SNOWFROC 2013

Data Mining a Mountain of Zero Day Vulnerabilities

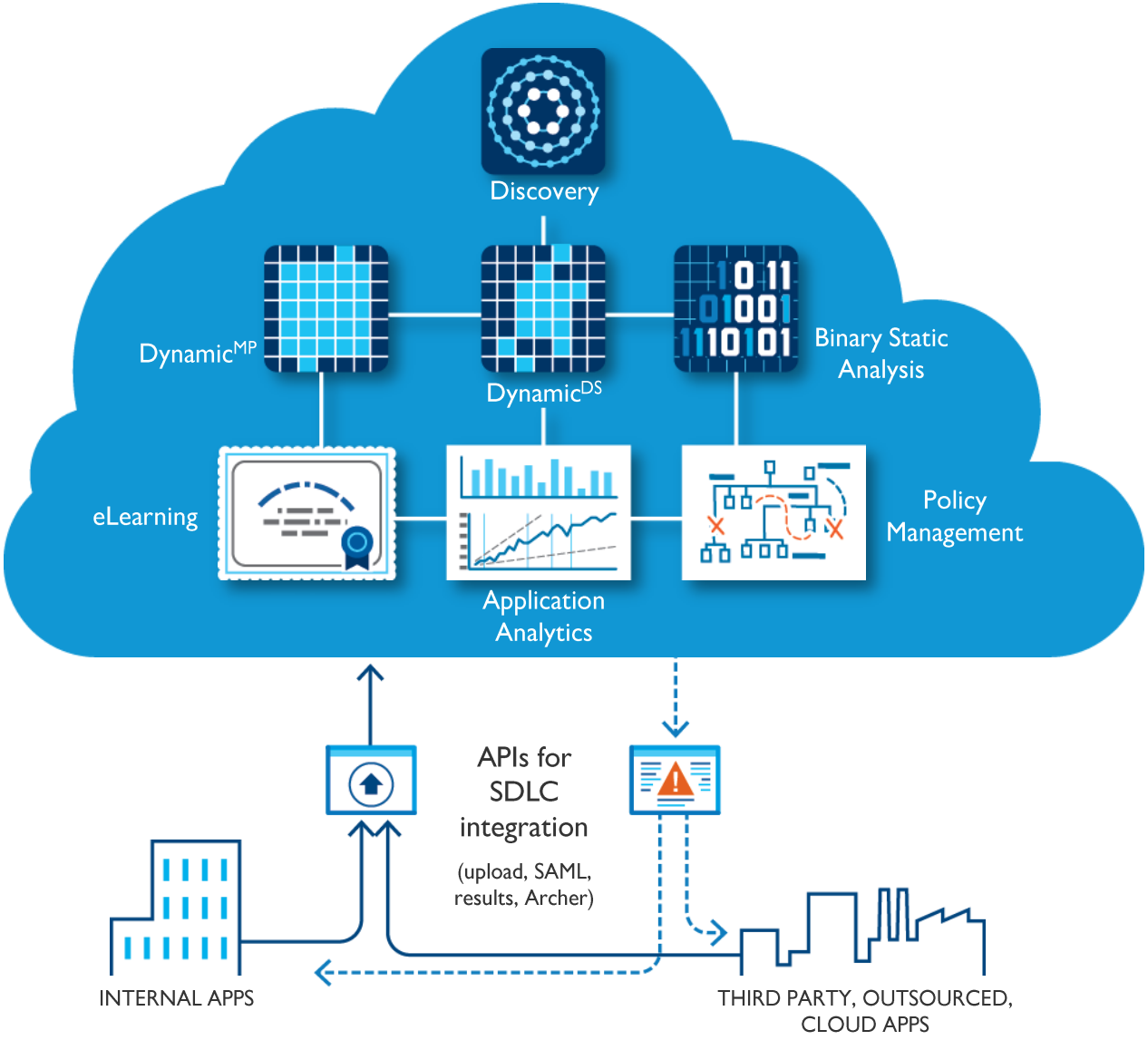
OWASP

The Open Web Application Security Project

Data Mining a Mountain of Zero Day Vulnerabilities

Joe Brady
Senior Solutions Architect
March 29, 2013

Central platform supports internal and third-party applications

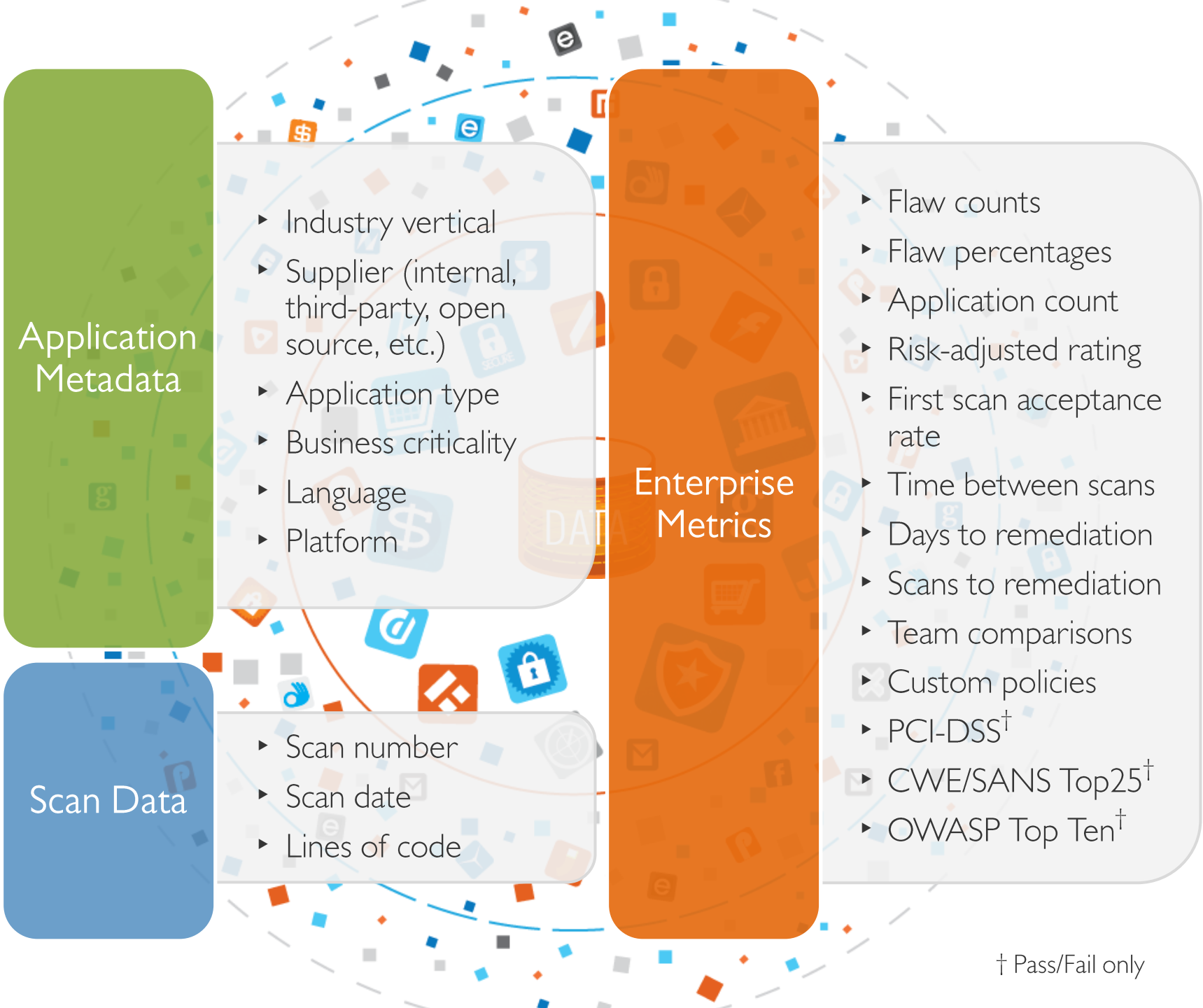


No hardware,
No software,
No maintenance

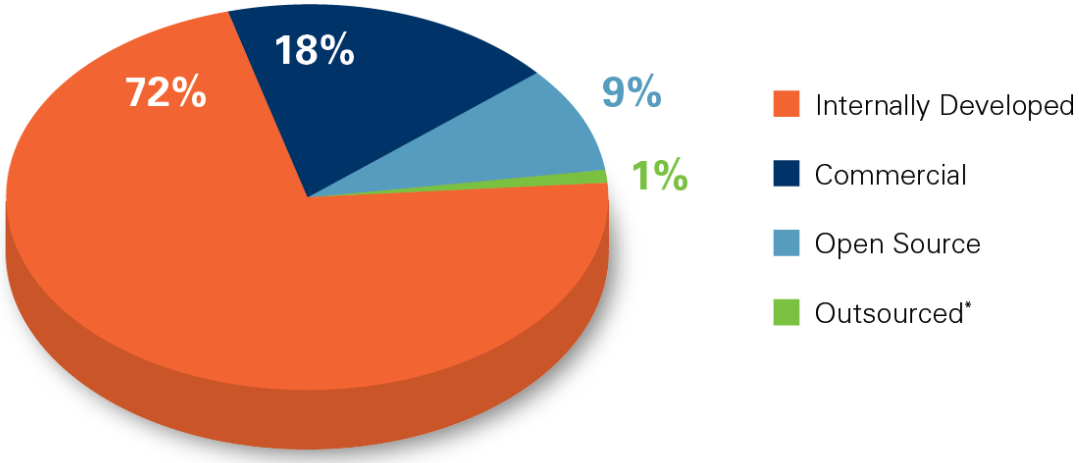
VERACODE

The Data Set

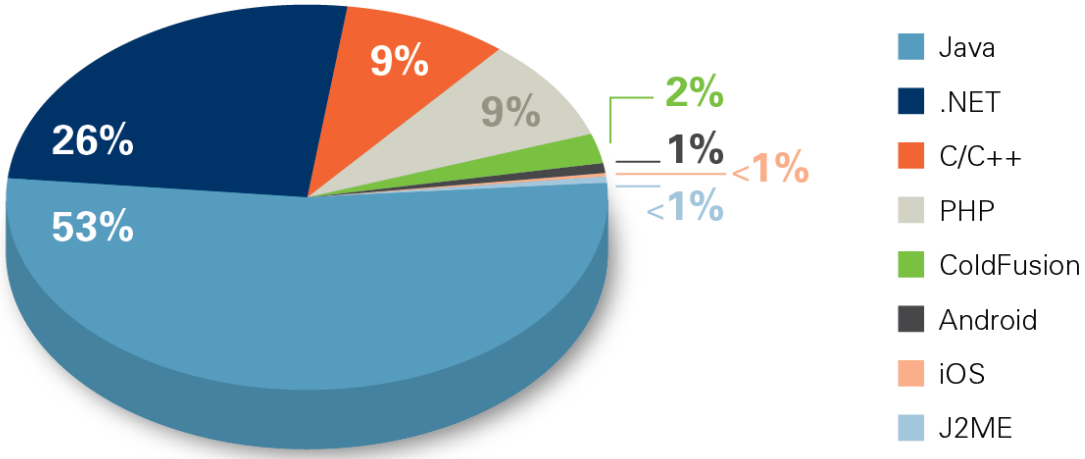
- Applications from over 300 commercial and US government customers
- Scanned 9,910 applications over 18 months
- Ranged in size from 100KB to 6GB
- Included both pre-release and production software
- Internally built, outsourced, open source, and commercial ISV code


Application Metadata
Industry vertical
Supplier (internal, third-party, open source, etc.)
Application type
Business criticality
Language
Platform
Scan Data
Scan number
Scan date
Lines of code
Enterprise Metrics
Flaw counts
Flaw percentages
Application count
Risk-adjusted rating
First scan acceptance rate
Time between scans
Days to remediation
Scans to remediation
Team comparisons
Custom policies
PCI-DSS†
CWE/SANS Top25†
OWASP Top Ten†
† Pass/Fail only

Applications by Supplier Type



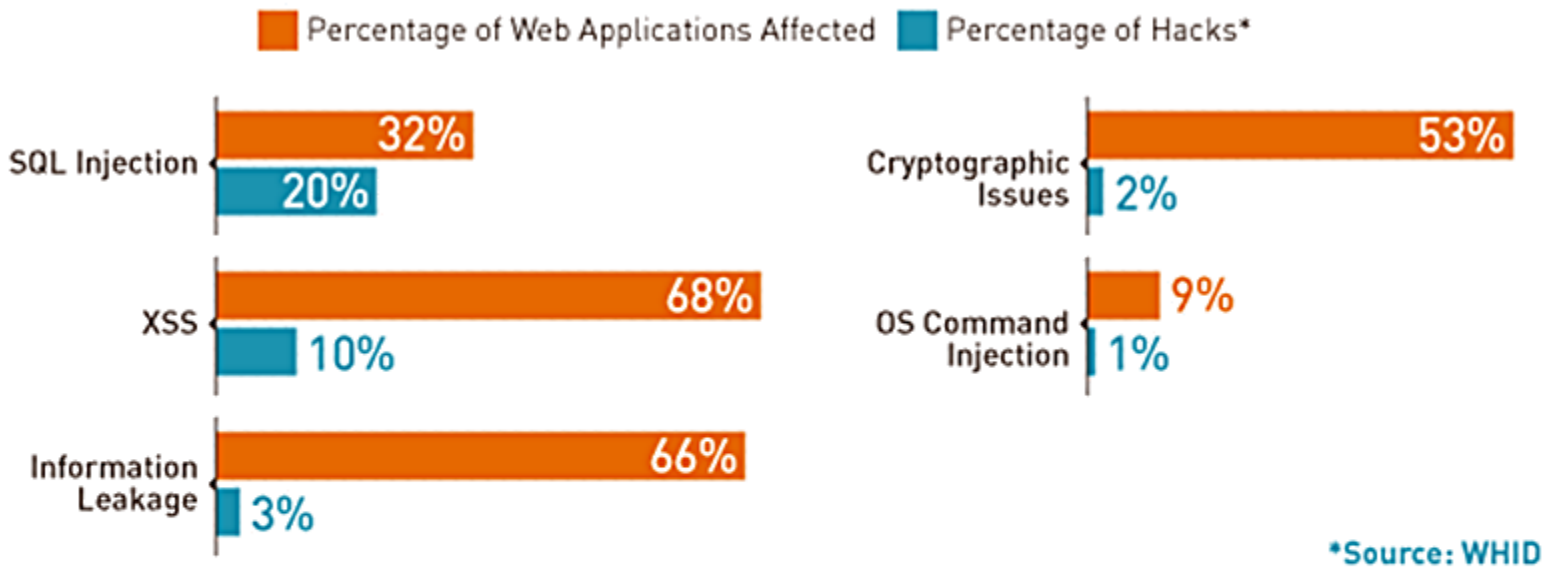
Applications by Language Family



Caveats

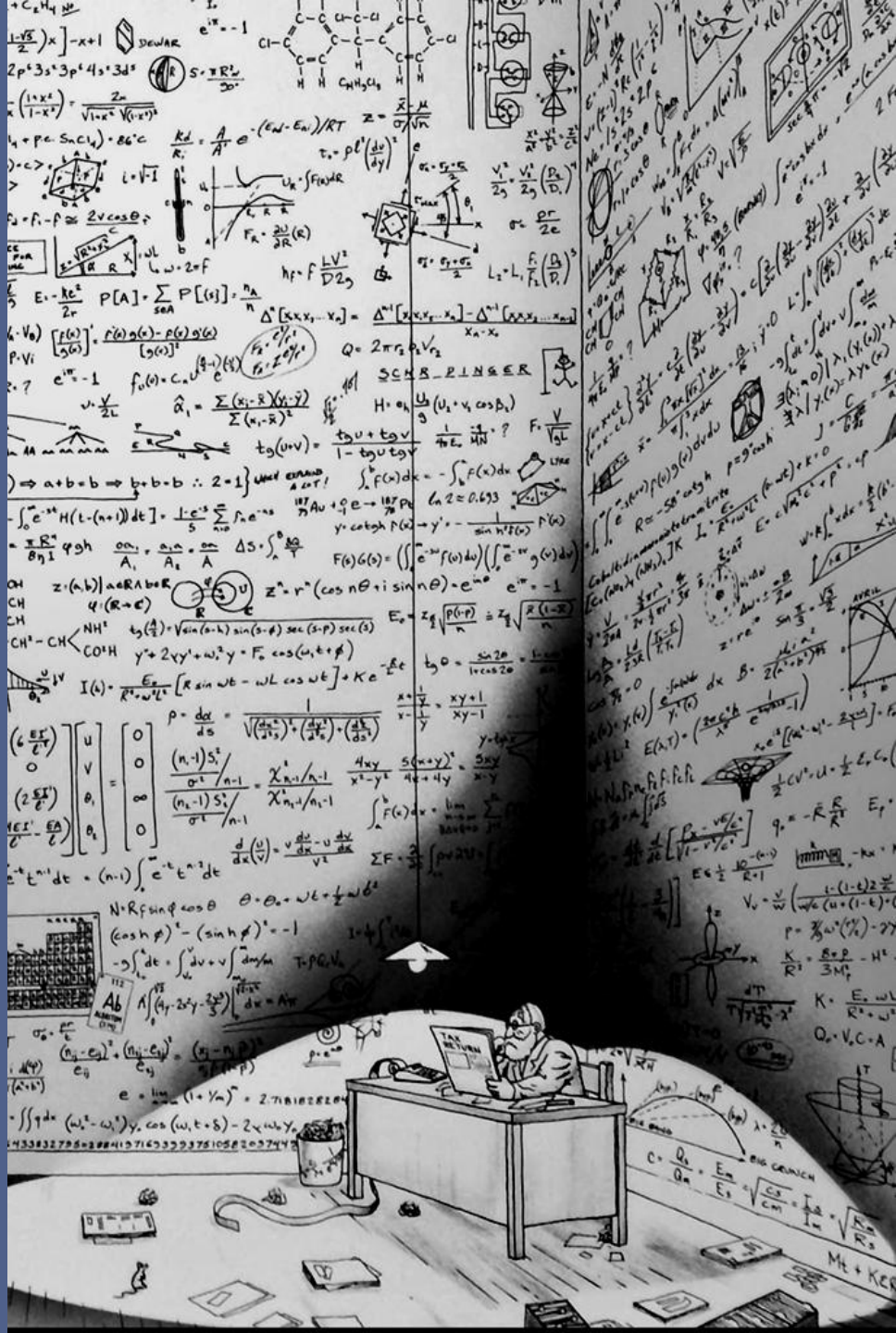
- Customer base is already security-conscious
- Bias toward business critical applications
- Applications are at inconsistent phases in the SDLC
- Not all flaws are necessarily easy to exploit
- Analysis technology is continuously being improved
- All security testing has False Negatives

THE LATENT VULNERABILITIES VS. THE ATTACKS



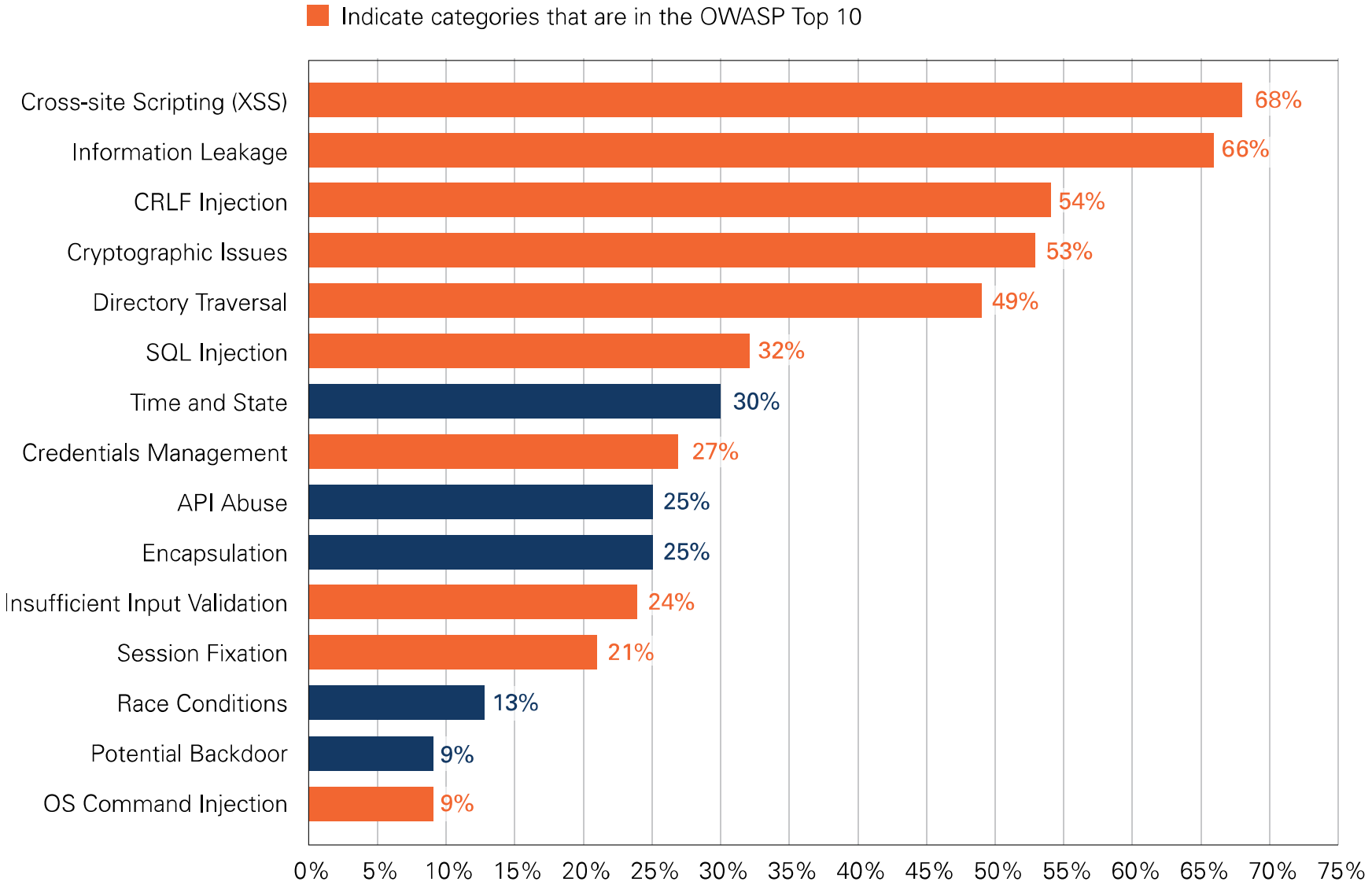
While other flaws such as XSS account for a higher volume of findings, SQL injection accounts for 20 percent of hacks.

LET'S TAKE A CLOSER LOOK AT THE NUMBERS



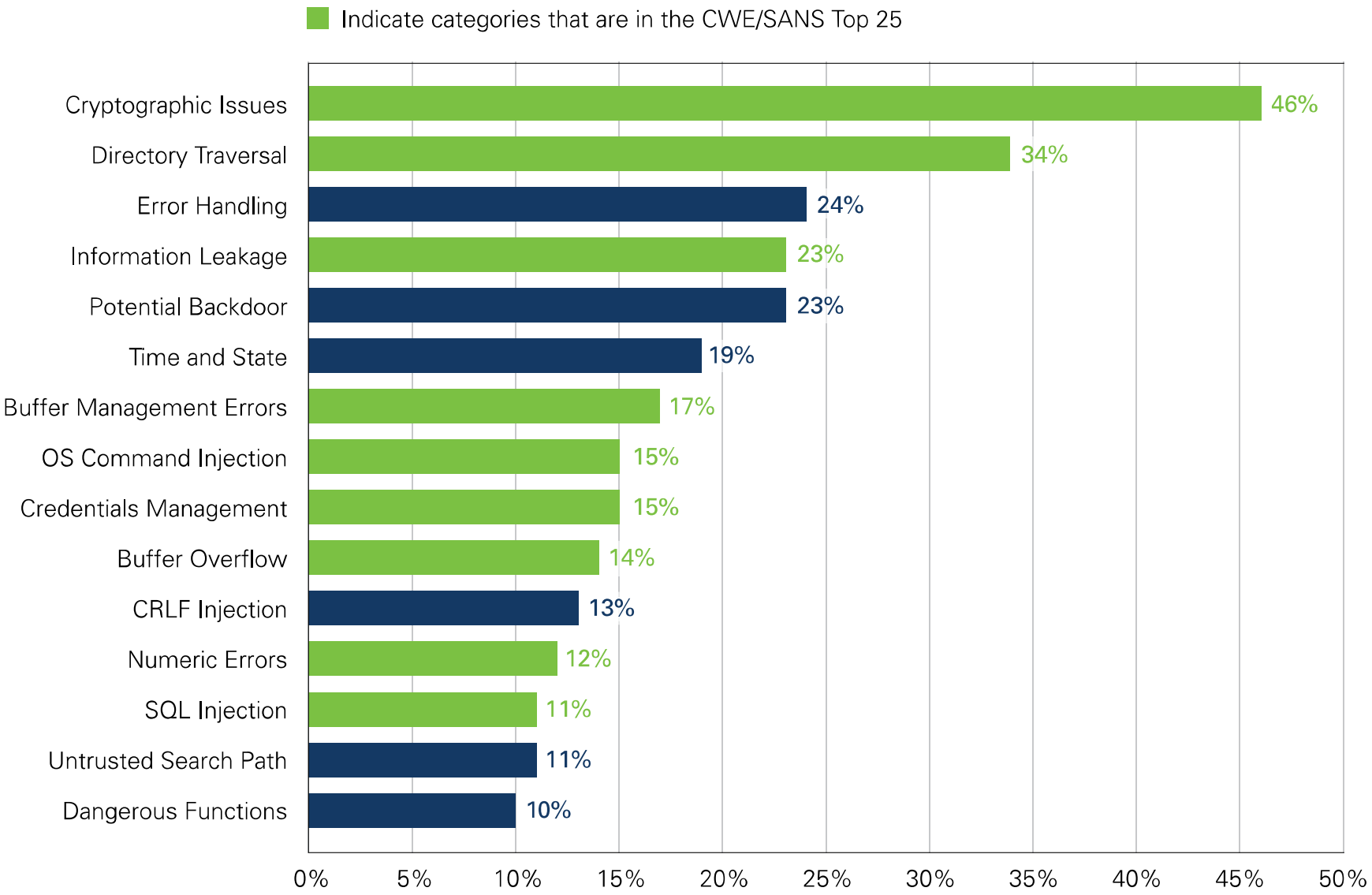
Top Vulnerability Categories

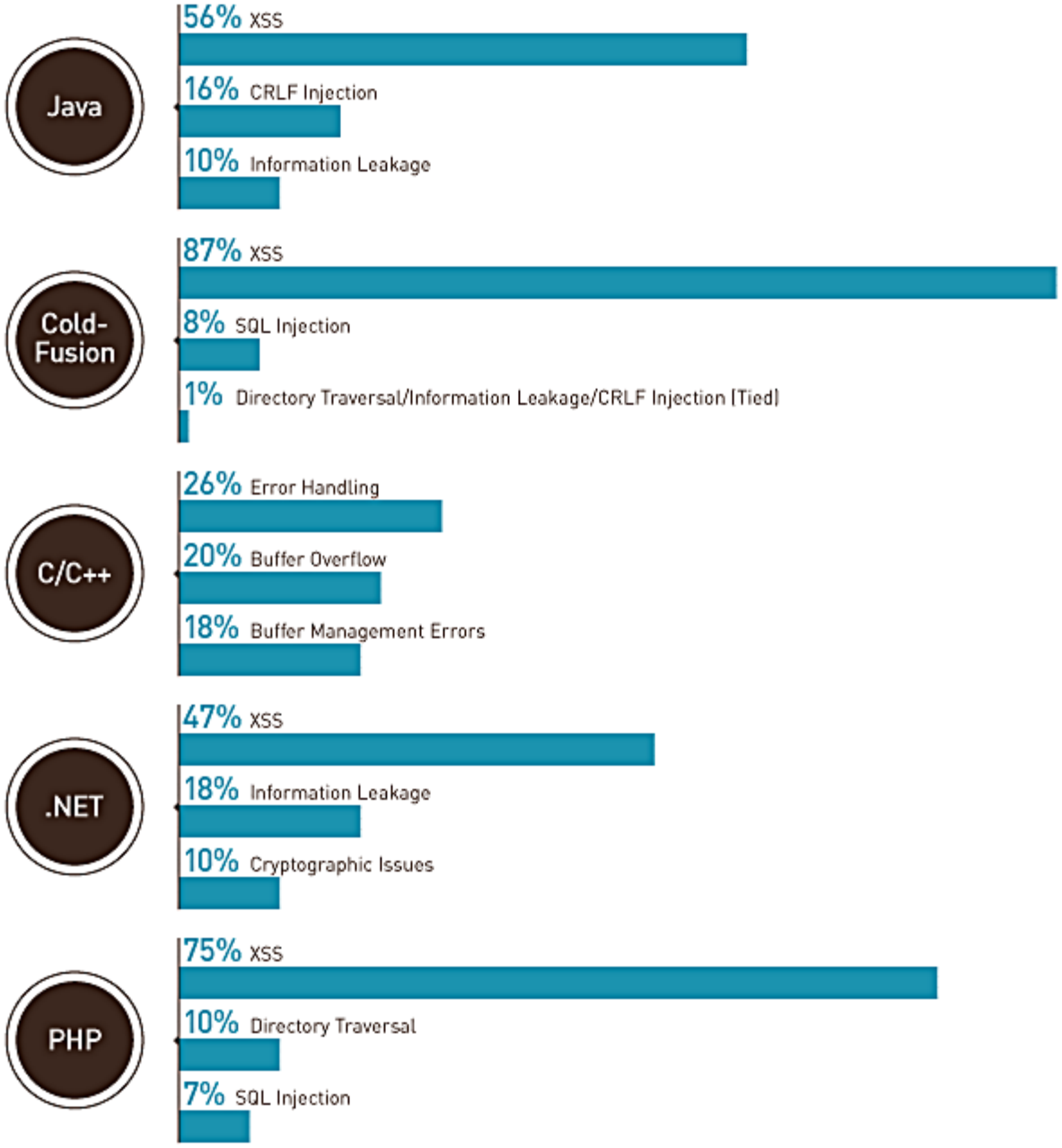
(Percent of Applications Affected for Web Applications)



Top Vulnerability Categories

(Percentage of Applications Affected for Non-Web Applications)

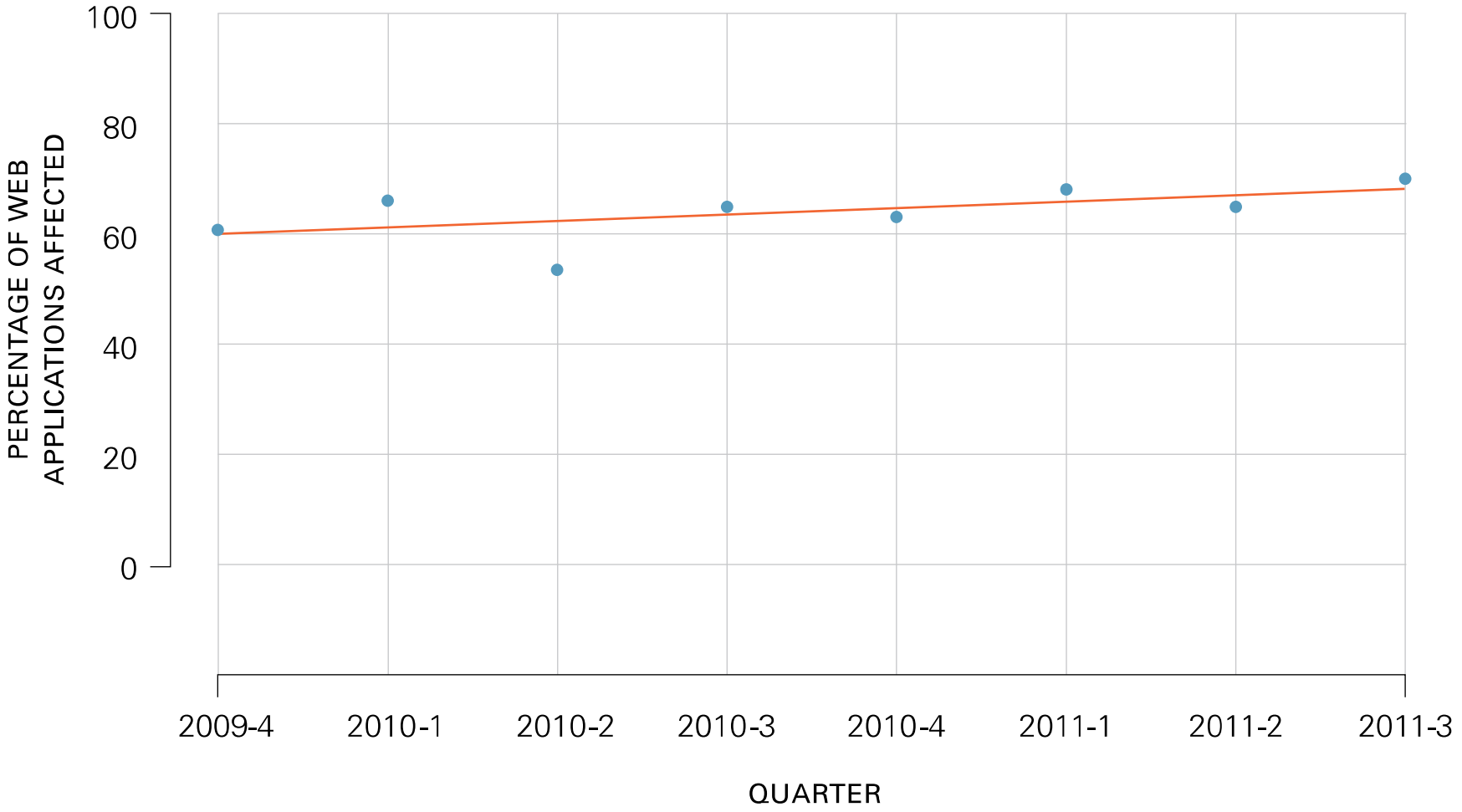



Java
56% XSS
16% CRLF Injection
10% Information Leakage
Cold-Fusion
87% XSS
8% SQL Injection
1% Directory Traversal/Information Leakage/CRLF Injection (Tied)
C/C++
26% Error Handling
20% Buffer Overflow
18% Buffer Management Errors
.NET
47% XSS
18% Information Leakage
10% Cryptographic Issues
PHP
75% XSS
10% Directory Traversal
7% SQL Injection

ARE WE MAKING ANY PROGRESS AT ERADICATING CROSS-SITE SCRIPTING OR SQL INJECTION?

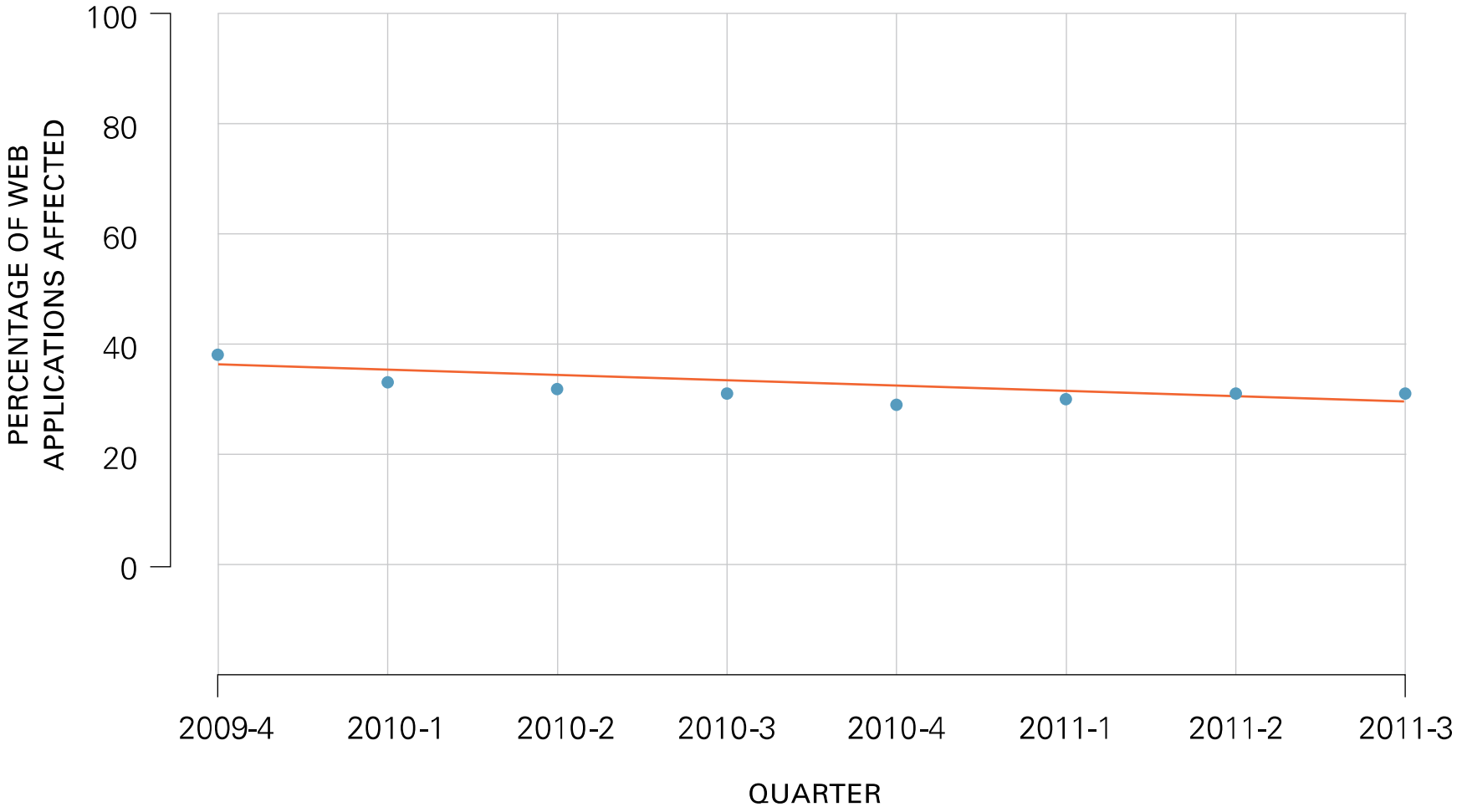
Quarterly Trend for XSS

pvalue = 0.124: Statistically, the trend is flat.



Quarterly Trend for SQL Injection

pvalue = 0.048: Statistically, the trend is down.



WHAT PERCENTAGE OF WEB APPLICATIONS FAIL THE OWASP TOP TEN?

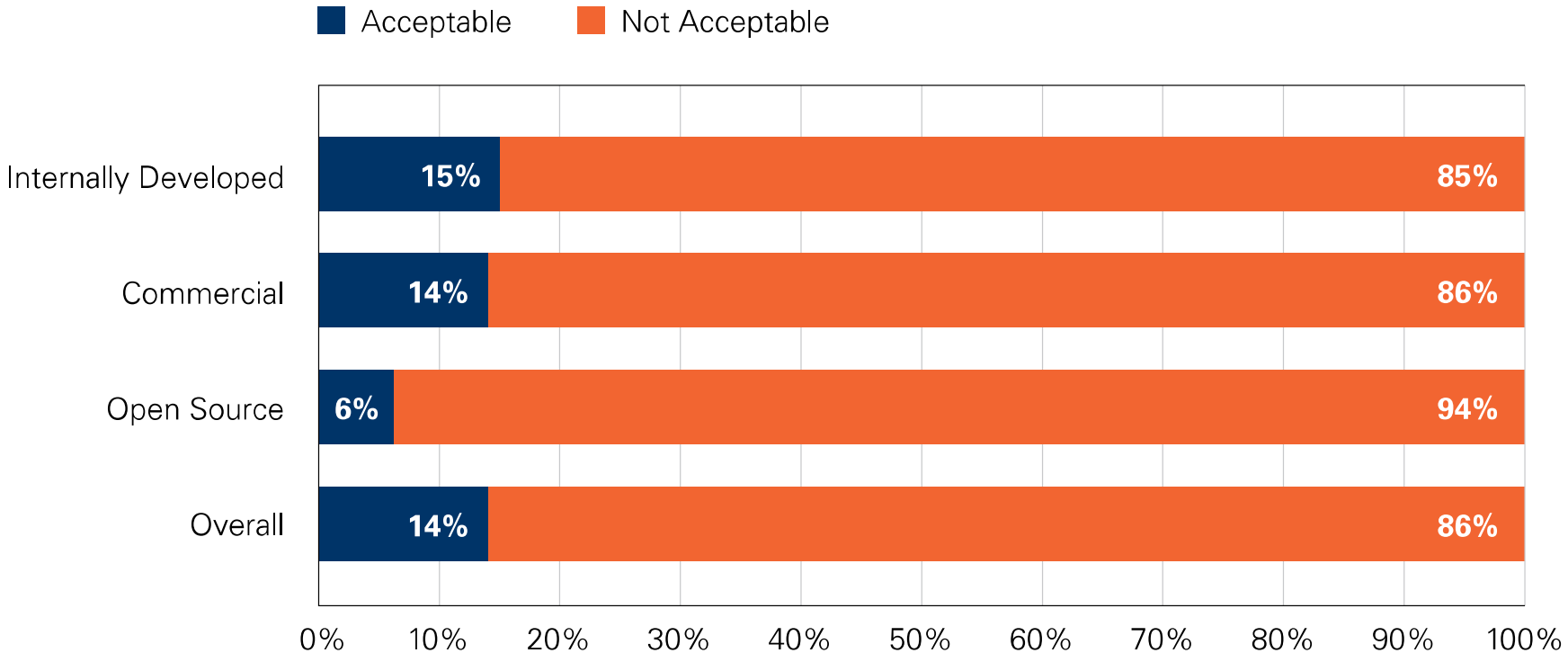
a) 34%

b) 57%

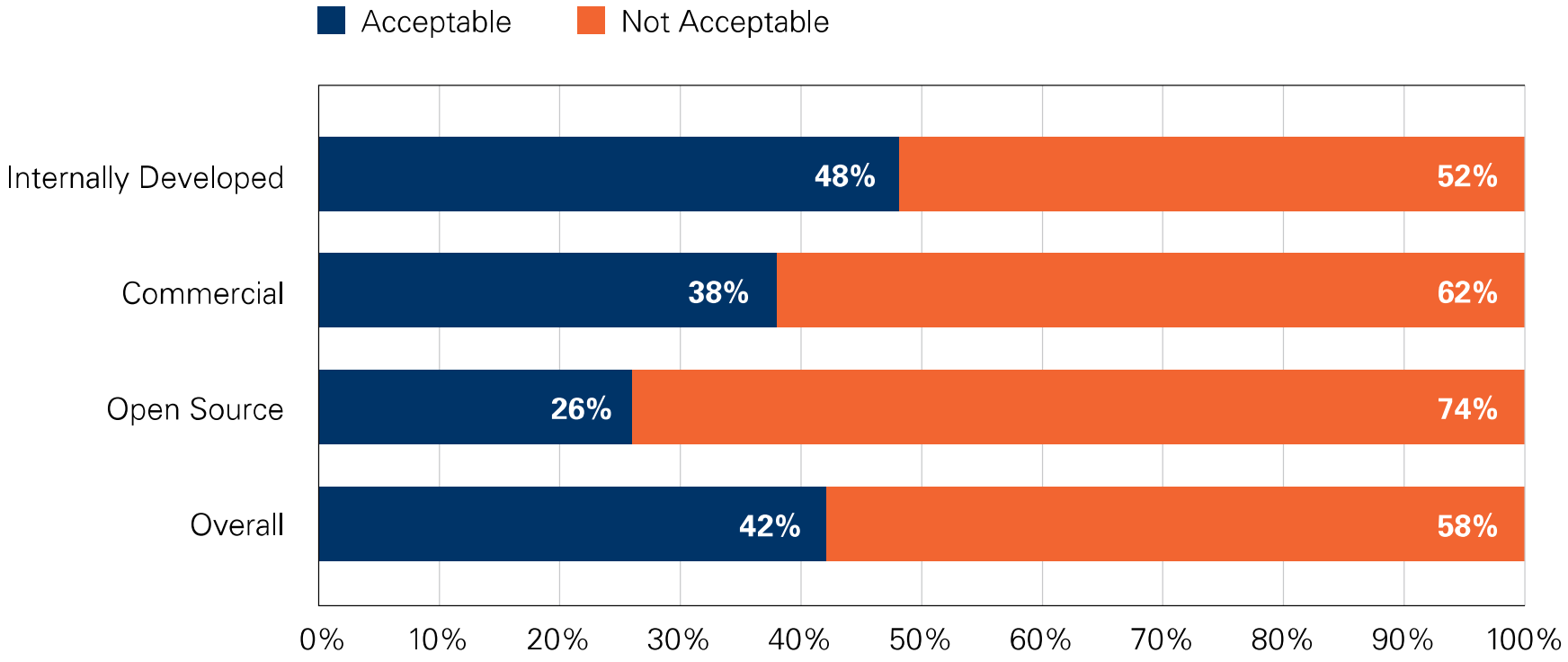
c) 86%

d) 99%

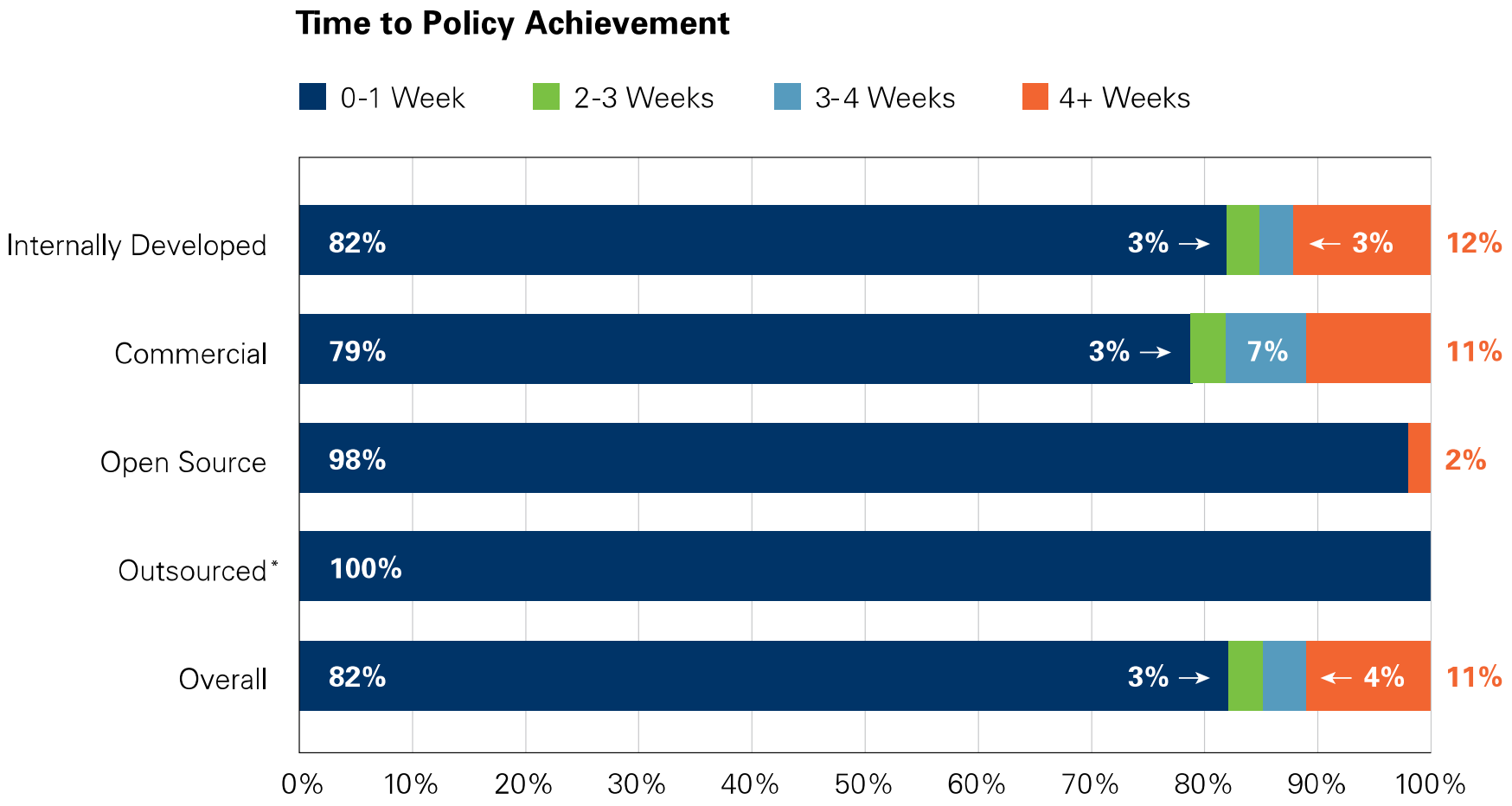
OWASP Top 10 Compliance by Supplier on First Submission
(Web Applications)



CWE/SANS Top 25 Compliance by Supplier on First Submission
(Non-Web Applications)

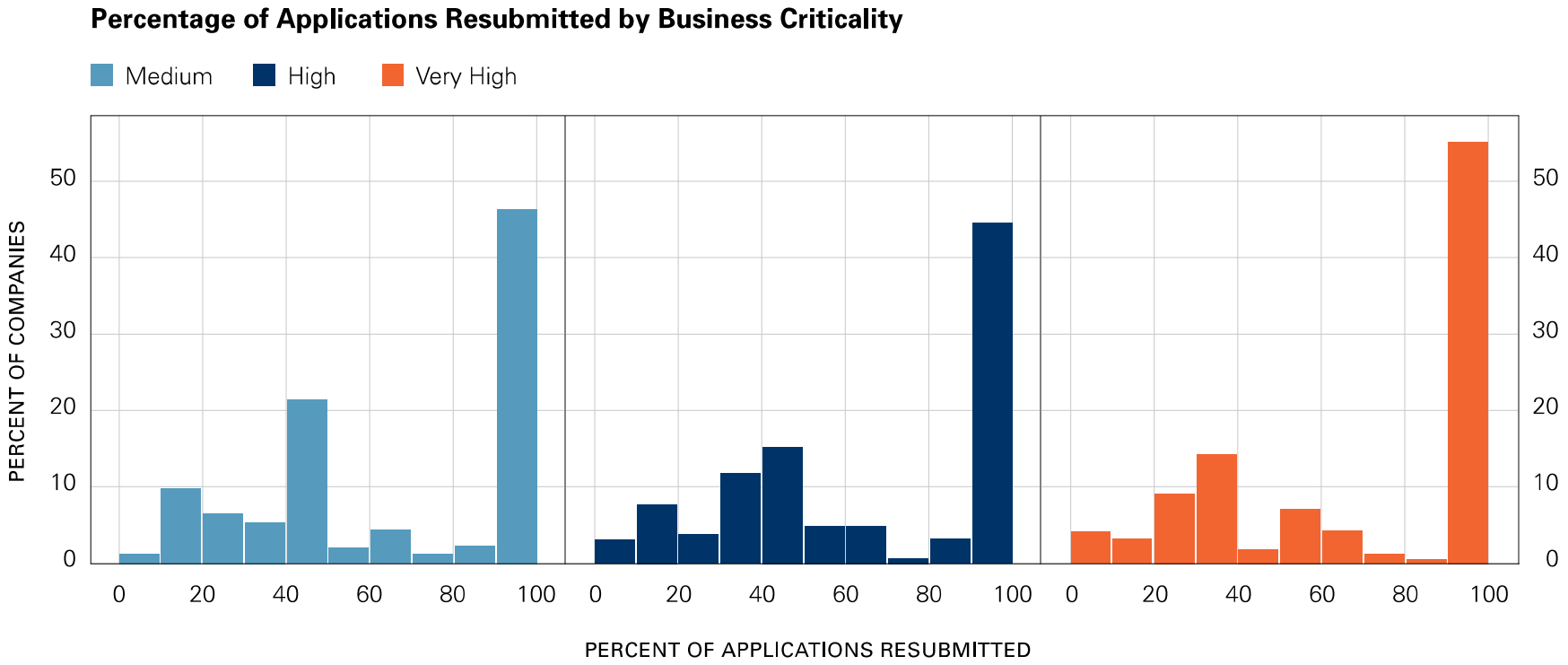


HOW LONG DOES IT TAKE APPLICATIONS TO ACHIEVE AN ACCEPTABLE RATING?



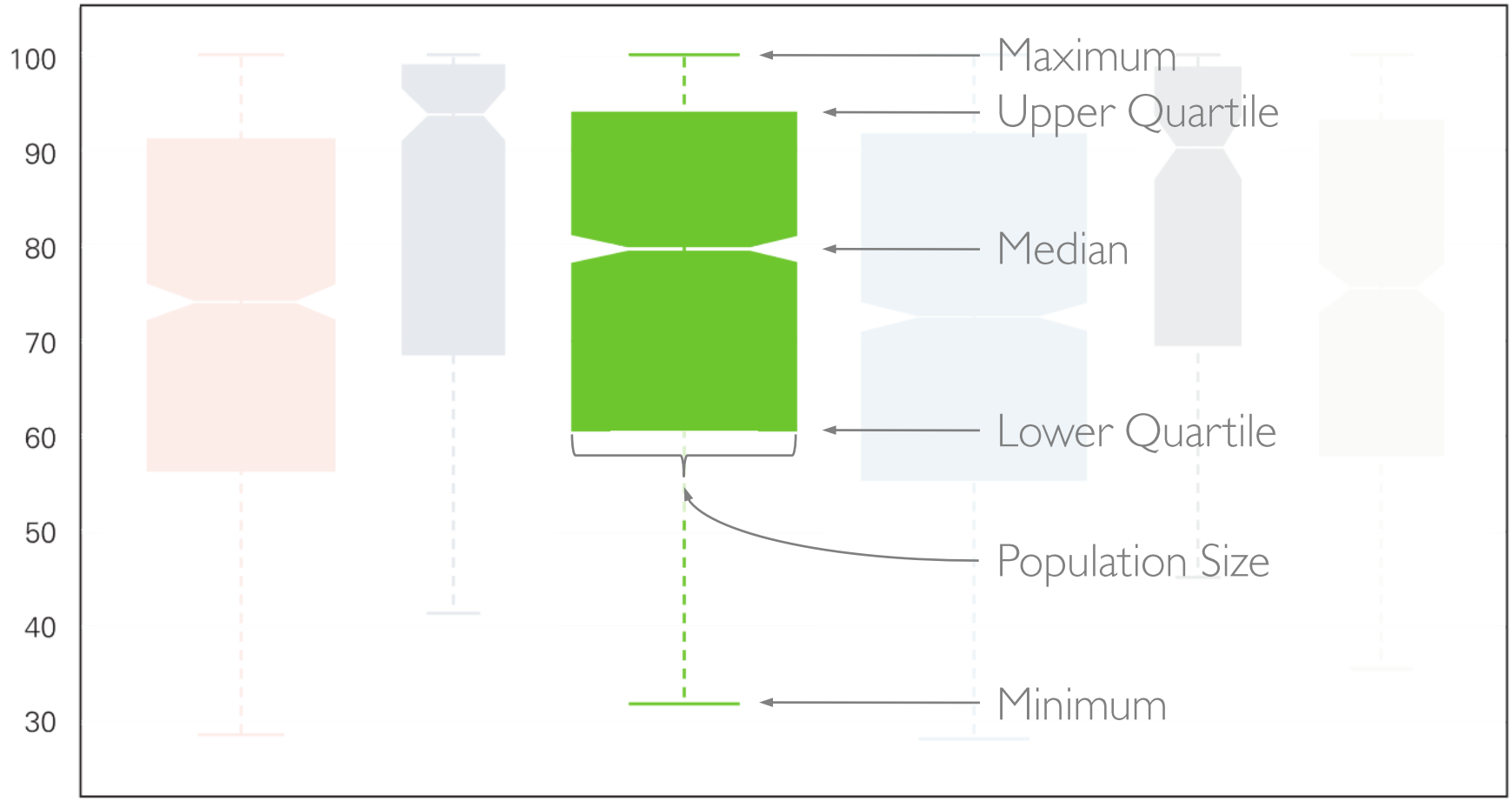
Development agility and application security are not mutually exclusive! (or are they…)

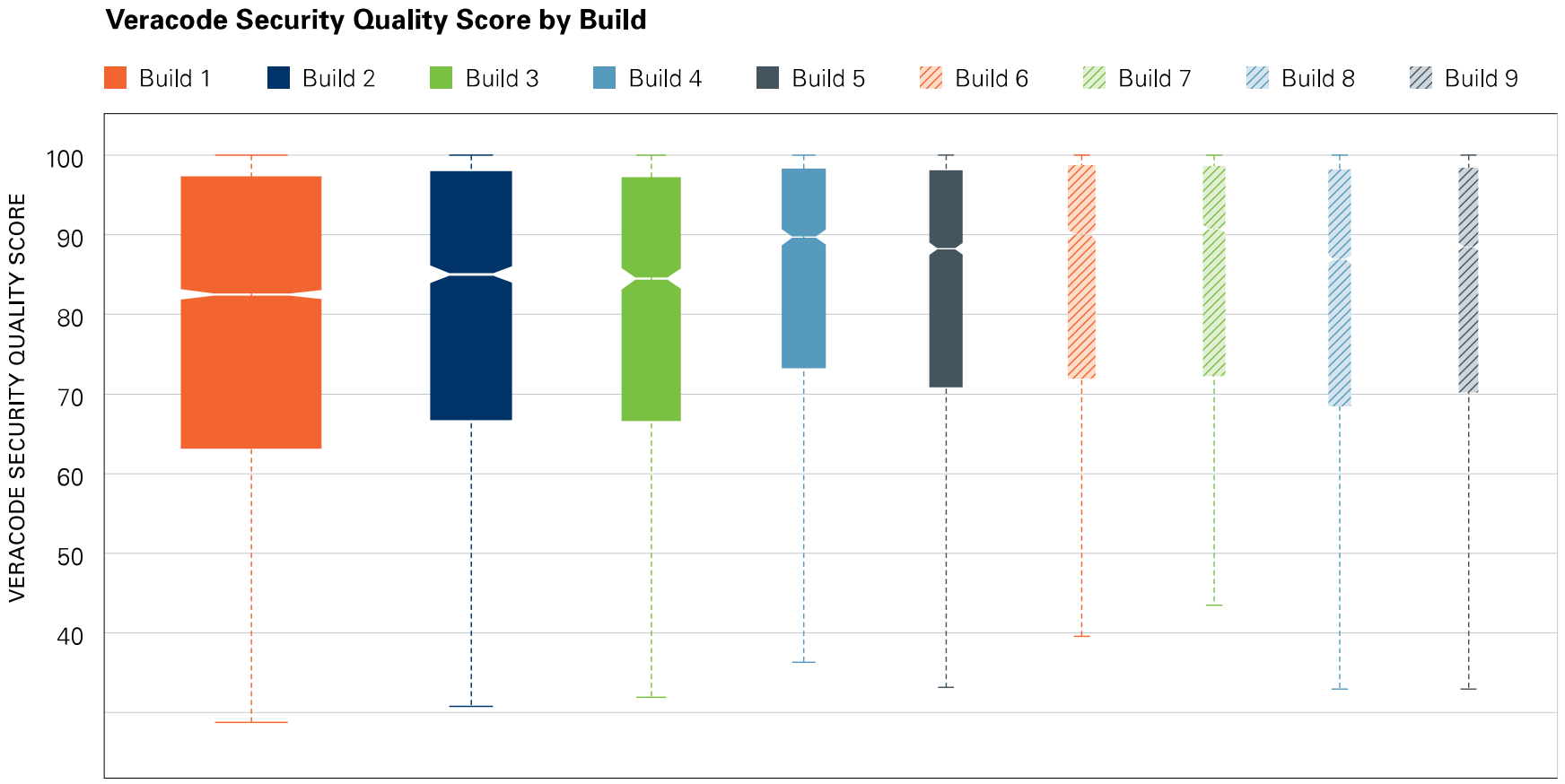
GREAT, BUT WHAT ABOUT ALL THE OTHER APPS?



Only about half of companies resubmit more than 90% of their *most critical* applications!

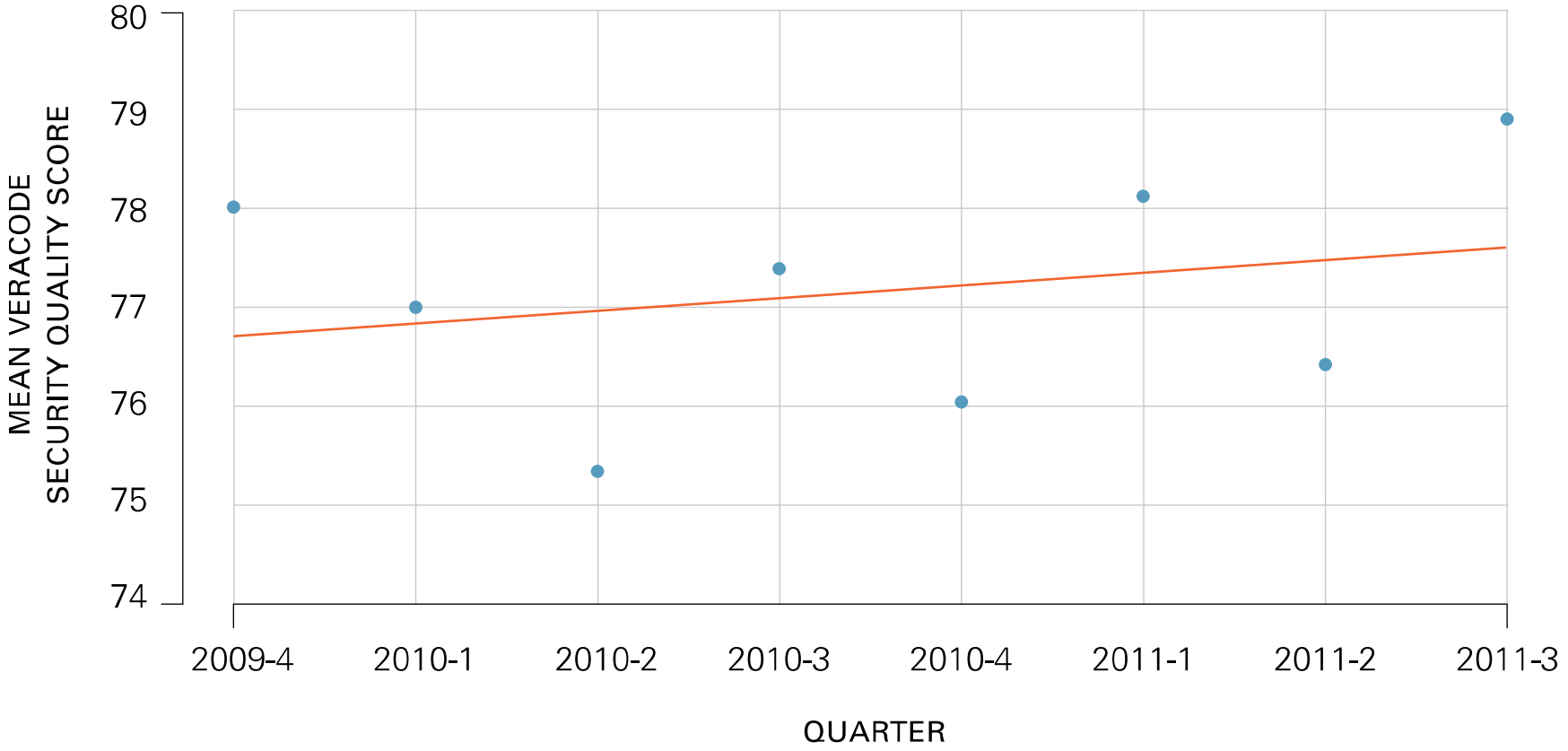
Refresher: Whisker Plots




Veracode Security Quality Score by Build
Build 1
Build 2
Build 3
Build 4
Build 5
Build 6
Build 7
Build 8
Build 9
VERACODE SECURITY QUALITY SCORE
100
90
80
70
60
50
40

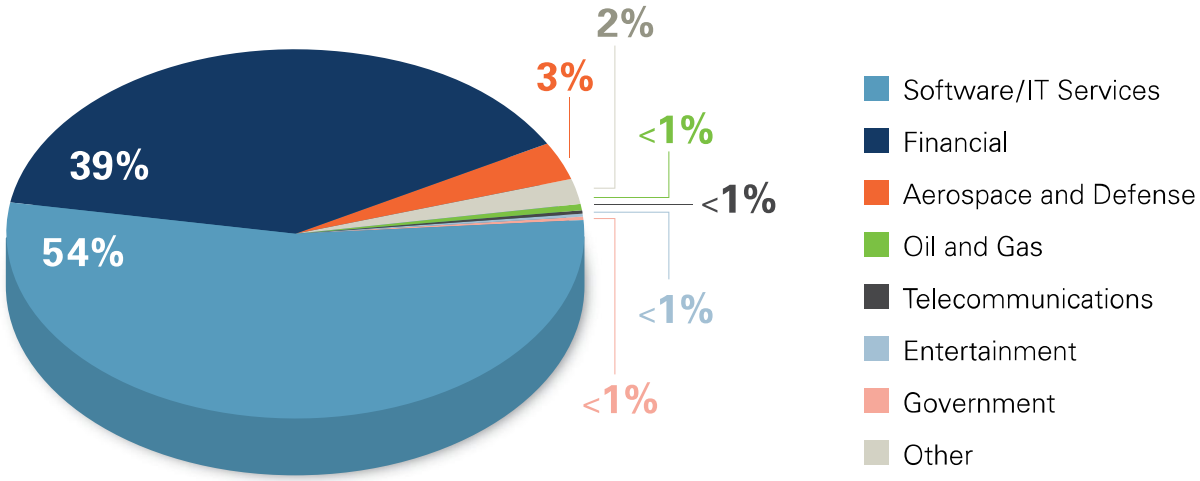
Veracode Security Quality Score Trend by Quarter

pvalue = 0.543: Statistically, the trend is flat.



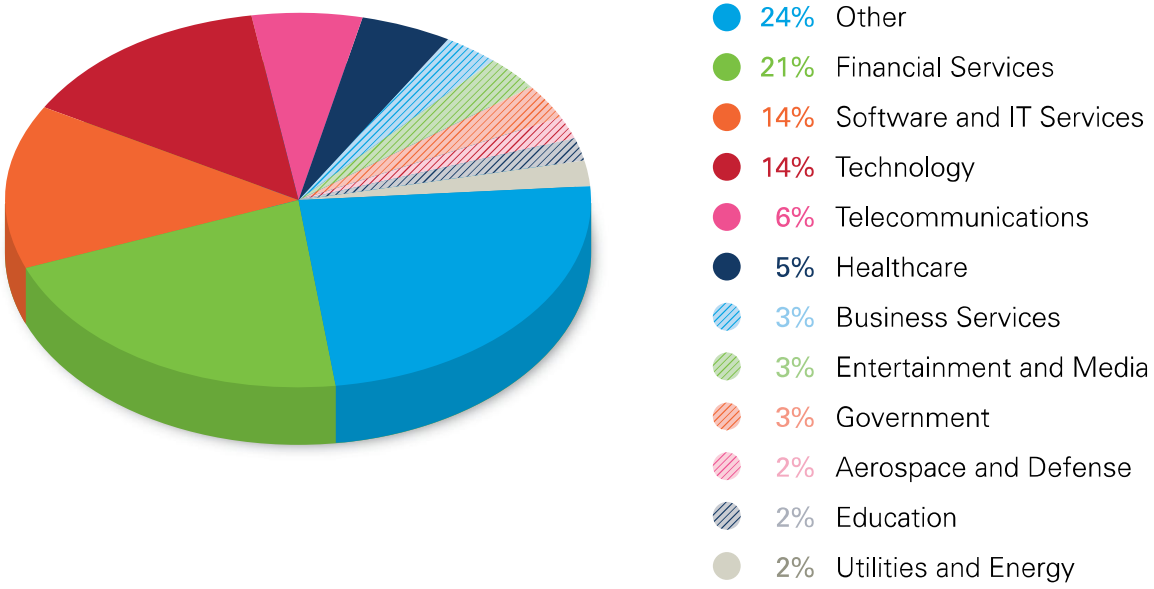
WHAT HAPPENS WHEN SOFTWARE VENDORS ARE HELD ACCOUNTABLE?

Requestor Type by Industry

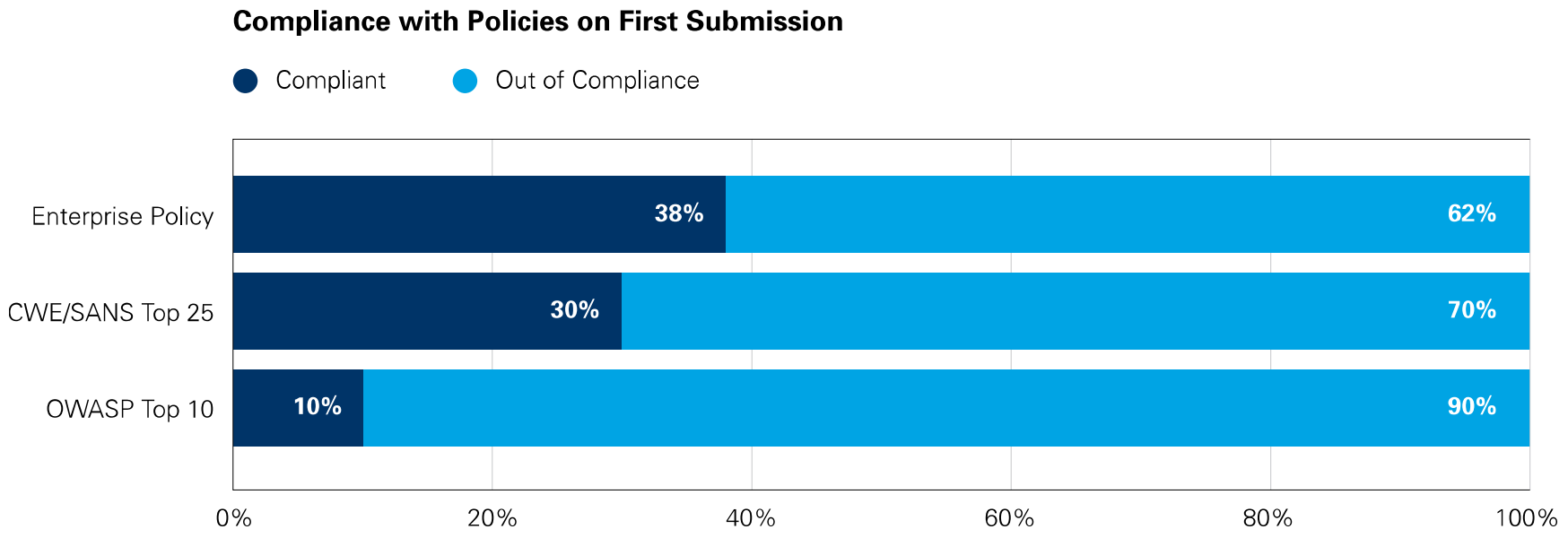


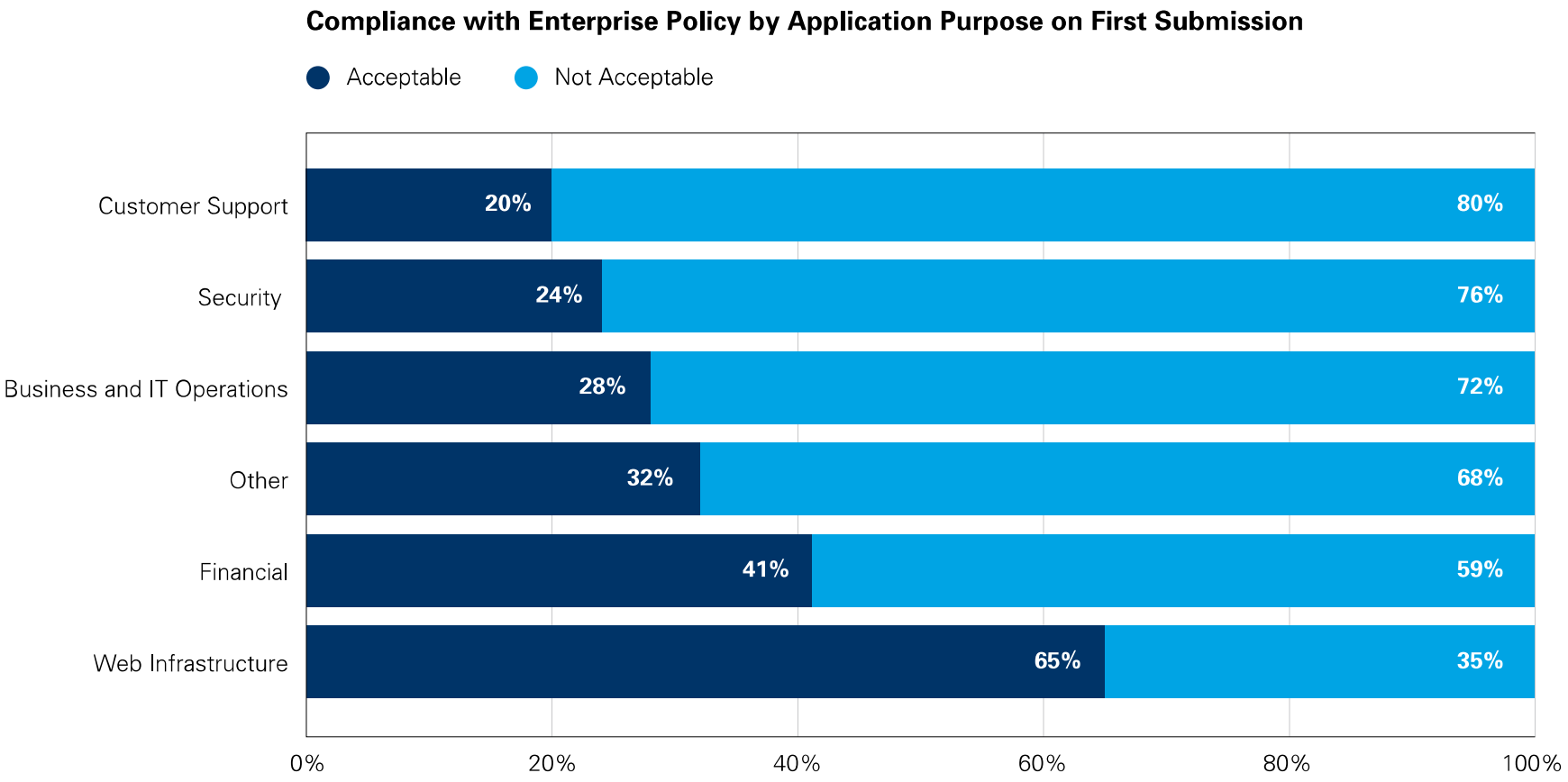
March 2010 – July 2011

Distribution of Enterprises Requesting Assessments by Industry



January 2011 – June 2012


Compliance with Policies on First Submission
Compliant
Out of Compliance
Enterprise Policy
38%
62%
CWE/SANS Top 25
30%
70%
OWASP Top 10
10%
90%
0%
20%
40%
60%
80%
100%

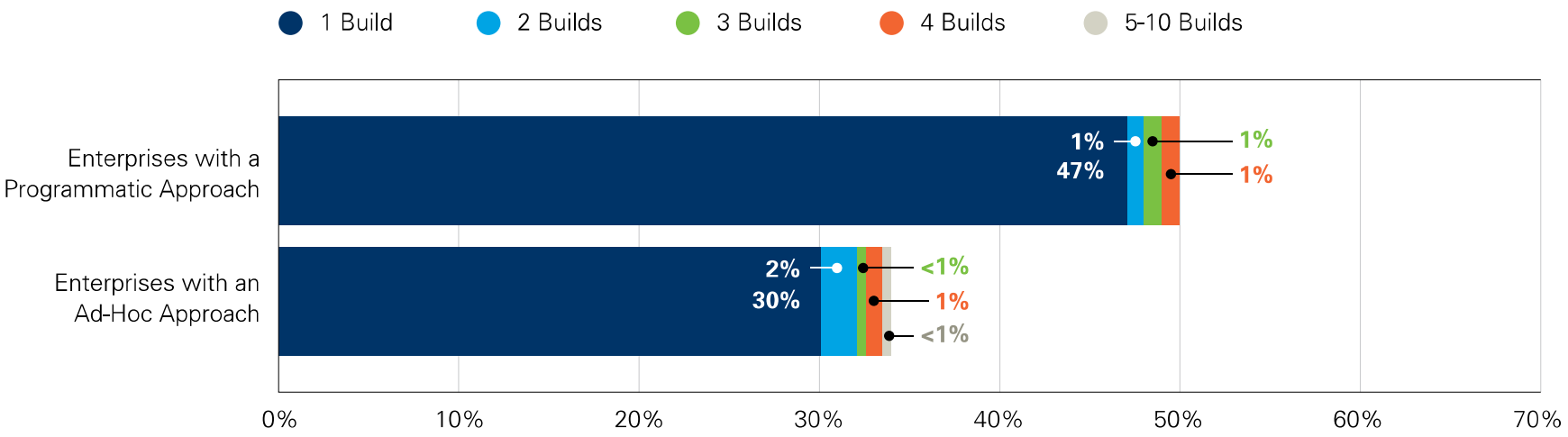

Compliance with Enterprise Policy by Application Purpose on First Submission
Acceptable
Not Acceptable
Customer Support
20%
80%
Security
24%
76%
Business and IT Operations
28%
72%
Other
32%
68%
Financial
41%
59%
Web Infrastructure
65%
35%
0%
20%
40%
60%
80%
100%

	Vendor-Supplied Software Testing Approaches	
	Enterprises with an Ad-Hoc Approach	Enterprises with a Programmatic Approach
Average number of vendors participating	4	**38**
Average number of applications assessed	7	**71**
Percent of applications achieving compliance	34%	52%
Percent of applications achieving compliance within one week	28%	45%
Percent of non-compliant applications that are out of compliance for more than six months	39%	**20%**

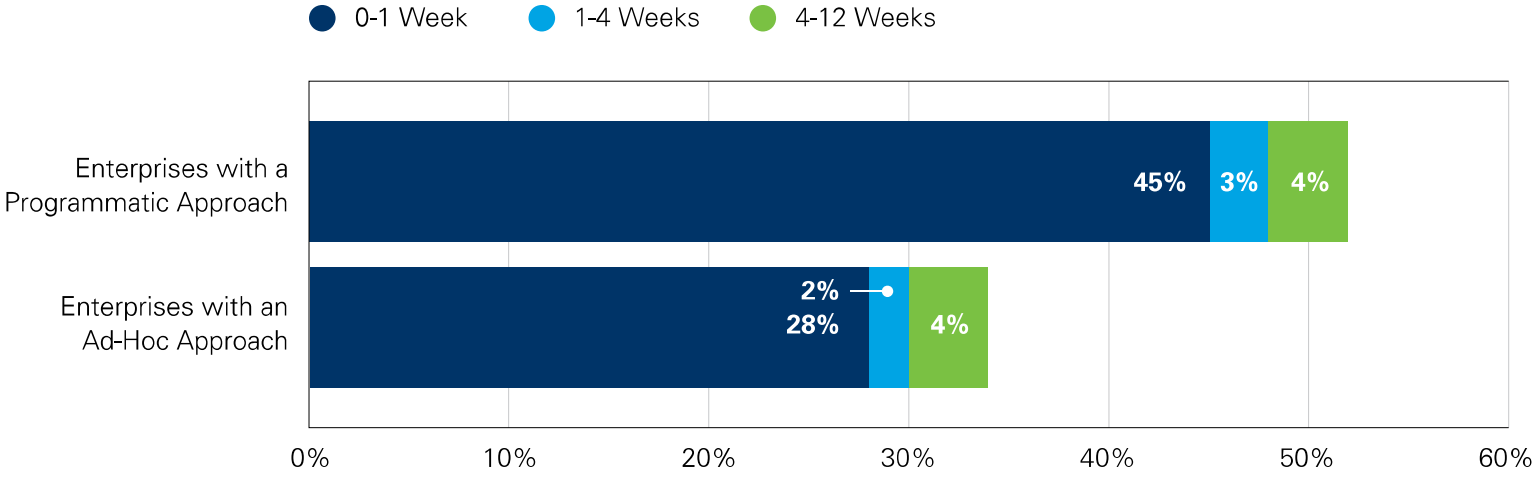
approximately **10 TIMES** MORE

LOWER IS BETTER

Number of Builds Submitted to Achieve Policy Compliance

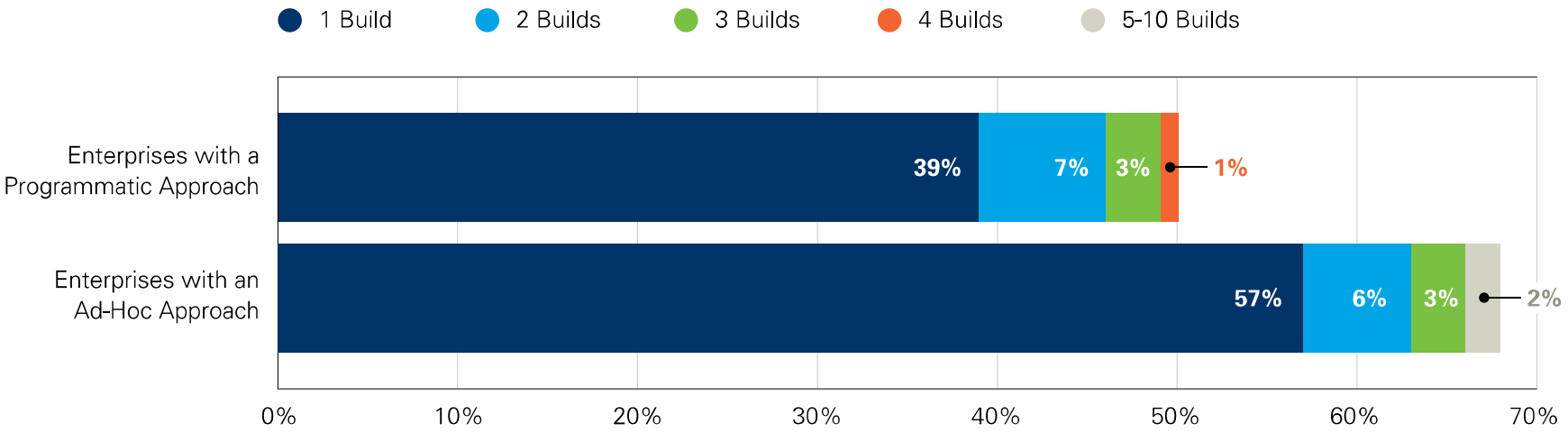


Time Taken to Achieve Policy Compliance*

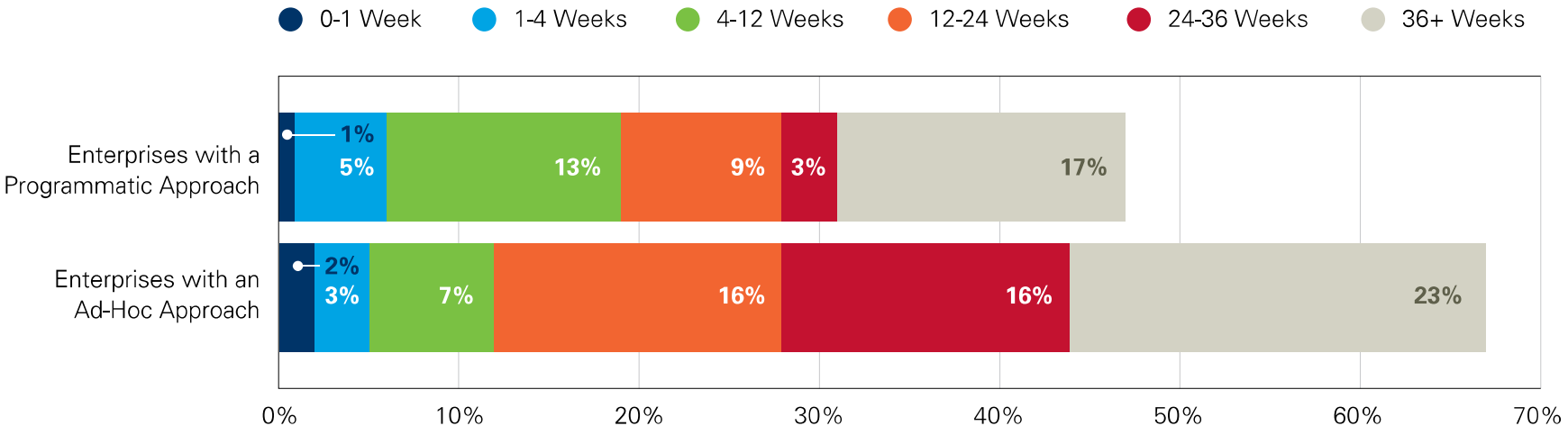


** Slight differences between the total percentages in figures are due to rounding*

Number of Builds Submitted for Non-Compliant Applications*



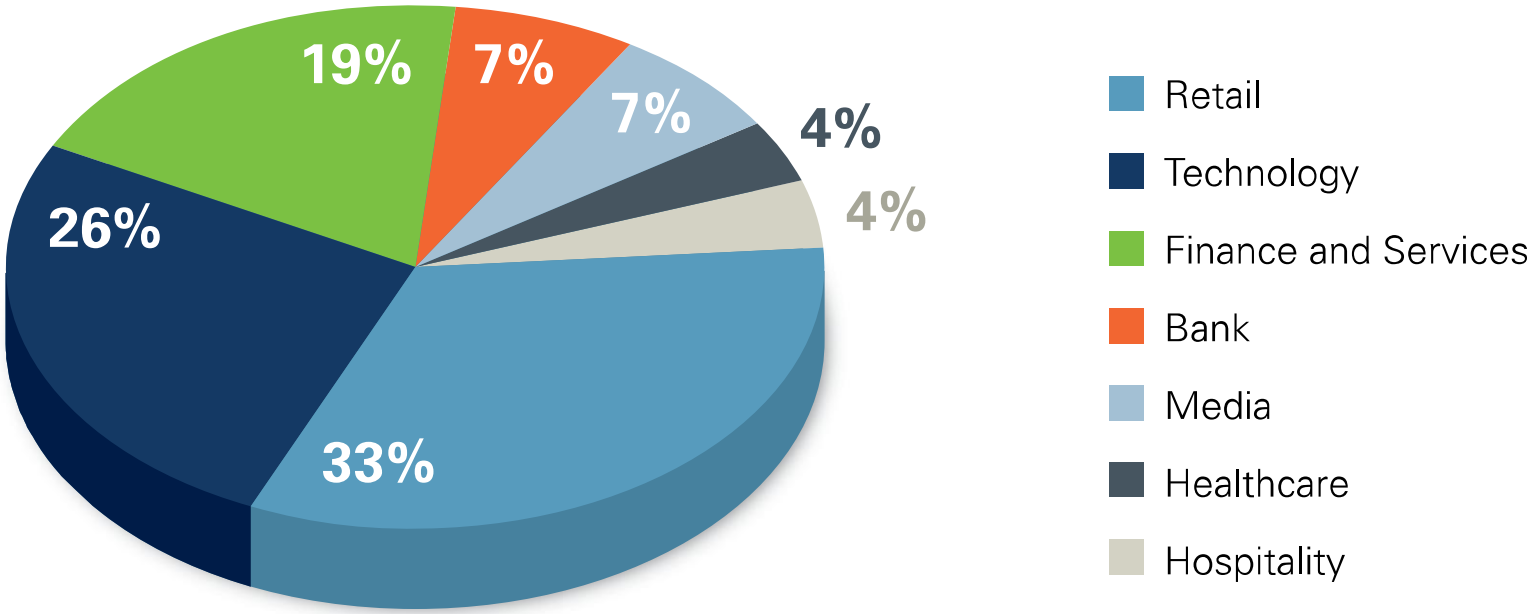
Time Spent Out of Compliance*



** Slight differences between the total percentages in figures are due to rounding*

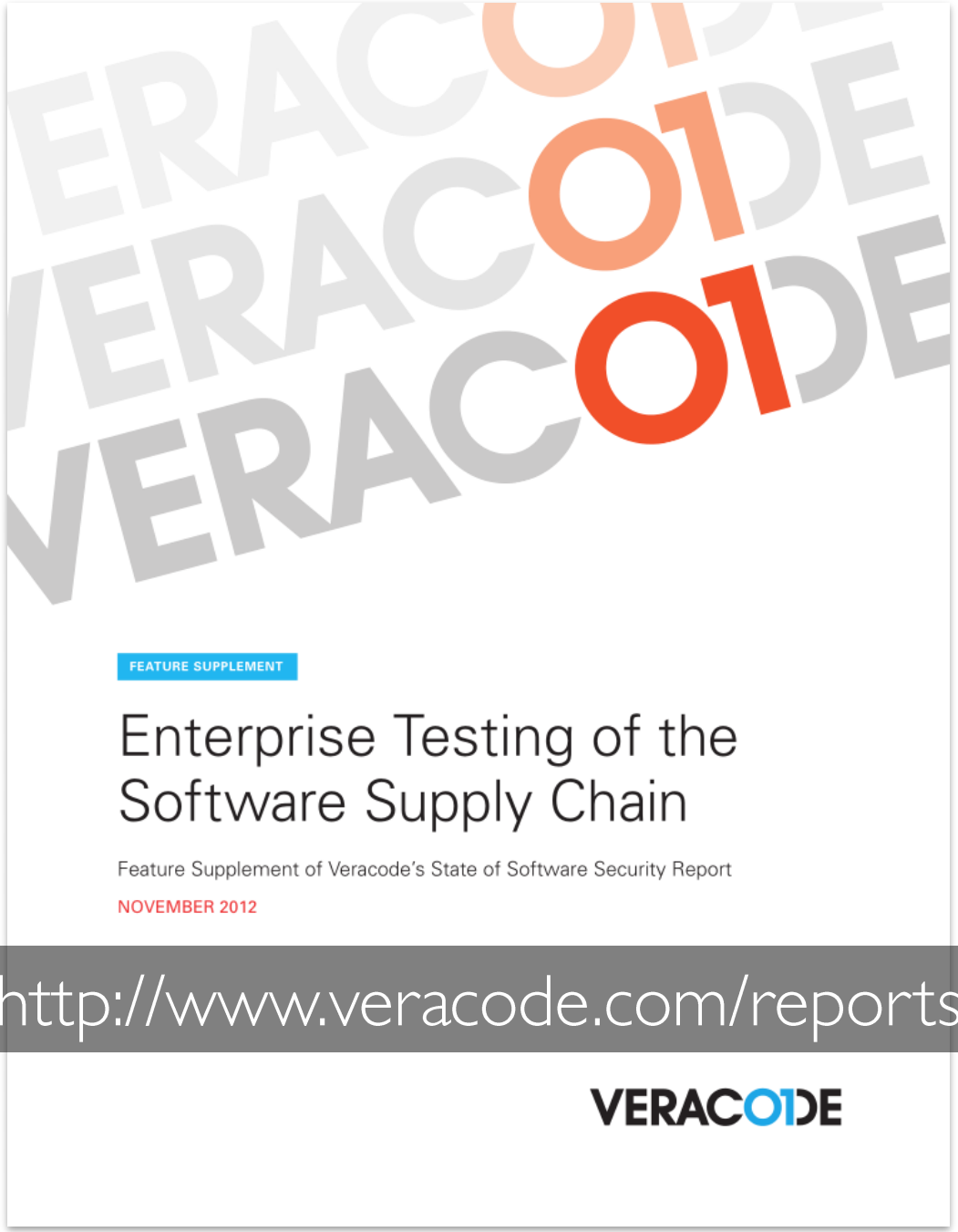
HOW ABOUT MOBILE APPS?

Android Applications by Industry Vertical



CWE Category	CWE	Percent Applications Affected
Insufficient Entropy	331	61%
Use of Hard-coded Cryptographic Key	321	42%
Information Exposure Through Sent Data	201	39%
Information Exposure Through Error Message	209	6%

http://www.veracode.com/reports



http://www.veracode.com/reports

QUESTIONS?

Speaker

Joe Brady

jbrady@veracode.com

Veracode Colleagues

Andre Gaeta

agaeta@veracode.com

Dave Gerry

dgerry@veracode.com