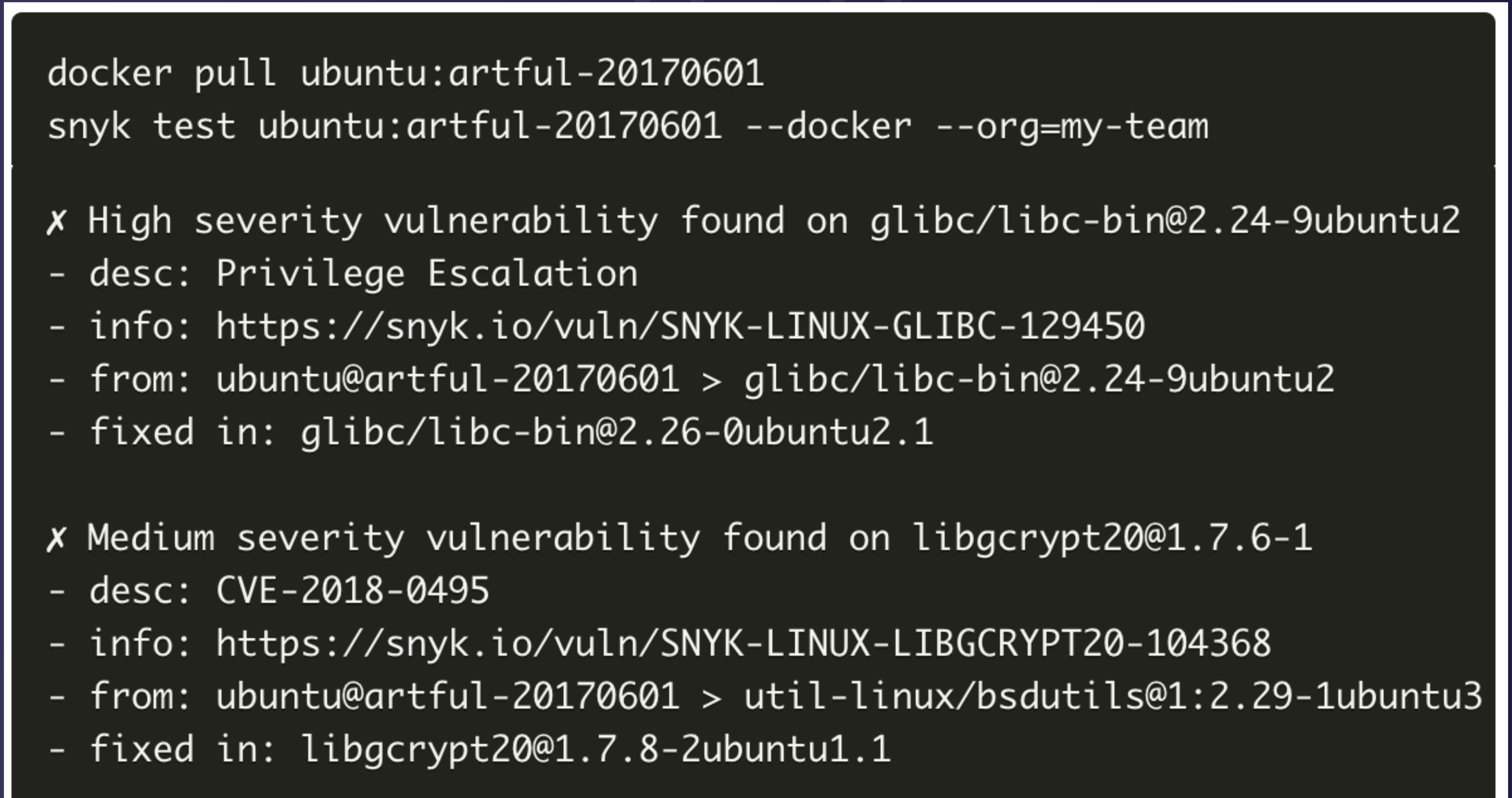
Symantec™

@guypod

snyk

How do you “patch your servers” in an ad-hoc, disposable container?

Scan Docker Images for OS Vulns



```
docker pull ubuntu:artful-20170601
snyk test ubuntu:artful-20170601 --docker --org=my-team
```

```
✗ High severity vulnerability found on glibc/libc-bin@2.24-9ubuntu2
- desc: Privilege Escalation
- info: https://snyk.io/vuln/SNYK-LINUX-GLIBC-129450
- from: ubuntu@artful-20170601 > glibc/libc-bin@2.24-9ubuntu2
- fixed in: glibc/libc-bin@2.26-0ubuntu2.1

✗ Medium severity vulnerability found on libgcrypt20@1.7.6-1
- desc: CVE-2018-0495
- info: https://snyk.io/vuln/SNYK-LINUX-LIBGCRYPT20-104368
- from: ubuntu@artful-20170601 > util-linux/bsdutils@1:2.29-1ubuntu3
- fixed in: libgcrypt20@1.7.8-2ubuntu1.1
```

First, Existing security solutions

are logically valuable

but need to

Technically adapt

Second, new technologies introduce

New Security Risks

that require new security solutions

Cloud introduces the risk

Unsecured Buckets

at an unprecedented scale

Uber hack of 2016

Attackers accessed details of **600,000 Uber drivers** and “some personal info” of **57M Uber users**

Uber hack details

- **Dev pushed S3 tokens to private github.com repo**
- **Attackers gained access to repo, stole tokens**
  - Uber was not using 2FA
- **Attackers used token to steal info from S3**

Uber hack of 2014

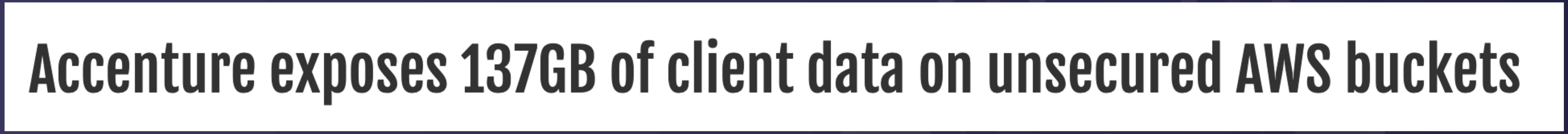
- Dev stored sensitive URL in public github.com gists
- Attacker accessed Uber data in May, 2014
  - “Only” 50,000 drivers exposed that time

You had an

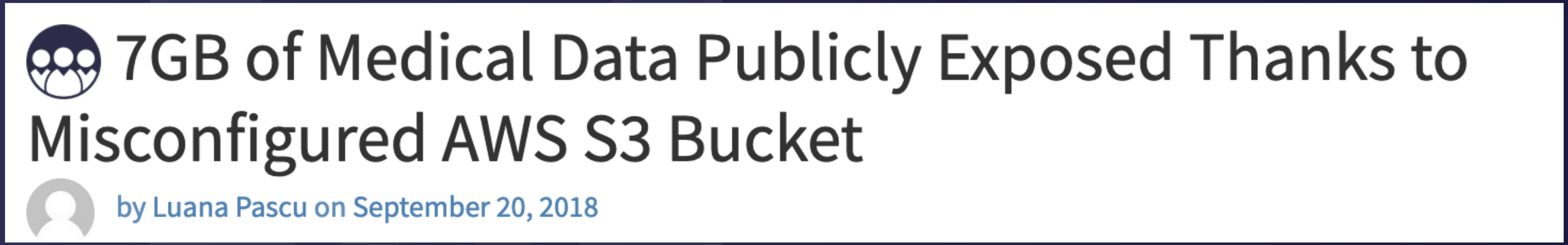
access key?

You were lucky!

Cloud buckets are often
Entirely unprotected

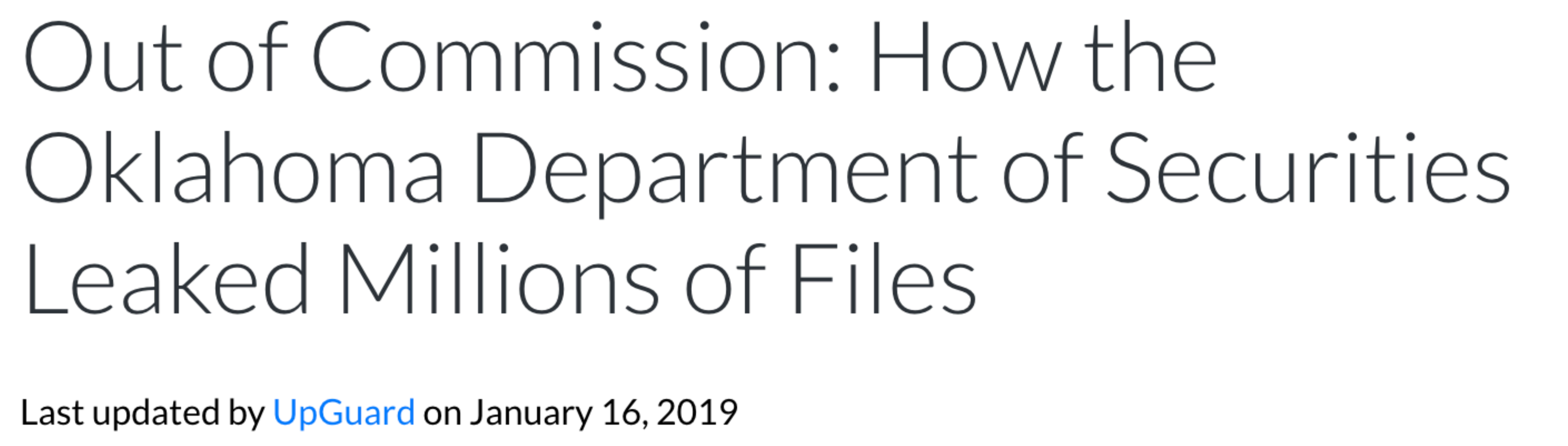


Accenture exposes 137GB of client data on unsecured AWS buckets



7GB of Medical Data Publicly Exposed Thanks to Misconfigured AWS S3 Bucket

by Luana Pascu on September 20, 2018

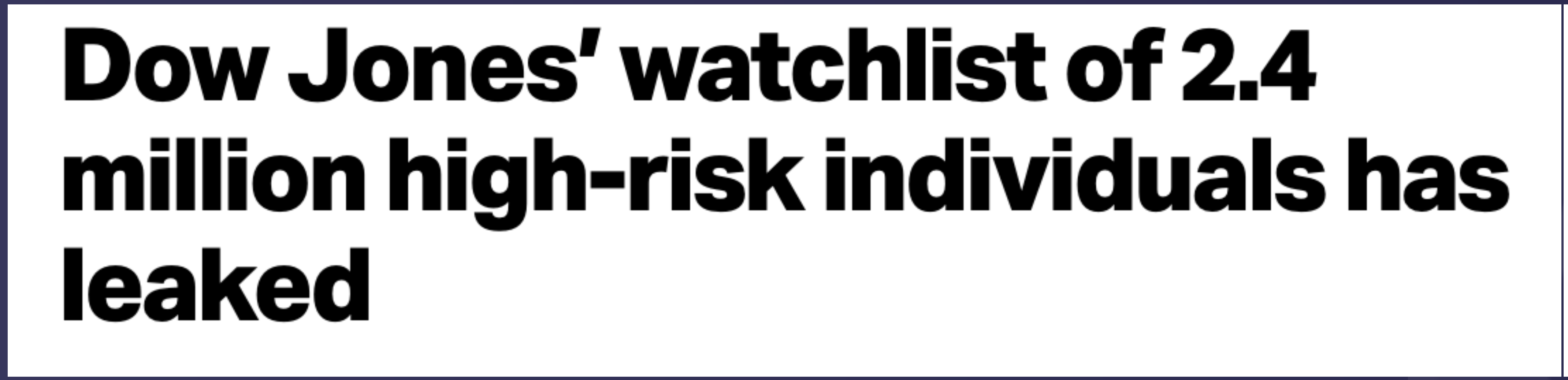


Out of Commission: How the Oklahoma Department of Securities Leaked Millions of Files

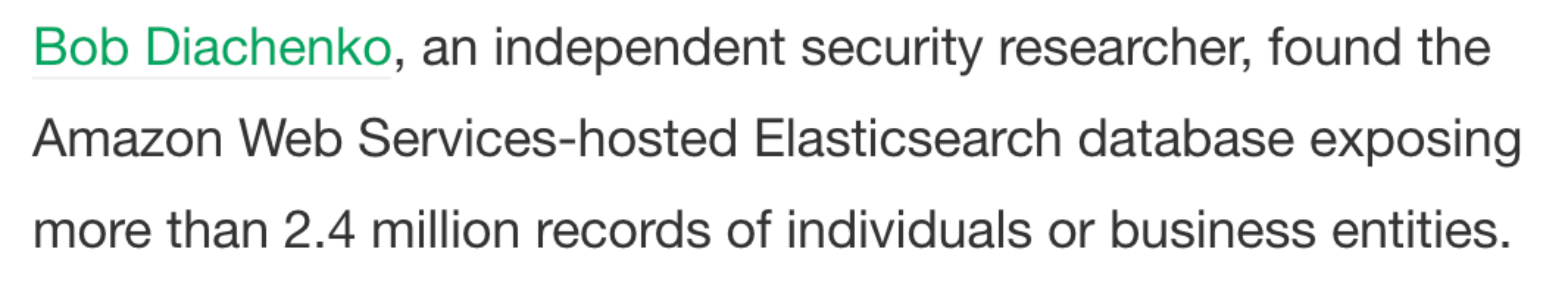
Last updated by UpGuard on January 16, 2019

New platforms also mean new **Insecure Configuration** risks

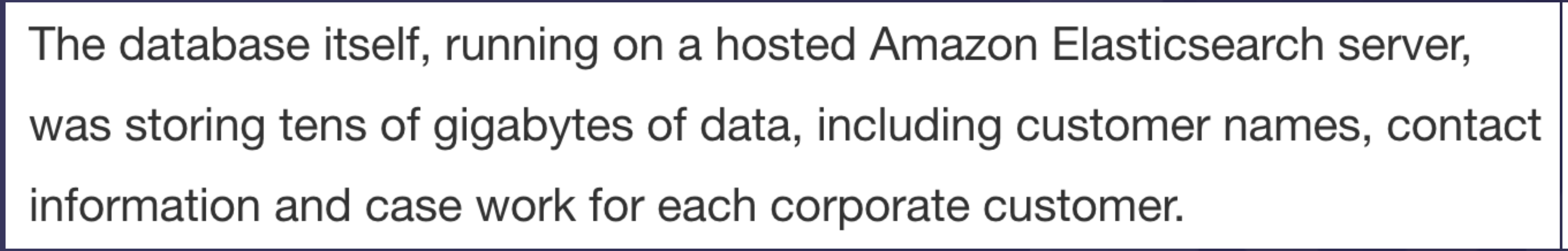
Insecure Config Breaches



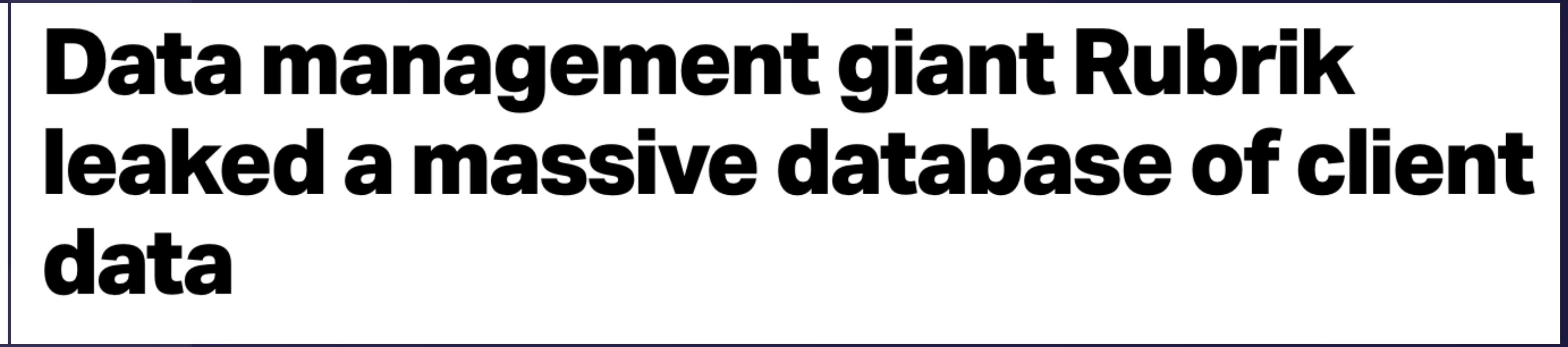
Dow Jones' watchlist of 2.4 million high-risk individuals has leaked



Bob Diachenko, an independent security researcher, found the Amazon Web Services-hosted Elasticsearch database exposing more than 2.4 million records of individuals or business entities.



The database itself, running on a hosted Amazon Elasticsearch server, was storing tens of gigabytes of data, including customer names, contact information and case work for each corporate customer.



Data management giant Rubrik leaked a massive database of client data

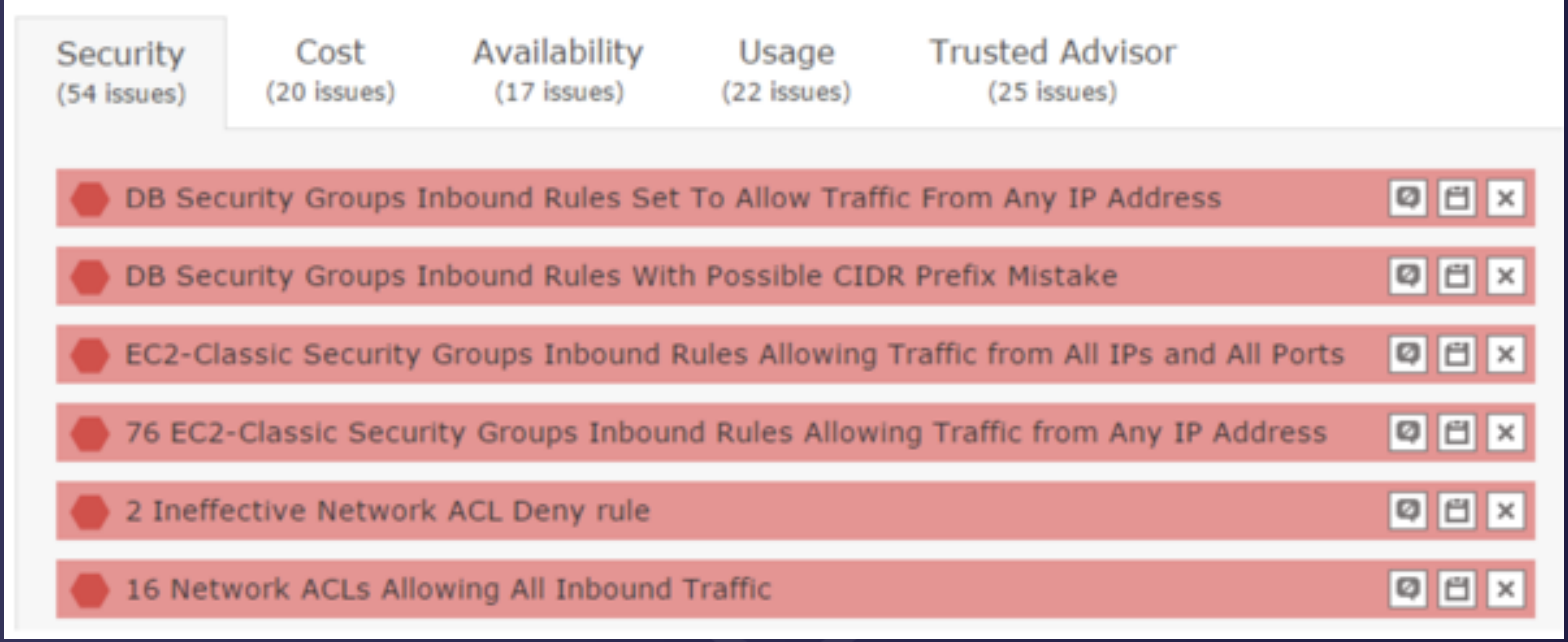
The MongoDB hack and the importance of secure defaults

JANUARY 10, 2017 | IN DEVSECOPS, V

If you have a MongoDB installation, now would be the time to verify that it is secure. Since just before Christmas, over 28,000 public MongoDB installs have been hacked.

Cloud Security Configuration

Static & Event Scan



Security (54 issues)	Cost (20 issues)	Availability (17 issues)	Usage (22 issues)	Trusted Advisor (25 issues)

- DB Security Groups Inbound Rules Set To Allow Traffic From Any IP Address
- DB Security Groups Inbound Rules With Possible CIDR Prefix Mistake
- EC2-Classic Security Groups Inbound Rules Allowing Traffic from All IPs and All Ports
- 76 EC2-Classic Security Groups Inbound Rules Allowing Traffic from Any IP Address
- 2 Ineffective Network ACL Deny rule
- 16 Network ACLs Allowing All Inbound Traffic

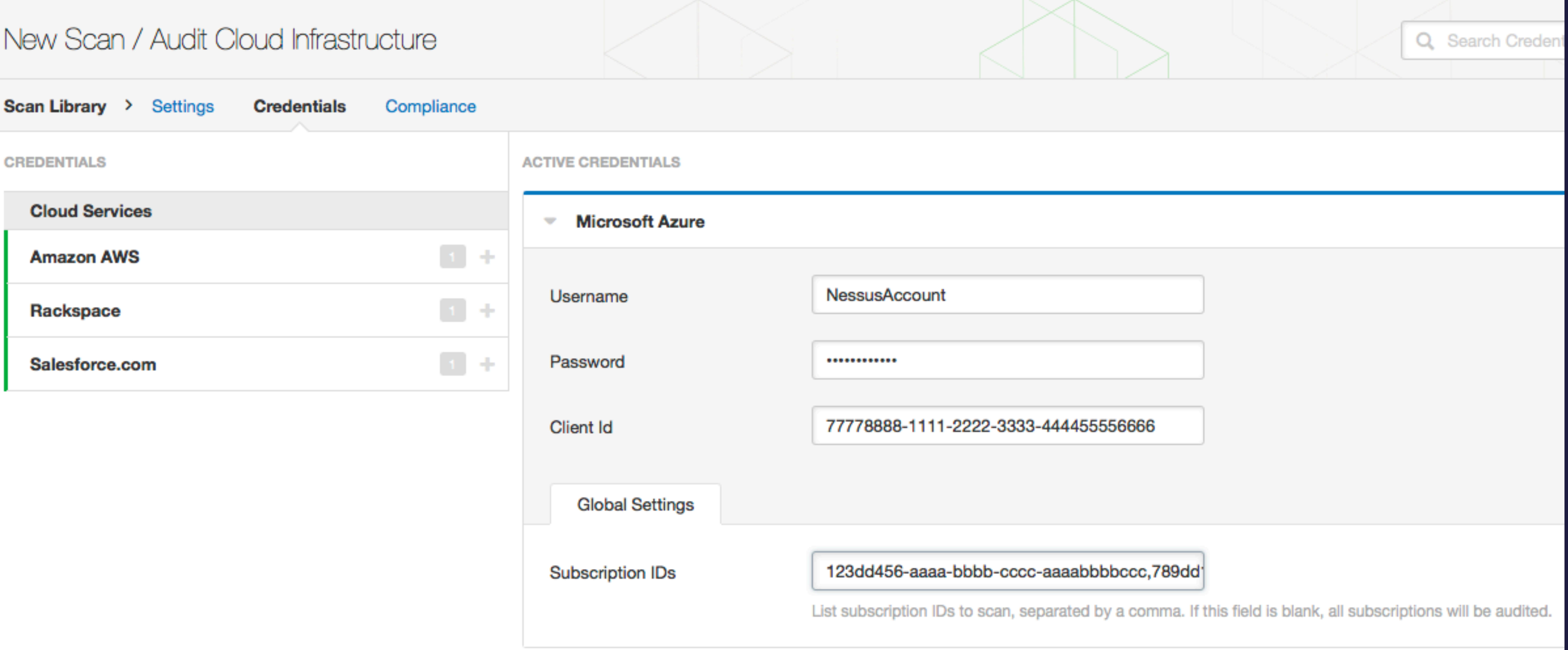
CloudCheckr

@guypod

snyk

Cloud Security Configuration

Audit Scan



New Scan / Audit Cloud Infrastructure

CREDENTIALS

Cloud Services

- Amazon AWS
- Rackspace
- Salesforce.com

ACTIVE CREDENTIALS

Microsoft Azure

Username	NessusAccount
Password	•••••••••••••
Client Id	77778888-1111-2222-3333-444455556666

Global Settings

Subscription IDs	123dd456-aaaa-bbbb-cccc-aaaabbbbcccc,789dd

List subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions will be audited.

tenable™

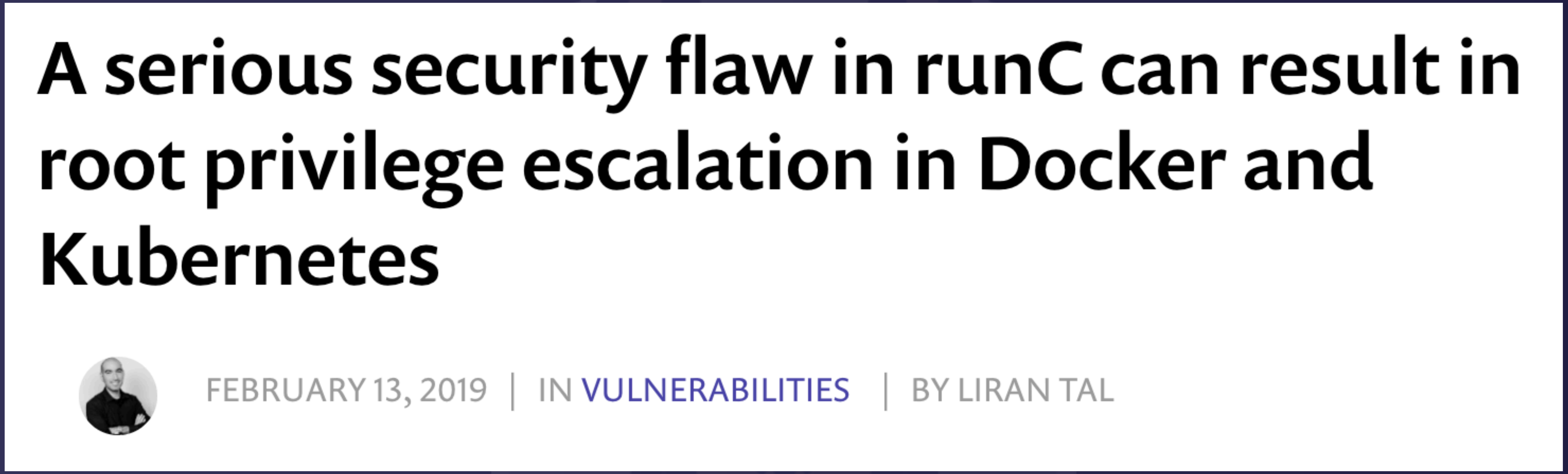
@guypod

snyk

Containers add the risk of

Sandbox Escaping

Jumping from container to its host



A serious security flaw in runC can result in root privilege escalation in Docker and Kubernetes

FEBRUARY 13, 2019 | IN VULNERABILITIES | BY LIRAN TAL

https://snyk.io/blog/a-serious-security-flaw-in-runc-can-result-in-root-privilege-escalation-in-docker-and-kubernetes/

@guypod

Container Sandbox Escaping protection

Twistlock

aqua

TREND MICRO™

Security For DevOps Technologies:

1. **Adapt existing** security tools to new tech
2. **Address new** security risks new tech introduced

Security in

DevOps Methodologies

DevOps also changes
Methodologies

CI/CD

Typical security approach:

Stop here for an audit

~~Typical security approach:~~

~~**Stop here for an audit**~~

With CI/CD

Stopping is not an option!

Solution:

Automated App Sec Testing!

Static & Dynamic… kinda.

Static Testing (SAST) in CI/CD

- Scan *your* code to find potential vulnerable code paths
- Scans take hours (or days) to run != builds take minutes

- Adaptation: incremental scans
  - Run long scans ~weekly
  - Run “Delta” scans in the build

- Still a problem with false positives… different topic!

@guypod

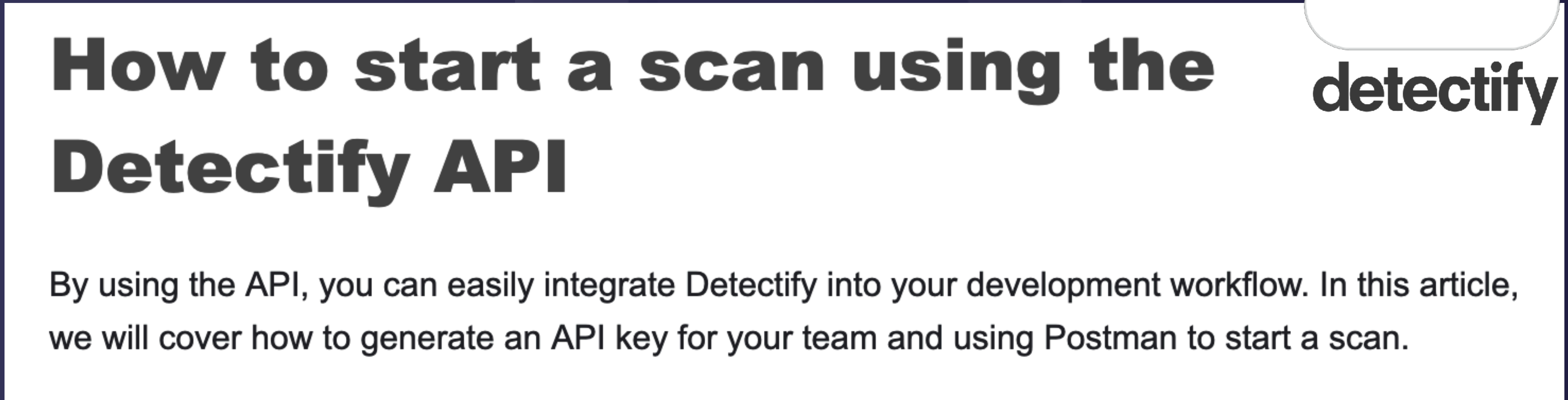
snyk

Dynamic Testing (DAST) in CI/CD

- Tests a deployed instance like a hacker to find vulnerabilities
- Scans require dedicated env… often doesn’t exist.
- Scans take way too long to complete

- Adaptation:
  - IAST - instrument app, run unit-tests, deduce security issues
  - Less comprehensive, but works with less overhead
  - Very imperfect… but sometimes work

New Alternative:
Invoke scan in build, test async



How to start a scan using the Detectify API

By using the API, you can easily integrate Detectify into your development workflow. In this article, we will cover how to generate an API key for your team and using Postman to start a scan.

SCA in CI/CD

- Flag use of libraries with known vulnerabilities
- “Break build” on vulnerability or otherwise alert
- Fast & accurate - naturally CI/CD friendly…

Microservices

@guypod

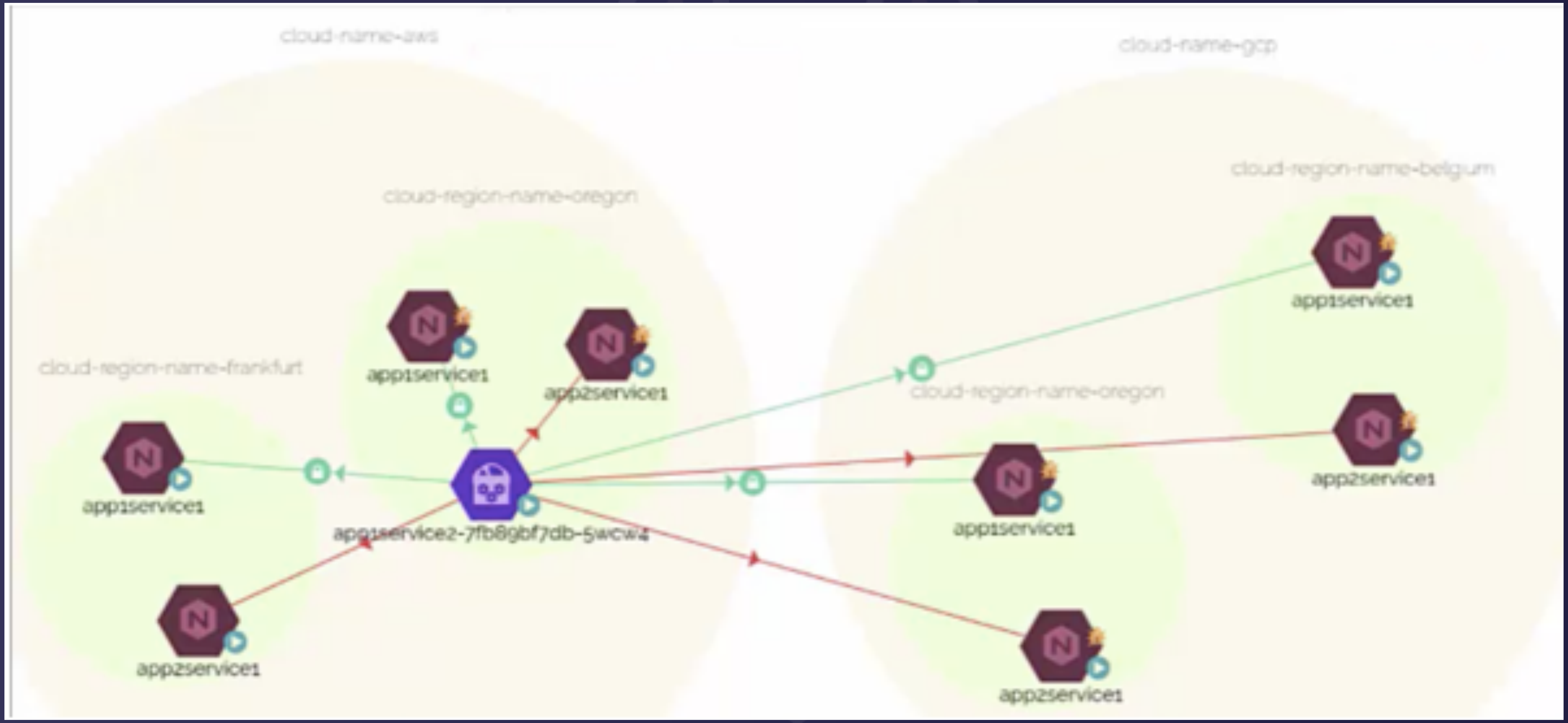
snyk

- Clear perimeter
- Constrained flow
- Wholesale deploys

- Many perimeters
- Flexible flow
- Constant deploys

Security monitoring in Microservices

- Adaptation: Track data flows across apps



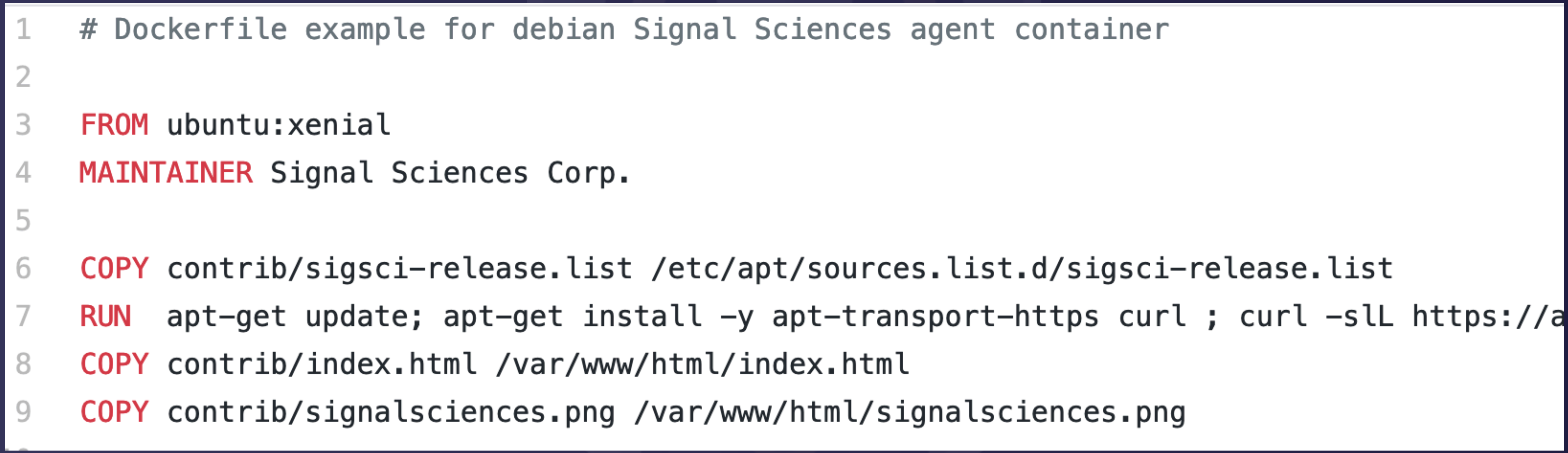
Aporeto

@guypod

snyk

Security monitoring in Microservices

- Adaptation: Embed installation into deploy flow



```
# Dockerfile example for debian Signal Sciences agent container

FROM ubuntu:xenial
MAINTAINER Signal Sciences Corp.

COPY contrib/sigsci-release.list /etc/apt/sources.list.d/sigsci-release.list
RUN  apt-get update; apt-get install -y apt-transport-https curl ; curl -slL https://a
COPY contrib/index.html /var/www/html/index.html
COPY contrib/signalsciences.png /var/www/html/signalsciences.png
```

Signal Sciences

Security solutions

Adapt to new methodologies

to stay relevant

DevOps methodologies also offer **Opportunities** for better security

When a container misbehaves…

Just kill it!

(It’ll start up again in no time)

Continuous Deployments mean

Fast security patch deployment!

(contain risks faster and more safely than ever)

CI/CD means easy

Automated security gating!

(block secrets or vulns from passing, enforce policies, etc.)

Powerful and pervasive use of Git allows

Securing Code via GitOps!

(test code deltas, automate code fixes, raise visibility)

Security For DevOps Methodologies:

1. Adapt how existing security tools are applied
2. Use the new opportunities to do security better

We’ve seen such changes before:

Virtualisation, Mobile…

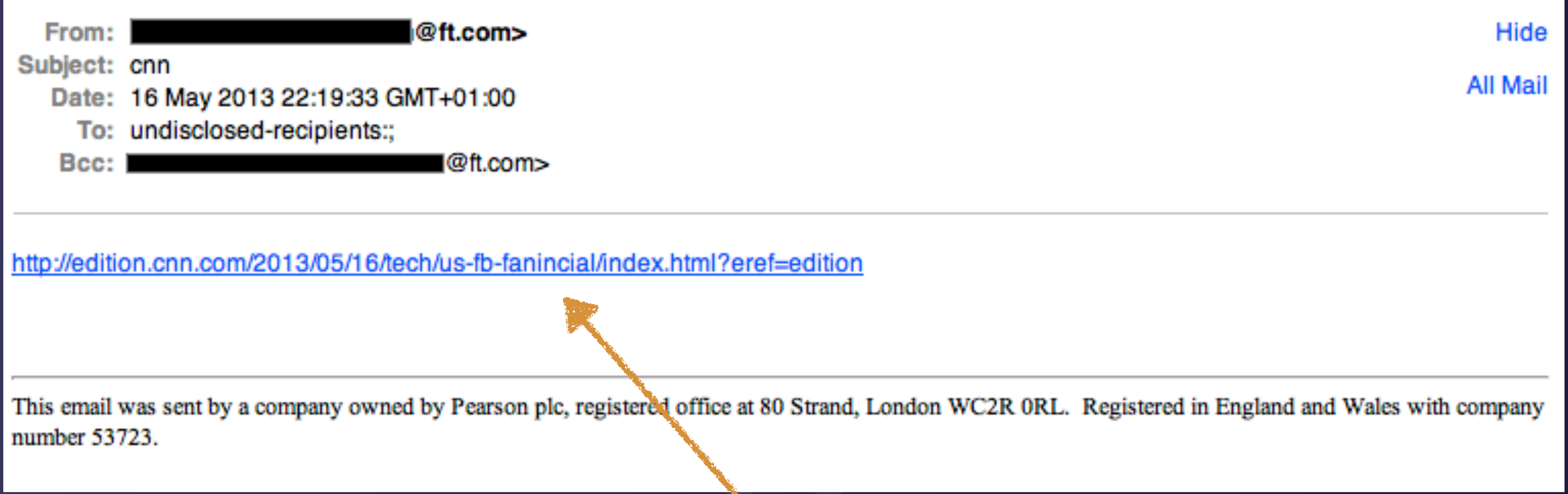
The bigger DevOps change:

People & Ownership

Include Security in DevOps Shared Ownership

The Syrian Electronic Army and the Financial Times

1. Phishing email to employees who had publicly shared their email



From: [redacted]@ft.com>

Subject: cnn

Date: 16 May 2013 22:19:33 GMT+01:00

To: undisclosed-recipients:;

Bcc: [redacted]@ft.com>

http://edition.cnn.com/2013/05/16/tech/us-fb-fanincial/index.html?eref=edition

This email was sent by a company owned by Pearson plc, registered office at 80 Strand, London WC2R 0RL. Registered in England and Wales with company number 53723.

Masked link to an attacker controlled compromised site

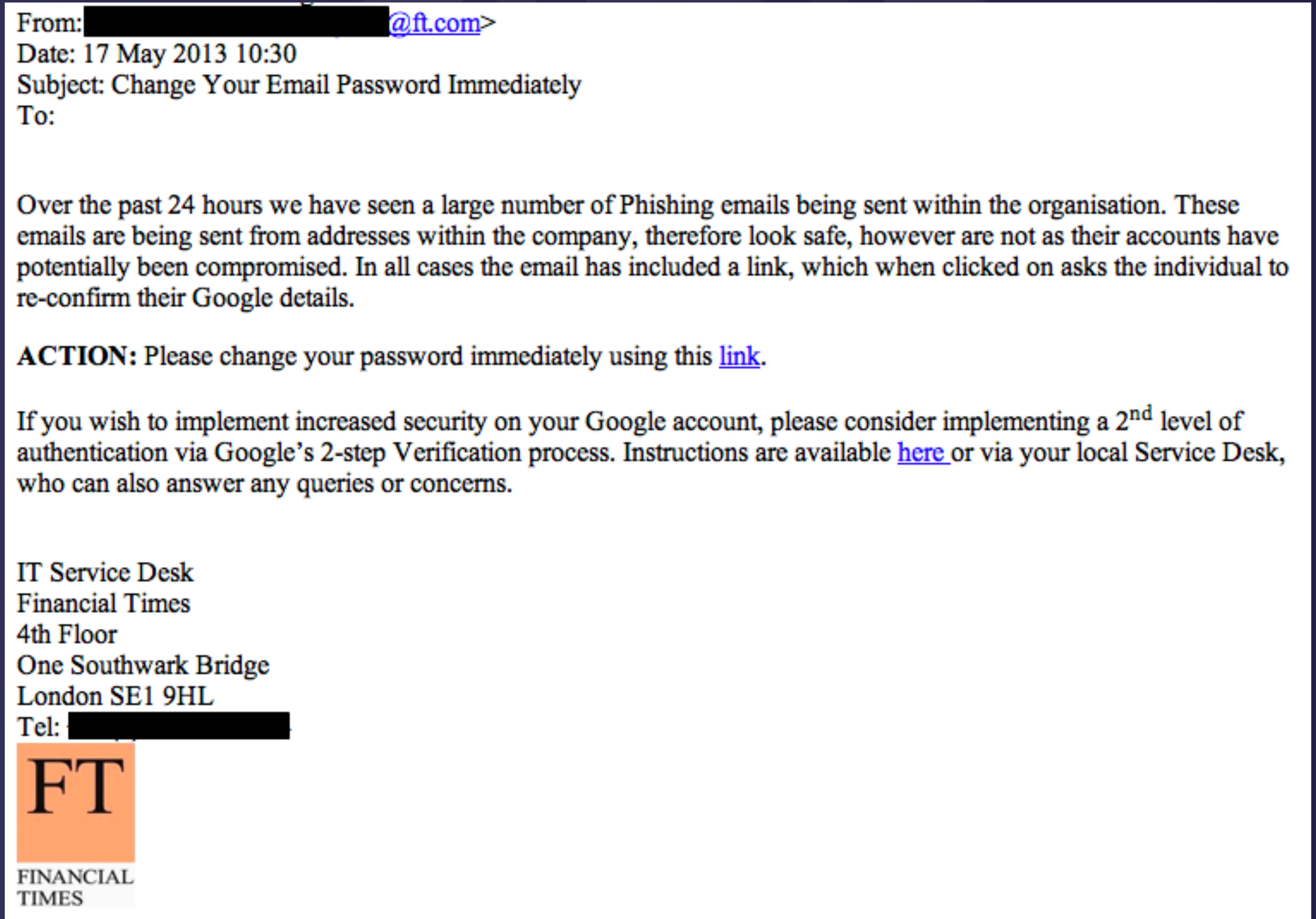
2. Link redirects to **spoofed FT Single Sign-on** page (for Google Apps)

Some users entered their passwords…

3. Attackers use compromised accounts to **Email more FT users** this time from an **FT email address**

More users are compromised…

4. IT finds out, sends warning email to all.
Attackers send identical email - with evil links



From: [redacted]@ft.com>
Date: 17 May 2013 10:30
Subject: Change Your Email Password Immediately
To:

Over the past 24 hours we have seen a large number of Phishing emails being sent within the organisation. These emails are being sent from addresses within the company, therefore look safe, however are not as their accounts have potentially been compromised. In all cases the email has included a link, which when clicked on asks the individual to re-confirm their Google details.

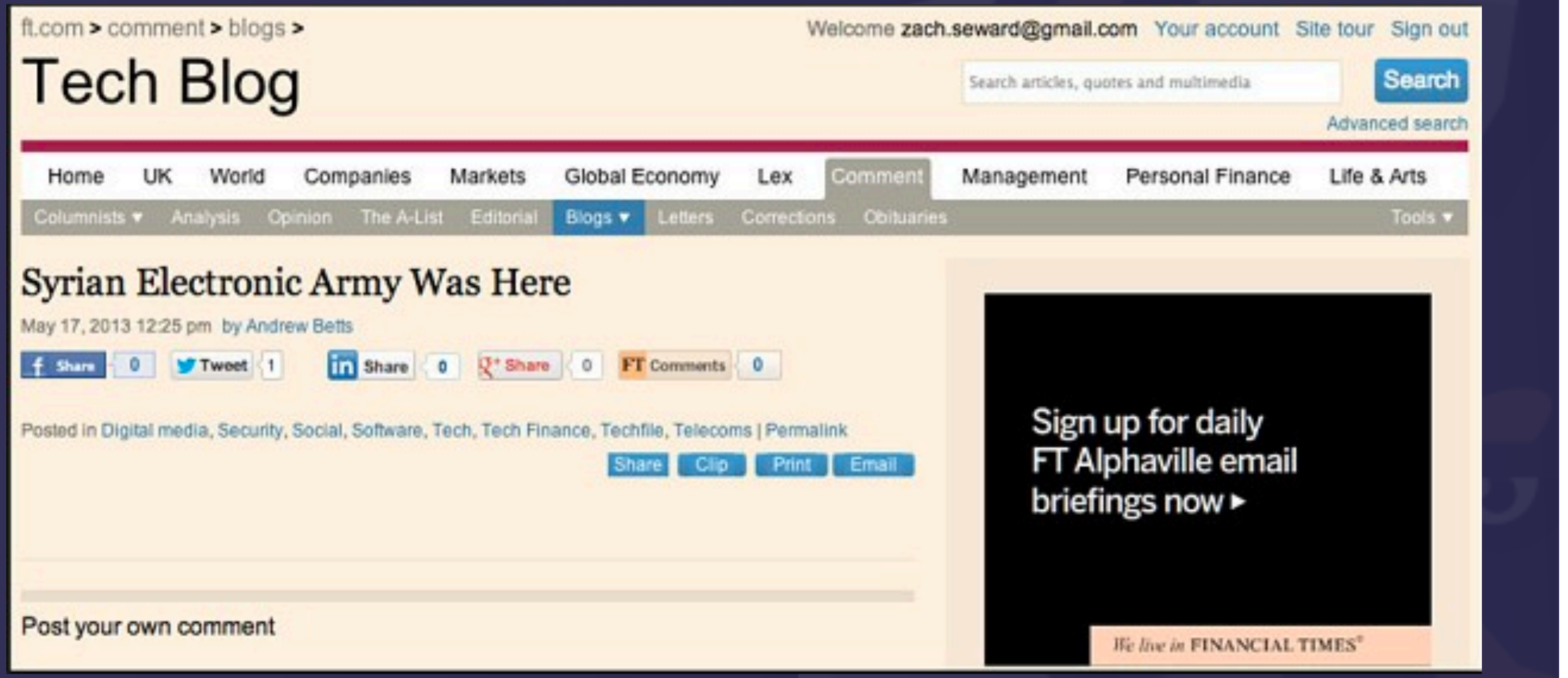
ACTION: Please change your password immediately using this link.

If you wish to implement increased security on your Google account, please consider implementing a 2nd level of authentication via Google's 2-step Verification process. Instructions are available here or via your local Service Desk, who can also answer any queries or concerns.

IT Service Desk
Financial Times
4th Floor
One Southwark Bridge
London SE1 9HL
Tel: [redacted]

FT
FINANCIAL
TIMES

5. Attackers gain access to several official Twitter accounts blog


ft.com > comment > blogs >
Welcome zach.seward@gmail.com Your account Site tour Sign out
Search articles, quotes and multimedia
Search
Advanced search
Home UK World Companies Markets Global Economy Lex Comment Management Personal Finance Life & Arts
Columnists ▾ Analysis Opinion The A-List Editorial Blogs ▾ Letters Corrections Obituaries Tools ▾
Share 0 Tweet 1 Share 0 Share 0 FT Comments 0
Share Clip Print Email

Tech Blog

Syrian Electronic Army Was Here

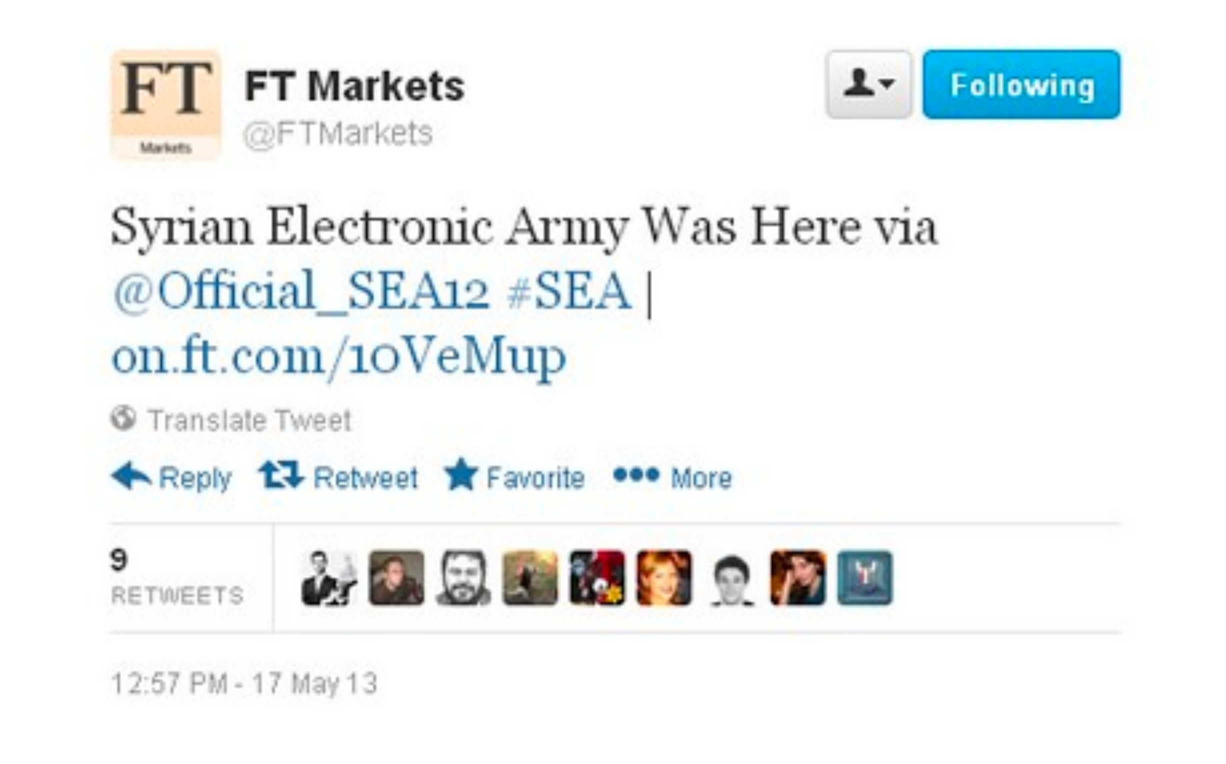
May 17, 2013 12:25 pm by Andrew Betts

Posted in Digital media, Security, Social, Software, Tech, Tech Finance, Techfile, Telecoms | Permalink

Post your own comment

Sign up for daily FT Alphaville email briefings now ▸

We live in FINANCIAL TIMES®

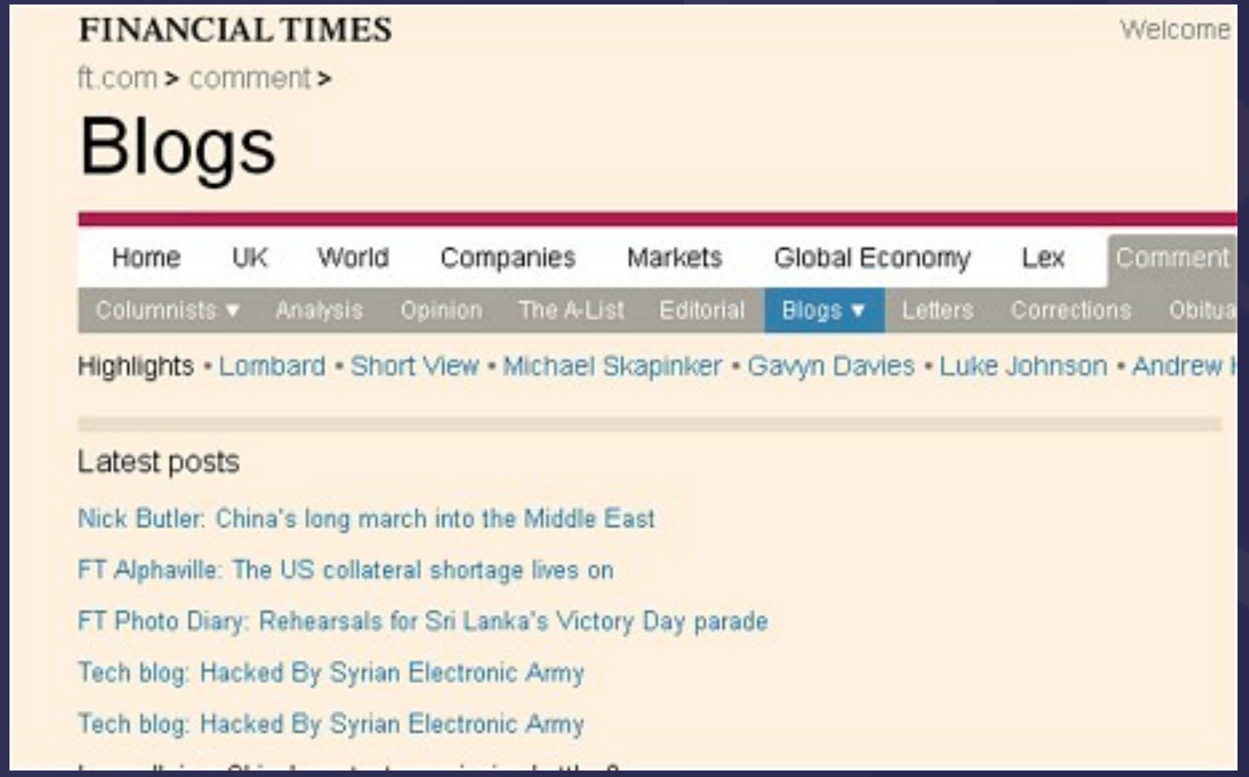


FT Markets @FTMarkets

Syrian Electronic Army Was Here via @Official_SEA12 #SEA | on.ft.com/10VeMup

9 RETWEETS

12:57 PM - 17 May 13


Welcome
ft.com > comment >
Home UK World Companies Markets Global Economy Lex Comment
Columnists ▾ Analysis Opinion The A-List Editorial Blogs ▾ Letters Corrections Obitua

FINANCIAL TIMES

Blogs

Highlights • Lombard • Short View • Michael Skapinker • Gavyn Davies • Luke Johnson • Andrew

Latest posts

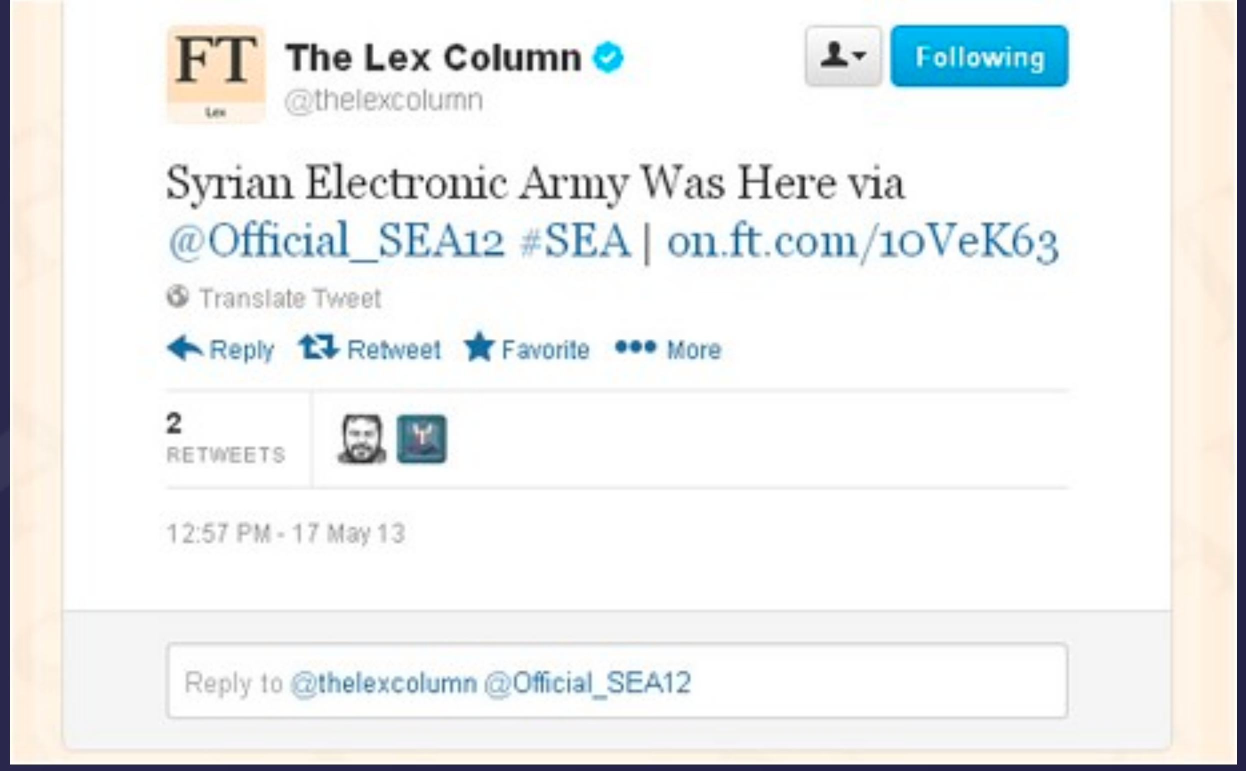
Nick Butler: China's long march into the Middle East

FT Alphaville: The US collateral shortage lives on

FT Photo Diary: Rehearsals for Sri Lanka's Victory Day parade

Tech blog: Hacked By Syrian Electronic Army

Tech blog: Hacked By Syrian Electronic Army



The Lex Column @thelexcolumn

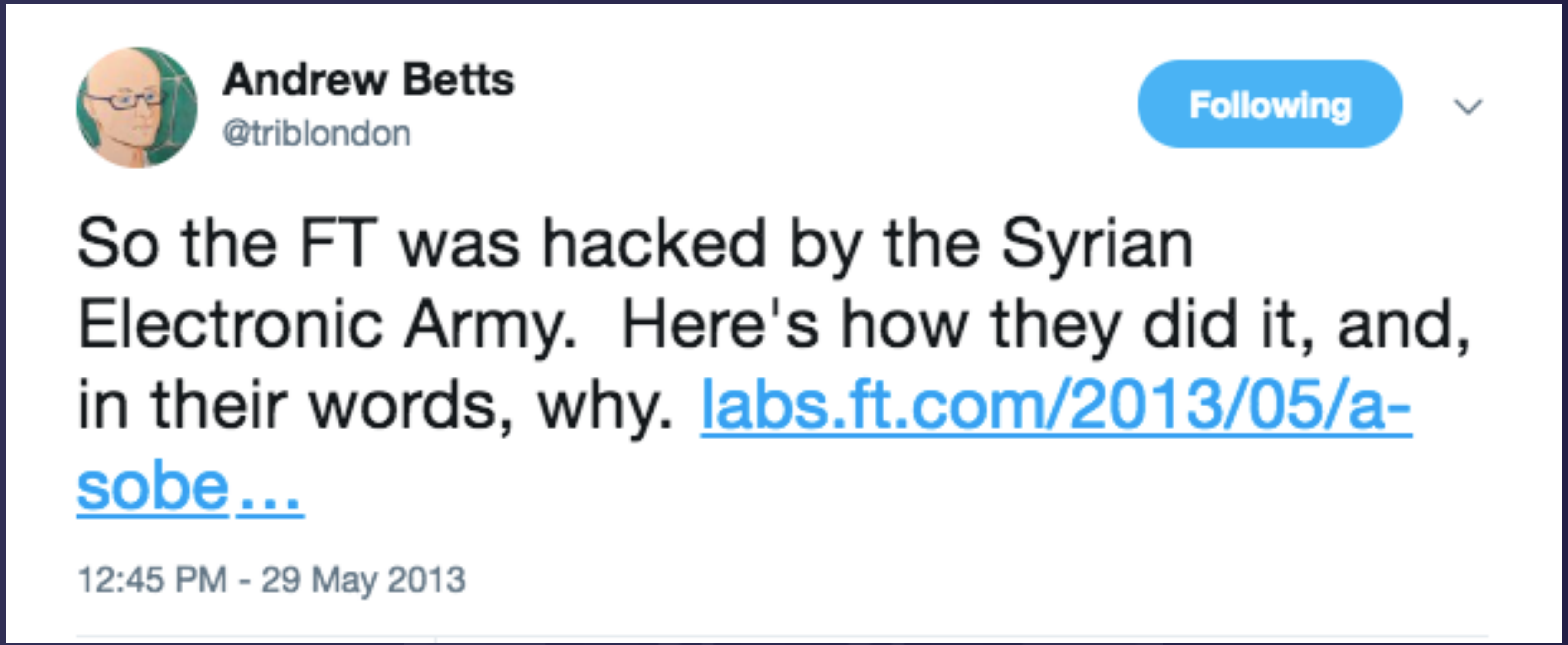
Syrian Electronic Army Was Here via @Official_SEA12 #SEA | on.ft.com/10VeK63

2 RETWEETS

12:57 PM - 17 May 13

Reply to @thelexcolumn @Official_SEA12

https://www.telegraph.co.uk/technology/twitter/10064184/Financial-Times-hacked-by-Syrian-Electronic-Army.html



Andrew Betts
@triblondon

So the FT was hacked by the Syrian Electronic Army. Here's how they did it, and, in their words, why. labs.ft.com/2013/05/a-sobe…

12:45 PM - 29 May 2013

“A sobering day”

by Andrew Betts,
a compromised FT developer

https://labs.ft.com/2013/05/a-sobering-day/

“Developers might well think they’d be wise to all this – and I thought I was.”

https://labs.ft.com/2013/05/a-sobering-day/

Internal Salesforce Phishing Test

run by Masha Sedova (@modMasha)

Developers were the 2nd most likely to click a link in a phishing email

https://www.heavybit.com/library/podcasts/the-secure-developer/ep-16-security-training-with-elevates-masha-sedova/

Compromising a

high privileged developer

is hitting the jackpot

DevOps means developers are

more powerful

than ever

The pace of **shipping code** is skyrocketing

Developers access

production systems

daily

Developers access

user data

daily

Typical team size ratios:

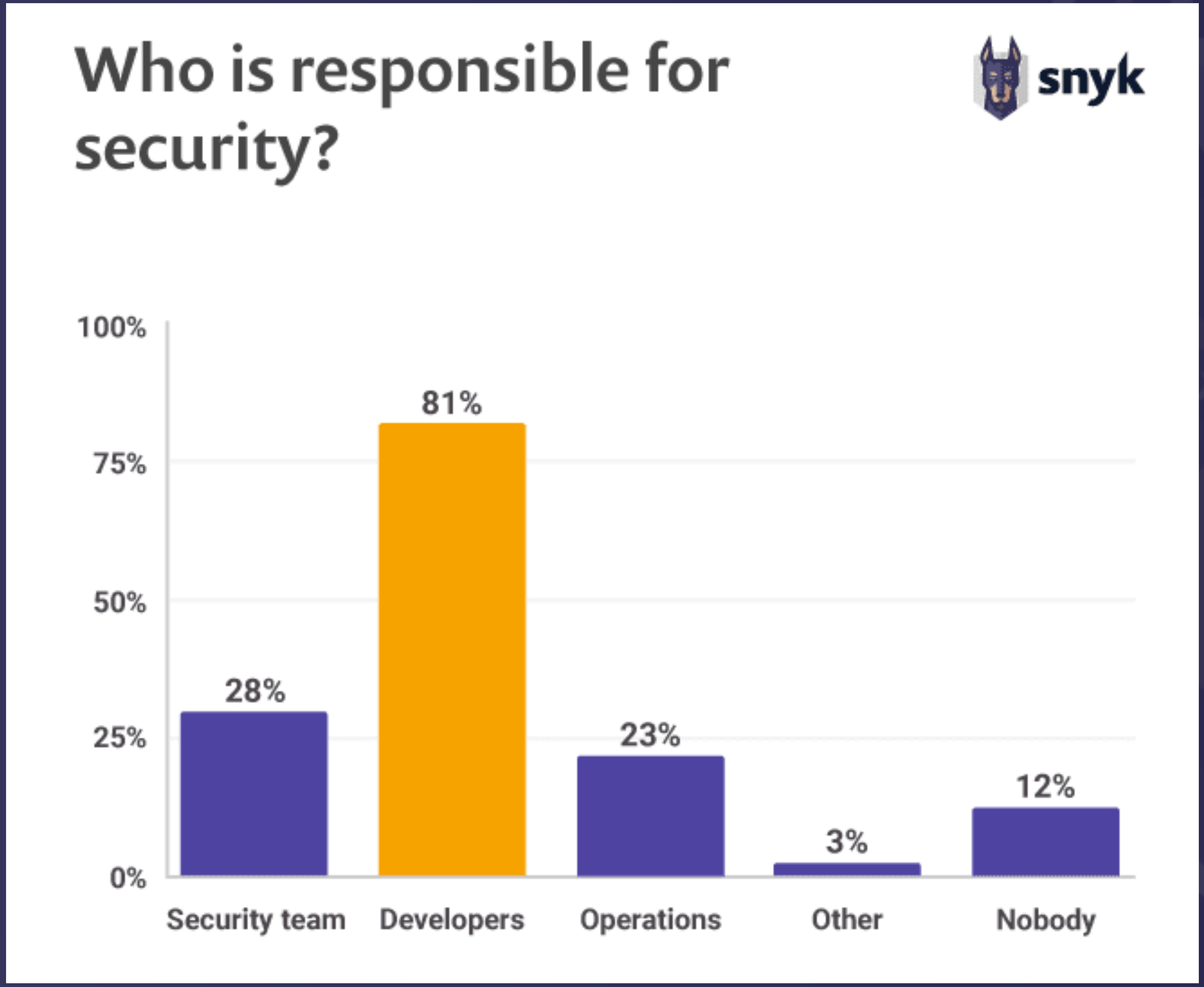
1 Sec

10 Ops

100 Dev

Developers cannot **outsource security**. Nobody else can keep up.

Developers believe
dev should (co)own security



68% of users feel developers should own security responsibility of container images

Source: **State of open source security**
https://snyk.io/blog/81-believe-developers-should-own-security-but-they-arent-well-equipped/

Challenge:

Security tools

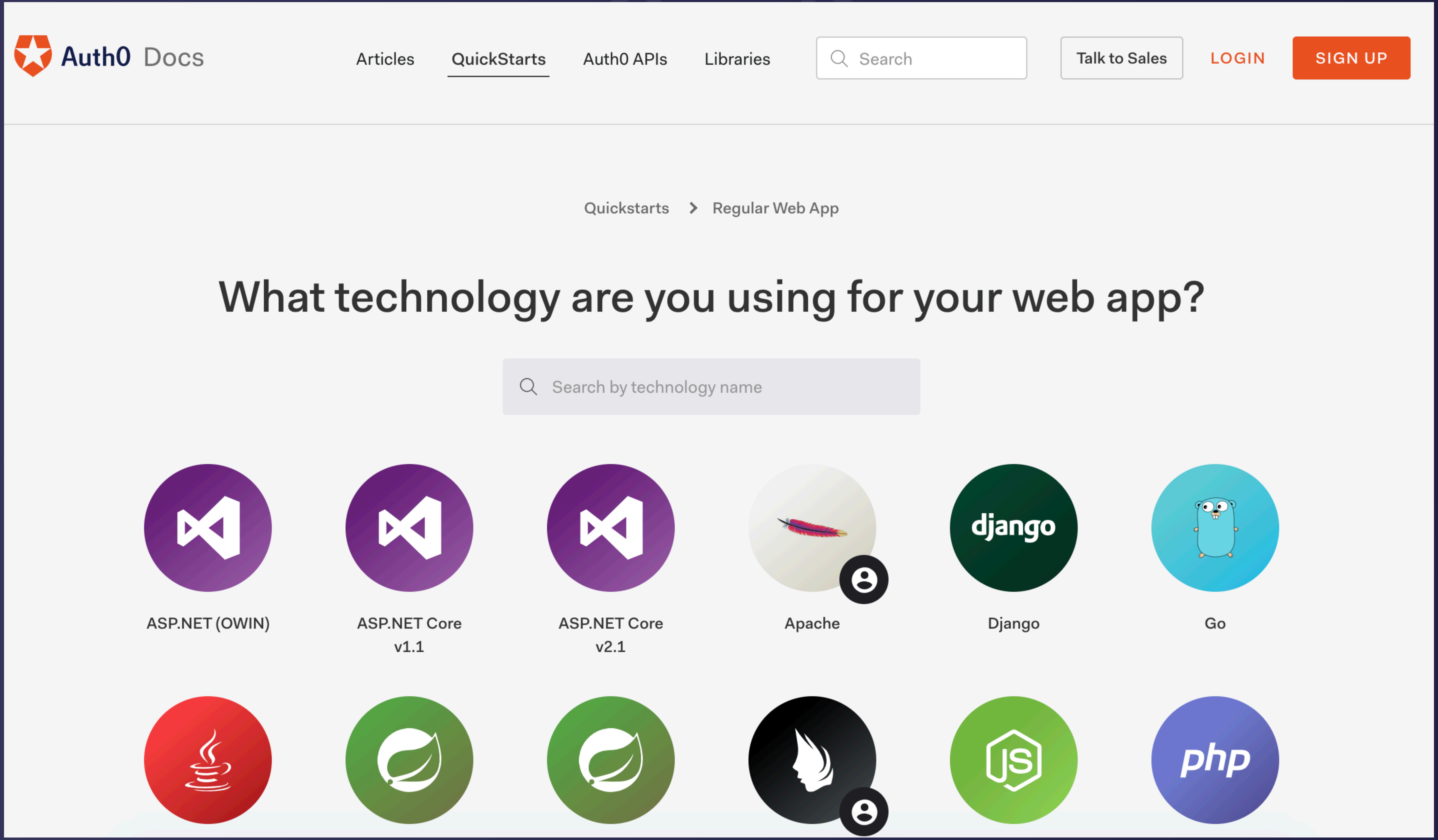
are designed for

security professionals

Integrating an **audit tool** into InteliJ
Does **not** make it a **developer tool**…

What does make a good Developer Tool?

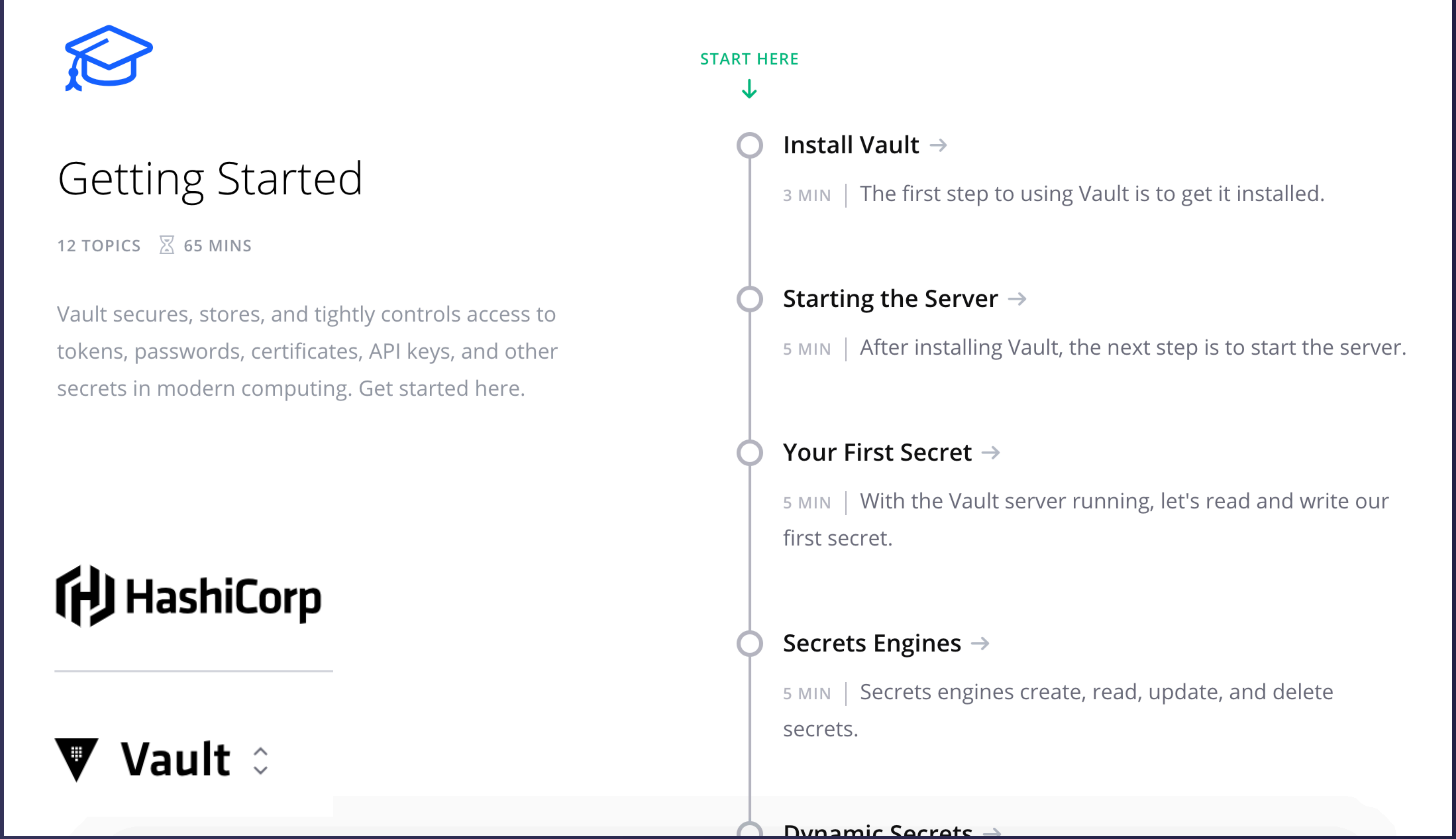
Great Documentation



Quickstarts > Regular Web App

What technology are you using for your web app?

Ability to try Self-Serve



Getting Started

12 TOPICS 65 MINS

Vault secures, stores, and tightly controls access to tokens, passwords, certificates, API keys, and other secrets in modern computing. Get started here.

HashiCorp

Vault

START HERE ↓

Install Vault →

3 MIN | The first step to using Vault is to get it installed.

Starting the Server →

5 MIN | After installing Vault, the next step is to start the server.

Your First Secret →

5 MIN | With the Vault server running, let's read and write our first secret.

Secrets Engines →

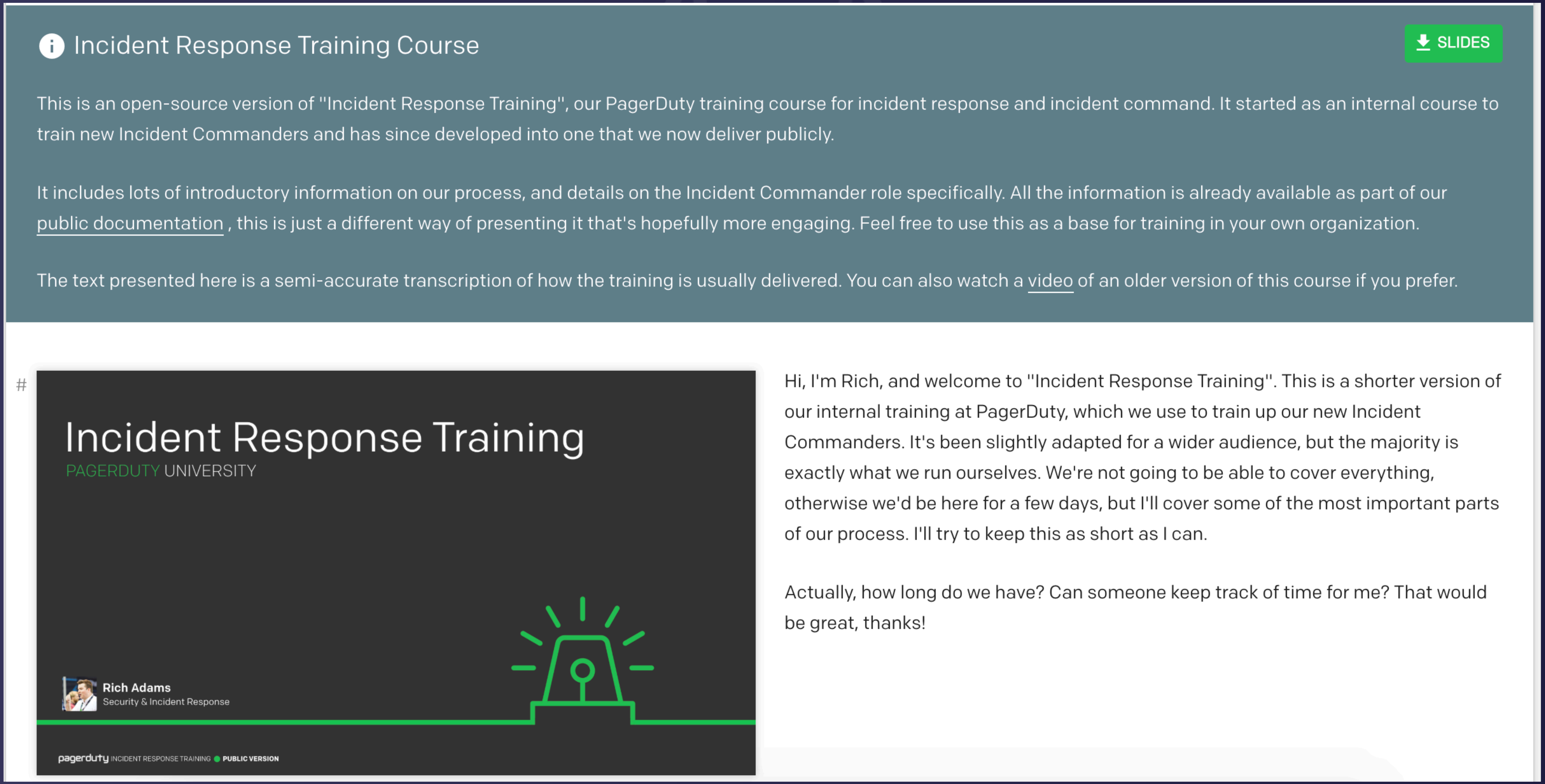
5 MIN | Secrets engines create, read, update, and delete secrets.

Dynamic Secrets →

@guypod

snyk

Education for Non-Security experts



Incident Response Training Course

This is an open-source version of "Incident Response Training", our PagerDuty training course for incident response and incident command. It started as an internal course to train new Incident Commanders and has since developed into one that we now deliver publicly.

It includes lots of introductory information on our process, and details on the Incident Commander role specifically. All the information is already available as part of our public documentation , this is just a different way of presenting it that's hopefully more engaging. Feel free to use this as a base for training in your own organization.

The text presented here is a semi-accurate transcription of how the training is usually delivered. You can also watch a video of an older version of this course if you prefer.

#

Incident Response Training
PAGERDUTY UNIVERSITY

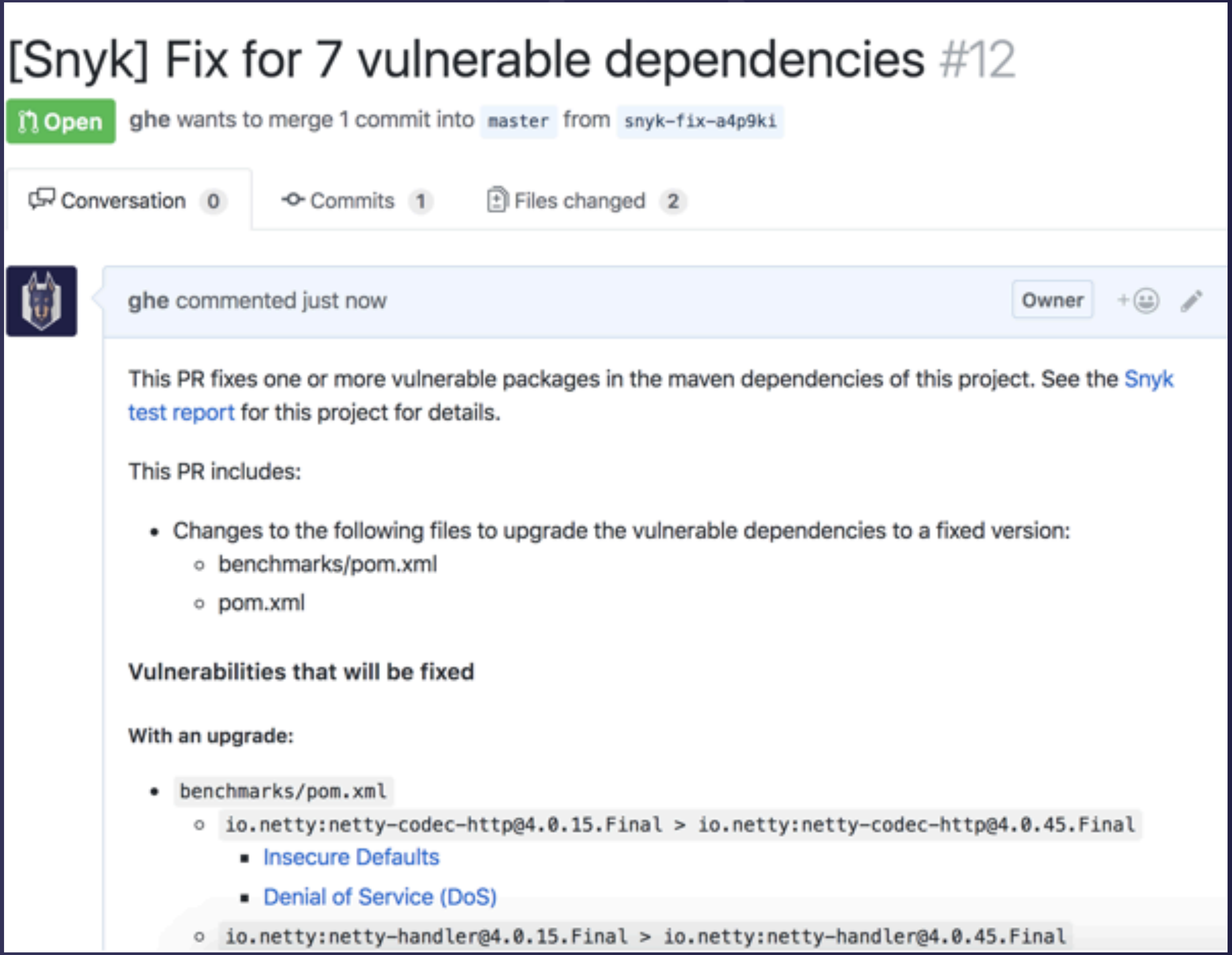
Rich Adams
Security & Incident Response

pagerduty INCIDENT RESPONSE TRAINING ● PUBLIC VERSION

Hi, I'm Rich, and welcome to "Incident Response Training". This is a shorter version of our internal training at PagerDuty, which we use to train up our new Incident Commanders. It's been slightly adapted for a wider audience, but the majority is exactly what we run ourselves. We're not going to be able to cover everything, otherwise we'd be here for a few days, but I'll cover some of the most important parts of our process. I'll try to keep this as short as I can.

Actually, how long do we have? Can someone keep track of time for me? That would be great, thanks!

Make issues actionable



[Snyk] Fix for 7 vulnerable dependencies #12

ghe wants to merge 1 commit into `master` from `snyk-fix-a4p9ki`

ghe commented just now

This PR fixes one or more vulnerable packages in the maven dependencies of this project. See the Snyk test report for this project for details.

This PR includes:

- Changes to the following files to upgrade the vulnerable dependencies to a fixed version:
  - benchmarks/pom.xml
  - pom.xml

Vulnerabilities that will be fixed

With an upgrade:

- `benchmarks/pom.xml`
  - `io.netty:netty-codec-http@4.0.15.Final > io.netty:netty-codec-http@4.0.45.Final`
    - Insecure Defaults
    - Denial of Service (DoS)
  - `io.netty:netty-handler@4.0.15.Final > io.netty:netty-handler@4.0.45.Final`

@guypod

Find/build the security tools

developers will actually use

Challenge:

Getting Dev to embrace security And security to embrace dev

Some ideas from

Security Teams that do it well

(via The Secure Developer podcast)

THE SECURE DEVELOPER

PagerDuty Security Team

- We have a phrase we like on our security team which is, “we're here to make it easy to do the right thing”
- … treating security problems as operational problems… things like Chef, Splunk, AWS tooling… use them for security challenges as well.

https://www.heavybit.com/library/podcasts/the-secure-developer/ep-11-keeping-pagerduty-secure/

Optimizely Security Lead

Kyle Randolph

- We actually give out T-shirts that say, "Security Hero" on them. This is more exclusive, so it makes people want to step it up and really go above and beyond to make a security contribution
- We're using a lot of Spinnaker for our deploy automation, which is not a security tool, but that's just the place that you can bundle in all the other security configuration that you want to have happen.

https://www.heavybit.com/library/podcasts/the-secure-developer/ep-1-prioritizing-secure-development/

New Relic CSO

Shaun Gordon

- It's very easy to turn a developer off of a tool very quickly by giving them unactionable information, by calling them out on something that they don't understand what it is, and more importantly, how to fix it
- change the way we do security to fit in with the way the developers perform their job, instead of trying to get them adapt the way they work to what we're doing.

https://www.heavybit.com/library/podcasts/the-secure-developer/ep-13-how-new-relic-does-security/

Slack CSO

Geoff Belknap

- The Slack Security team was originally part of the privacy and policy organization,.. now I report directly to Cal Henderson, our CTO… and you know a first-class citizen in engineering
- we sent Atlassian some cake or some cookies recently… in the past we've also sent cake or pizza when friends are having a bad day… even though we're all in this market, and we're competing against each other… we all rise and fall together, right?

https://www.heavybit.com/library/podcasts/the-secure-developer/ep-14-how-slack-stays-secure-during-hyper-growth/

Look for ways to

Engage Dev in Security

Include Security in DevOps Shared ownership:

1. Find security tools dev will actually use
2. Look for ways to engage dev in security

DevOps helps

deliver value and adapt to market needs

faster and at scale

1. **Securing DevOps Technologies**
2. **Security in DevOps Methodologies**
3. **Include Security in DevOps Shared Ownership**

Security For DevOps Technologies:

1. Adapt existing security tools to new tech
2. Address new security risks new tech introduced

Security For DevOps Methodologies:

1. Adapt how existing security tools are applied
2. Use the new opportunities to do security better

Include Security in DevOps Shared ownership:

1. Find security tools dev will actually use
2. Look for ways to engage dev in security

One

Last Point…

We have it

Backwards!

DevOps is first and foremost
About People!

Embrace the DevOps
Shared Ownership of Security
and the rest will follow…

Check out Snyk at the Expo Hall!

The Three Faces of DevSecOps

Guy Podjarny (@guypod)

Thank you!