The State of DevSecOps

Stefan Streichsbier
@s_streichsbier

Background

- Professional white-hat hacker
- Actively involved in building the DevSecOps community
- Identified severe shortcomings in security processes and tech resulting in GuardRails

What are we going to cover?

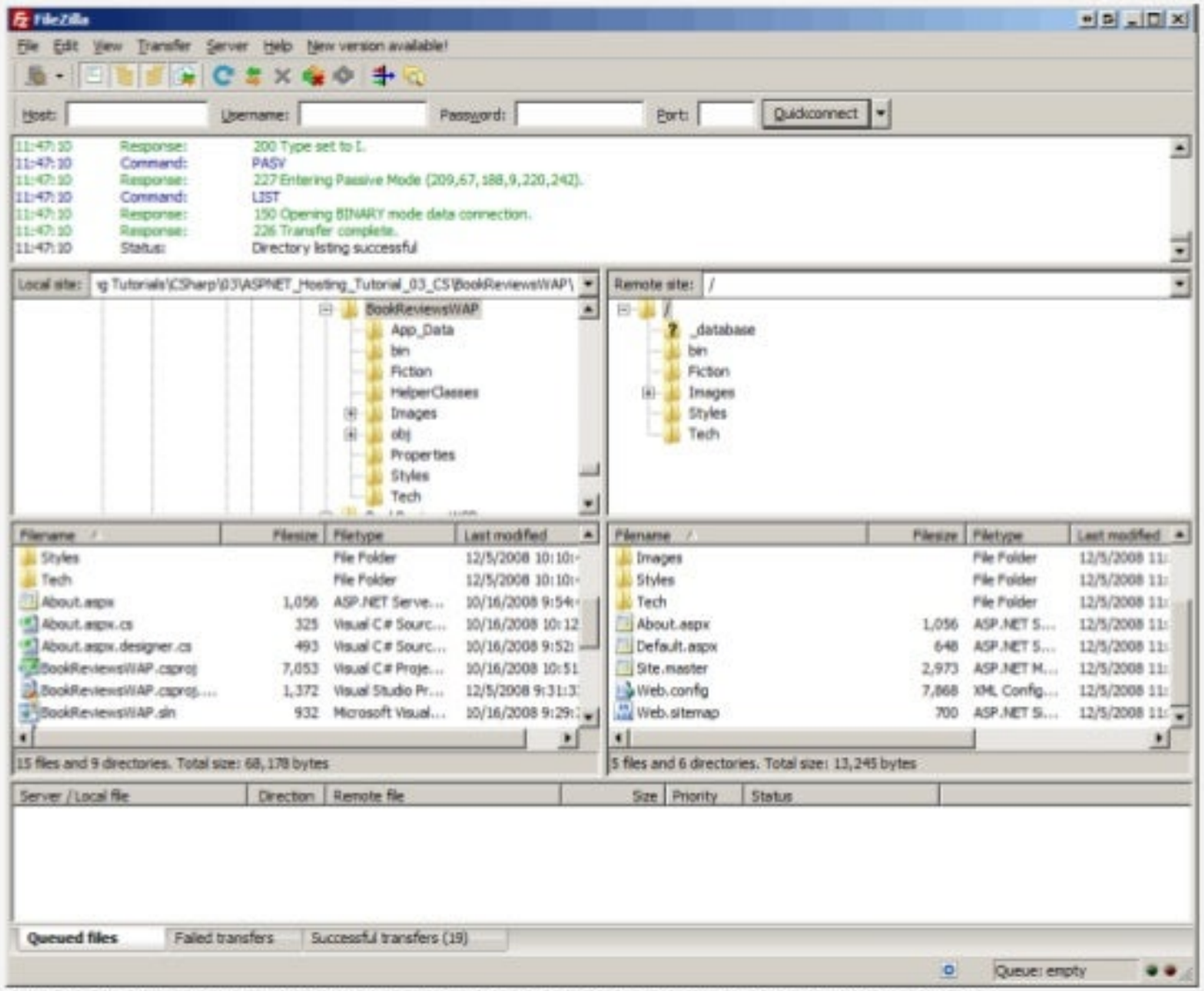
Brief History of DevOps

State of Security in DevOps

Common Pitfalls and suggestions For DevSecOps

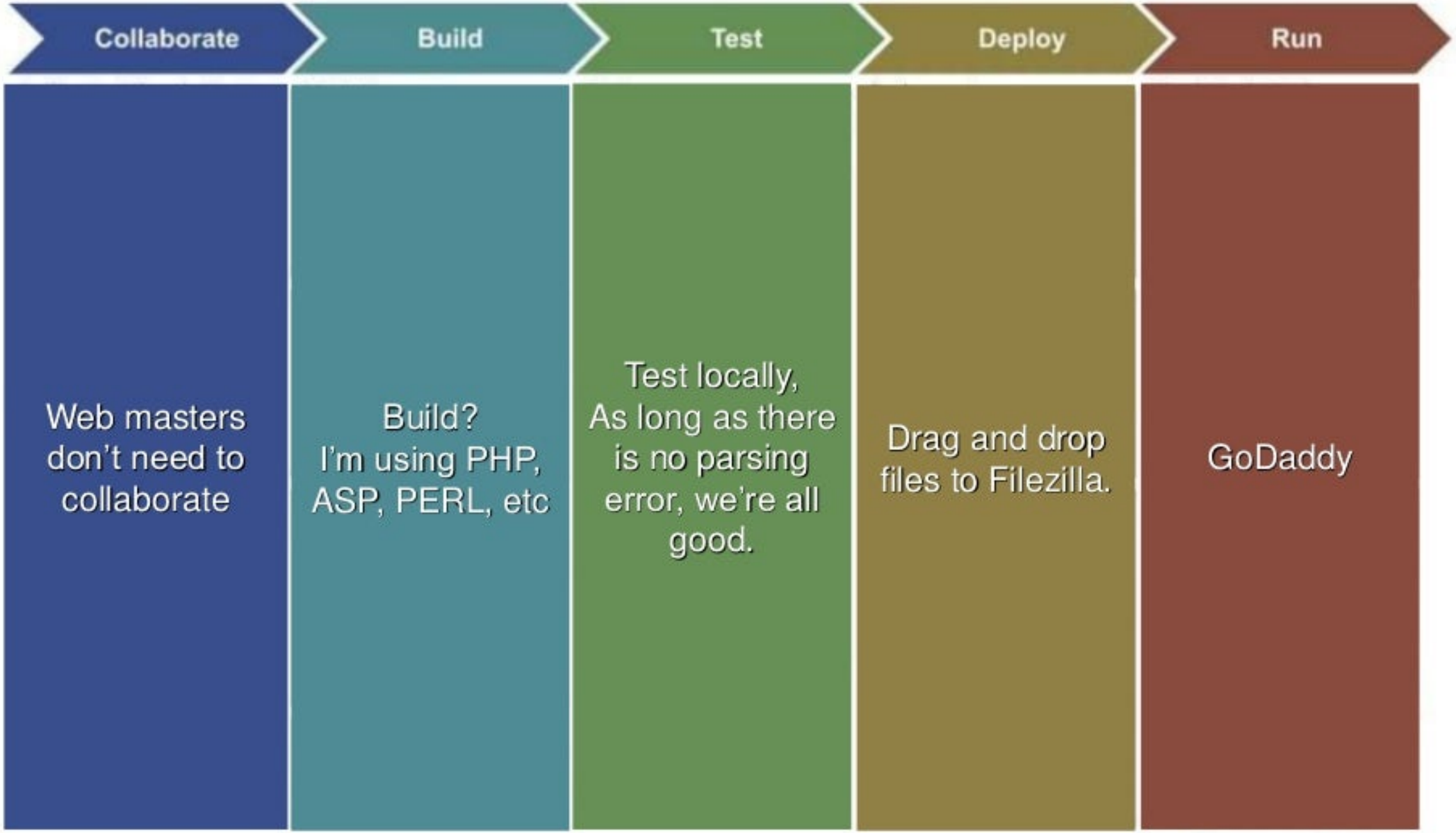
And also, how security and developer experience are related.

It used to be so simple



Source: https://docs.microsoft.com/en-us/aspnet/web-forms/overview/older-versions-getting-started/deploying-web-site-projects/deploying-your-site-using-an-ftp-client-cs

Figure 1: Use an FTP Client to Copy the Necessary Files from Your Desktop to the Web Server at the Web Host Provider.


Collaborate
Build
Test
Deploy
Run
Web masters don't need to collaborate
Build? I'm using PHP, ASP, PERL, etc
Test locally, As long as there is no parsing error, we're all good.
Drag and drop files to Filezilla.
GoDaddy

Tech Startups in Asia – #10YearChallenge

tokopedia

2009

vs

2019

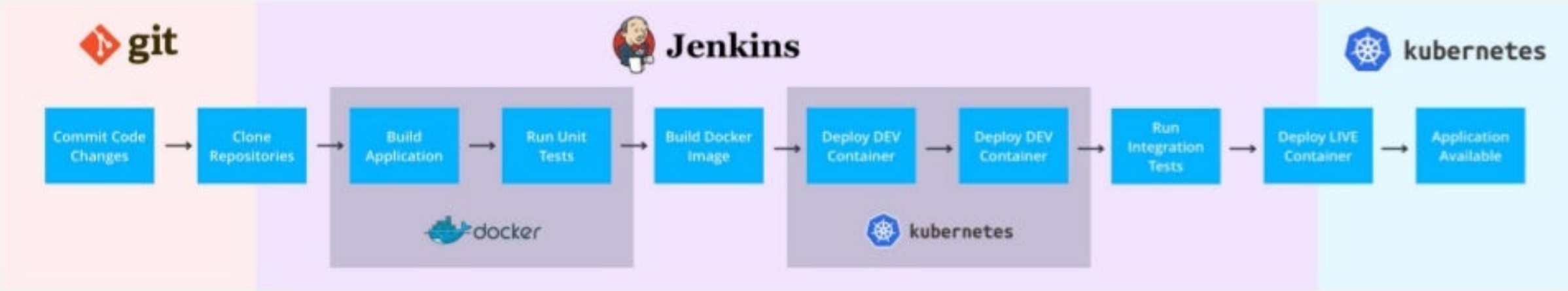
How is that possible?

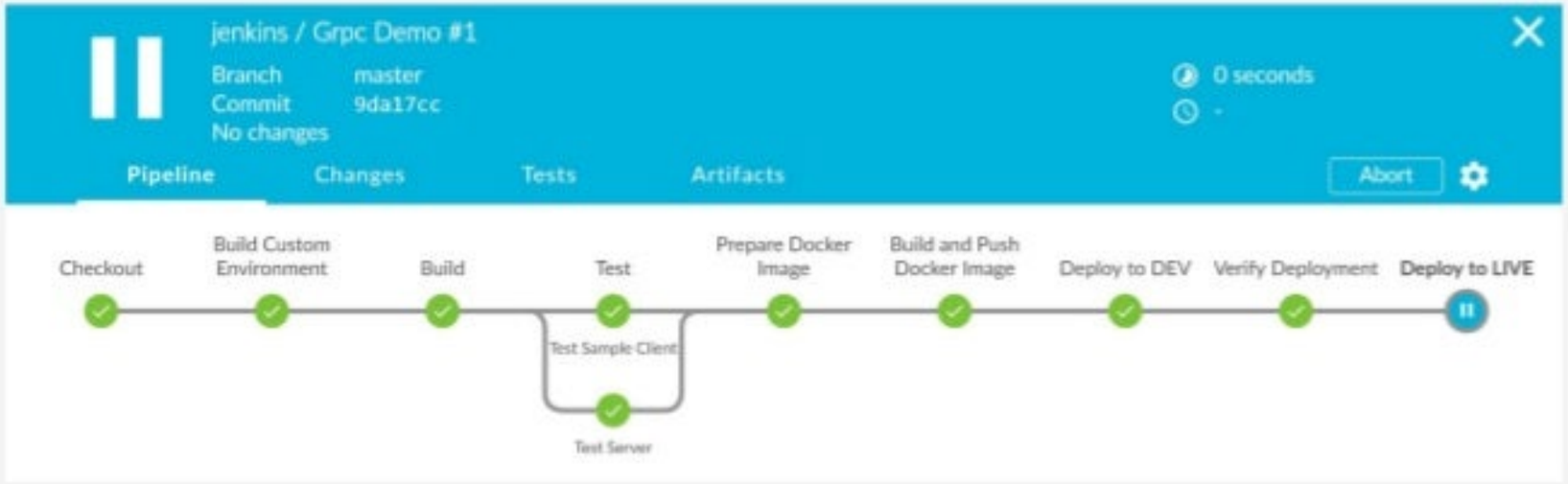
Creating new technology solutions was never faster or cheaper

Software can built locally but distributed globally

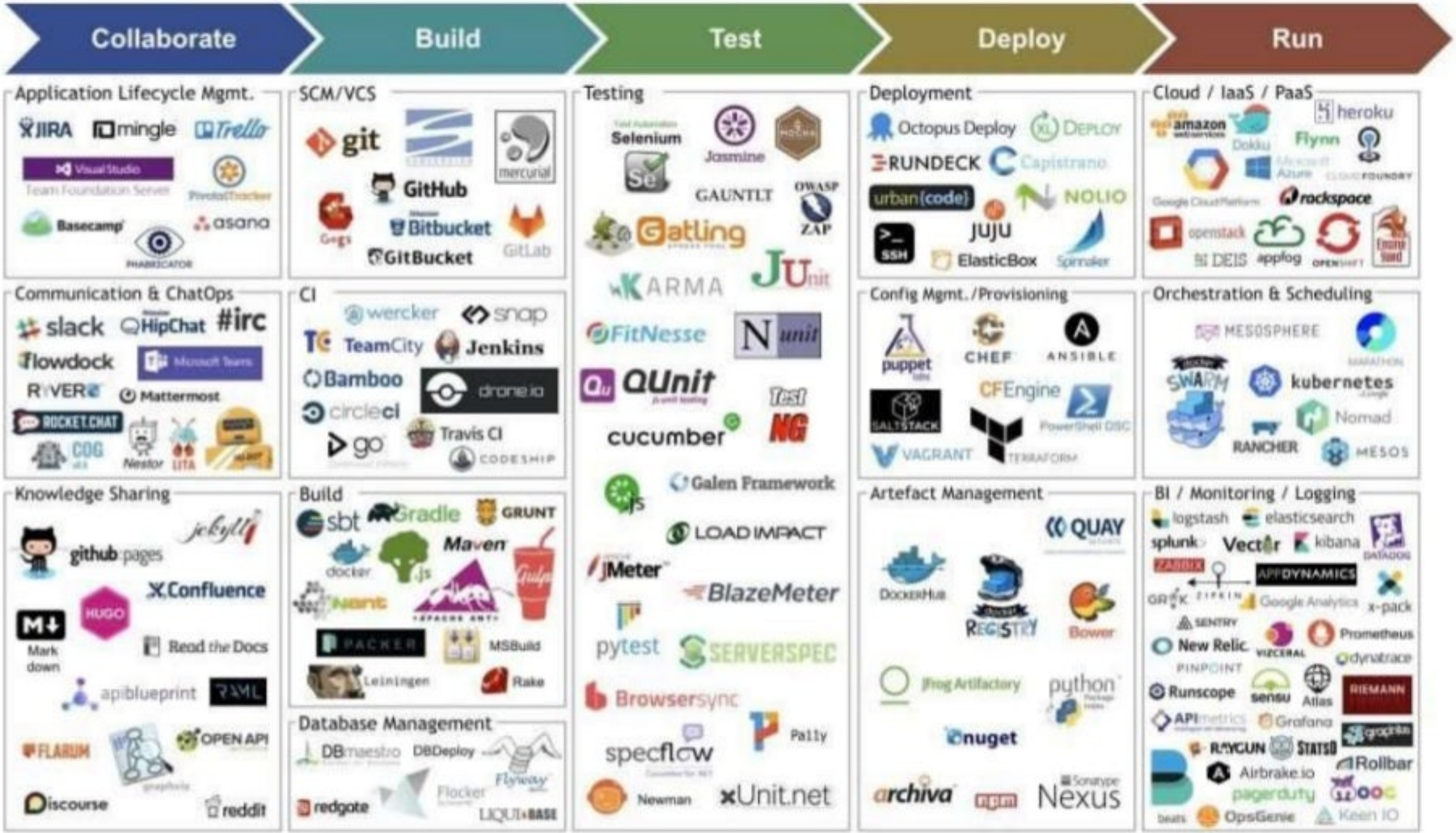
Existing markets are ripe for disruption

It’s better now, but is it simpler?





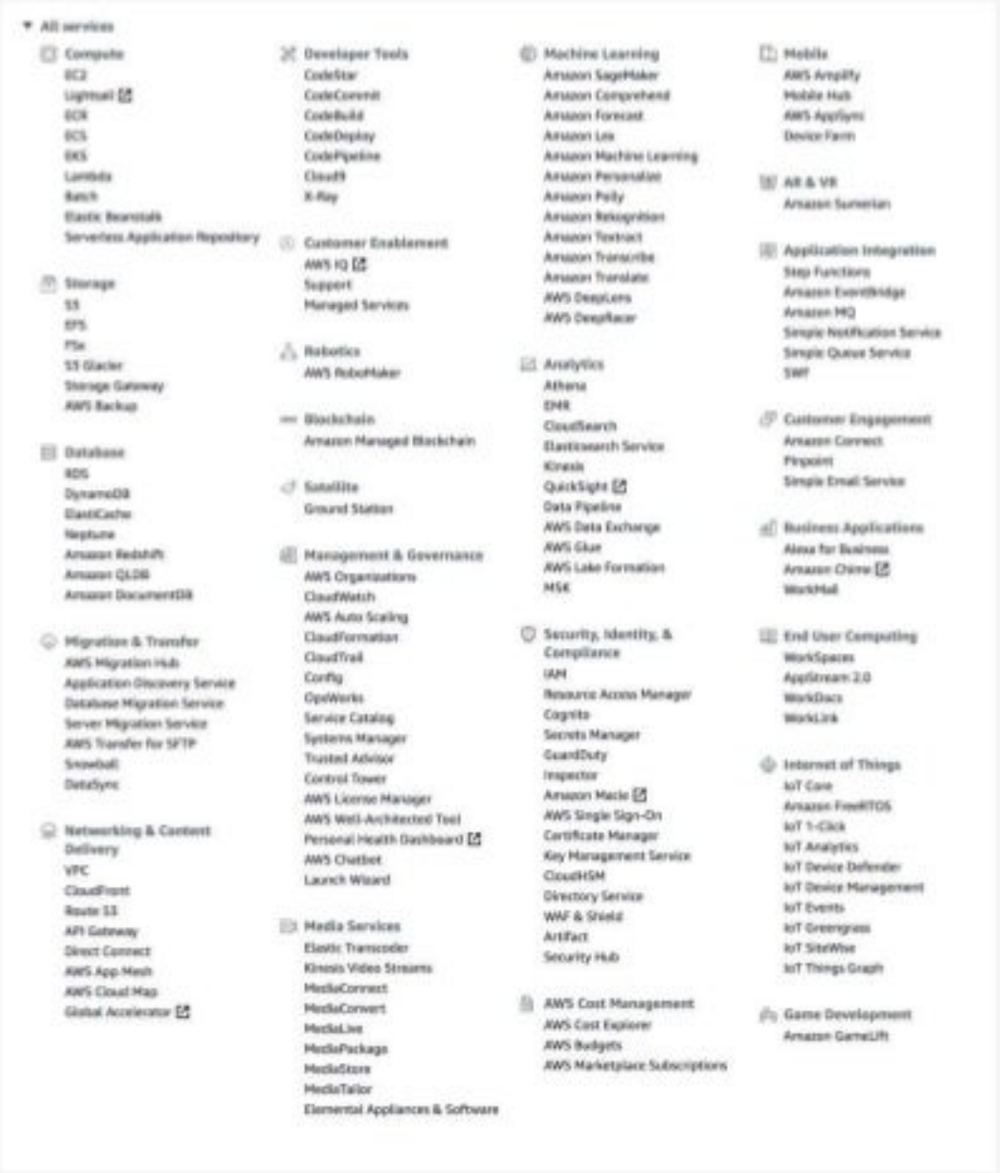
https://gist.github.com/rashwedamir/7da0145ae1b5d6889e4085d1ed21d1acb



http://devopedia.org/devops

Complexity Is Increasing

AWS Console
Left: 2018
Right: 2019




THIS IS FINE.

How does security fit into this?

AWS Security Primer

https://cloudonaut.io/aws-security-primer/

I have **worked extensively** with **AWS** over the last **4 years**, and I **can barely wrap my head around** the scope of managing **security in AWS**.

We have an **entire department dedicated to security** in our company, and **none of them are remotely** close to being **experts in AWS** security either.

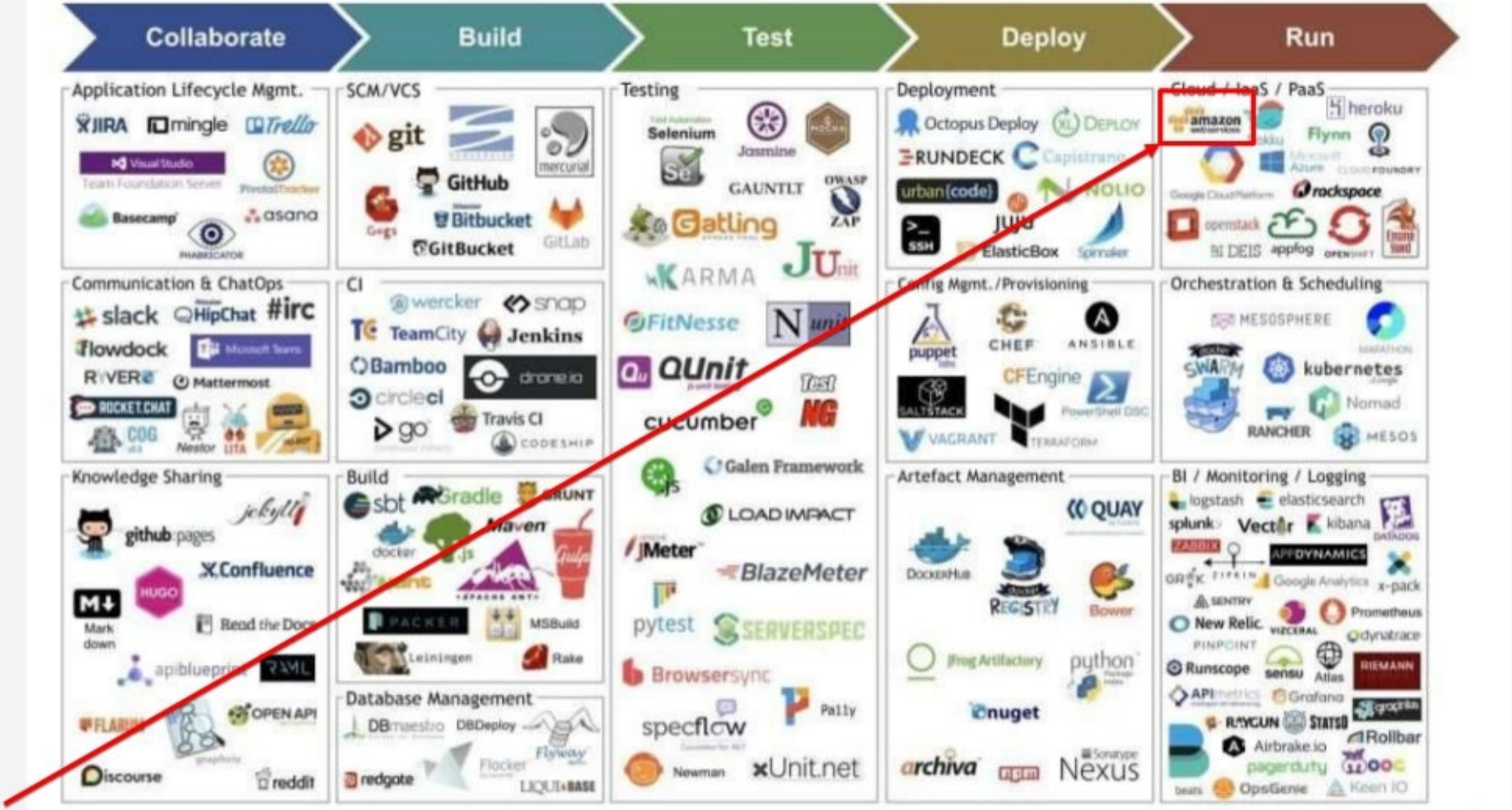
I'm starting to get curious **if there even is an expert** who could **set up and maintain a bulletproof AWS** account.

▲ falcolas on June 25, 2017 [-]

Such a shallow dive: there really needs to be a lot more ink spilled on this topic in great depth. I've worked extensively with AWS over the last 4 years, and I can barely wrap my head around the scope of managing security in AWS. We have an entire department dedicated to security in our company, and none of them are remotely close to being experts in AWS security either.

I'm starting to get curious if there even is an expert who could set up and maintain a bulletproof AWS Account. From the dev/admin accounts to API Gateway to Lambda to RDS and S3; there's just too much to be an expert on. And it's all handled differently (not to mention how many times it's changed in my mere 4 years of experience).

https://news.ycombinator.com/item?id=14628108

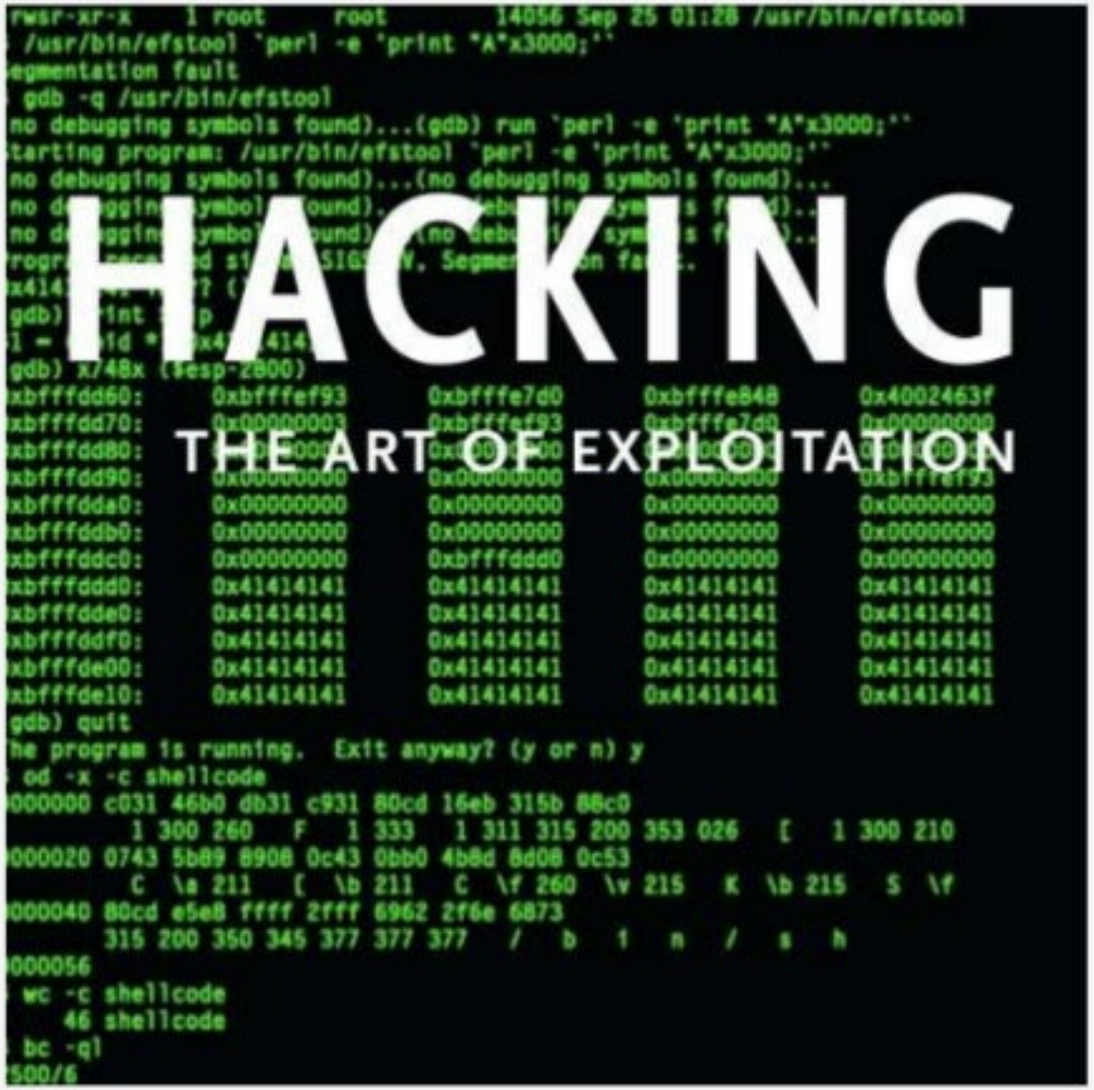


http://devopedia.org/devops

DevSecOps:
How important is it really?

- Agile took us from months to days to deliver software
- DevOps took us from months to minutes to deploy software
- More applications are mission critical
- Now security has become the bottleneck

The real impact of hacks & breaches



News is full of high-profile breaches that get widespread attention.

EQUIFAX HBO YAHOO! SONY

But they are not the only target of hackers

43% of all **cyber attacks** target **small businesses.**

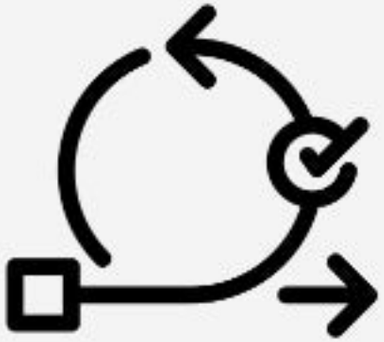
1/5 **data breaches** are the **result** of attackers abusing **insecure web applications.**

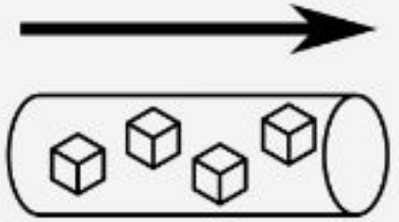
60% of **small businesses** that are **Hacked** go **out of business** within **6 months.**

Who is responsible?

The Evolution of Security Tools

Duration 2-4 weeks | 1-2 weeks | Continuous and Real-time





Penetration Testing

Tools
- Port Scanners
- Vulnerability Scanners
- Exploitation Tools

Audience
- Security Professionals

Secure SDLC

Tools
- Code Security Scanners
- Dynamic Security Scanners
- Vulnerability Scanners

Audience
- Security Professionals in Enterprise Security Teams

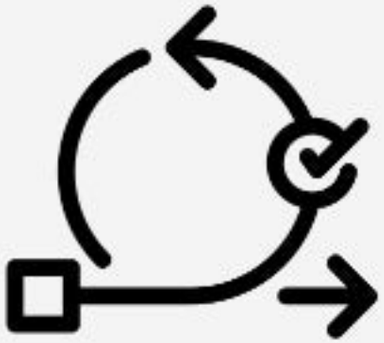
DevSecOps

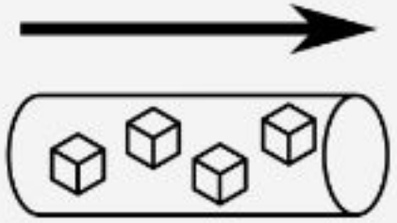
Tools
- Code Security Scanners
- Interactive Security Scanners
- Runtime Application Self Protection

Audience
- Developers in Product Teams

The Evolution of Security Teams

"Department of NO" → "Let's work together" → "How can we help you succeed?"





Penetration Testing

- Security
- Development
- Operations

Secure SDLC

- Security
- Development
- Operations

DevSecOps

- Security
- Development
- Operations

Modern security teams empower dev teams!

Dev : Ops : Sec

100 : 10 : 1

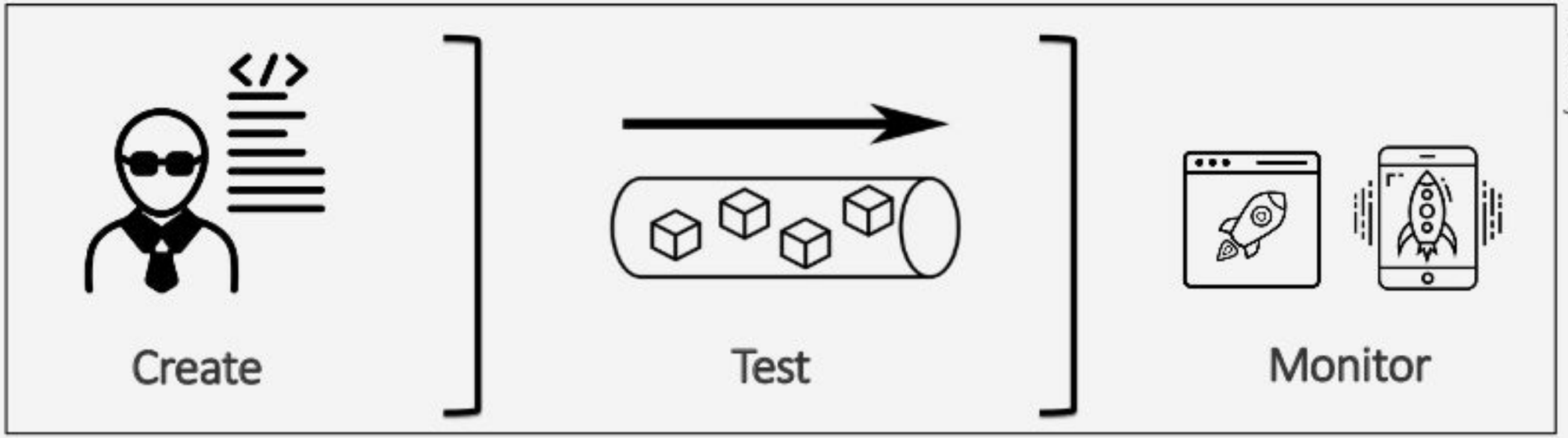
Looks like we have a scale problem


“ You build it, you run it.
- Werner Vogels (CTO, Amazon)

You build it, you secure it.

- John Willis

Understanding benefits of security controls



Challenges
- Changing human behavior
- Difficult to enforce
- People churn

Benefits
- Reduce new vulnerabilities

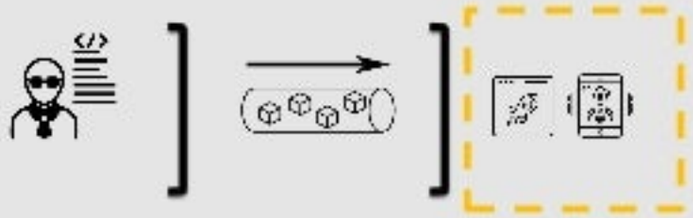
Challenges
- Vulnerability Noise
- Fixing issues
- Coverage of issues

Benefits
- Enforceable
- Provide Metrics

Challenges
- Coverage of issues
- Org wide rollout

Benefits
- Enforceable
- Provide Metrics
- Block attacks

DevSecOps - Monitor



Available Technologies

- Micro Segmentation
- Runtime Application Self Protection (RASP)
- Bug Bounties

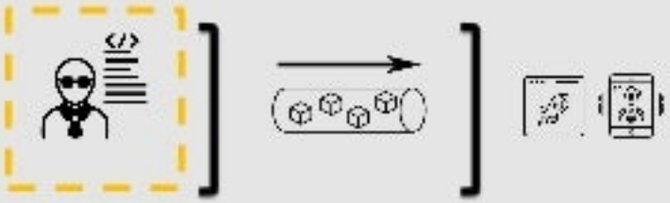
Questions you should be able to answer

Are your applications currently under attack?

What are attackers going after?

Are we automatically defending against this attack?

DevSecOps - Create



Available Options

- Security Awareness
- Secure Coding Training
- Shared Knowledge Base
- Security Focused Hackathons
- Security Champion Program

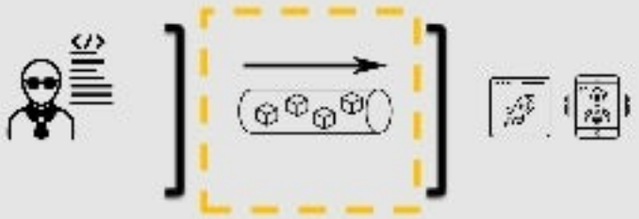
Questions you should be able to answer

Do your teams know the most common successful attacks?

Do your teams know how to detect and avoid them?

Who is the dedicated security contact in a team?

DevSecOps - Test



Available Technologies

- Static Application Security Testing (SAST)
- Sensitive Information Scanners (SIS)
- Software Composition Analysis (SCA/CCA)
- Dynamic Security Scanning (DAST)
- Interactive Application Security Testing (IAST)

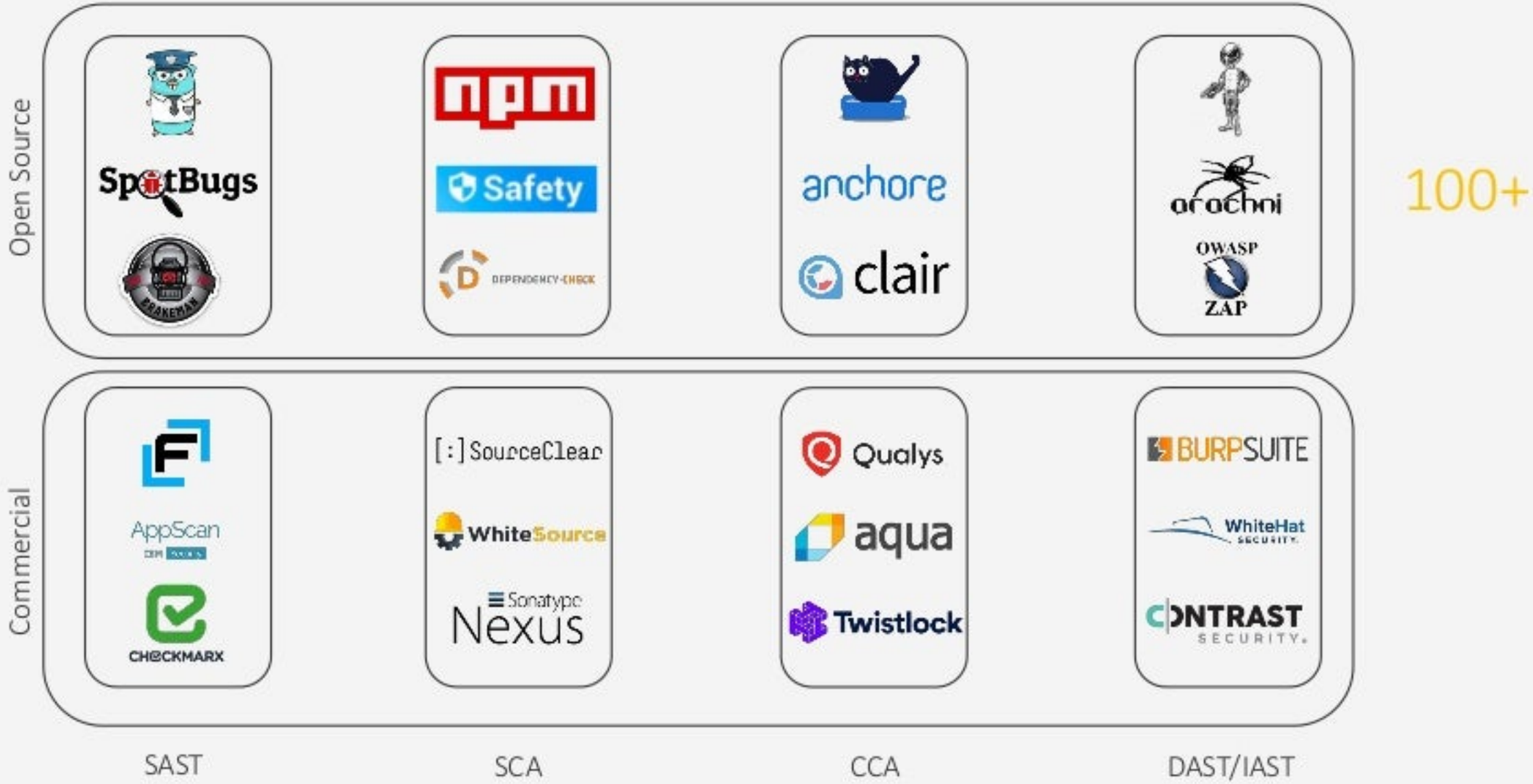
Questions you should be able to answer

Do the latest changes introduce new security issues?

Do any of our 3rd party libraries have known security issues?

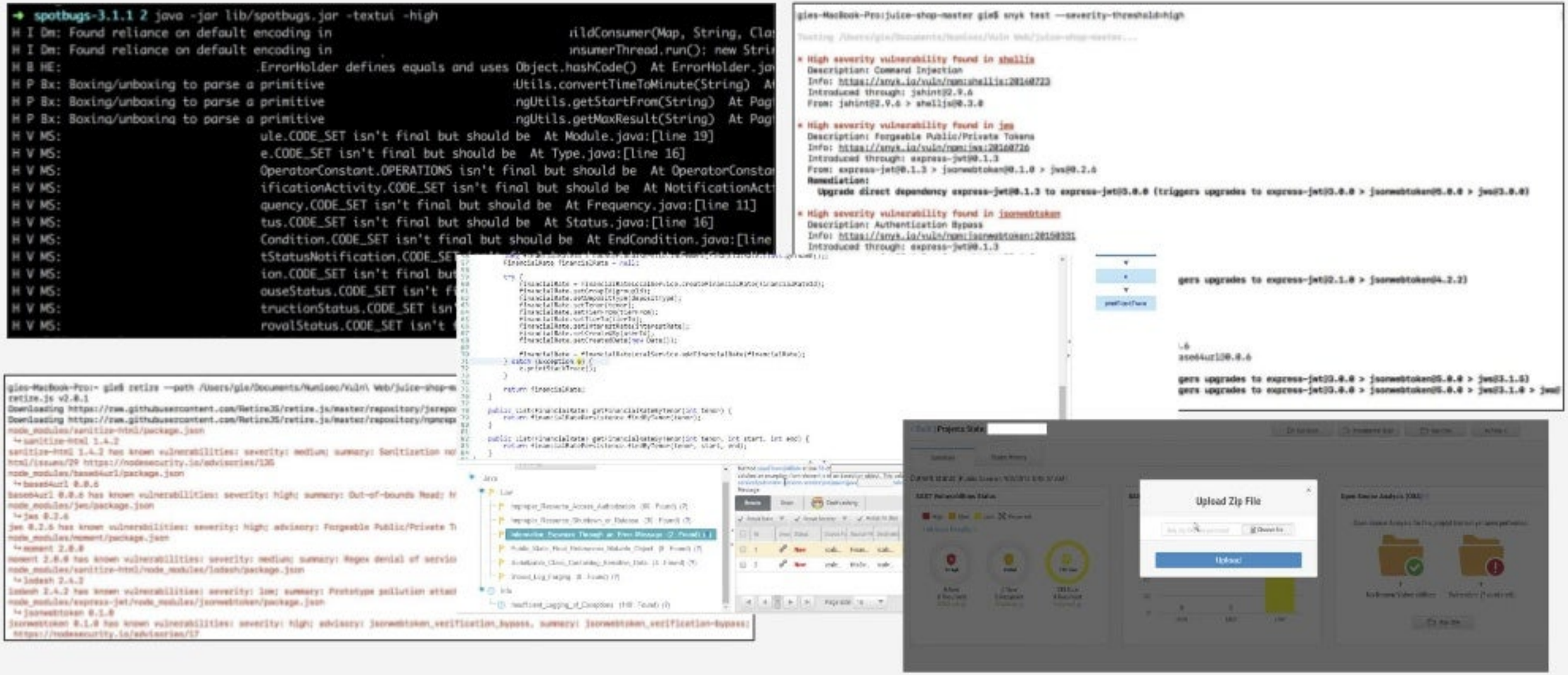
Does our code contain hard-coded secrets?

Automated Security Testing

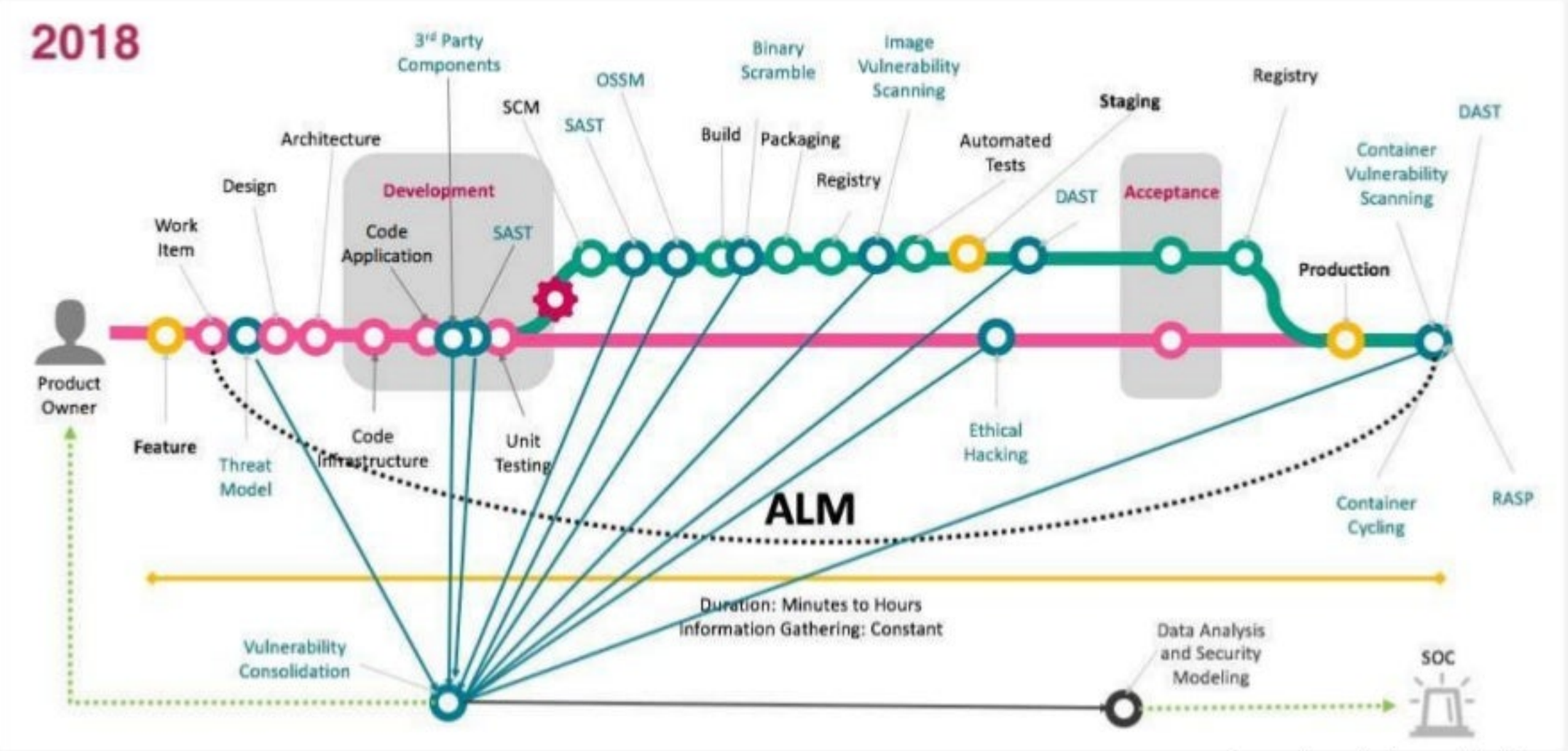


100+

Automated Security Testing – Fragmentation



Where do these tools live?



Source: https://twitter.com/djschleen


SECURITY TOOLS
SECURITY TOOLS EVERYWHERE
imgflip.com


Developers
Security

“The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency. ”

Bill Gates

What has to be different then?

Signals vs Noise

Don’t add to the noise

Focus on high-impact issues

Ensure the issues have high accuracy

Security Trivia #213: What is the largest security tool report that has been recorded?

13,000 pages

Lost in Translation

Speak the same language as developers

Leverage the right communication channel

Issues are useless until they are fixed

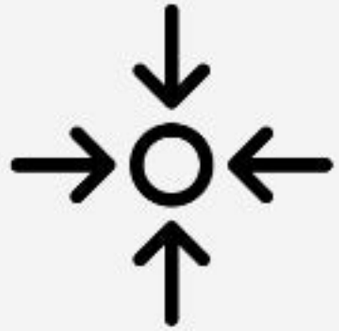
Security Trivia #937: What is the official CWE title for a SQL Injection?

Improper Neutralization of Special Elements used in an SQL Command

Make it easy

Allow developers to get started in minutes

Tightly integrated



Provide all the needed functionality

Security Trivia #23: How many of the 12 leading AST companies - according to the Gartner Magic Quadrant – have clear pricing information on their website?

DevSecOps
Do we really need it now?

There are some compelling statistics

- It's **30 times cheaper** to fix security defects in development vs production
- **80% to 90%** of modern applications consist of **open source components**
- An average data **breach** costs **5M+ USD**
- Most of the DevOps **high-performers include security** in their delivery process

Security as Competitive Advantage

State of DevSecOps - Conclusion

Technologies

- Tools have improved
- Choose them wisely
- Solve technology problems
- Cover the whole portfolio
- Start acting on data in prod

Security Team

- Department of YES
- Empowering product teams
- Use scarce resources wisely
- Respect complexity, but provide focus
- Make security a non-event

Product Team

- Acknowledge that developers are key
- Knowledge is power
- Turn developers into security champs
- Be mindful that change is slow
- Build it, run it, secure it

Get a curated list of security resources

Consisting of:

- Awesome security lists
- Developer trainings
- List of great security tools
- Security Page templates
- Free digital copy of my book
- the slides
- … and more

Then send an email to:
iwant@guardrails.io