

The background of the slide is a composite image. The top half shows a starry night sky with a prominent meteor streak. The bottom half shows a landscape with several tents pitched in a field, with a warm, golden light on the horizon suggesting a sunset or sunrise. A large, semi-transparent blue triangle is overlaid on the right side of the image, containing the event title and speaker information.

VERACODE

You change the world, we'll secure it.

Chris Wysopal
CTO & co-founder
Veracode

Supply Chain Security for Modern Development

December 4, 2019
FinTech Connect

One of the 1st vulnerability researchers at the hacker think tank, L0pht in 90's.



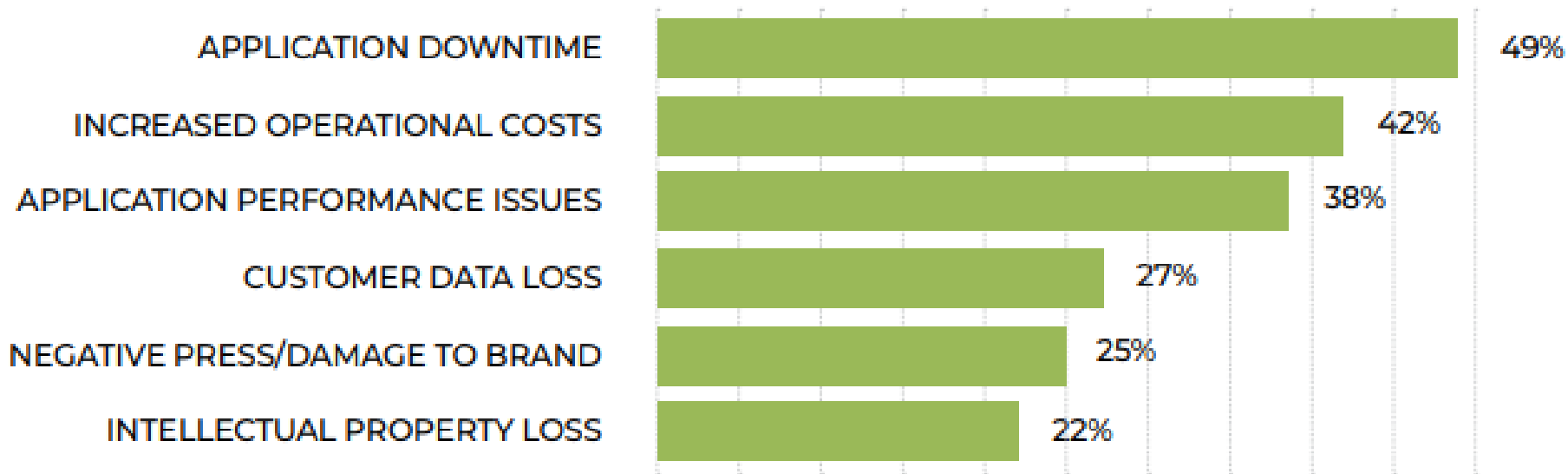
Unites States Senate testimony. May 19, 1998



You change the world, we'll secure it.

VERACODE

Impacts from application security vulnerability



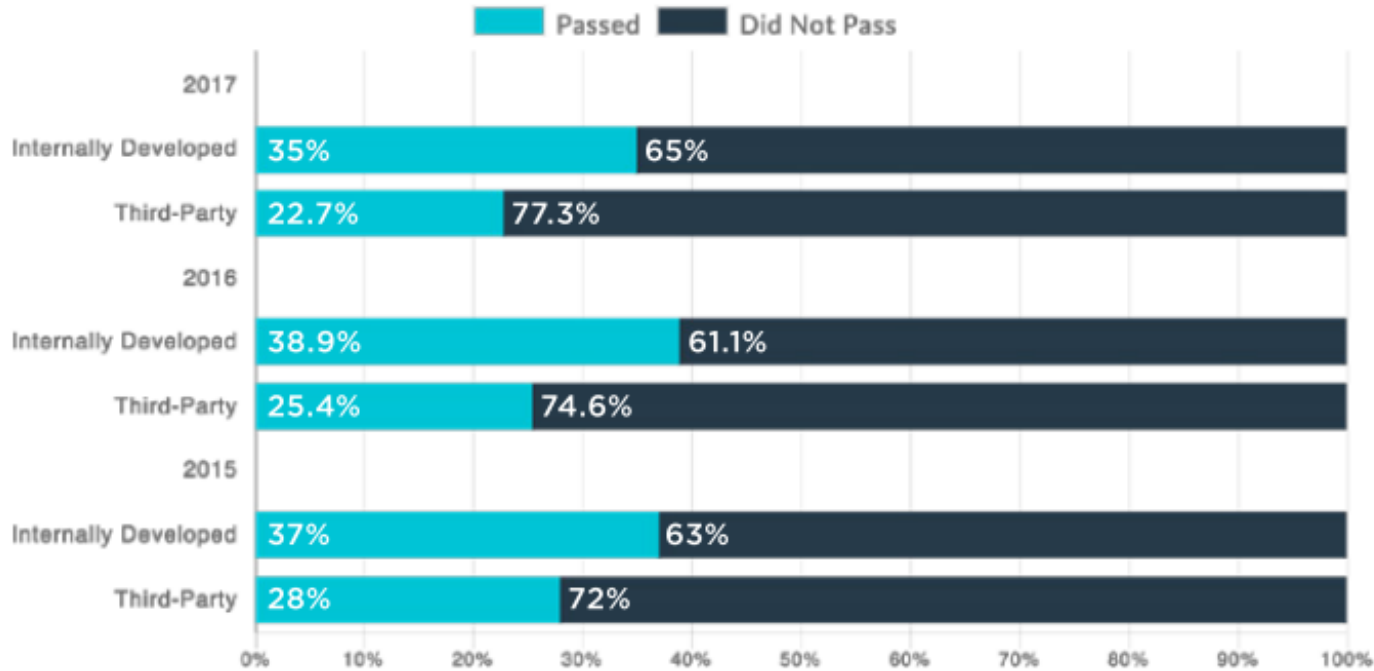
How to Make Application Security a Competitive Advantage, IDG Market Survey, March 2018



You change the world, we'll secure it.

INTERNALLY DEVELOPED VS. THIRD-PARTY (COMMERCIAL) APPLICATIONS

Applications Passing OWASP Top 10 Policy

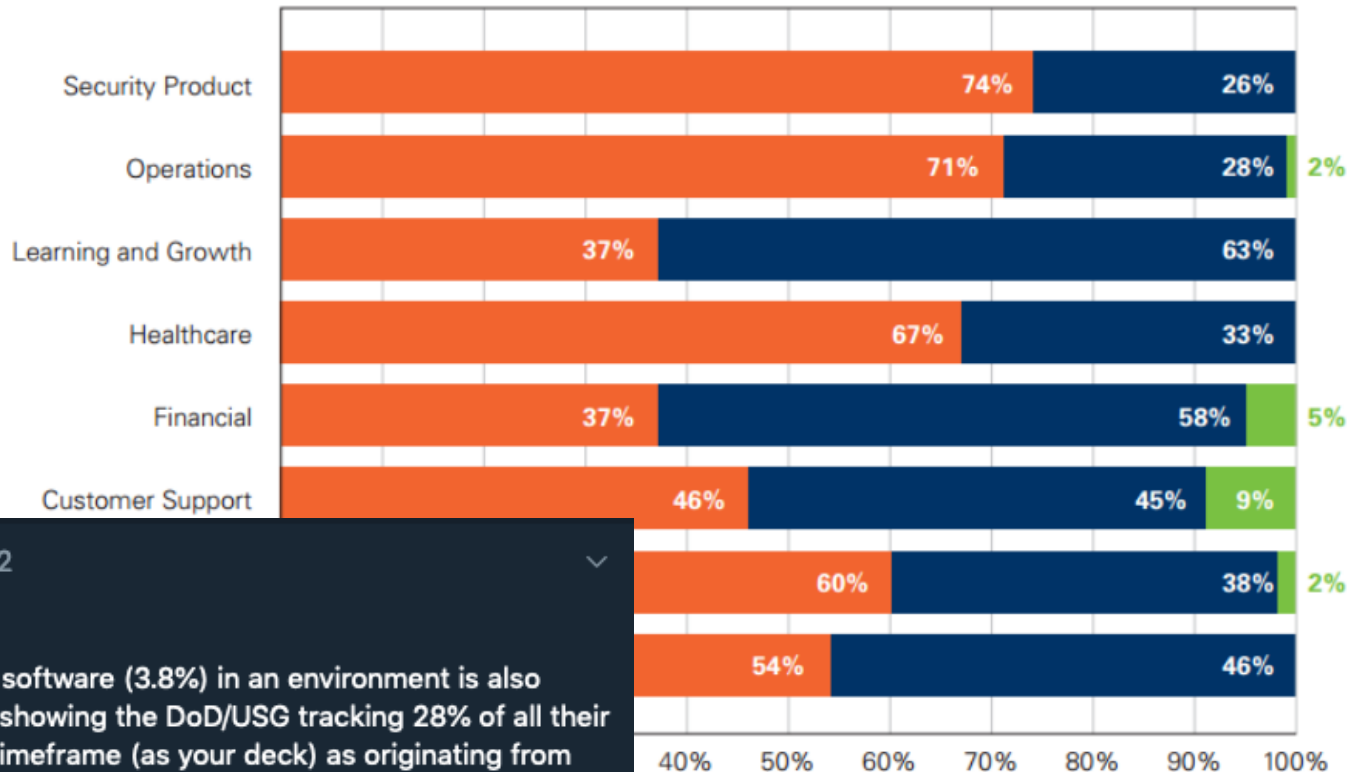


You change the world, we'll secure it.



Performance Against Enterprise Policy by Application Purpose

Fail Pass Pass Conditionally



Mudge @dotMudge · Jul 22

Thanks.

The percentage of security software (3.8%) in an environment is also helpful as I have data/stats showing the DoD/USG tracking 28% of all their security vulns in the same timeframe (as your deck) as originating from deployed security solutions.



You change the world, we'll secure it.

VERACODE

Evaluating the Security of Software

1st Party Code

Secure Coding

Scan Frequency

Pre- / Post-Production

Code

Developer Training

Assessment Target

Open Sourced Code

How to Fix

Integrated Scanning

Kashi®
7 Whole Grain Flakes

Nutrition Facts	
Serving Size 1 Cup (50g)	
Amount Per Serving	
Calories 170	Calories from Fat 5
% Daily Value*	
Total Fat 0.5g	1%
Saturated Fat 0g	0%
Trans Fat 0g	
Polyunsaturated Fat 0g	
Monounsaturated Fat 0g	
Cholesterol 0mg	0%
Sodium 150mg	6%
Potassium 120mg	3%
Total Carbohydrate 41g	14%
Dietary Fiber 6g	24%
Soluble Fiber 0g	
Insoluble Fiber 6g	
Sugars 6g	
Protein 6g	4%
Vitamin A 0%	Vitamin C 0%
Calcium 0%	Iron 8%
*Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs.	
	Calories: 2,000 2,500
Total Fat	Less than 65g 80g
Sat. Fat	Less than 20g 25g
Cholesterol	Less than 300mg 300mg
Sodium	Less than 2,400mg 2,400mg
Potassium	3,500mg 3,500mg
Total Carbohydrate	300g 375g
Dietary Fiber	25g 30g
Protein	50g 65g
Calories per gram:	
Fat 9	Carbohydrate 4 Protein 4

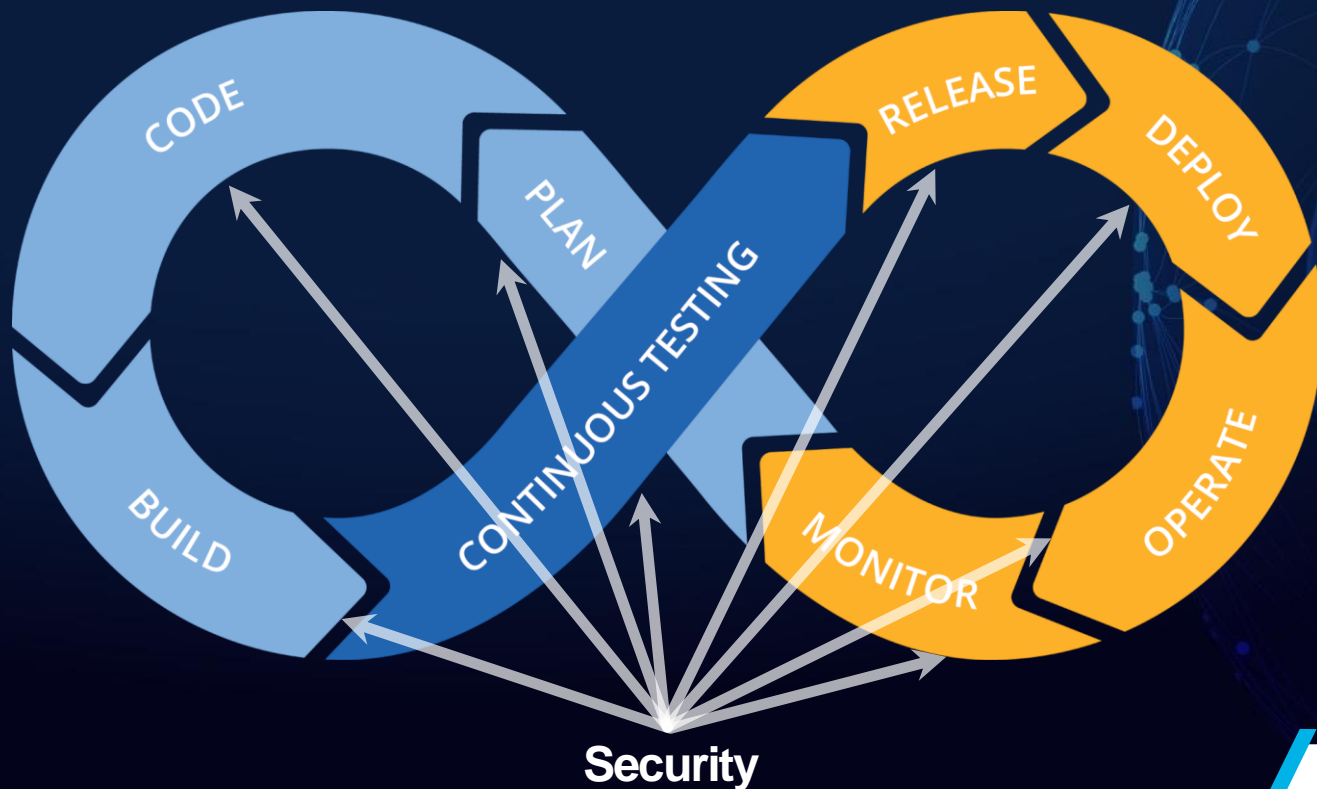
INGREDIENTS: KASHI SEVEN WHOLE GRAIN BLEND (WHOLE: ORGANIC HARD RED WHEAT, OATS, BROWN RICE, TRITICALE, RYE, BARLEY, BUCKWHEAT), ORGANIC LONG GRAIN RICE, ORGANIC DRIED CANE SYRUP, ORGANIC WHEAT BRAN, OAT FIBER, BARLEY MALT EXTRACT, BROWN RICE SYRUP, SALT, SESAME SEEDS.
CONTAINS WHEAT INGREDIENTS.

NLI#10410



You change the world, we'll secure it.

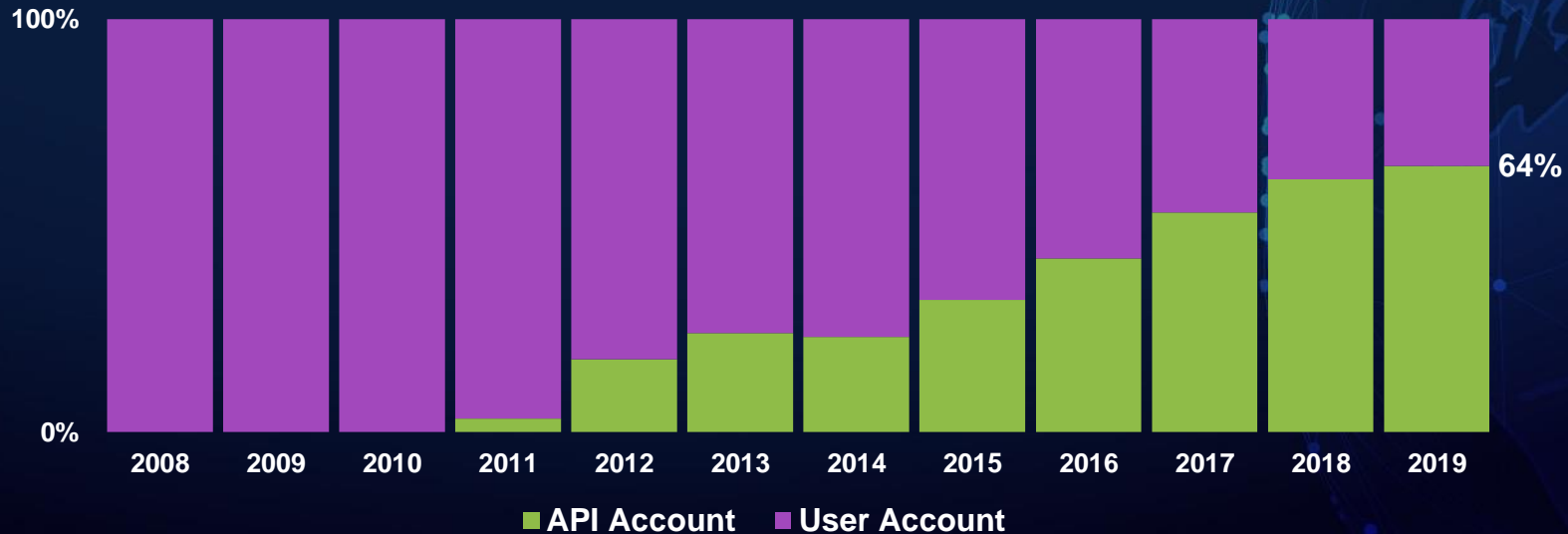
DevSecOps is becoming the norm.



You change the world, we'll secure it.

VERACODE

DevSecOps Indicator: Percentage of Scans by Account Type

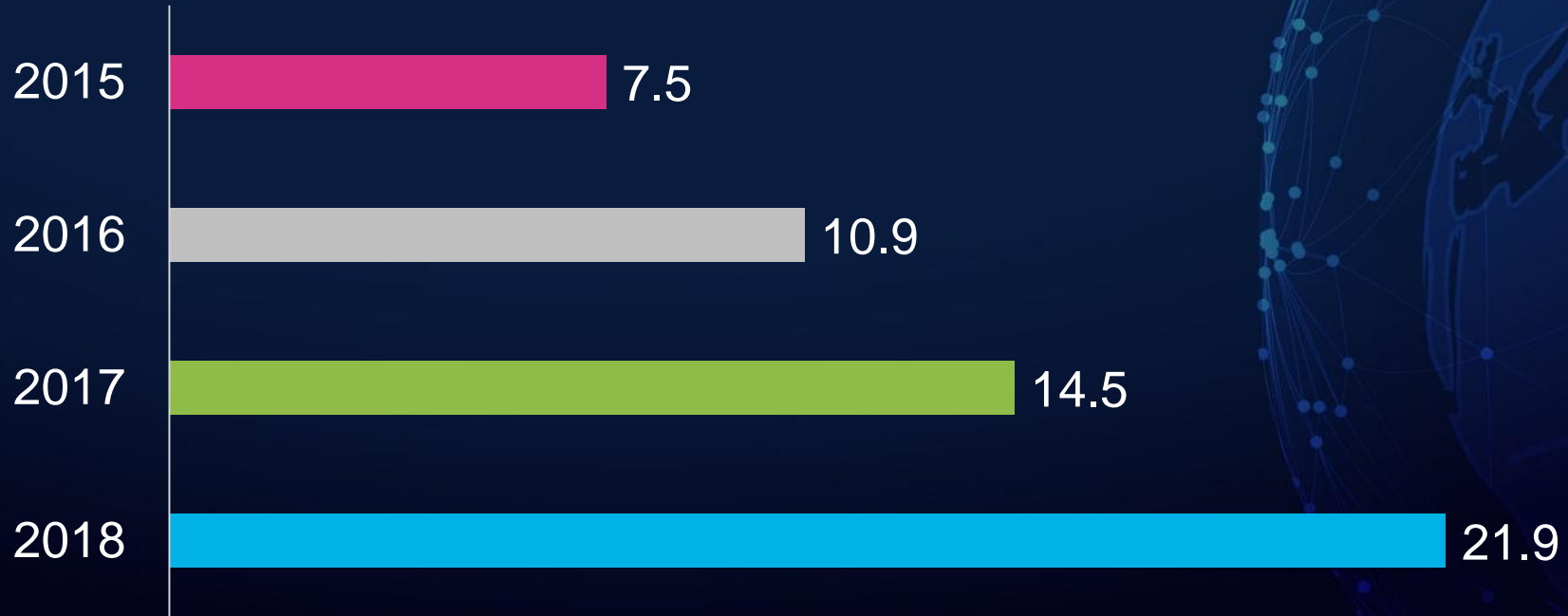


You change the world, we'll secure it.

SOURCE: Veracode, State of Software Security Volume 8, 2017-10-18

VERACODE

DevSecOps Indicator: Average Number of Scans Per Application



You change the world, we'll secure it.

SOURCE: Veracode, State of Software Security Volume 8, 2017-10-18

VERACODE

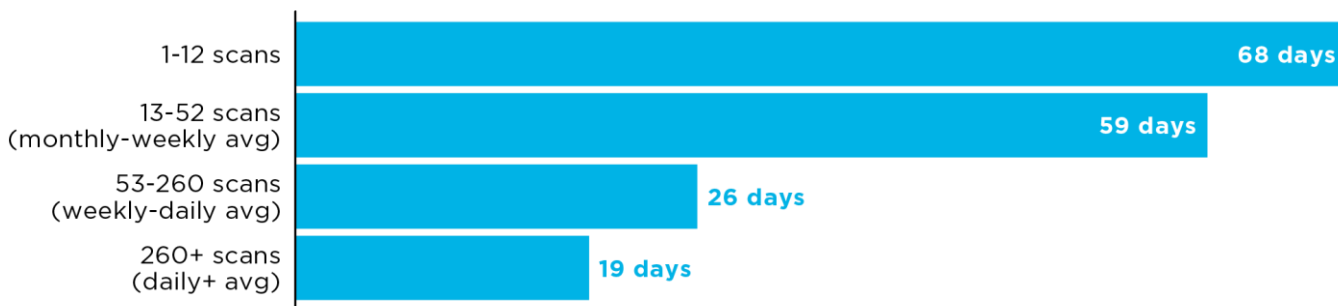
DevSecOps Improves Time To Remediate

3X

**Reduction in
MTTR**

3X

Higher Fix Rate



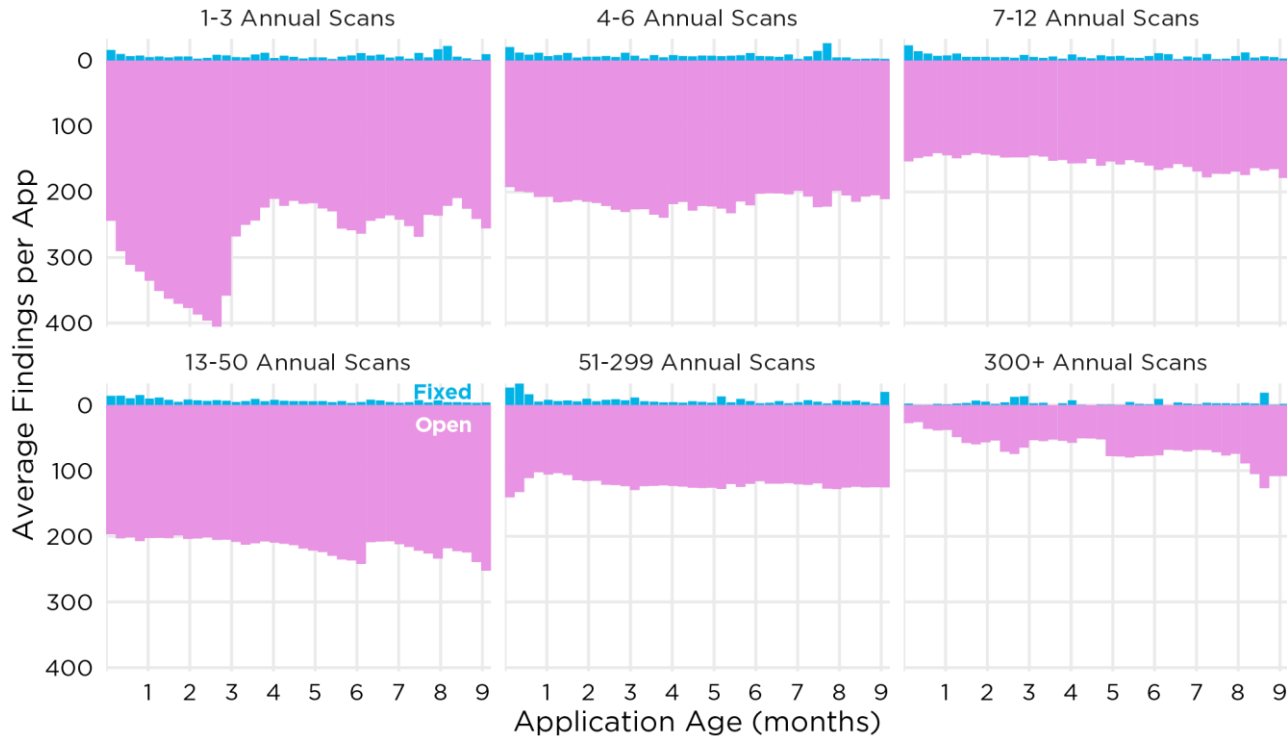
Median TTR

Source: Veracode SOSS Volume 10



You change the world, we'll secure it.

DevSecOps Effect



Source: Veracode SOSS Volume 10

5X
Less Security Debt



You change the world, we'll secure it.



Vulnerable Modules/Libraries

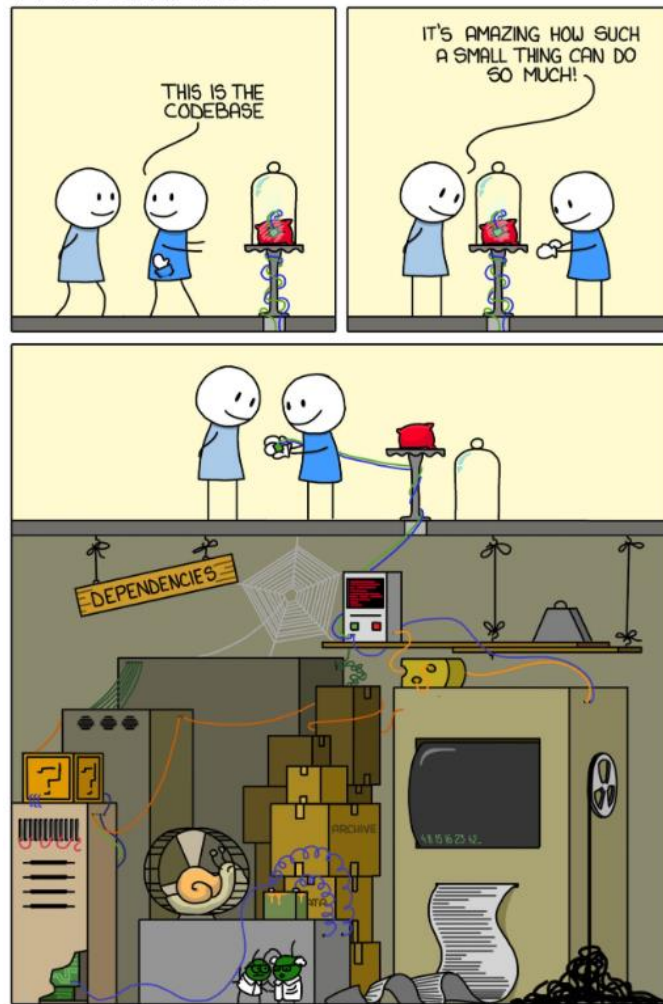
Thousands of CVEs in open source packages

Need to be continuous about library and package inspection and monitoring

How fast can you determine if a new vulnerability in an open source package effects one of your apps?

How fast can you rebuild and redeploy?

IMPLEMENTATION



You change the world, we'll secure it.

Validating a Secure Development Process

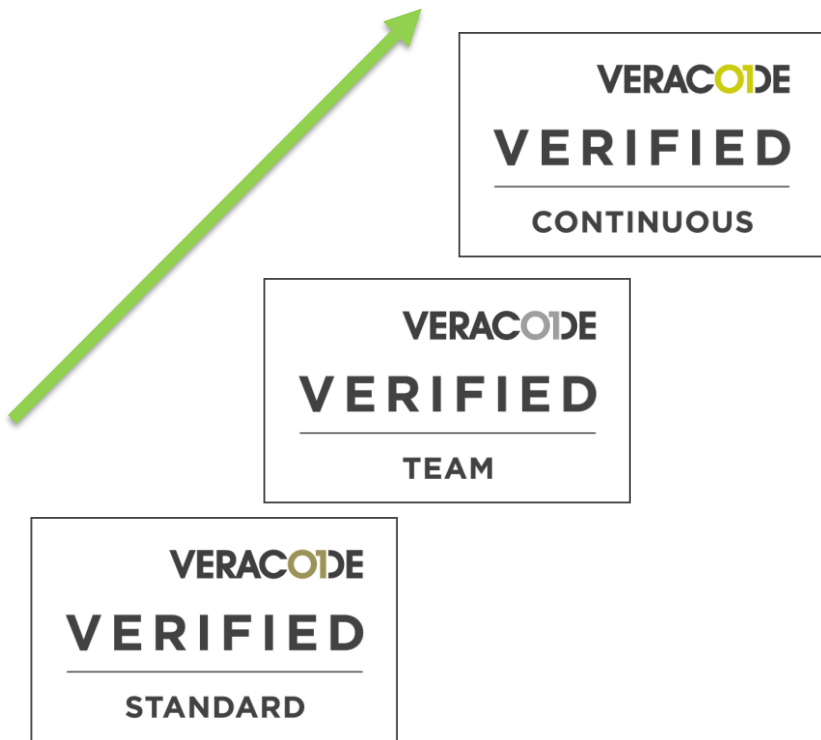
Veracode Verified	Verified Standard <i>Security Baseline</i>	Verified Team <i>Secure Coding Culture</i>	Verified Continuous <i>Business-Driven Maturity</i>
Code Security	No Very High Flaws	No Very High Flaws No High Flaws	No Very High Flaws No High Flaws No Medium Flaws
Developer Training		Security Champion	Security Champion Secure Coding Training
Assessment Target	Assess 1 st Party Code	Assess 1 st Party Code Assess 3 rd Party Code	Assess 1 st Party Code Assess 3 rd Party Code Integrated Scanning



You change the world, we'll secure it.

VERACODE

A Roadmap to Compliance



A collection of compliance and certification logos:

- HITRUST CSF Certified**
- PCI DSS COMPLIANT v3.2**
- NIST National Institute of Standards and Technology U.S. Department of Commerce**
- General Data Protection Regulation**
- NY State Cybersecurity Regulation**



You change the world, we'll secure it.

VERACODE

<https://www.veracode.com/verified/directory>






VERACODE

You change the world, we'll secure it.

Chris Wysopal

cwysopal@veracode.com

@weldpond

 FLIP Training	 Search Guard Security for Elasticsearch floragunn GmbH	 HID Global SAFE	 Icertis
 The home of UltraEdit IDM	 JAMIS	 Joyful Joyful Inc. Member of the LIFESTYLE LEADER	 JReview® Integrated Clinical Systems, Inc. JReview®
 Katabat	 Kyriba	 NETFOUNDRY SHINE UP YOUR NETWORK NetFoundry	 Nlyte Software Nlyte Software
 OLS ON-LINE STRATEGIES OLS Strategies	 OneVizion	 PORTAL GUARD® Engineered by PPIUS STAX, INC. PortalGuard	 PPI AG PPI AG
 Prophecy Prophecy International	 QAD QAD Channel Islands	 Rekener Rekener	 SAVO SAVO
 Sensibill™ Sensibill	 STRATUS™ video Stratus Video	 terida Our work. Your flow. Terida	 TreeBox Solutions TreeBox Solutions
 TRUE FIT™	 UiPath	 ZOOMDATA®	