RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: OST-T10

Time to Spell Out Open Source Software Security

Brittany O'Shea

Senior Manager
Veracode

Agenda

- Nice to meet you
- What is Open Source Software?
- What Risks Does Open Source Software introduce?
- How you mitigate these risks in your organization?

What is Open Source Software?

Who crafts it?

So is it all basic features and functionality?

VERACODE

Who's using it?

100M+
* Repositories

40M+
* Developers Worldwide

2.9M+
* Organizations

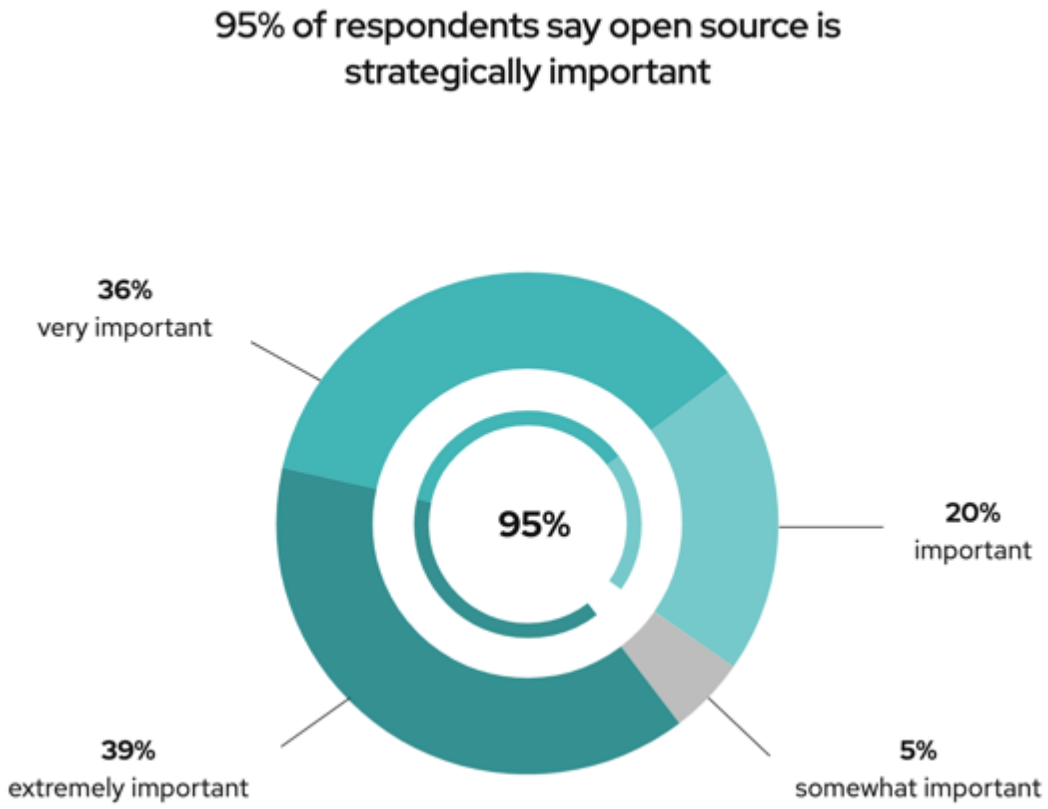
44M+
* Repositories Created in 2019

1.3M+
* First Time Contributors in 2019

VERACODE

* Source: State of the Octoverse, GitHub, November 2019

How important is it really?



86% of IT leaders say the **most innovative companies** are using enterprise open source

* Source: State of Enterprise Open Source, Redhat, 2020

What risk does Open Source Software introduce?

Legal

Security

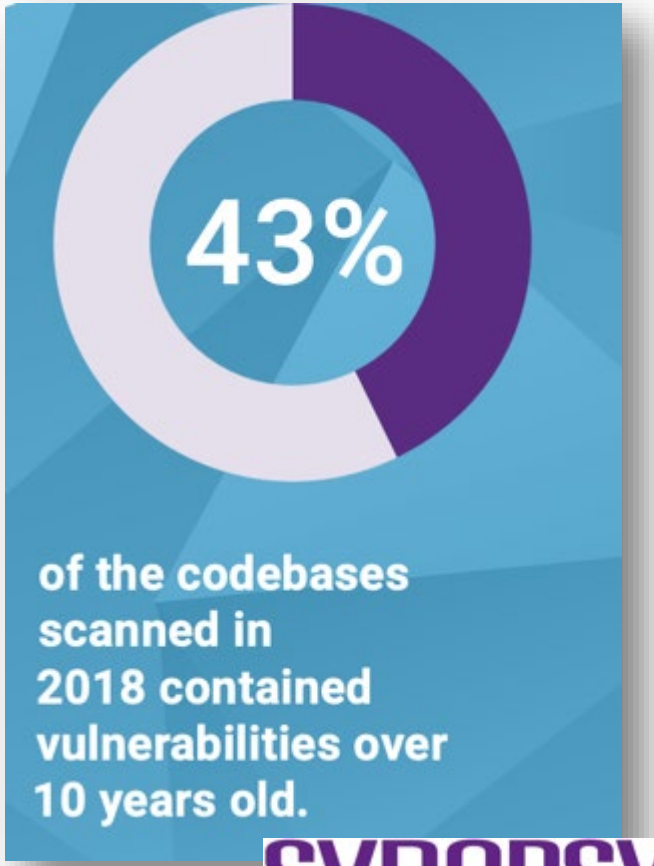
How Risky is Open Source Software…Really?

Up to 90% of applications contain at least one vulnerable component.

– *State of Software Security Volume 9*

VERACODE

WhiteSource



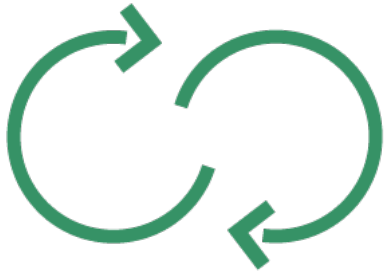
SYNOPSYS®

What's blocking us from fixing this?

Silent Fixes

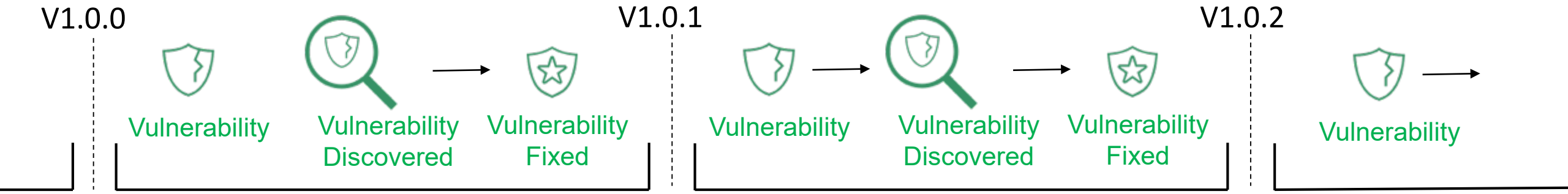
Risk prioritization

Transitive vulnerabilities



Speed of DevOps

Silent Fixes



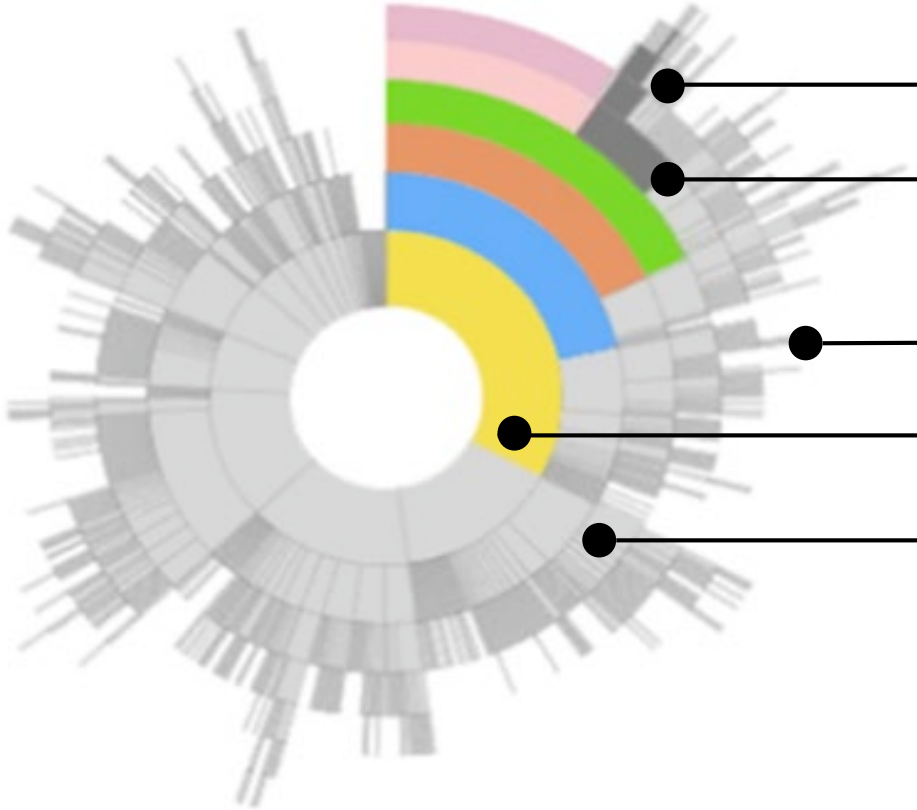
VERACODE

Risk prioritization

Is this even exploitable?

VERACODE

Transitive vulnerabilities



Transitive library w/vulnerability

Transitive Library

Transitive Library

Source Code

Open source library used - Direct Dependency

Hundreds of Transitive Dependencies

Speed of DevOps

- **Software is being released quicker then ever:** 43% of developers' organizations deploy code continuously, and 41% deploy between once a day and once a month

- **Current Security implementations don't work:** 50% of developers' organizations agree security vulnerabilities are most discovered by security team after code is merged in a test environment, and 49% encounter most delays in the testing phase of lifecycle.

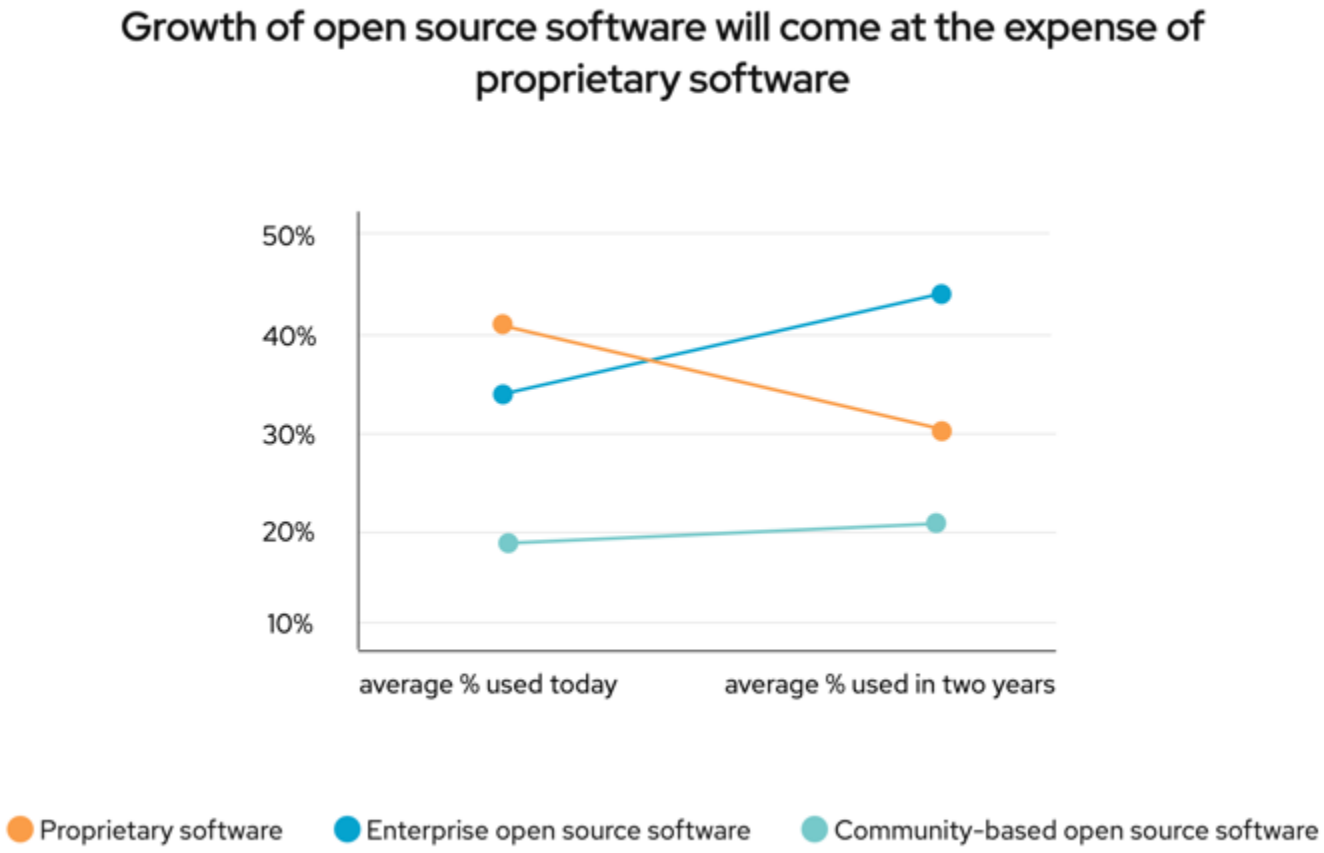
- **Finding flaws is easy, fixing them is hard**: When examining the top forty computer science programs in the United States, Forrester found that zero of the forty schools require a class about secure coding or secure application design.

VERACODE

How do I translate this to my organization

1. Create and enforce security policies
2. Understand what open source libraries are being used and where the vulnerabilities are
3. Update vulnerable libraries
4. Engage your developers

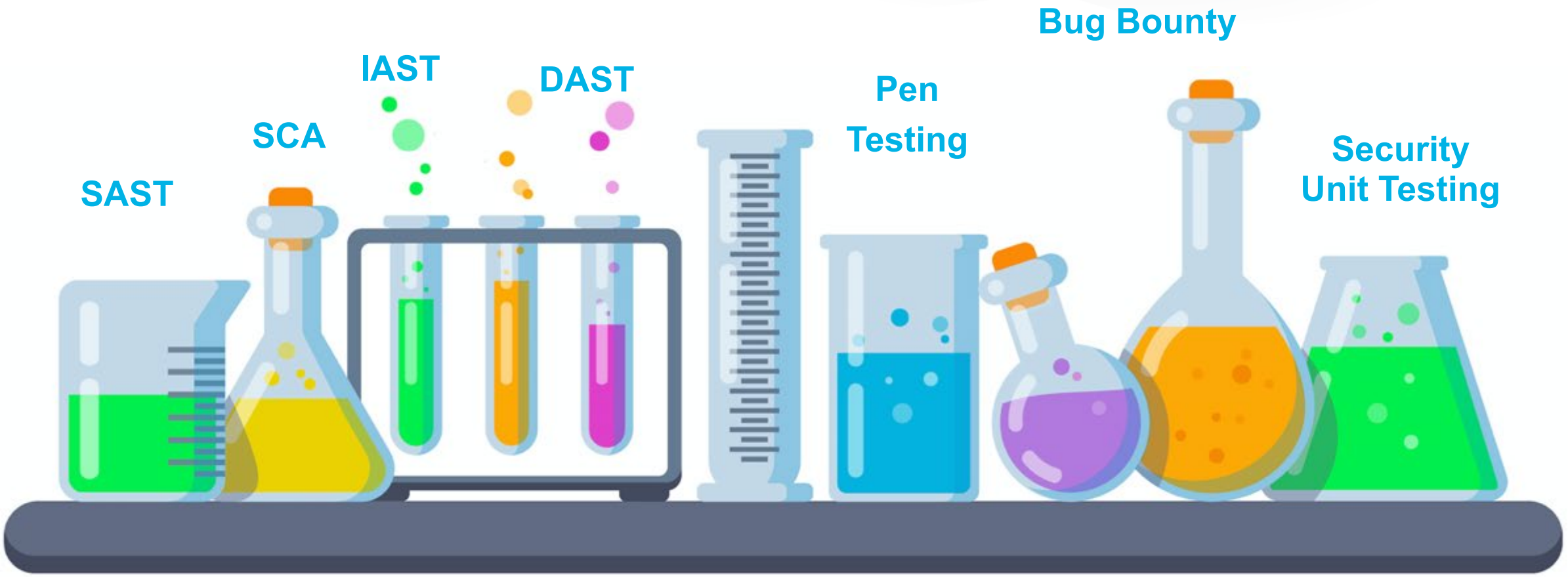
But what about my other code?

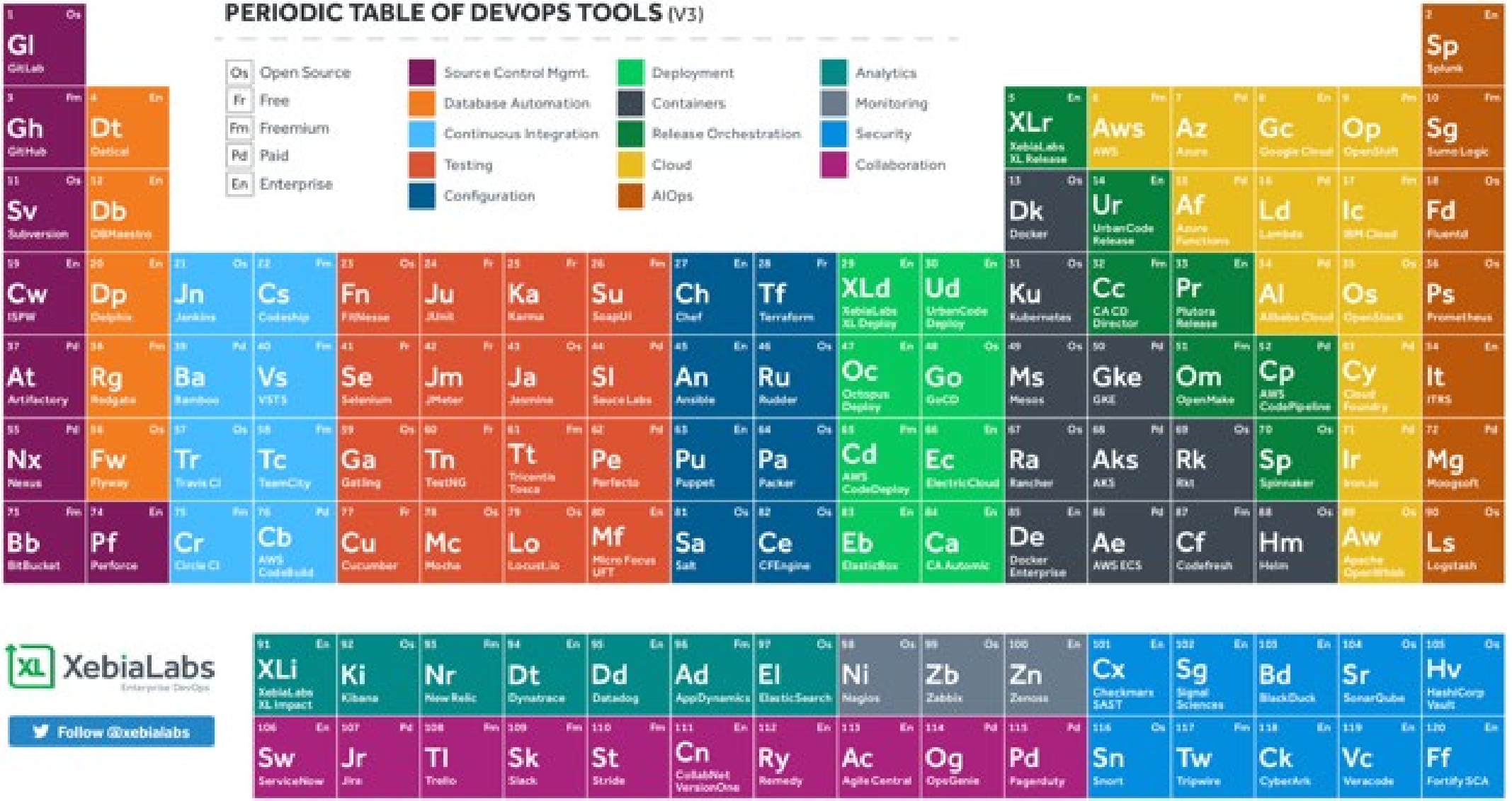


More then 70% applications **are made up of open source code**

* Source: State of Enterprise Open Source, Redhat 2020


Vulnerability
Be Gone


SAST
SCA
IAST
DAST
Pen Testing
Bug Bounty
Security Unit Testing


PERIODIC TABLE OF DEVOPS TOOLS (V3)
Os Open Source
Fr Free
Fm Freemium
Pd Paid
En Enterprise
Source Control Mgmt.
Database Automation
Continuous Integration
Testing
Configuration
Deployment
Containers
Release Orchestration
Cloud
AIOps
Analytics
Monitoring
Security
Collaboration
Gl GitLab
Gh GitHub
Dt Datical
Sv Subversion
Db DBMaestro
Cw ISPW
Dp Delphix
Jn Jenkins
Cs Codeship
Fn FitNesse
Ju JUnit
Ka Karma
Su SoapUI
Ch Chef
Tf Terraform
XLd XebiaLabs XL Deploy
Ud UrbanCode Deploy
Ku Kubernetes
Cc CA CD Director
Pr Plutora Release
Al Alibaba Cloud
Os OpenStack
Ps Prometheus
At Artifactory
Rg Redgate
Ba Bamboo
Vs VSTS
Se Selenium
Jm JMeter
Ja Jasmine
Sl Sauce Labs
An Ansible
Ru Rudder
Oc Octopus Deploy
Go GoCD
Ms Mesos
Gke GKE
Om OpenMake
Cp AWS CodePipeline
Cy Cloud Foundry
It ITRS
Nx Nexus
Fw Flyway
Tr Travis CI
Tc TeamCity
Ga Gatling
Tn TestNG
Tt Tricentis Tosca
Pe Perfecto
Pu Puppet
Pa Packer
Cd AWS CodeDeploy
Ec ElectricCloud
Ra Rancher
Aks AKS
Rk Rkt
Sp Spinnaker
Ir Iron.io
Mg Moogsoft
Bb BitBucket
Pf Perforce
Cr Circle CI
Cb AWS CodeBuild
Cu Cucumber
Mc Mocha
Lo Locust.io
Mf Micro Focus UFT
Sa Salt
Ce CFEngine
Eb ElasticBox
Ca CA Automic
De Docker Enterprise
Ae AWS ECS
Cf Codefresh
Hm Helm
Aw Apache OpenWhisk
Ls Logstash
Sp Splunk
XLr XebiaLabs XL Release
Aws AWS
Az Azure
Gc Google Cloud
Op OpenShift
Sg Sumo Logic
Dk Docker
Ur UrbanCode Release
Af Azure Functions
Ld Lambda
Ic IBM Cloud
Fd Fluentd
XebiaLabs
Follow @xebialabs
XLi XebiaLabs XL Impact
Ki Kibana
Nr New Relic
Dt Dynatrace
Dd Datadog
Ad AppDynamics
El ElasticSearch
Ni Nagios
Zb Zabbix
Zn Zenoss
Cx Checkmarx SAST
Sg Signal Sciences
Bd BlackDuck
Sr SonarQube
Hv HashiCorp Vault
Sw ServiceNow
Jr Jira
Tl Trello
Sk Slack
St Stride
Cn CollabNet VersionOne
Ry Remedy
Ac Agile Central
Og OpsGenie
Pd Pagerduty
Sn Snort
Tw Tripwire
Ck CyberArk
Vc Veracode
Ff Fortify SCA

Recommended Research

- Veracode State of Software Security
- State of the Octoverse, GitHub
- State of Enterprise Open Source, Redhat
- Upcoming webinars:
  - Innovative Application Security Testing Techniques for Modern Software Development (March 12th)
  - Accelerate Open Source Adoption, Not Open Source Risk (March 26th)

RSAConference2020

Thank you!

Brittany O’Shea, Senior Manager, Veracode