DEVSECOPS

Integratring Security in the Development Process

(with memes)

Magno (Logan) Rodrigues

Magnologan at gmail

HELLO WORLD!

- Systems and Network Security Specialist(Developer Background)
- Works directly with Application Security, Penetration Testing,Vuln Management, WAF and some Code Review
- Studied Security and Computer Forensics in the US
- CompTIA Security+ and EXIN Secure Programming Certified
- Spoke at many events such as OWASP AppSec LATAM, BHack, Just4Meeting, GTS, JampaSec

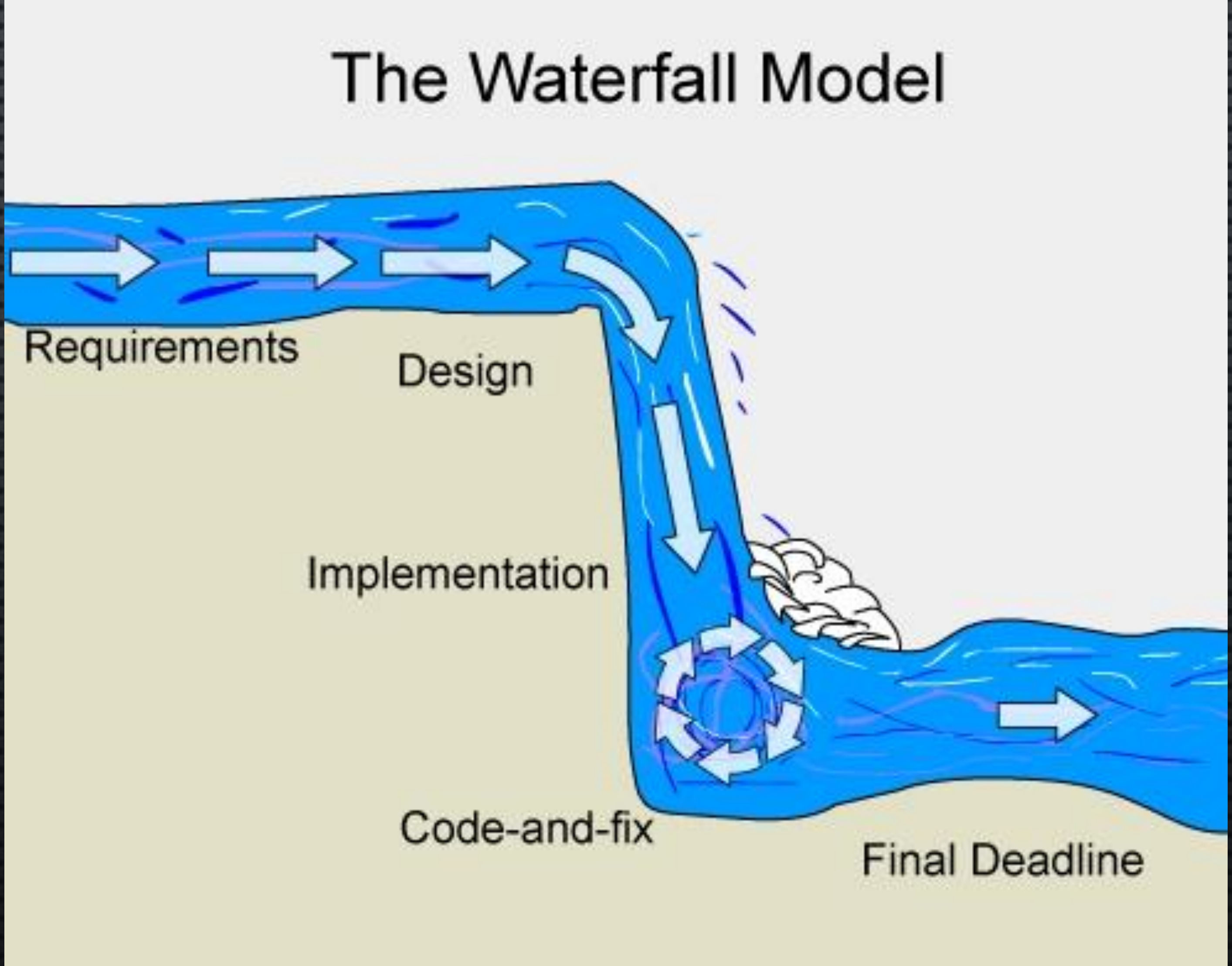
SOFTWARE DEVELOPMENT IS LIKE A MMORPG…

IT NEVER ENDS!

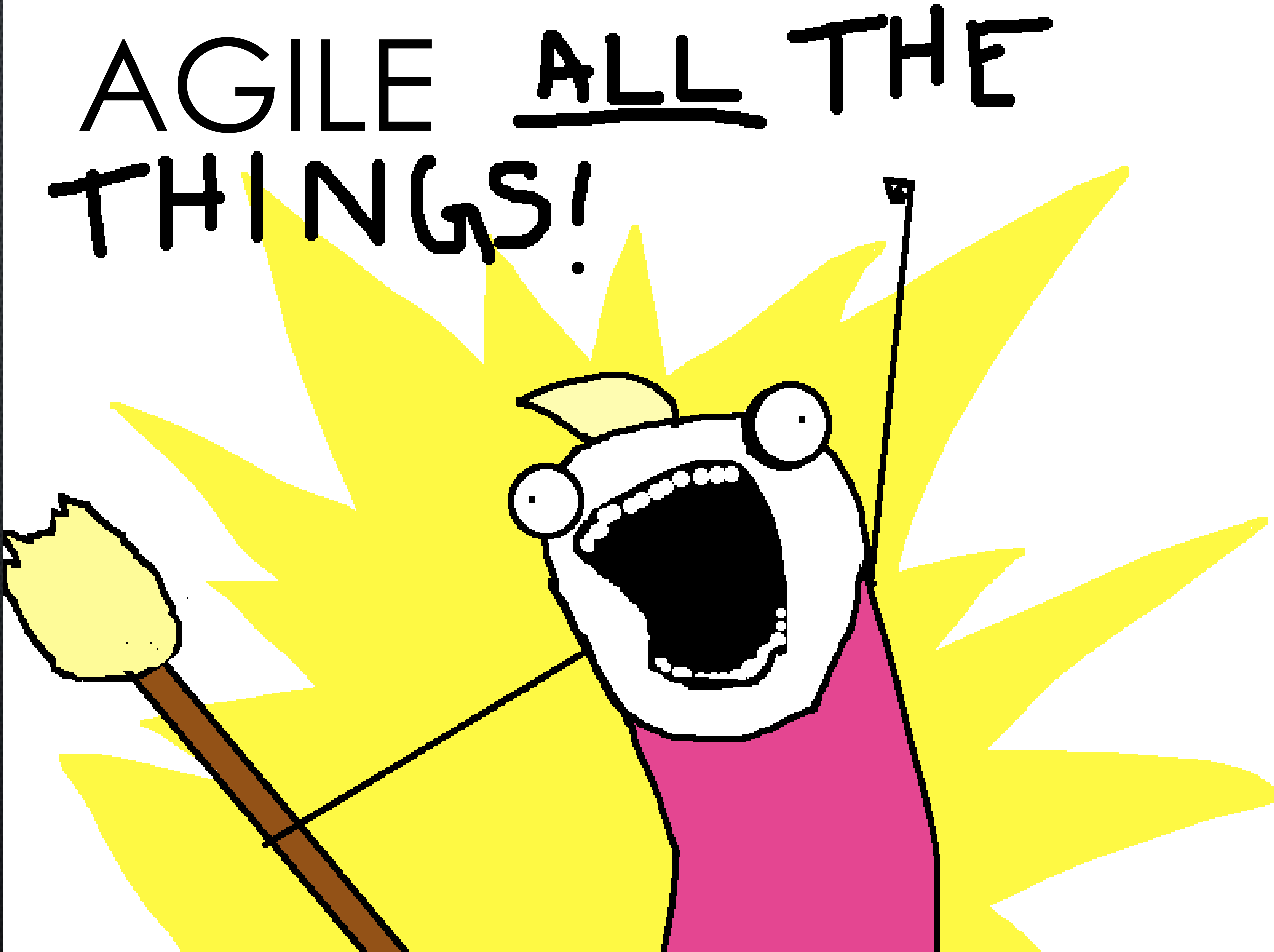
SECURITY CAN'T KEEP BEING A BOTTLENECK!

OTHERWISE THEY DON'T MAKE MONEY!

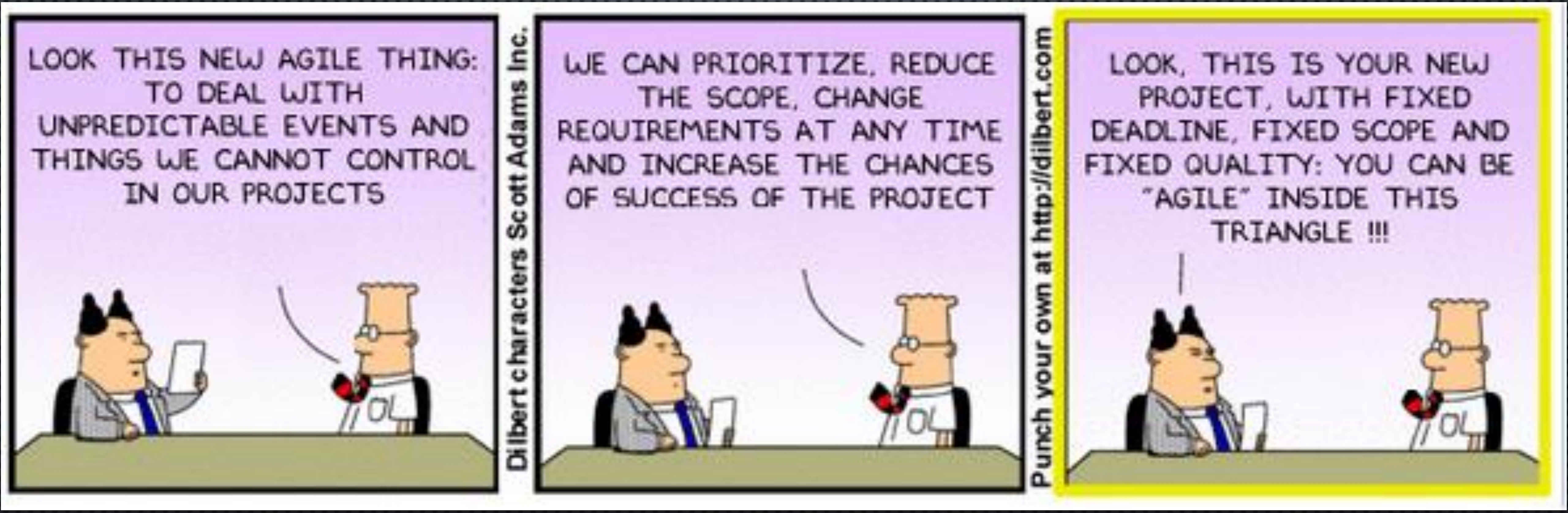
FIRST THERE WAS WATERFALL...



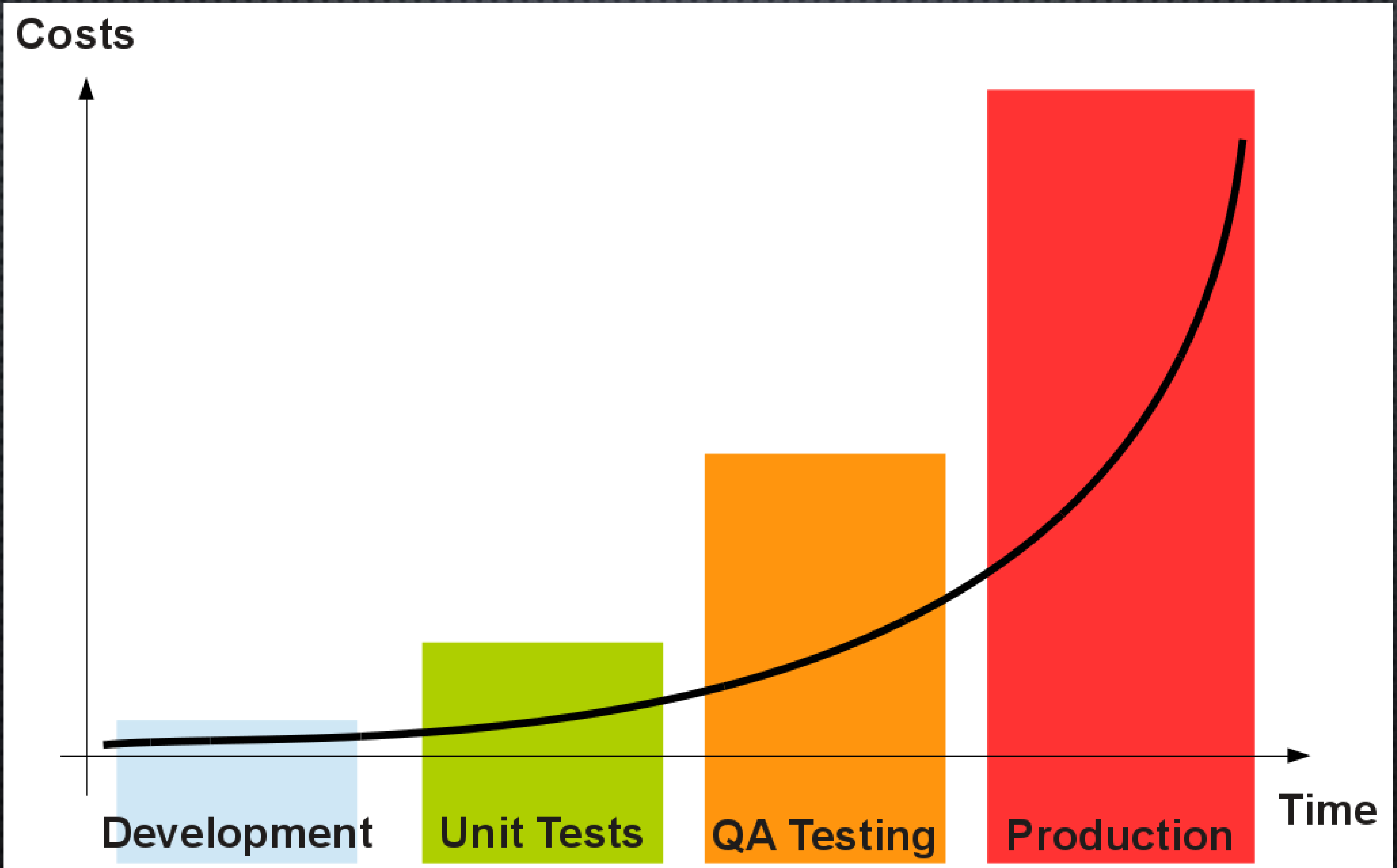
THEN ALL BECAME AGILE!


AGILE ALL THE THINGS!

AGILE NEEDS CULTURE CHANGE


LOOK THIS NEW AGILE THING: TO DEAL WITH UNPREDICTABLE EVENTS AND THINGS WE CANNOT CONTROL IN OUR PROJECTS
Dilbert characters Scott Adams Inc.
WE CAN PRIORITIZE, REDUCE THE SCOPE, CHANGE REQUIREMENTS AT ANY TIME AND INCREASE THE CHANCES OF SUCCESS OF THE PROJECT
Punch your own at http://dilbert.com
LOOK, THIS IS YOUR NEW PROJECT, WITH FIXED DEADLINE, FIXED SCOPE AND FIXED QUALITY: YOU CAN BE "AGILE" INSIDE THIS TRIANGLE !!!

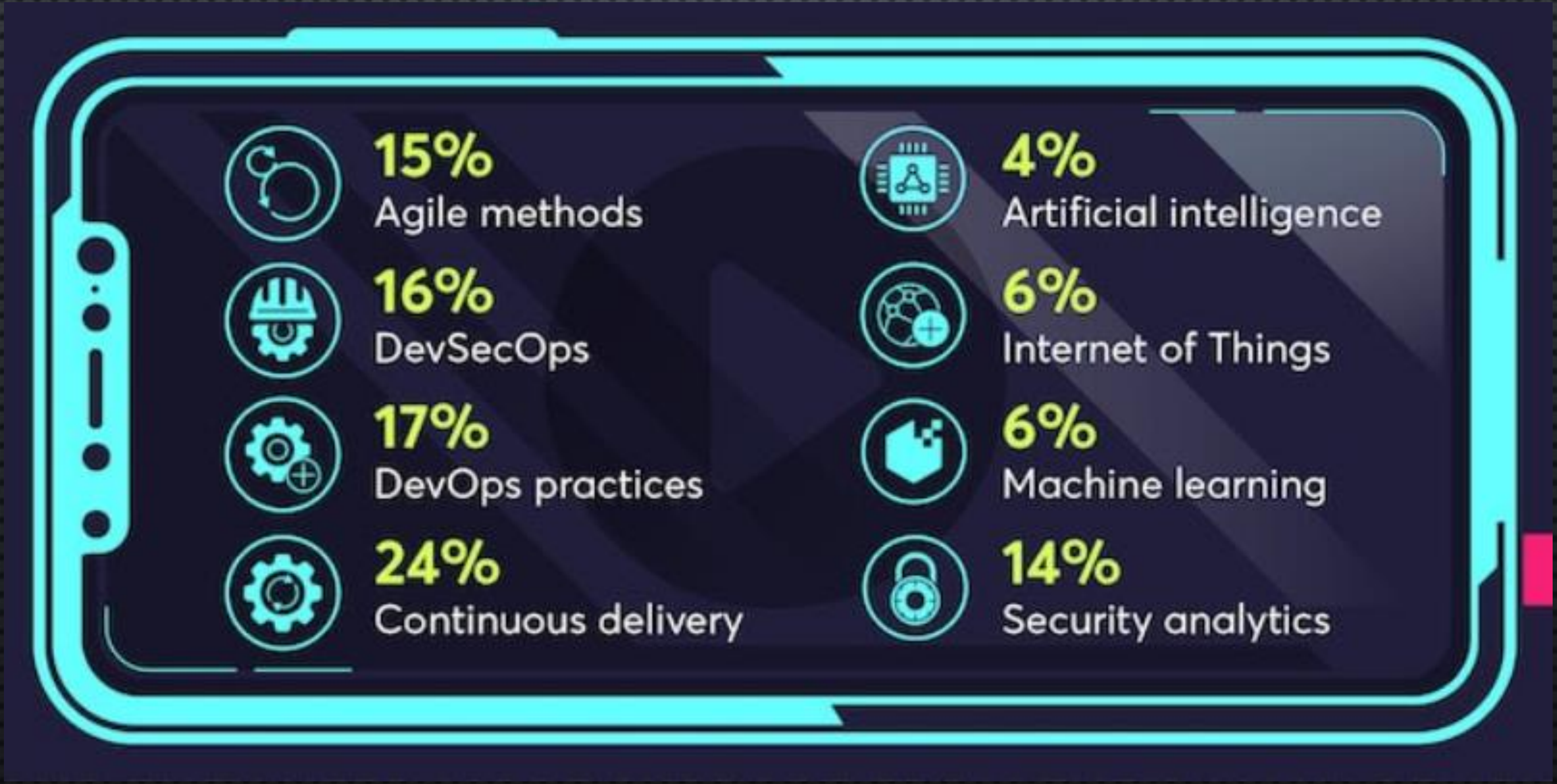
WHAT ABOUT SECURITY?



IF IT COMPILES, SHIP IT!

BY DINIS CRUZ

DEVS NEED TRAINING. LISTEN TO THEM!



15%
Agile methods

16%
DevSecOps

17%
DevOps practices

24%
Continuous delivery

4%
Artificial intelligence

6%
Internet of Things

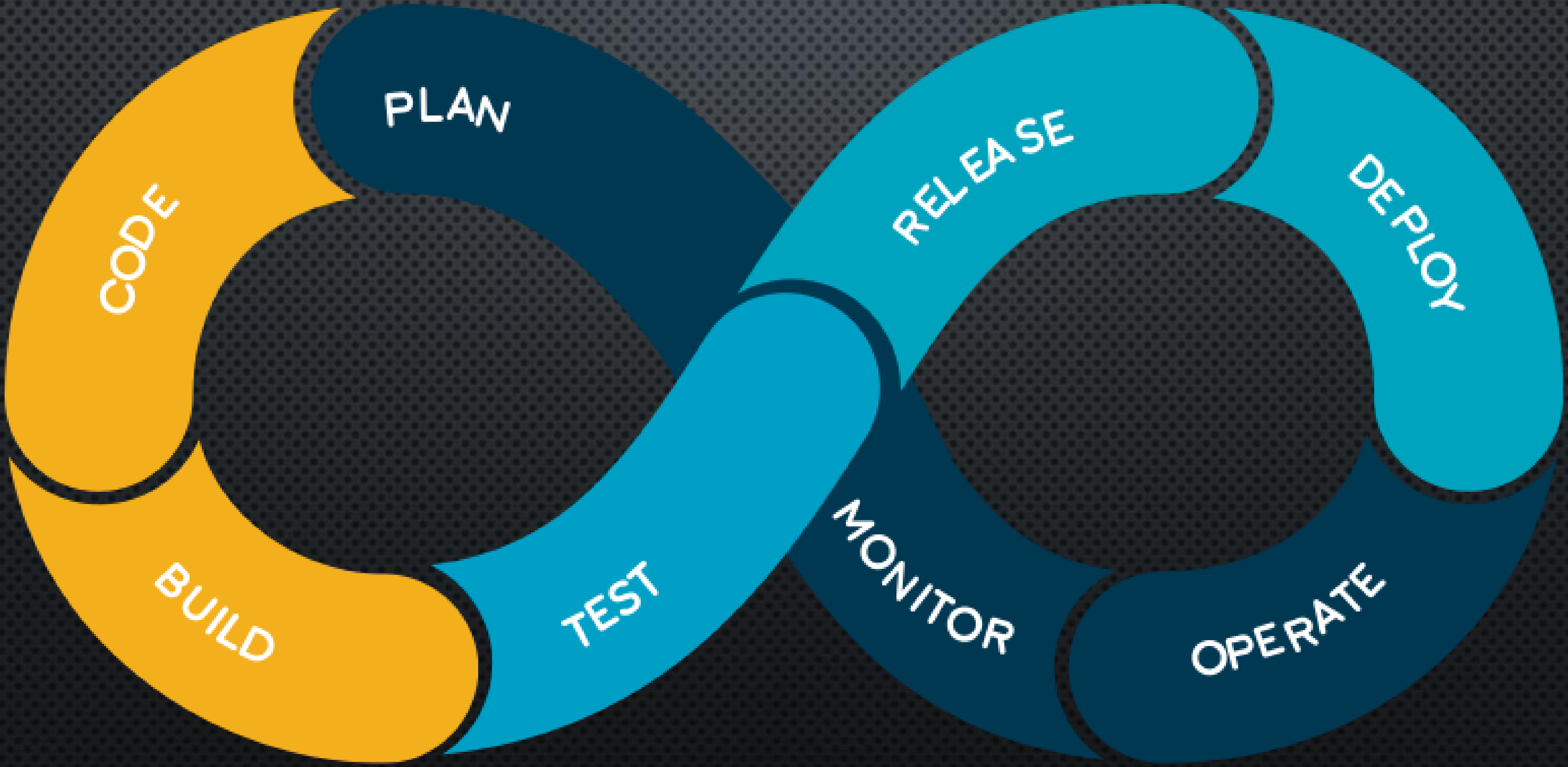
6%
Machine learning

14%
Security analytics

https://www.ca.com/us/modern-software-factory/content/are-you-listening-to-your-software-developers.html

WORKED FINE IN DEV
OPS PROBLEM NOW
memegenerator.net

DEVOPS



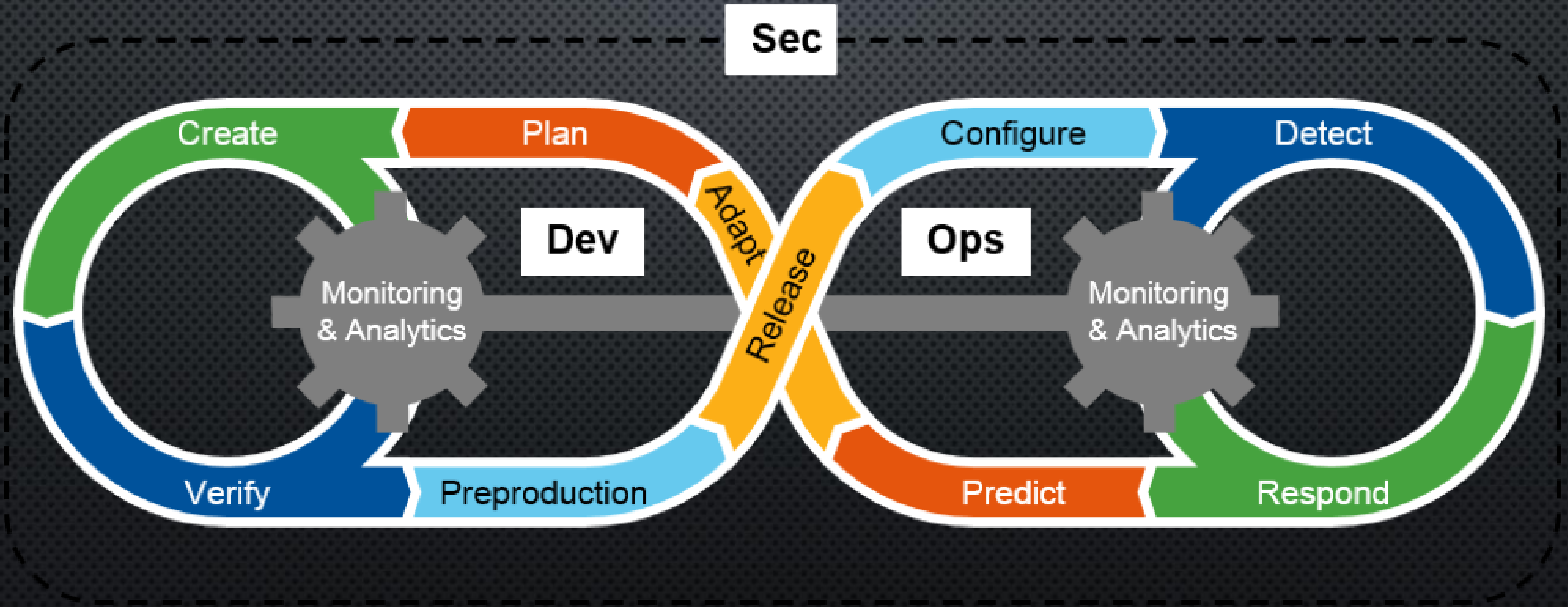
DEVOPS

- Foundations
  - Culture/Objectives
  - Automation/Integration
  - Indicators/KPIs

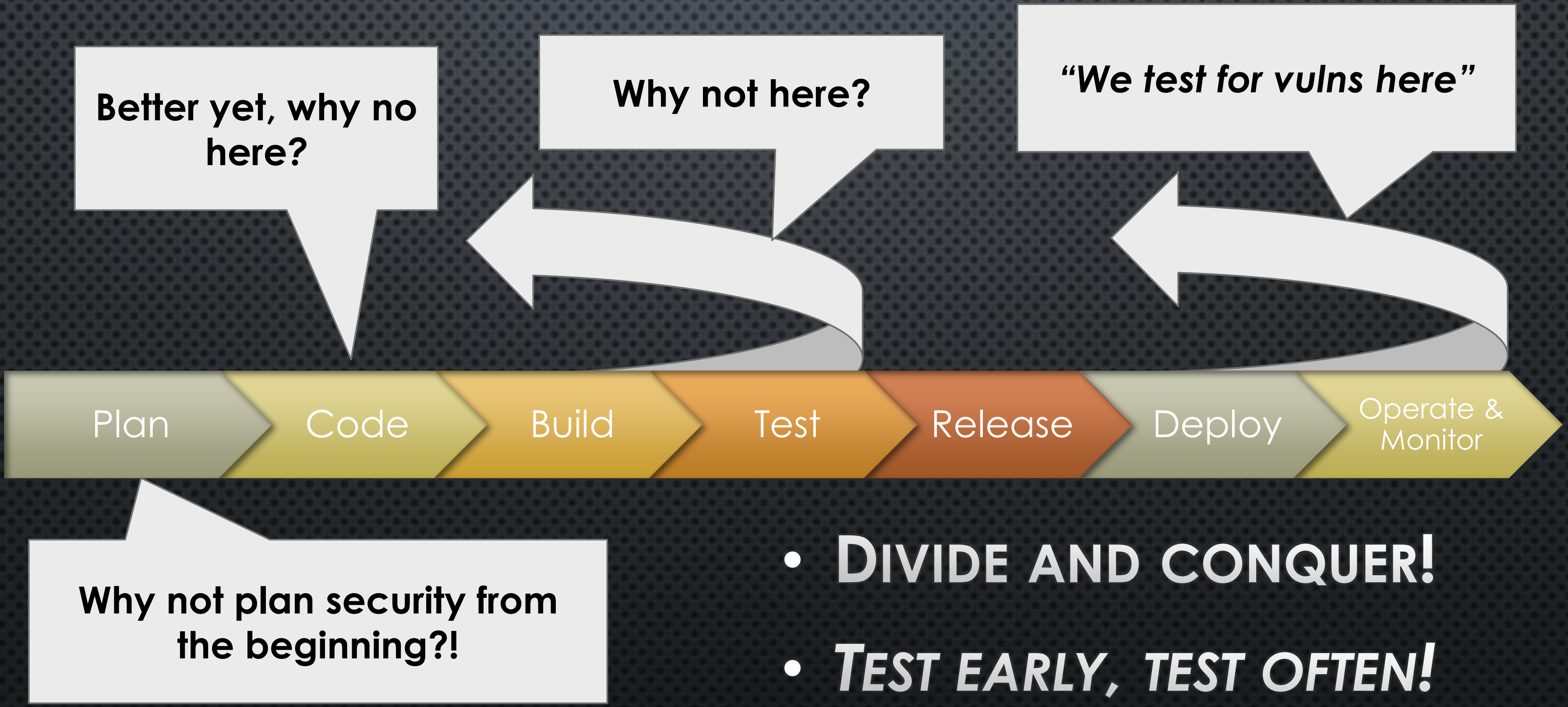
- Principles
  - Limit the work in progress
  - Increase the feedback
  - Eliminate re-work

RUGGED DEVOPS?
DEVOPSSEC?
SECDEVOPS?
DEVSECOPS?

DEVSECOPS = DEVOPS + SECURITY



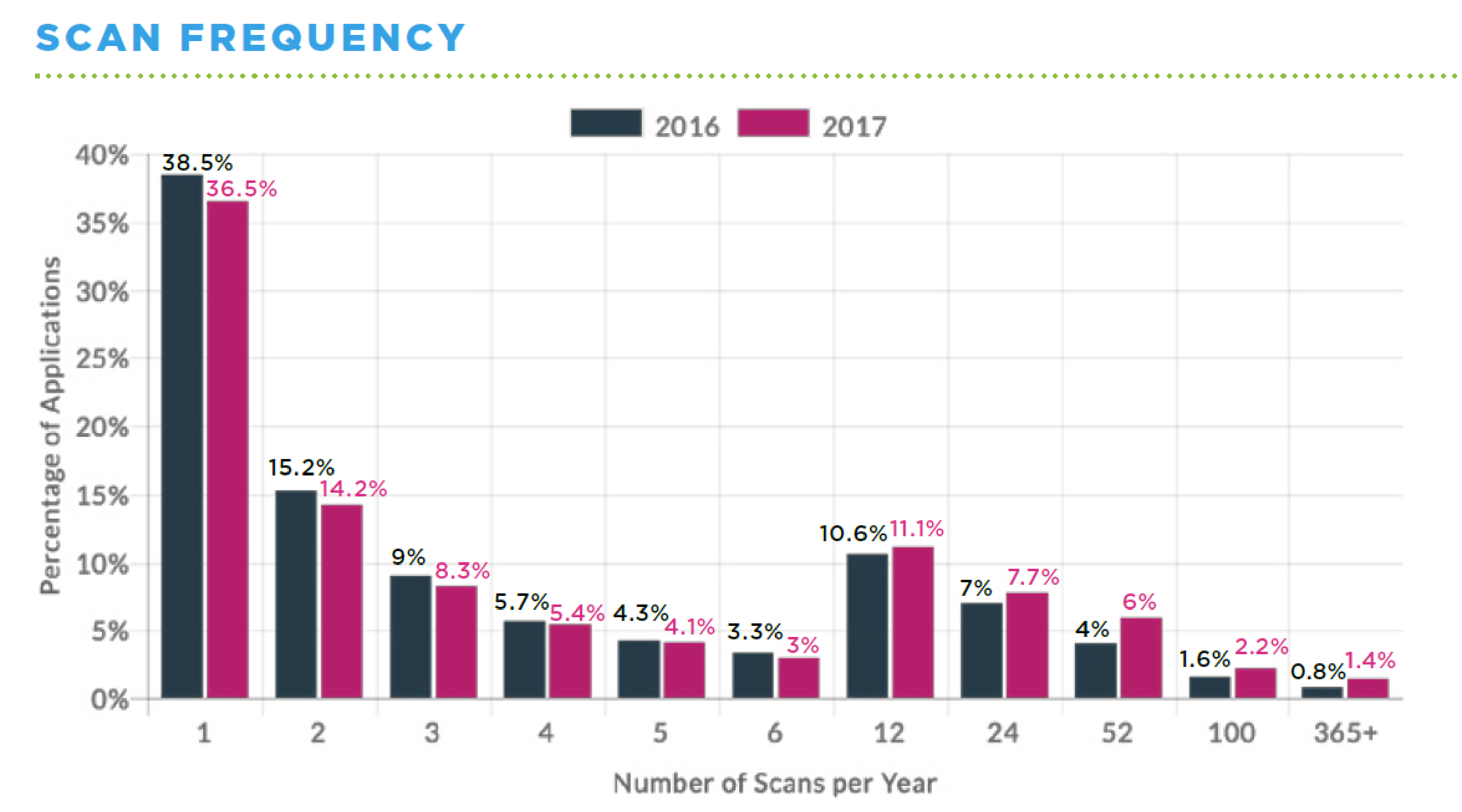
DEVSECOPS



- **DIVIDE AND CONQUER!**
- ***TEST EARLY, TEST OFTEN!***

SSL Approach – Shifting Security Left

SHIFTING SECURITY LEFT

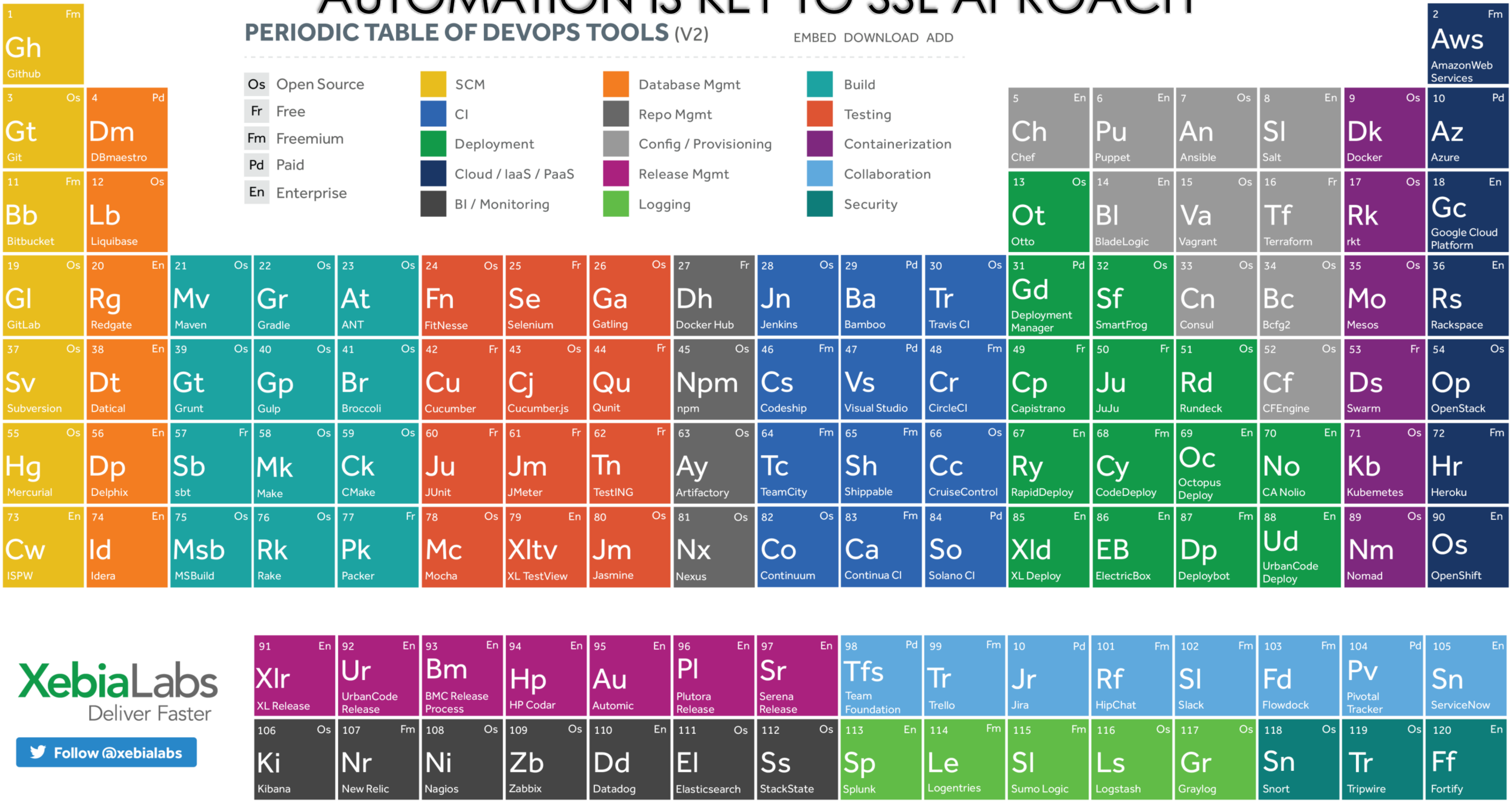


https://www.veracode.com/state-of-software-security-report

ONE DOES NOT SIMPLY
SHIFT TO DEVSECOPS
imgflip.com

KEEP
CALM
AND
AUTOMATE
ALL THE THINGS
KeepCalmAndPosters.com

AUTOMATION IS KEY TO SSL APROACH



PERIODIC TABLE OF DEVOPS TOOLS (V2)

EMBED DOWNLOAD ADD

Os Open Source	■ SCM	■ Database Mgmt	■ Build
Fr Free	■ CI	■ Repo Mgmt	■ Testing
Fm Freemium	■ Deployment	■ Config / Provisioning	■ Containerization
Pd Paid	■ Cloud / IaaS / PaaS	■ Release Mgmt	■ Collaboration
En Enterprise	■ BI / Monitoring	■ Logging	■ Security

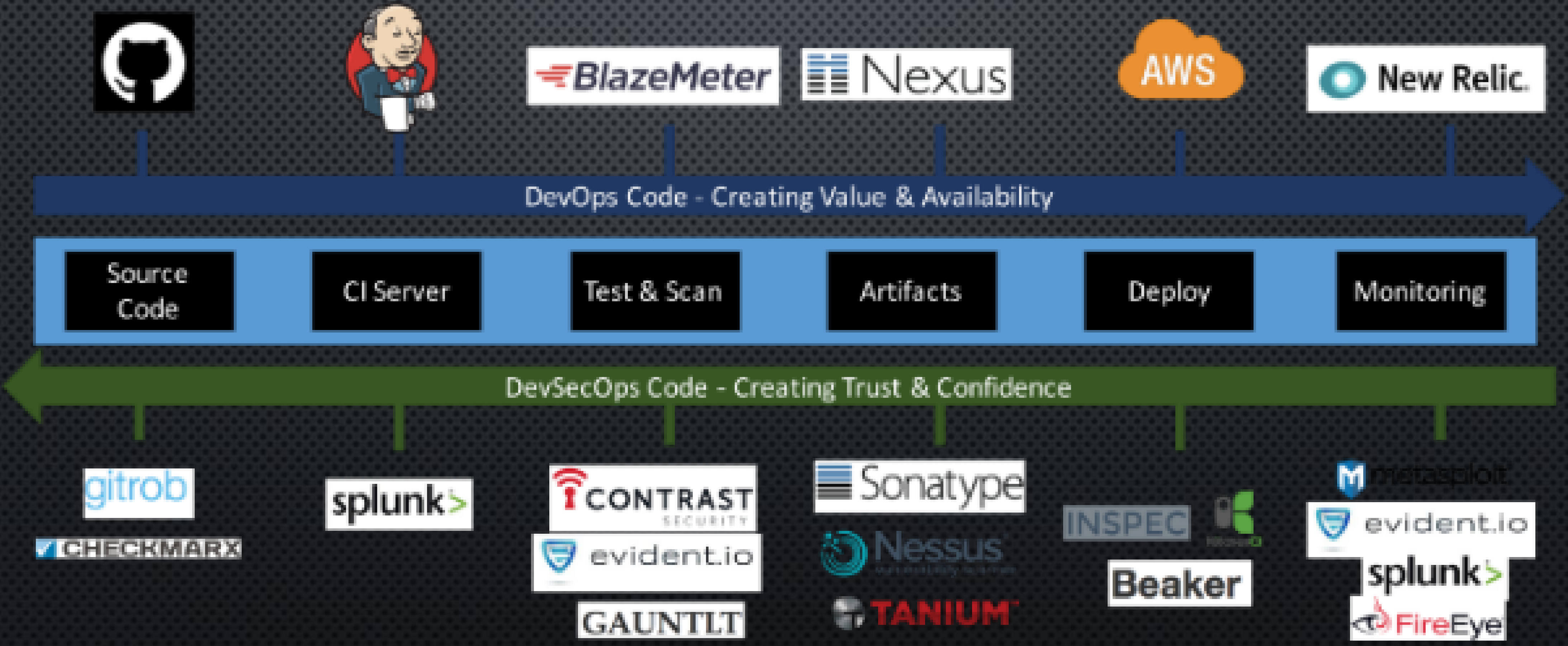
1 Fm Gh Github																	2 Fm Aws AmazonWeb Services
3 Os Gt Git	4 Pd Dm DBmaestro											5 En Ch Chef	6 En Pu Puppet	7 Os An Ansible	8 En Sl Salt	9 Os Dk Docker	10 Pd Az Azure
11 Fm Bb Bitbucket	12 Os Lb Liquibase											13 Os Ot Otto	14 En Bl BladeLogic	15 Os Va Vagrant	16 Fr Tf Terraform	17 Os Rk rkt	18 En Gc Google Cloud Platform
19 Os Gl GitLab	20 En Rg Redgate	21 Os Mv Maven	22 Os Gr Gradle	23 Os At ANT	24 Os Fn FitNesse	25 Fr Se Selenium	26 Os Ga Gatling	27 Fr Dh Docker Hub	28 Os Jn Jenkins	29 Pd Ba Bamboo	30 Os Tr Travis CI	31 Pd Gd Deployment Manager	32 Os Sf SmartFrog	33 Os Cn Consul	34 Os Bc Bcfg2	35 Os Mo Mesos	36 En Rs Rackspace
37 Os Sv Subversion	38 En Dt Datical	39 Os Gt Grunt	40 Os Gp Gulp	41 Os Br Broccoli	42 Fr Cu Cucumber	43 Os Cj Cucumber.js	44 Fr Qu Qunit	45 Os Npm npm	46 Fm Cs Codeship	47 Pd Vs Visual Studio	48 Fm Cr CircleCI	49 Fr Cp Capistrano	50 Fr Ju JuJu	51 Os Rd Rundeck	52 Os Cf CFEngine	53 Fr Ds Swarm	54 Os Op OpenStack
55 Os Hg Mercurial	56 En Dp Delphix	57 Fr Sb sbt	58 Os Mk Make	59 Os Ck CMake	60 Fr Ju JUnit	61 Fr Jm JMeter	62 Fr Tn TestING	63 Os Ay Artifactory	64 Fm Tc TeamCity	65 Fm Sh Shippable	66 Os Cc CruiseControl	67 En Ry RapidDeploy	68 Fm Cy CodeDeploy	69 En Oc Octopus Deploy	70 En No CA Nolio	71 Os Kb Kubemetes	72 Fm Hr Heroku
73 En Cw ISPW	74 En Id Idera	75 Os Msb MSBuild	76 Os Rk Rake	77 Fr Pk Packer	78 Os Mc Mocha	79 En Xltv XL TestView	80 Os Jm Jasmine	81 Os Nx Nexus	82 Os Co Continuum	83 Fm Ca Continua CI	84 Pd So Solano CI	85 En Xld XL Deploy	86 En EB ElectricBox	87 Fm Dp Deploybot	88 En Ud UrbanCode Deploy	89 Os Nm Nomad	90 En Os OpenShift
			91 En Xlr XL Release	92 En Ur UrbanCode Release	93 En Bm BMC Release Process	94 En Hp HP Codar	95 En Au Automic	96 En Pl Plutora Release	97 En Sr Serena Release	98 Pd Tfs Team Foundation	99 Fm Tr Trello	10 Pd Jr Jira	101 Fm Rf HipChat	102 Fm Sl Slack	103 Fm Fd Flowdock	104 Pd Pv Pivotal Tracker	105 En Sn ServiceNow
			106 Os Ki Kibana	107 Fm Nr New Relic	108 Os Ni Nagios	109 Os Zb Zabbix	110 En Dd Datadog	111 Os El Elasticsearch	112 Os Ss StackState	113 En Sp Splunk	114 Fm Le Logentries	115 Fm Sl Sumo Logic	116 Os Ls Logstash	117 Os Gr Graylog	118 Os Sn Snort	119 Os Tr Tripwire	120 En Ff Fortify

XebiaLabs
Deliver Faster

Follow @xebialabs

Canon
EOS
wat

TESTING! TESTING! TESTING!



DevOps Code - Creating Value & Availability

Source Code

CI Server

Test & Scan

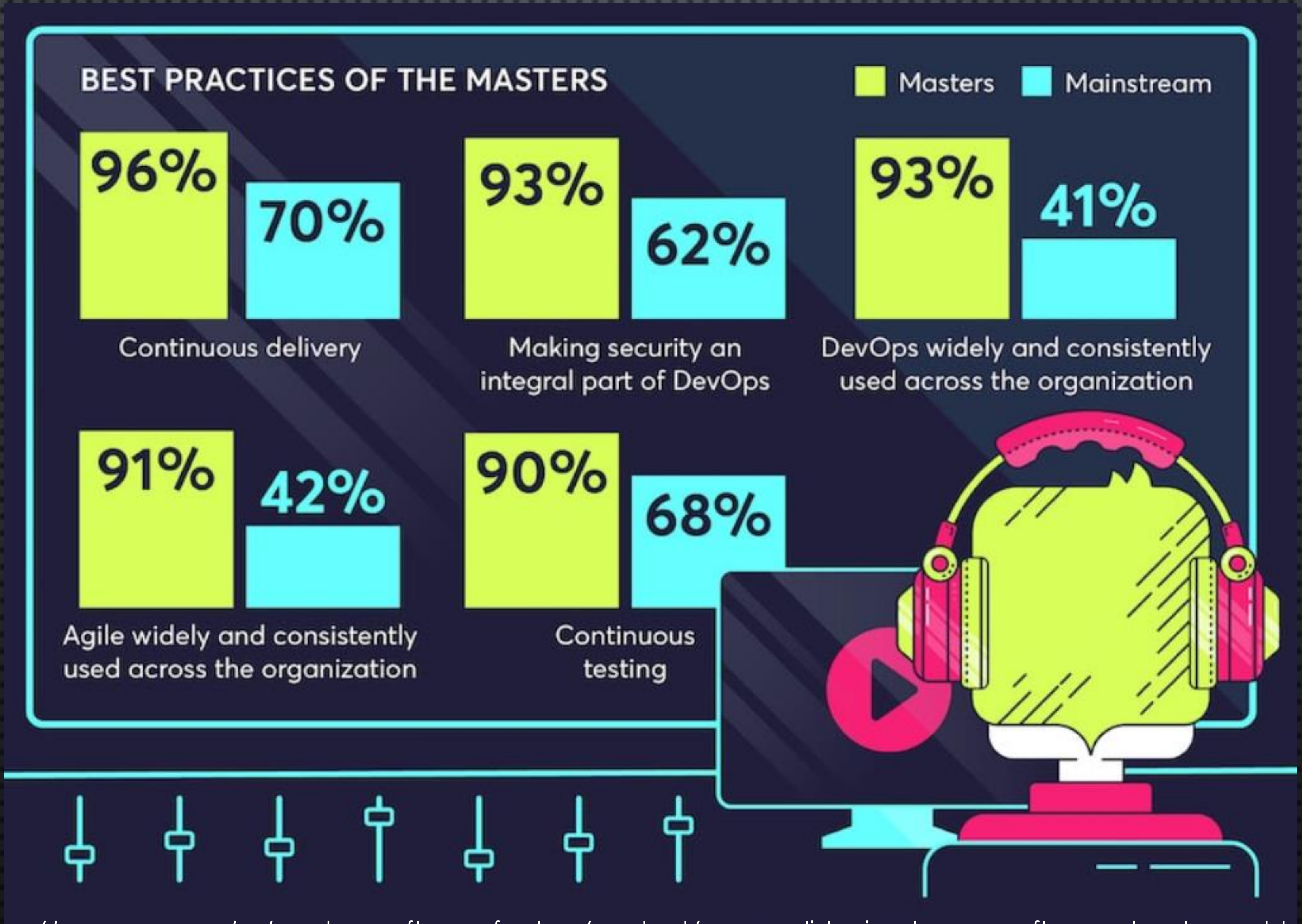
Artifacts

Deploy

Monitoring

DevSecOps Code - Creating Trust & Confidence

AND PROFIT!



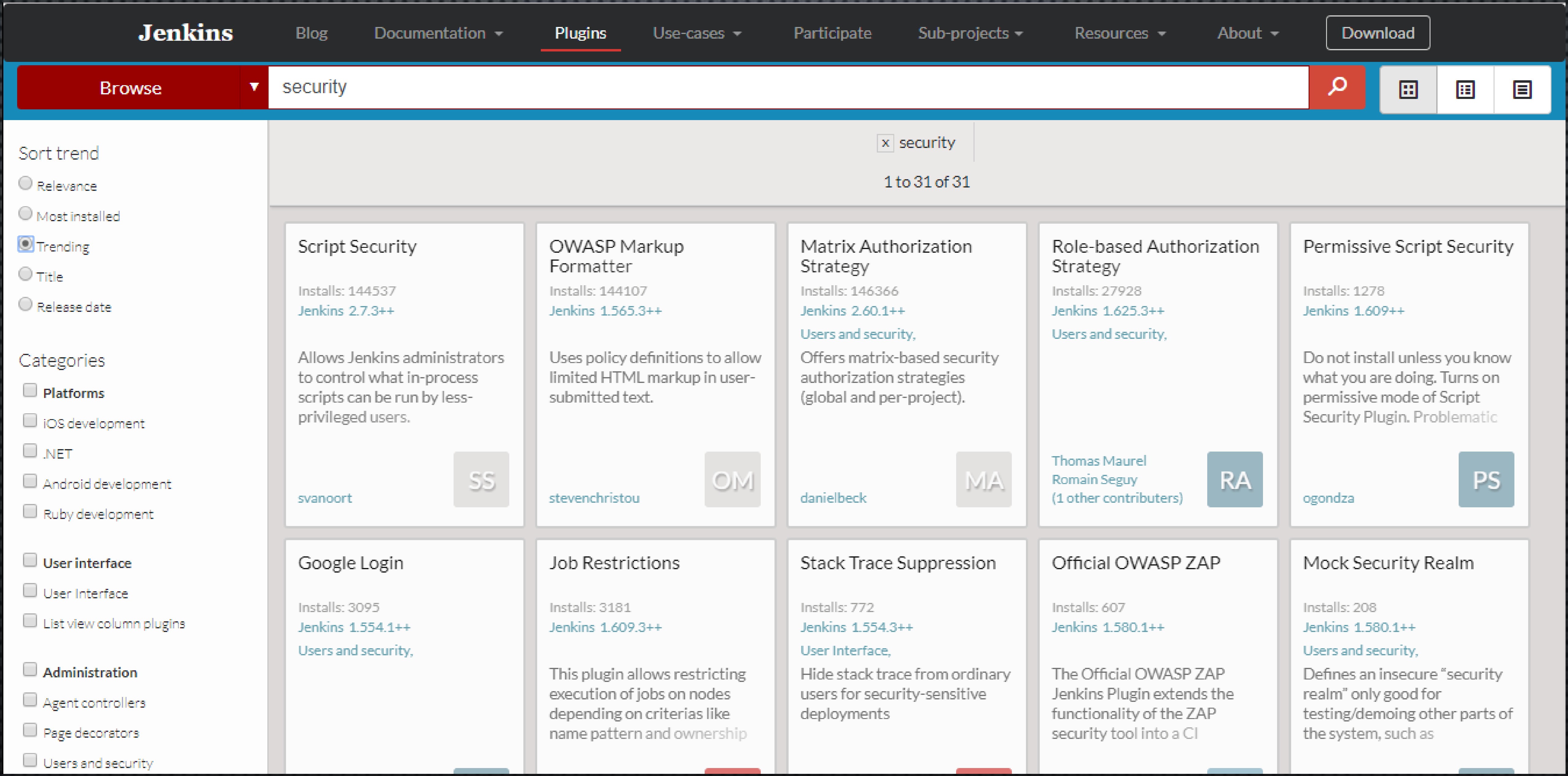
https://www.ca.com/us/modern-software-factory/content/are-you-listening-to-your-software-developers.html

I DON'T ALWAYS TEST MY CODE
BUT WHEN I DO, I DO IT IN PRODUCTION
quickmeme.com

TALK IS CHEAP
TOOLS
SHOW ME THE C✗E
imgflip.com

JENKINS

- Open source continuous integration server
- Each integration is verified and tested over automated builds
- Detects integration errors as fast as possible
- Has many security plugins available!



security

Sort trend

○ Relevance
○ Most installed
● Trending
○ Title
○ Release date

Categories

□ **Platforms**
□ iOS development
□ .NET
□ Android development
□ Ruby development

□ **User interface**
□ User Interface
□ List view column plugins

□ **Administration**
□ Agent controllers
□ Page decorators
□ Users and security

x security

1 to 31 of 31

Script Security
Installs: 144537
Jenkins 2.7.3++
Allows Jenkins administrators to control what in-process scripts can be run by less-privileged users.
svanoort
SS

OWASP Markup Formatter
Installs: 144107
Jenkins 1.565.3++
Uses policy definitions to allow limited HTML markup in user-submitted text.
stevenchristou
OM

Matrix Authorization Strategy
Installs: 146366
Jenkins 2.60.1++
Users and security,
Offers matrix-based security authorization strategies (global and per-project).
danielbeck
MA

Role-based Authorization Strategy
Installs: 27928
Jenkins 1.625.3++
Users and security,
Thomas Maurel
Romain Seguy
(1 other contributers)
RA

Permissive Script Security
Installs: 1278
Jenkins 1.609++
Do not install unless you know what you are doing. Turns on permissive mode of Script Security Plugin. Problematic
ogondza
PS

Google Login
Installs: 3095
Jenkins 1.554.1++
Users and security,

Job Restrictions
Installs: 3181
Jenkins 1.609.3++
This plugin allows restricting execution of jobs on nodes depending on criterias like name pattern and ownership

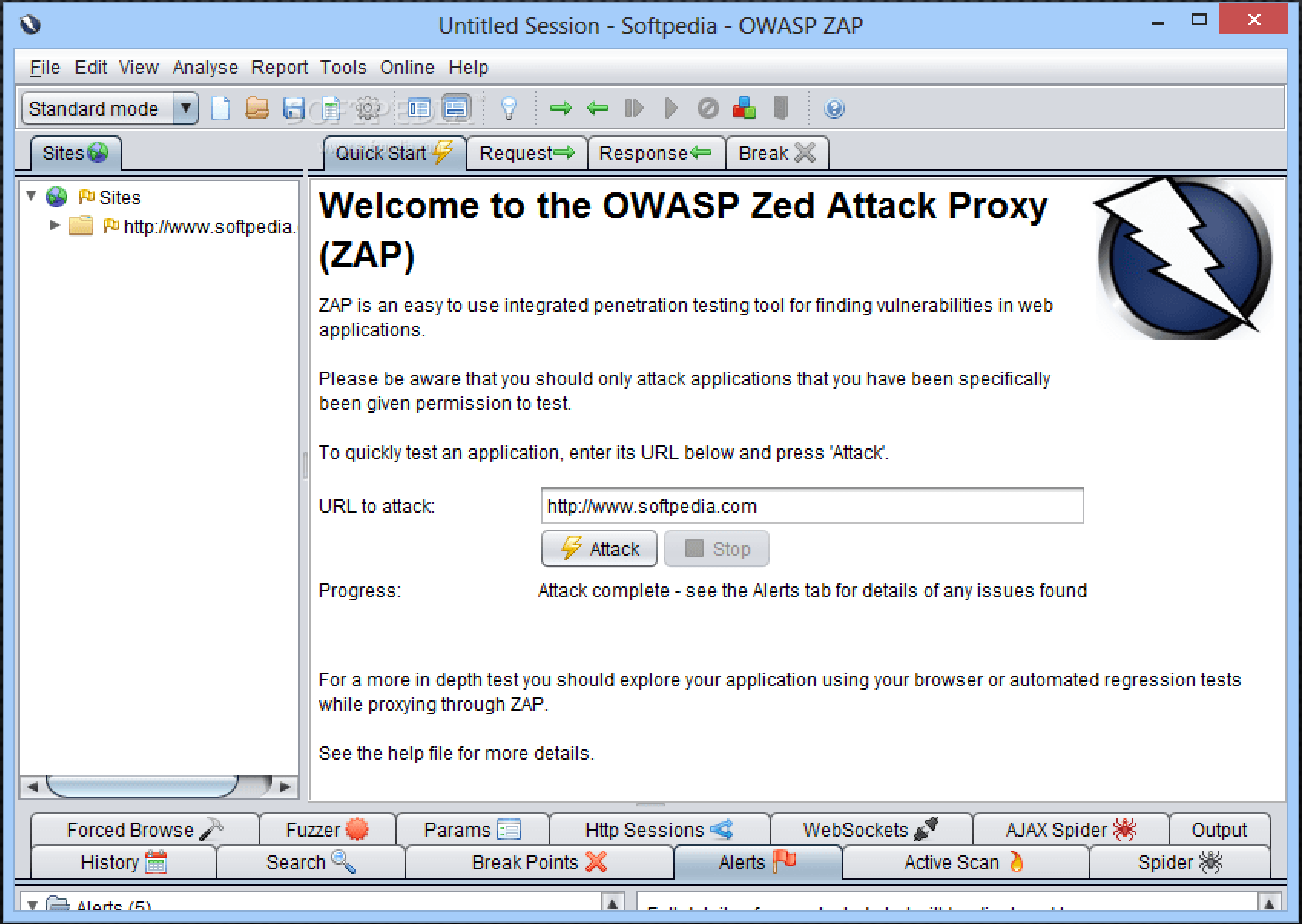
Stack Trace Suppression
Installs: 772
Jenkins 1.554.3++
User Interface,
Hide stack trace from ordinary users for security-sensitive deployments

Official OWASP ZAP
Installs: 607
Jenkins 1.580.1++
The Official OWASP ZAP Jenkins Plugin extends the functionality of the ZAP security tool into a CI

Mock Security Realm
Installs: 208
Jenkins 1.580.1++
Users and security,
Defines an insecure “security realm” only good for testing/demoing other parts of the system, such as

OWASP ZAP

- Zed Attack Proxy by Simon Bennetts
- Ideal for beginners but also used by professionals
- Can find security vulnerabilities in web applications automatically (good for devs)
- Also enables manual security testing (pentests)
- Some features include: Proxy, Scanner, Spider, Brute Force and Fuzzing



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.softpedia.com

Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

See the help file for more details.

OWASP DEPENDENCY CHECK

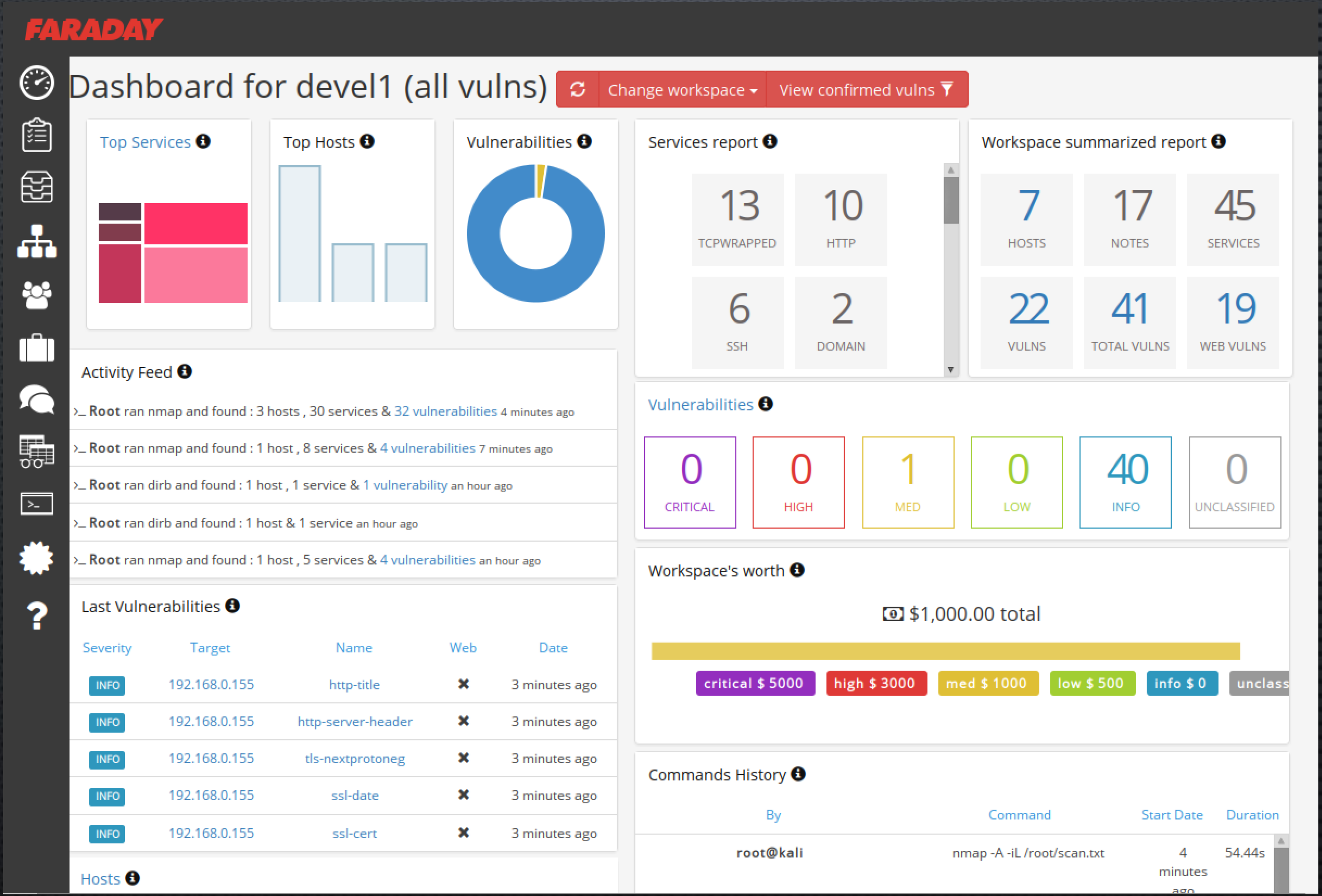
- identifies project dependencies and checks if there are any known, publicly disclosed, vulnerabilities
- Currently Java and .NET are supported
- Protects against OWASP Top 10 2017 RC2 A9 - Using Components with Known Vulnerabilities
- Has plugins for Maven, Gradle, Jenkins and SonarQube
- 95% of applications include open source
- 67% of applications contained open source vulnerabilities

Faraday

OpenVAS
Nessus vulnerability scanner
nexpose enterprise
netsparker
acunetix WEB APPLICATION SECURITY
w3af
BURPSUITE PROFESSIONAL
skipfish
QUALYS
BeEF
SHODAN
X1
metasploit
CORE IMPACT

- Created by Infobyte (Go Ekoparty!)
- Works as penetration testing collaboration tool
- Designed for distribution, indexation and analysis of the data generated during a security audit
- re-use the available tools in the community to take advantage of them in a multiuser way
- Designed for simplicity, users should notice no difference between their own terminal application and the one included in Faraday
- Has more than 60 plug-ins for security tools

FARADAY



FARADAY

Dashboard for devel1 (all vulns)

Change workspace ▾ | View confirmed vulns

Top Services ℹ

Top Hosts ℹ

Vulnerabilities ℹ

Services report ℹ

13 TCPWRAPPED	10 HTTP
6 SSH	2 DOMAIN

Workspace summarized report ℹ

7 HOSTS	17 NOTES	45 SERVICES
22 VULNS	41 TOTAL VULNS	19 WEB VULNS

Activity Feed ℹ

>_ **Root** ran nmap and found : 3 hosts , 30 services & 32 vulnerabilities 4 minutes ago

>_ **Root** ran nmap and found : 1 host , 8 services & 4 vulnerabilities 7 minutes ago

>_ **Root** ran dirb and found : 1 host , 1 service & 1 vulnerability an hour ago

>_ **Root** ran dirb and found : 1 host & 1 service an hour ago

>_ **Root** ran nmap and found : 1 host , 5 services & 4 vulnerabilities an hour ago

Vulnerabilities ℹ

0 CRITICAL	0 HIGH	1 MED	0 LOW	40 INFO	0 UNCLASSIFIED

Last Vulnerabilities ℹ

Severity	Target	Name	Web	Date
INFO	192.168.0.155	http-title	✖	3 minutes ago
INFO	192.168.0.155	http-server-header	✖	3 minutes ago
INFO	192.168.0.155	tls-nextprotoneg	✖	3 minutes ago
INFO	192.168.0.155	ssl-date	✖	3 minutes ago
INFO	192.168.0.155	ssl-cert	✖	3 minutes ago

Workspace's worth ℹ

$1,000.00 total

critical $ 5000 | high $ 3000 | med $ 1000 | low $ 500 | info $ 0 | unclass

Hosts ℹ

Commands History ℹ

By	Command	Start Date	Duration
root@kali	nmap -A -iL /root/scan.txt	4 minutes ago	54.44s

Remarks – Understand this!

- Dev are not security experts!
- Make security as much part of the dev process as writing code
- make it Transparent and part of the dev flow, without adding more barriers or bottlenecks
- Nobody likes bugs, not even devs, it makes them look bad
- Nobody likes being told they are wrong, especially in a report format
- Become the devs best friend and they will help you without even knowing (Security Champions Iniative)
- Remember what matters to the business and balance security with features

References

- DevOpsSec book – Jim Bird
- Securing DevOps Book - Julien Vehent
- The Phoenix Project Book – Gene Kim, Kevin Behr, George Spafford
- https://pt.slideshare.net/DinisCruz/owasp-brazil-making-security-invisible-by-becoming-the-developers-best-friends-v2
- https://www.youtube.com/watch?v=x9NOUtCNtAc
- http://www.devsecops.org/blog/2016/5/20/-security
- https://cdn2.hubspot.net/hubfs/1958393/White_Papers/devsecops_how_to_seamlessly__315283.pdf?t=1482418124868
- https://www.sans.org/reading-room/whitepapers/analyst/devsecops-playbook-36792
- https://www.ca.com/us/modern-software-factory/content/are-you-listening-to-your-software-developers.html
- https://www.veracode.com/state-of-software-security-report

THANK YOU
FOR YOUR ATTENTION