The Race for Your Data

And How to Win.

David Fidler
@IT-SA 2019

What do we expect from cybersecurity

Secure Systems.

Every Day is Race Day

- Every New CVE announcement signals a new race for your data
- Hackers, Organized crime, Governments, Script Kiddies, etc
- Attackers are Organised

- Today, they have an Unfair Advantage

99% of exploits...occur on systems where the vulnerability is already known*.

- Gartner

*** Full Quote:** **"**Gartner believes that 99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident… Zero day vulnerabilities made up only approximately 0.4% of vulnerabilities in the past decade**",** - *Craig Lawson, "Implement a Risk-Based Approach to Vulnerability Management", Gartner*

99% exploited more than a year after the vulnerability was published*

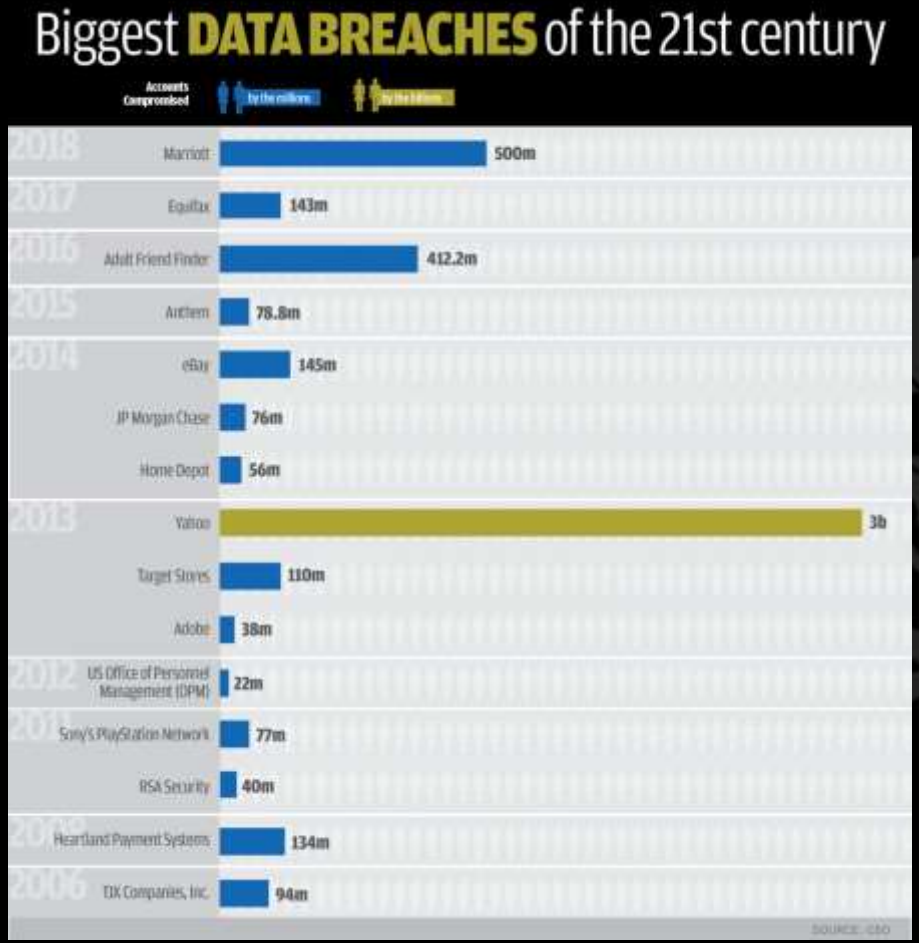
-Verizon

*** Full Quote:** “We found that 99.9% of the exploited vulnerabilities had been compromised more than a year after the associated CVE was published”, - - 2015 Data Breach Investigations Report, Verizon

The Result...

Collectively, tens of Billions of personal records compromised, costing more than that in damages to businesses and their brands*.

*Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021
https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/



Are we doing a bad job?

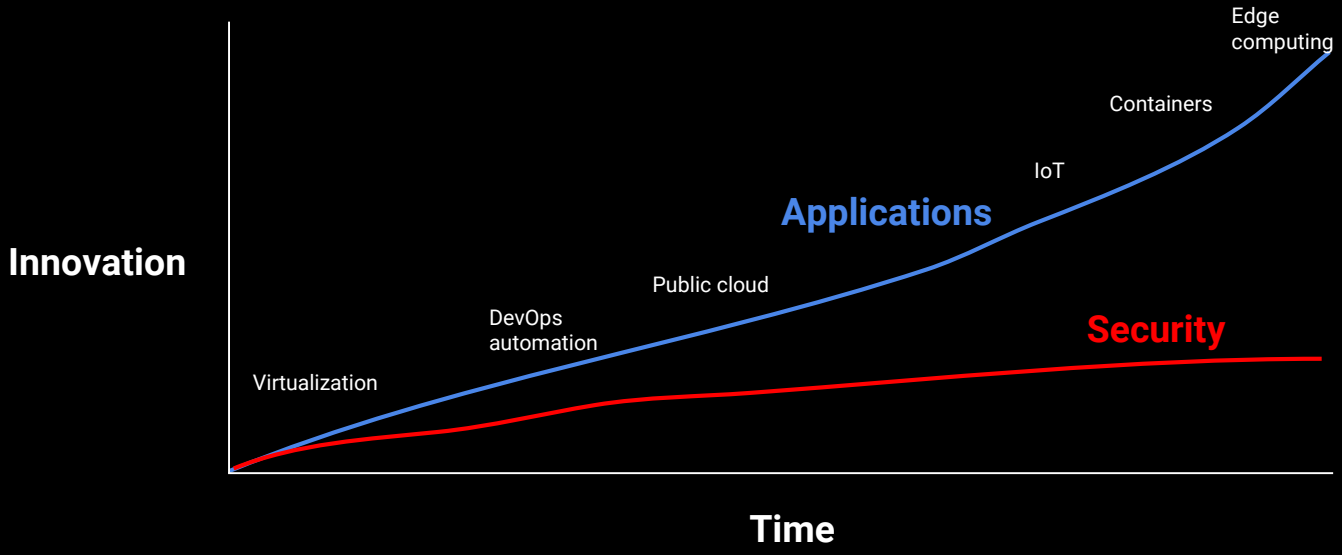
No.

(but we're losing some races and it's costing us)

Configuration Standards
Patch Management
CVE Telemetry
Passwords
Network Access
Log & Pattern Analysis
Code Analysis
Anti-Virus
Access Control
Bastions
Firewalls
Network Segregation
Configuration Drift
Unauthorized Changes
End-User Education
Phishing Attacks/Spam
Breach Forensics
Public Cloud
IoT / Mobile Devices

Scale. Only Getting Harder.

Innovation Has Outpaced Security



Secure Systems.

How?

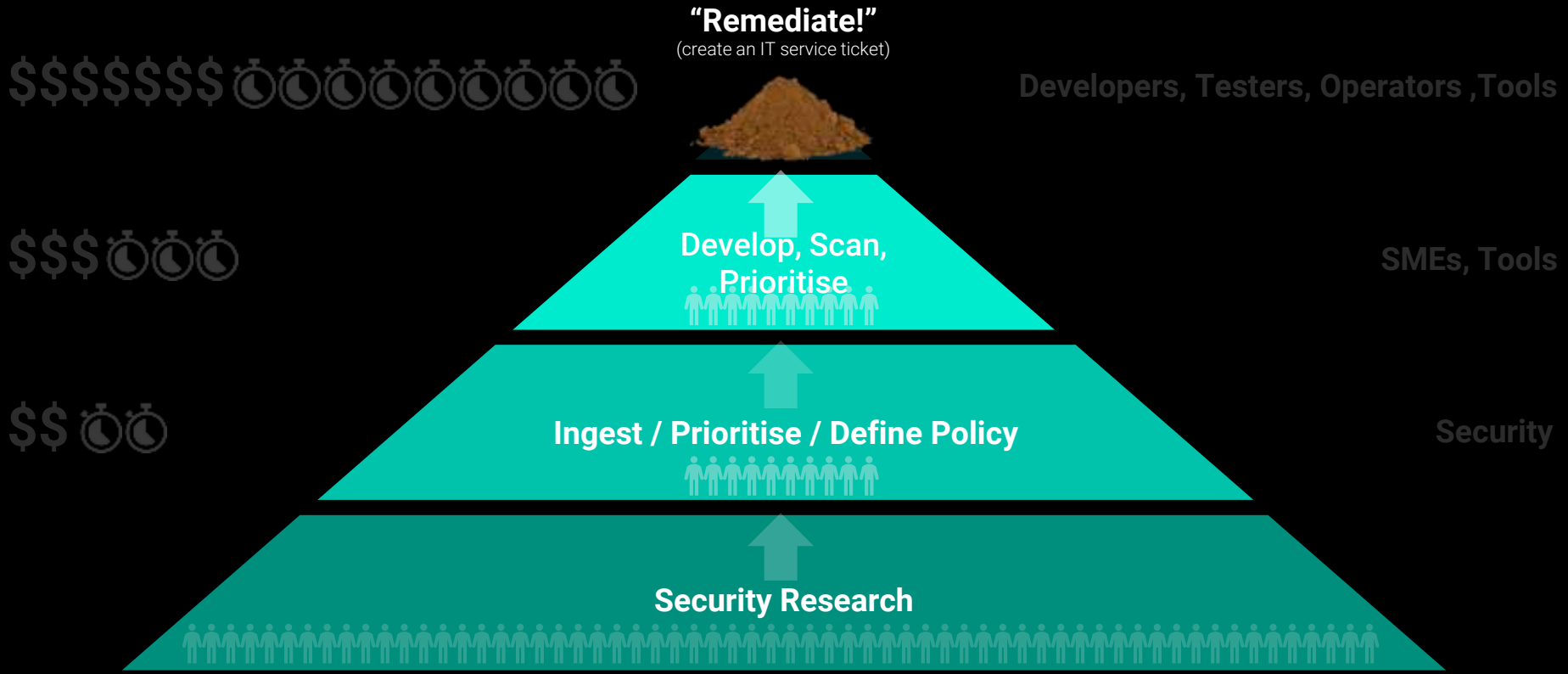
- Constant / *Timely* Configuration Compliance
- Constant / *Timely* Vulnerability Management (~Patching)
- Reduce Complexity (fewer point solutions/integrations)
- Secure / *Timely* Processes
- *Scale*…
- Evidence to Auditor…

Security wasn’t invited to the DevOps Party.

DevOps movement focused on release cadence.

Oops. Let’s try “DevSecOps”.

Current Security Model



SecOps in Legacy Estates

- Monolithic Applications
- Long Release Cycles
- The Truth: There's more of these than DevOps lead projects

We don’t have the luxuries of the DevOps movement

- Can’t rewrite how existing systems work with Kubernetes
- No container “Silver Bullet”
- Legacy systems need to be kept secure alongside new systems
- Application deployment tech exacerbates security issues
- DevOps doesn’t fit [and won’t for decades]

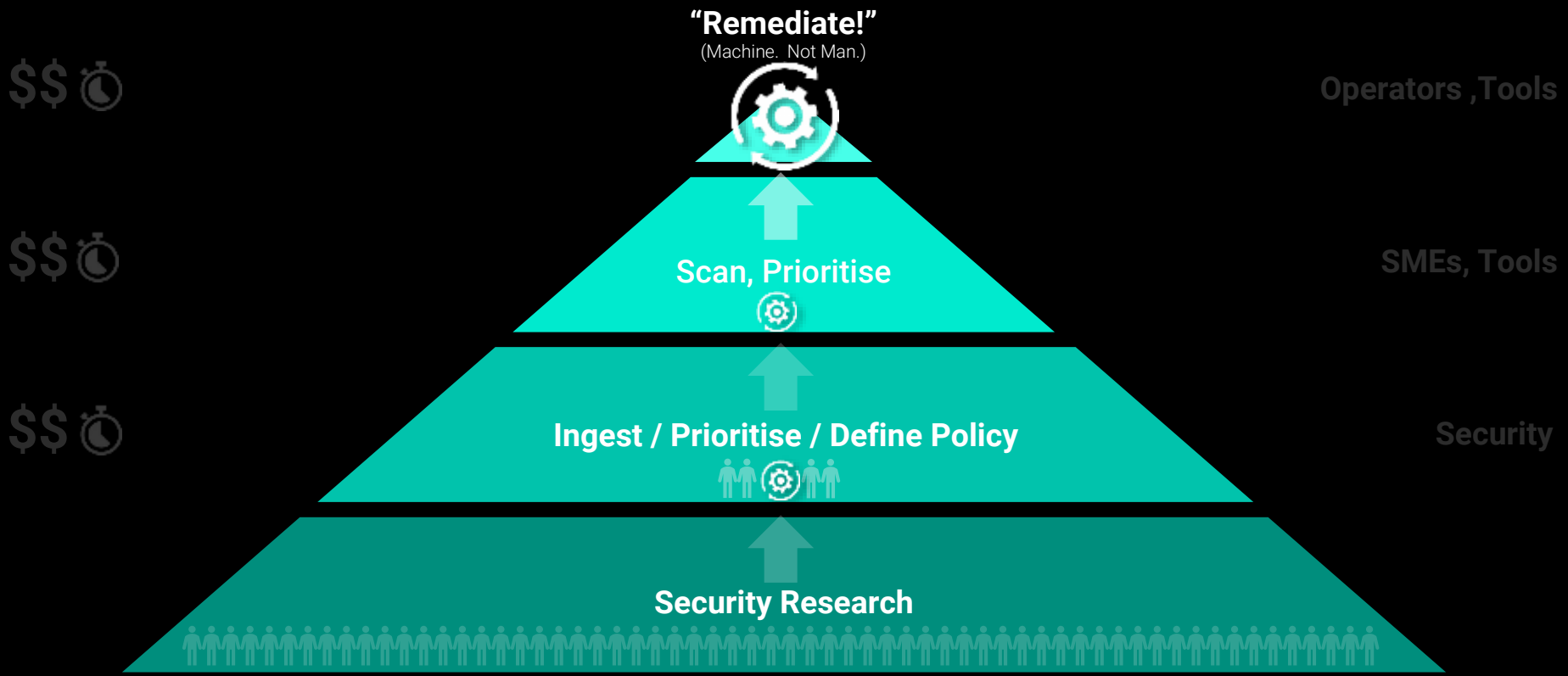
Win the Race?

Make it Timely.
Make it Scale.

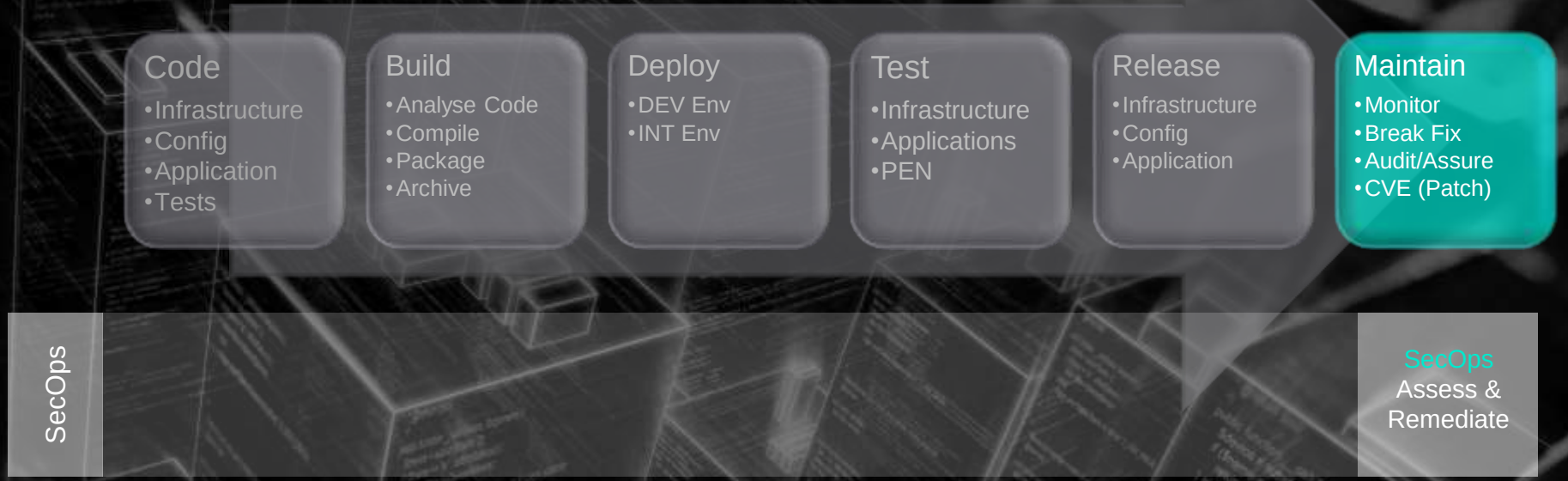
Security as Code. Machine. Not Man.

- Key: Vendors with *certified* content services that Identify and FIX issues based on policy
- Key: Define automation policy (and exceptions) – what is allowed to be fixed automatically
  - Automatically scan for config non-compliance / vulnerabilities
  - Automatically enforce config compliance
  - Automatically patch to policy
- Key: Define policy in the same system that is used by operations; Fewer systems = fewer handoffs / integrations / complexity

Target Security Model



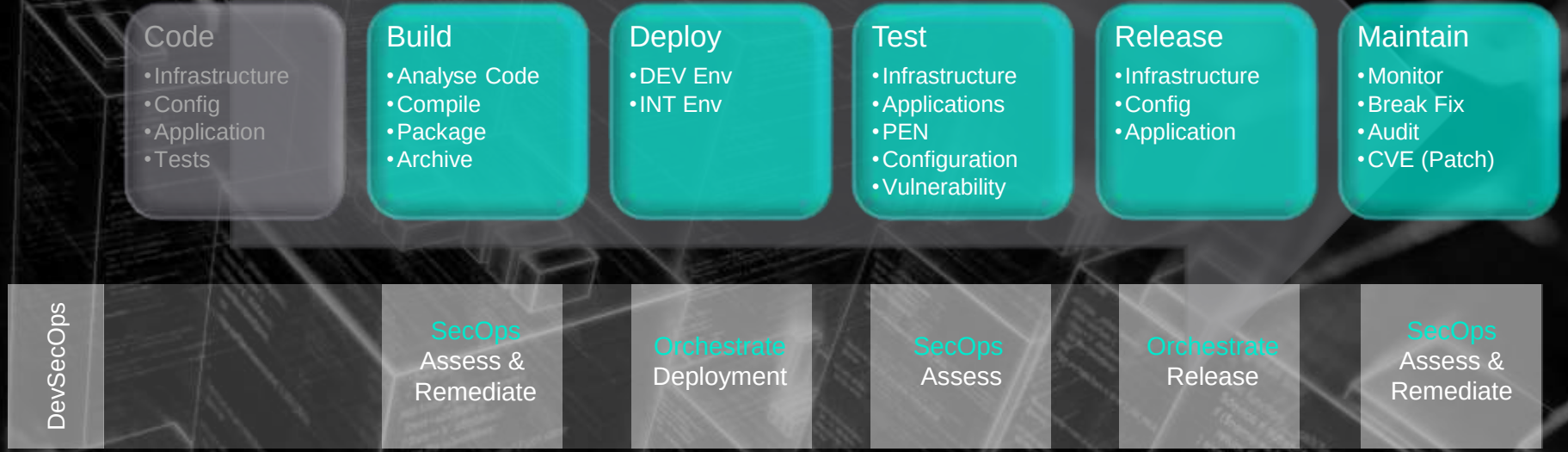
SecOps Pipeline



DevSecOps?

- Security Patch to DevOps…

“DevSecOps” Release Pipelines



DevSecOps is not complicated

With the right tools and services.

Who am I?

David Fidler @ SaltStack, Inc

17 Years designing, deploying or supporting automation software and solutions for security purposes

- Developer
- Operations/Admin
- DevOps Leader
- Automation Architect
  - Cloud / Finance / Telecom / Public Sector

In my experience…

- Companies are re-inventing the wheel with in-house content creation
- Haven't met a Cybersecurity team that has met it's aspirational patching goals – always fall short of CIO response targets
- Companies are struggling to manage at the scale they have, let alone what they project

- *Until I joined SaltStack, I didn't think there was a product that could deliver all of this without investing many point solutions with an expensive integration project.*

Come say Hi

Hall 10.1 / 10.1-625