Losing my Religion

Successful and unsuccessful approaches to API security in a global enterprise

Darren Shelcusky
Manager Vehicle and Connected Cybersecurity
Ford Motor Company
dshelcus@ford.com

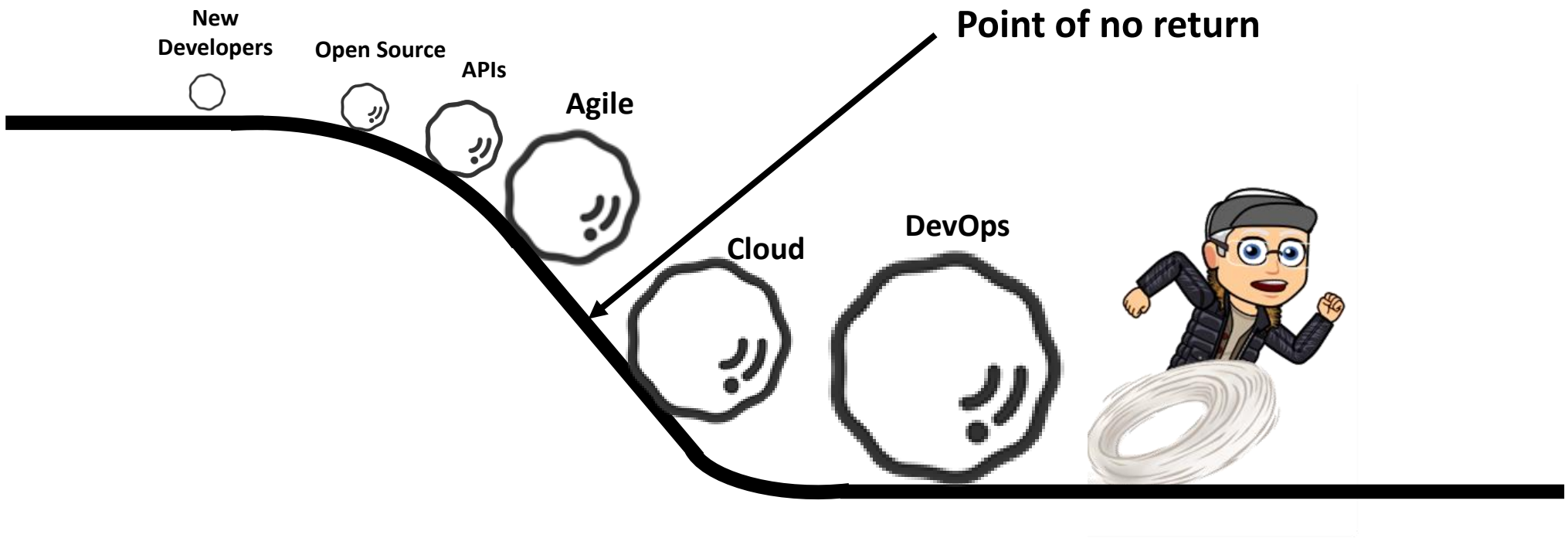
Cybersecurity == Unrequited Love

At My Wit's End…..

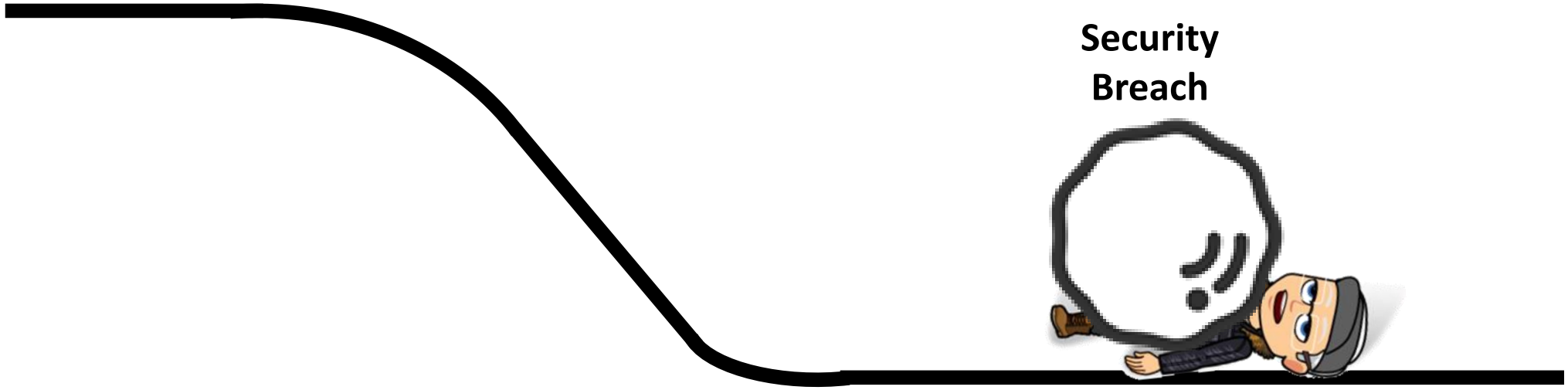
R.E.M. Losing My Religion

Oh, life is bigger, It's bigger
than you and you are not me
The lengths that I will go to
the distance in your eyes
Oh no, I've said too much, I set it up
That's me in the corner
That's me in the spotlight
Losing my religion

The Cybersecurity Snowball Effect



Eventually It Is Too Late



Result: A Terrible Horrible No Good Very Bad Day

That's me in the corner…

That's me in the spotlight
Losing my religion

Question: How Do You Prevent An API Dumpster Fire?

- API Cybersecurity has not been a priority for many companies
- APIs provide vectors that attackers can easily exploit
- The OWASP API Security Top 10 list was only released on 31 Dec 2019

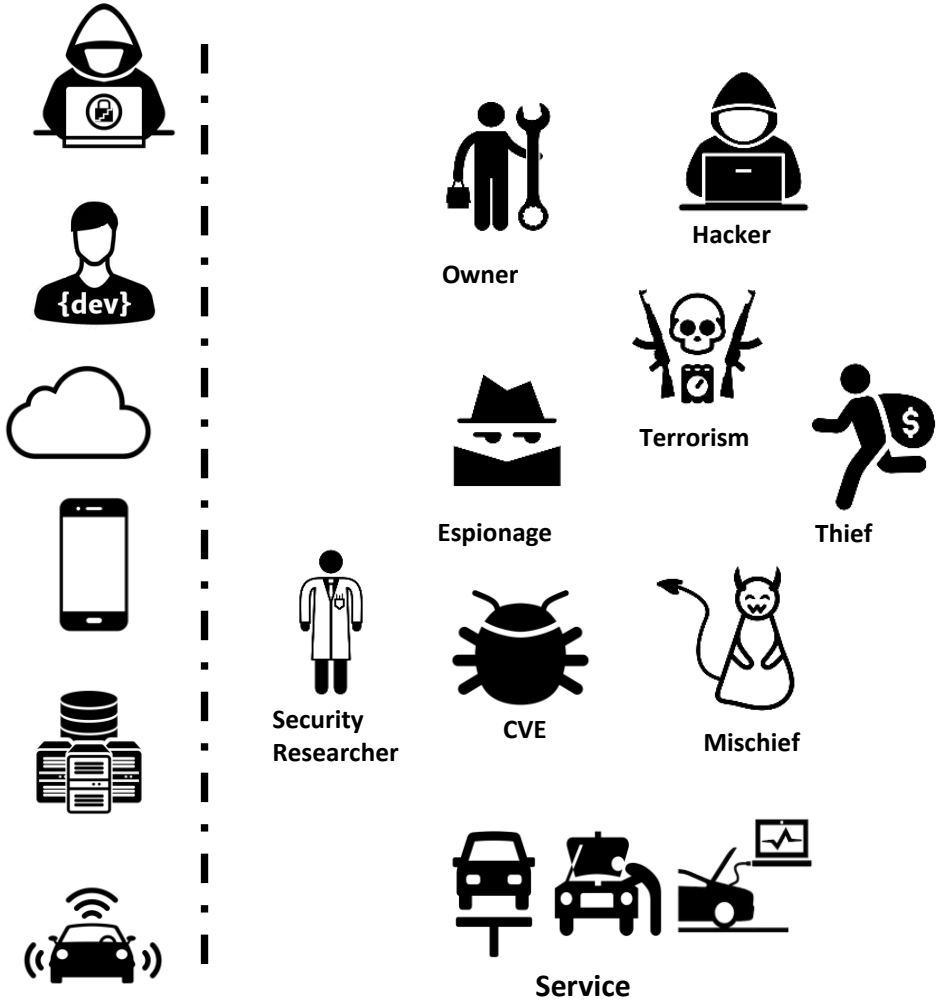
How Do You Approach These API Cybersecurity Questions?

What are the failure modes for API security in a global enterprise?

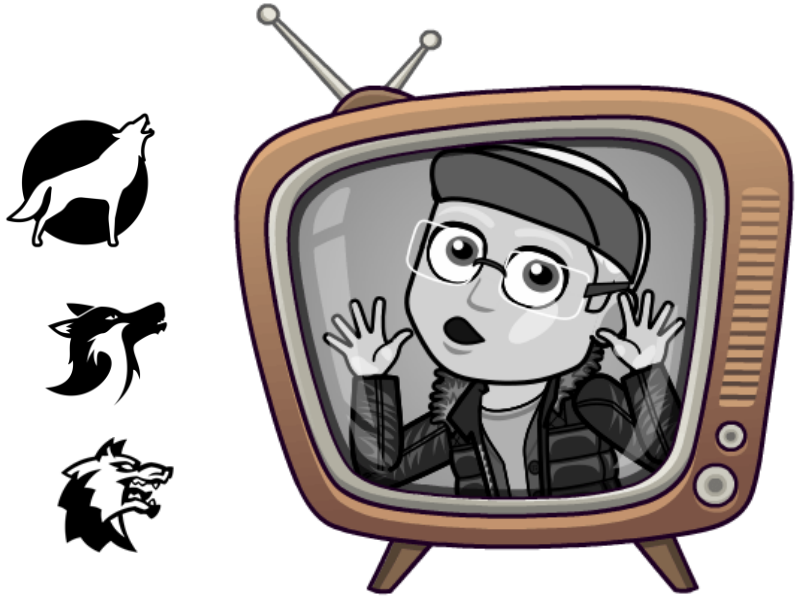
What are the consequences of these failures?

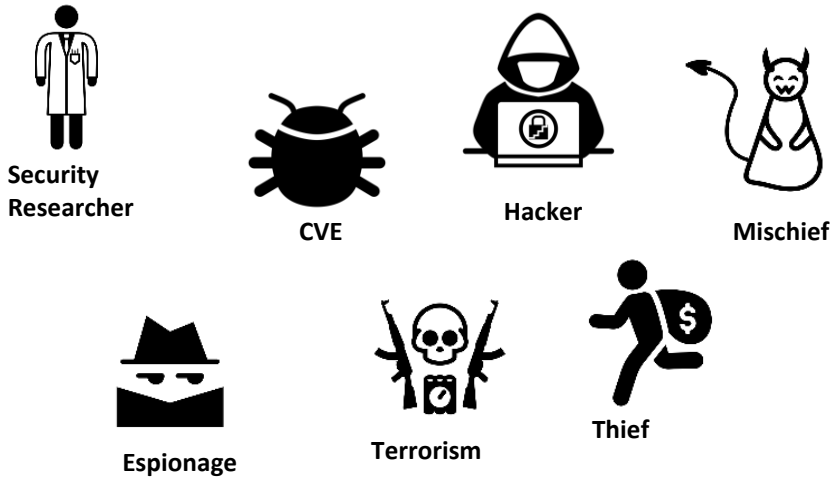
How can global enterprises prevent and remediate these failure modes?

Fail: Try A Wack-A-Mole Approach To API Cybersecurity



Fail: Try Monitoring Everything





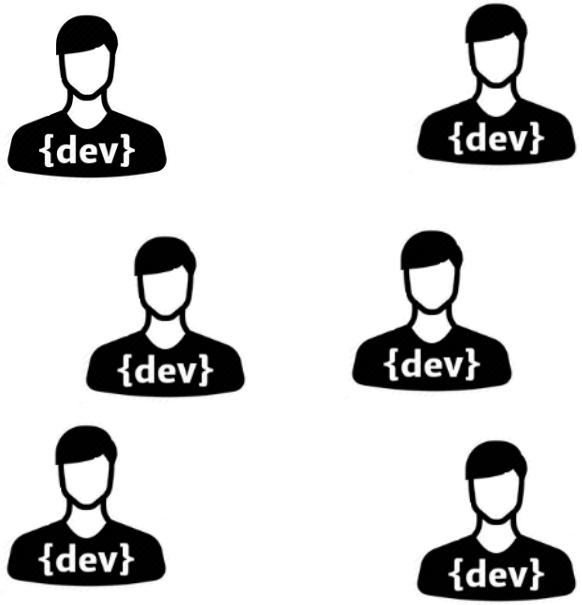
Like the boy who cried wolf, security professionals are prophets of woe until someone sees a wolf

It is notoriously difficult to prove the absence of something

We all know wolves exist and that they are dangerous, but until they attack us, the guidance of security professionals is often reduced to hyperbole

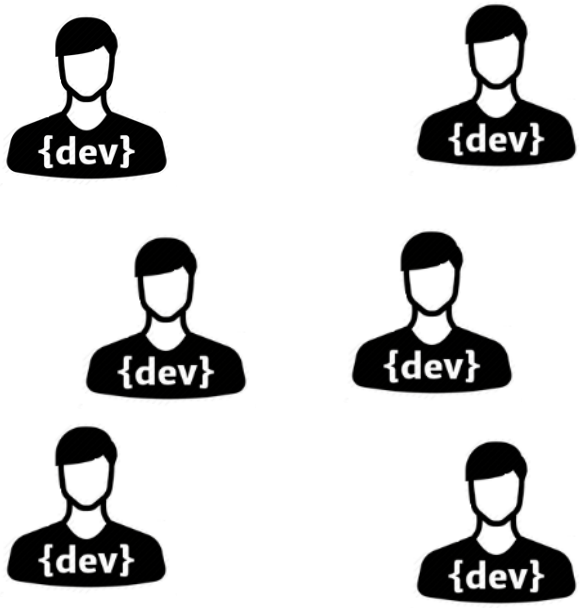
Fail: Try Mandating Policy And Standards For Everything

Having a policy or standard is not enough



A policy is only effective when employees understand and use it in the development process

Fail: Try A Command-And-Control Approach To API Security



Hierarchical organizations with no employee autonomy or input do not work for agile product teams

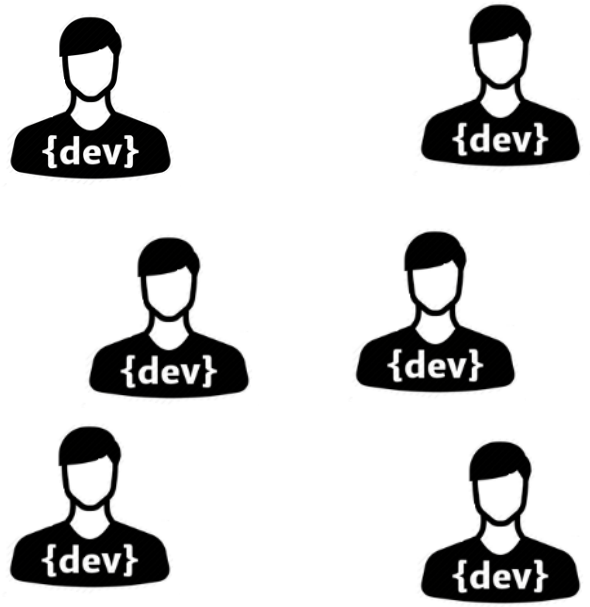
Leaders who insist teams follow their decisions without question are shutting off constructive feedback that could reshape a product, preempt a poor decision, or even change the company for the better

Fail: Try Fear

If your emotional outbursts simply provoke another emotional reaction, like fear, nobody benefits

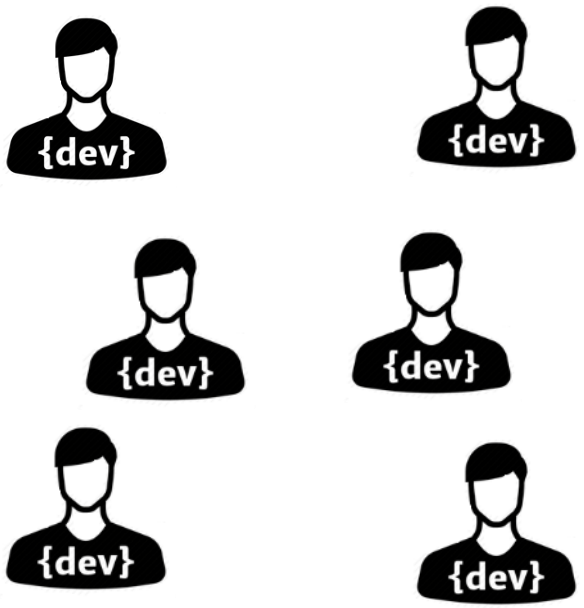
“Anyone who doesn’t do this will be fired”

Jeff Bezos Amazon API mandate



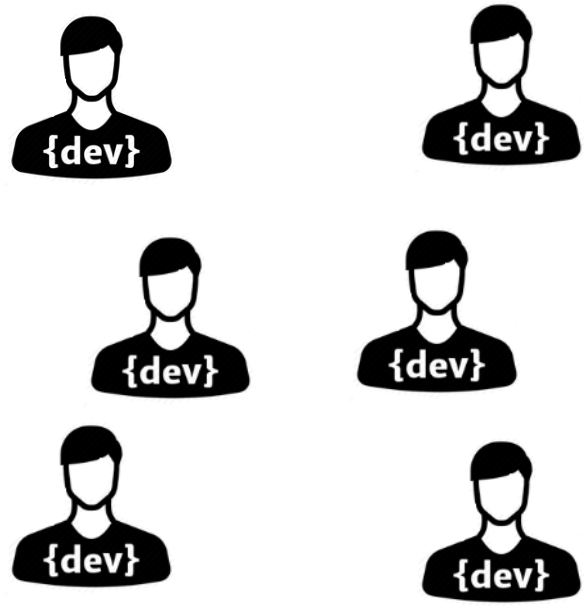
Nothing makes us more uncomfortable than fear, while fear is a powerful motivator, but it is a negative one

Fail: Run Everything Through Governance



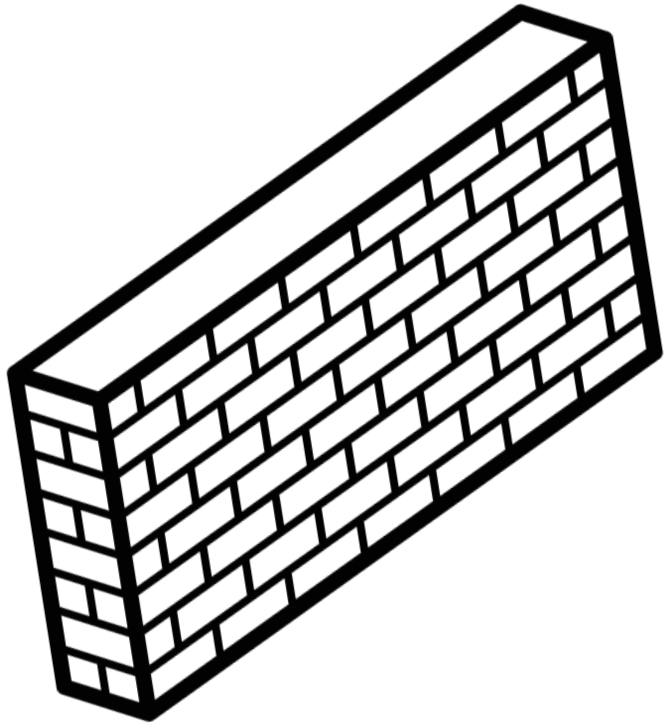
Governance checkpoints can wreak havoc on an agile team as it is often incompatible with work done in an iterative manner

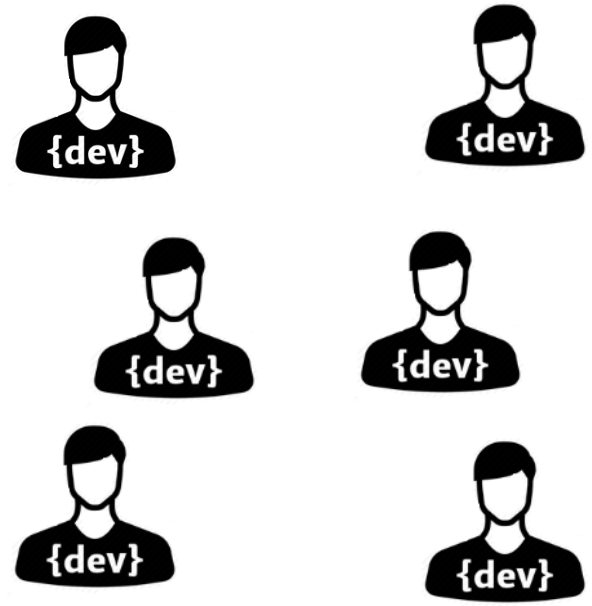
Consequence: You Eventually Get Ignored Or Malicious Obedience



“Our product is late because of cybersecurity”

Consequence: Product Teams Will Erect A Security Firewall





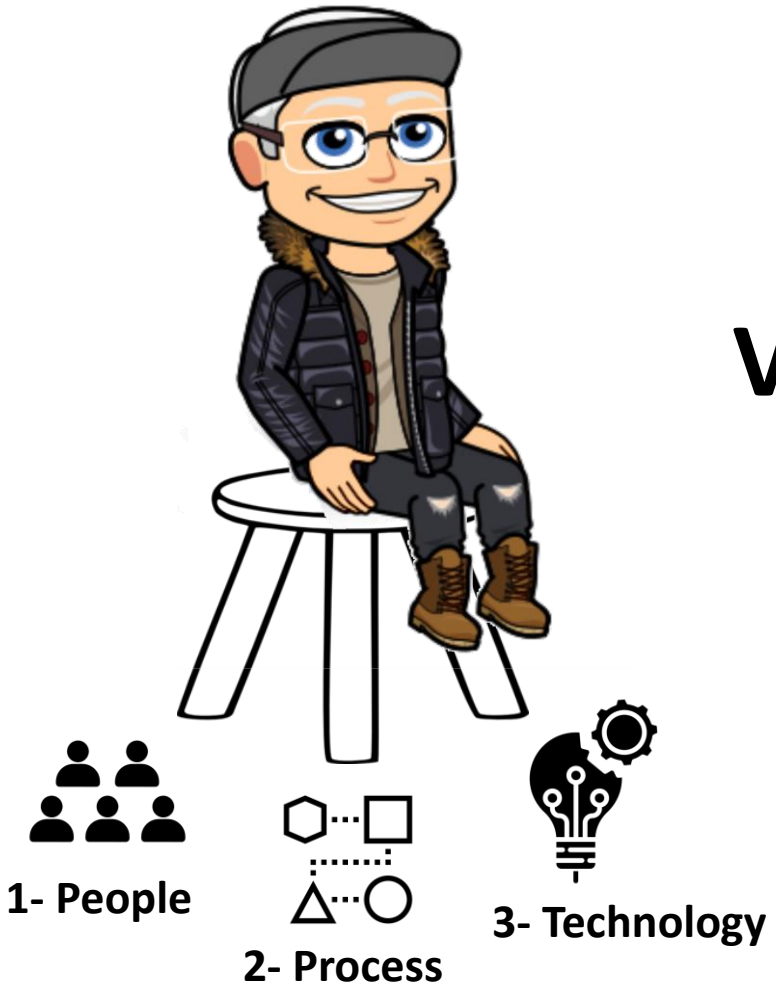
"You have to remediate this because our checker found it"

Developers are often resistant to their company creating an API security program for fear of being slowed down in delivering their products

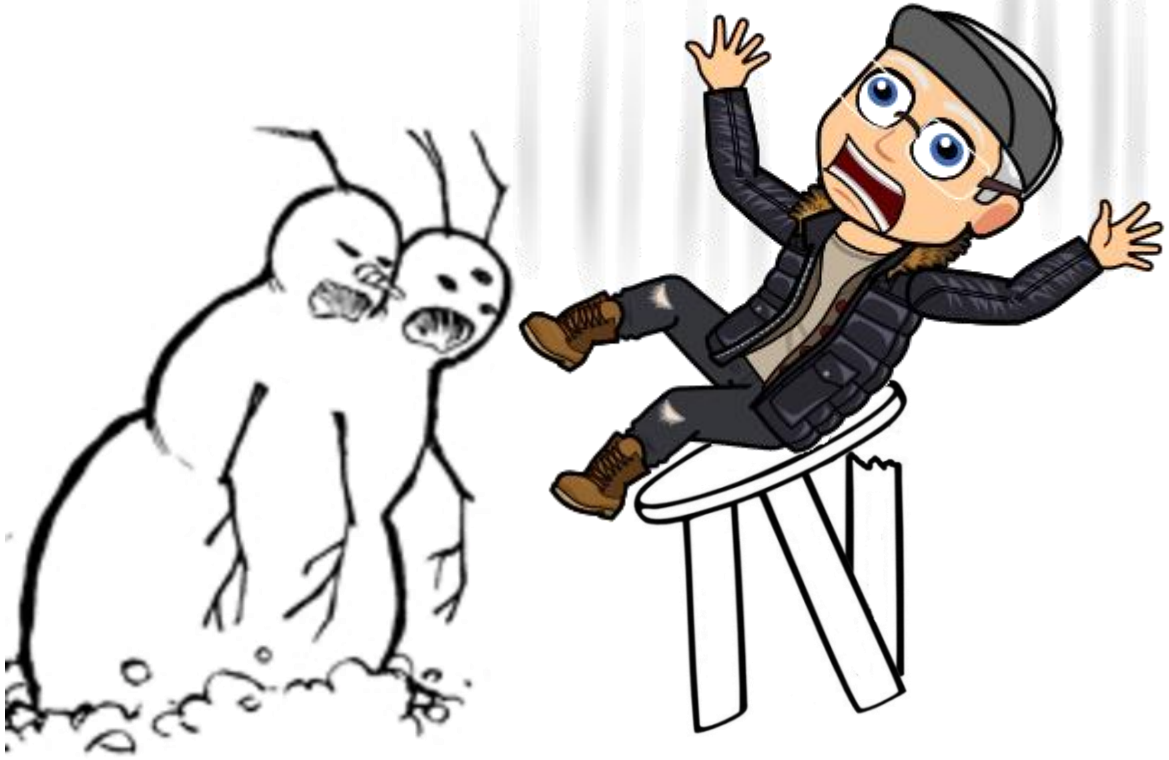
Insight: You Must Address API Cybersecurity Systemically

How Do You Build A Snowman?

Approach: API Security Is A Balancing Act



Versus



Cybersecurity is **NOT** a security problem, it is a shared business responsibility – people, processes, technologies that work together to manage risk

Approach: API Security Mandates Continuously Listening

“Relationships precede processes and outlive transactions” – **Bob Lewis**

Organization are collections of relationships, with good relationships, everything can work, without them, nothing can

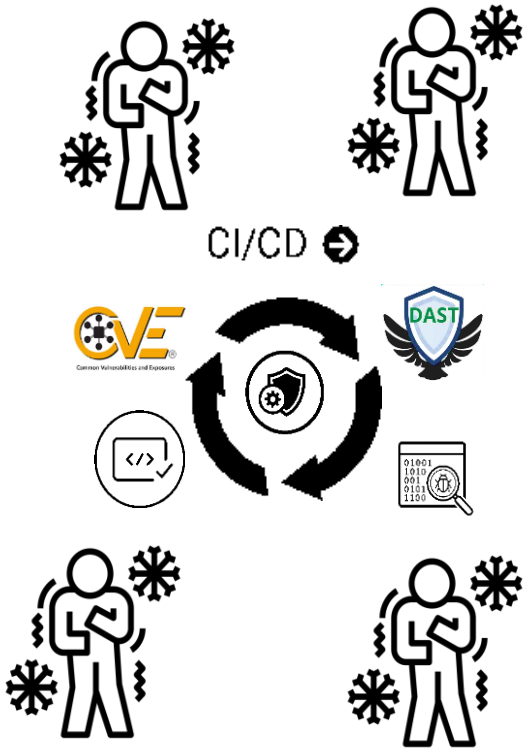
Approach: API Security Requires You To Roll Up Your Sleeves And Become Part of The Solution

Developers do not appreciate manual security mandates

Security must find ways to eliminate manual work wherever possible, and augment manual efforts with automation

Approach: Your Most Important Skill: Empathy

Empathy, the ability to share someone else's feelings, is perhaps the most important trait humans demonstrate



Empathy is the Secret Sauce for Security, as human interactions are at the heart of most issues

Plan: 5 Steps to Strengthen API Security Posture

Manage Business Risks, Not Security…

1. Know your inventory
2. Audit your sensitive APIs
3. Attack the OWASP top 10
4. Trust but verify
5. Coordinated disclosure and bug bounty

Plan: Make The Right Thing The Easiest Thing To Do

1. Complete API catalog
2. Self-Service onboarding and publishing
3. Trust but verify
4. Focus On API Quality
5. Automated governance
6. Ensure API documentation a 1st class artefact
7. API Style Guide (actually use it)
8. API Standard (actually follow it)
9. Monitor API Health using SRE principles
10. Make security artefacts a 1st class deliverable

“If it doesn't add value, it's waste" - Henry Ford

Result: Only Then Will You Earn Trust and Respect

The negative perception of security is often the result of security dictating rules, workflows and tools on developers instead of creating strong partnerships, common goals, and tools that seamlessly integrate with the development toolchain

Building An API Security Program Takes Time, Dedication, And A Plan

APIs have evolved from an obscure technical term for developers to the backbone of the Digital Transformation and a major source of income and innovation for many businesses

But The Results Are Worth It

The biggest challenge of API security is still raising awareness of API risks and methods/tools that exist to mitigate them

APIs are one of the “crown jewels” of many modern businesses

Questions

ENTERPRISE API SECURITY

HOW CAN 42CRUNCH HELP?

DARREN SHELCULSKY
Manager of Vehicle/Cybersecurity @ Ford

ISABELLE MAUNY
Field Chief Technical Officer @ 42Crunch

API SECURITY THE “ARTISANAL” WAY

And then, **this** happens…

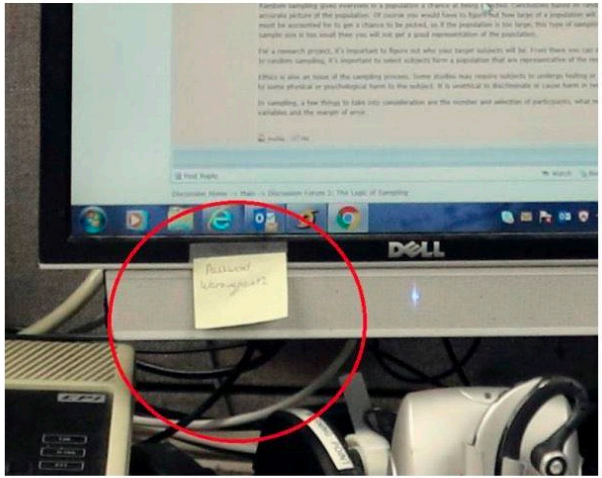
Hawaii prepares for 'unlikely' North Korea missile threat

Associated Press Friday, July 21, 2017

Credit: The Associated Press

Jeffrey Wong, the Hawaii Emergency Management Agency's current operations officer, shows computer screens monitoring hazards at the agency's headquarters in Honolulu on Friday, July 31, 2017. Hawaii is the first state to prepare the public for the possibility of a ballistic missile strike from North Korea. (AP Photo/Jennifer Sinco Kelleher)

Wong and the operators in the room forgot to take down the sticky notes with the passwords on the screens.



The system password is **"Password Warningpoint2".**


MAIN GOAL
Ensure APIs are as secure as possible before they get deployed in production

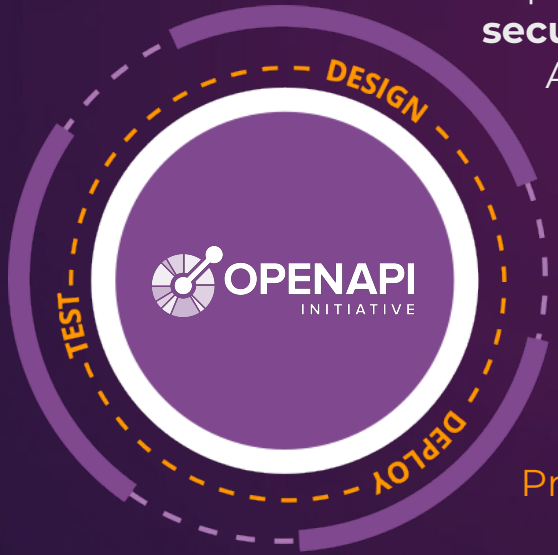
OpenAPI: a de-facto standard

OpenAPI Specification (formerly Swagger Specification) is an API description format for REST APIs. An **OpenAPI** file allows you to describe your entire API, including available endpoints like /users, operations on each endpoint GET /users , POST /users) and payloads.

3scale BY RED HAT
42crunch
ably
Acumatica The Cloud ERP
AMBASSADOR LABS
APImetrics API INTELLIGENCE
Band Protocol
Bloomberg
Checkly
ebay
Google
HM Government
HSIS
IBM
IFS
Intento
Interzoid
Isa
Kong
LEVEL 250
LinksRez
Microsoft
MuleSoft
NHS X
opentravel enabling the future
ORACLE
Osaango
POSTMAN
RepreZen
SAP
SMARTBEAR
Stoplight
talend
TeejLab DATA | RESEARCH | SOFTWARE | INNOVATIONS
Timewarp
TORO CLOUD
Tyk
VONAGE

HOW 42CRUNCH LEVERAGES OAS

Audit Service performs **200+ security checks** on API Contract



Scan service ensures API implementation **conforms to API contract**

Protection service is **automatically configured** from API contract

Security Virtuous Loop

OpenAPI definition & code pushed to repository

Automated Security Assessment

Automated Security Policies Attachment

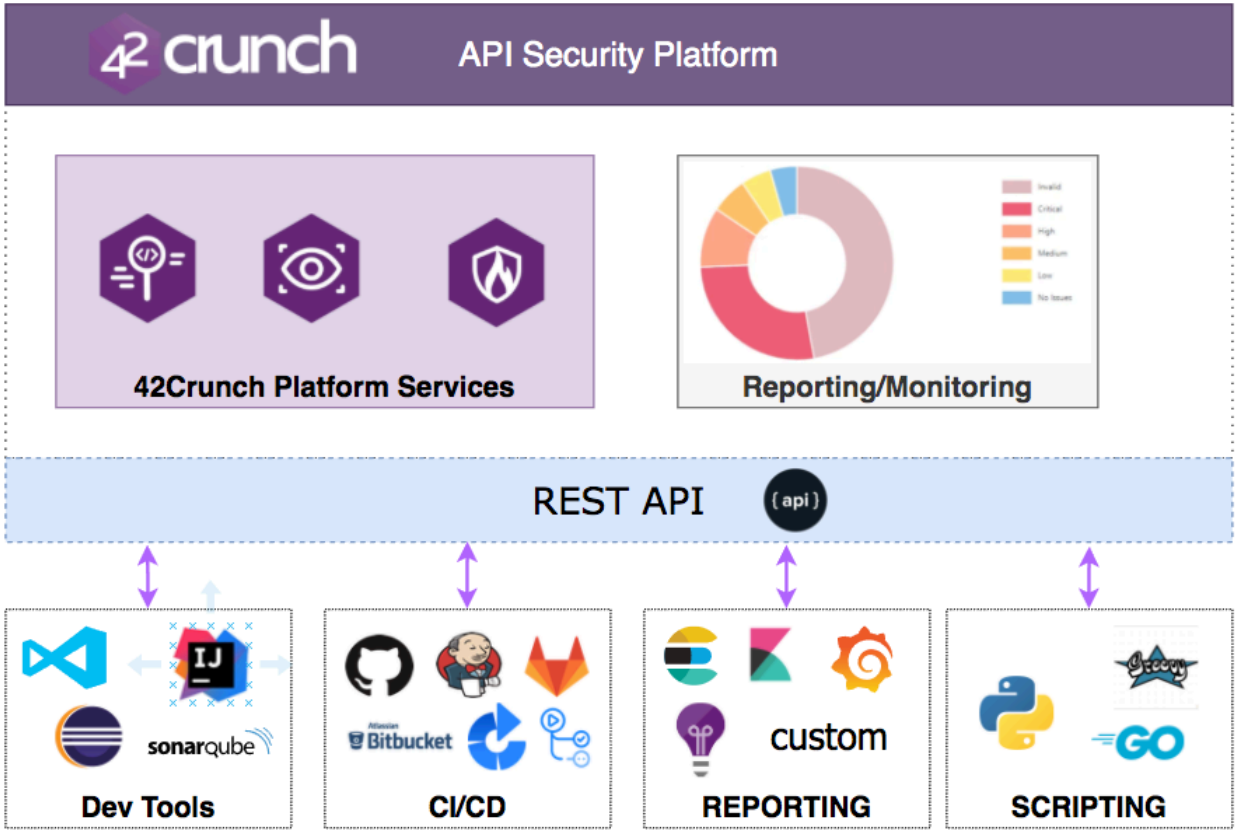
Micro Firewall Image Generation

Firewall Deployed to Protect API

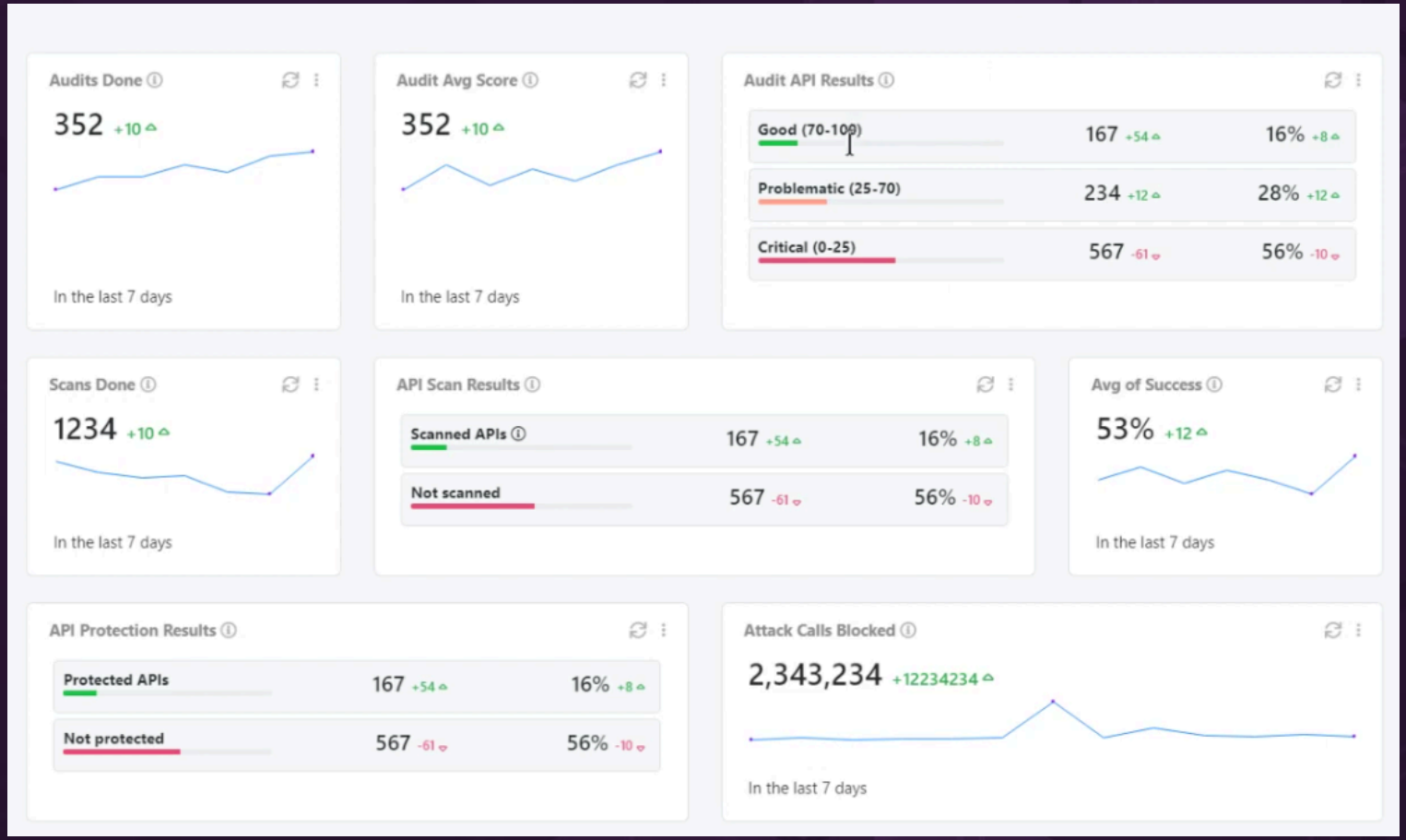
CONTINUOUS, AUTOMATED API SECURITY

Capturing and addressing security issues early without affecting developer's productivity

Blending into Development Ecosystem



SINGLE PANE OF GLASS



42crunch

Thank you!

Contact us | info@42crunch.com | 42crunch.com

Free security tools from 42Crunch

https://42crunch.com/resources-free-tools/