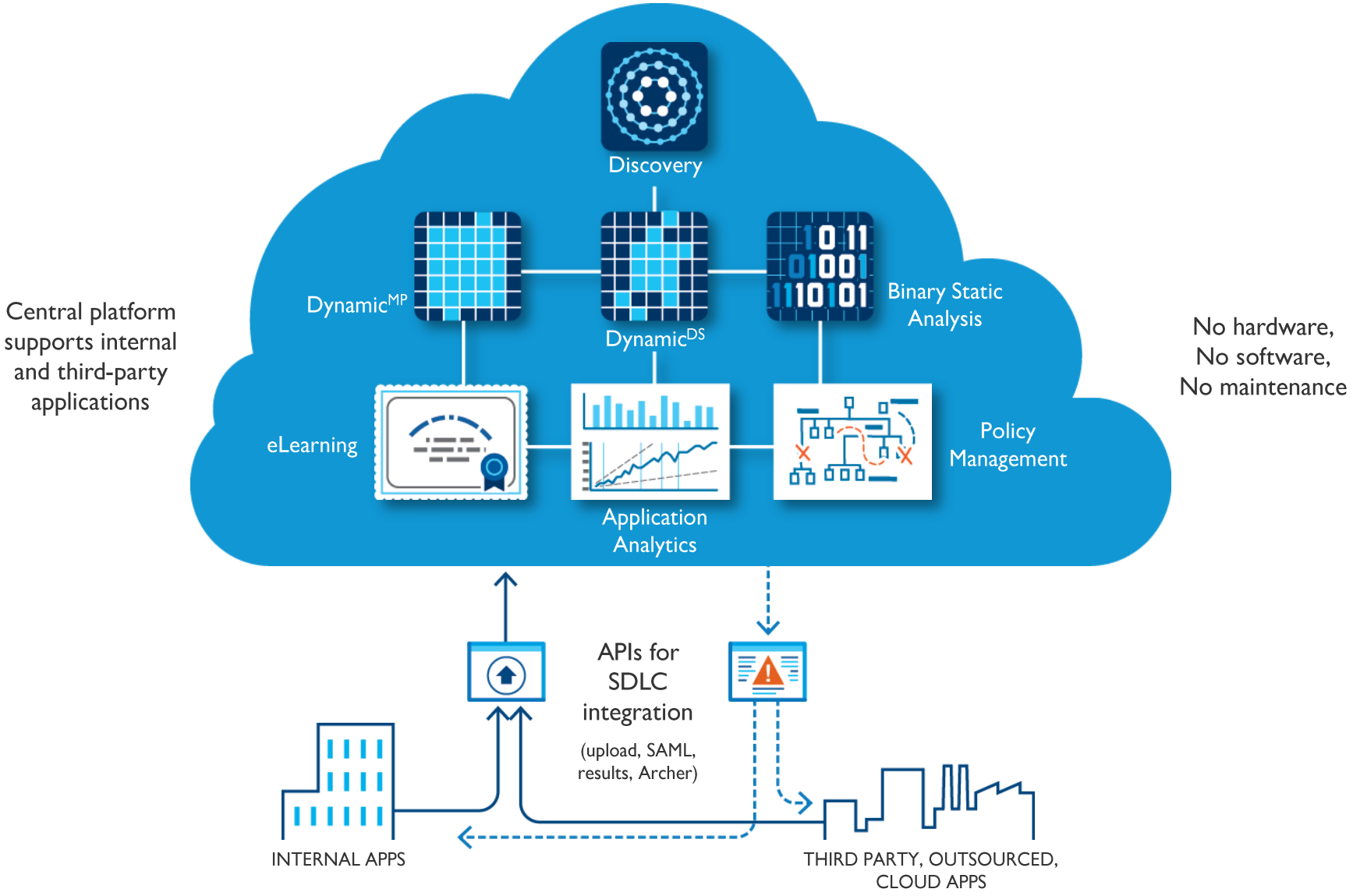
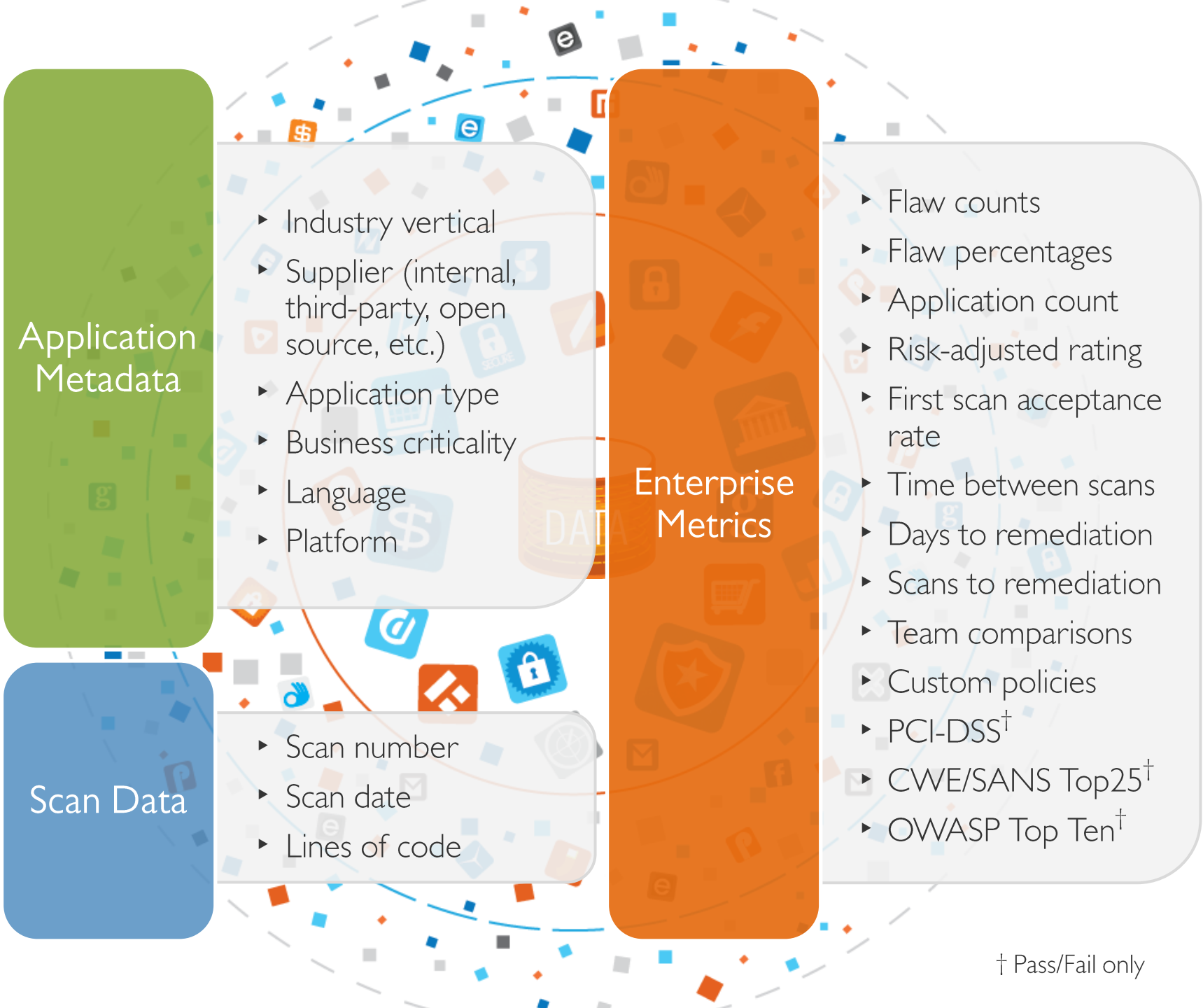
Data Mining a Mountain of Zero Day Vulnerabilities

Chris Eng
VP Research, Veracode
July 13, 2012

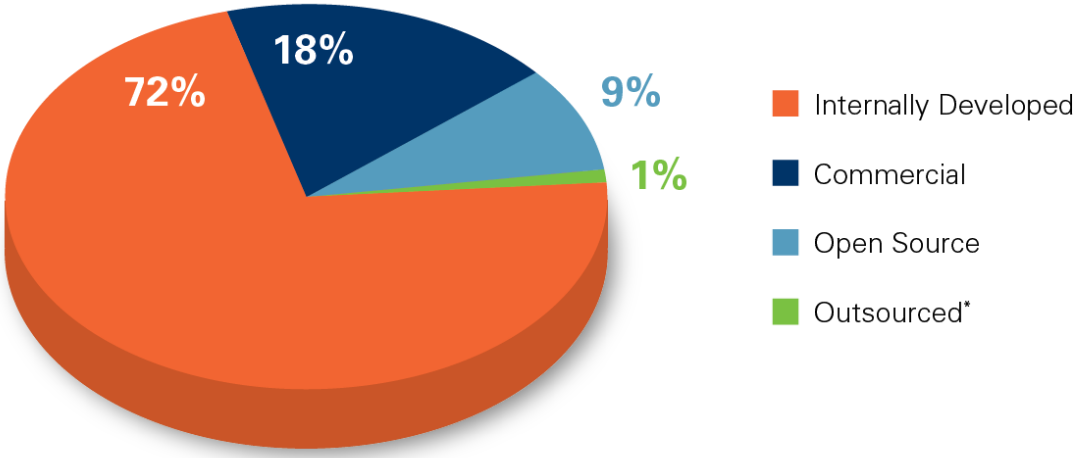

Central platform supports internal and third-party applications
Discovery
Dynamic^MP
Dynamic^DS
Binary Static Analysis
eLearning
Application Analytics
Policy Management
No hardware, No software, No maintenance
APIs for SDLC integration
(upload, SAML, results, Archer)
INTERNAL APPS
THIRD PARTY, OUTSOURCED, CLOUD APPS
VERACODE


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

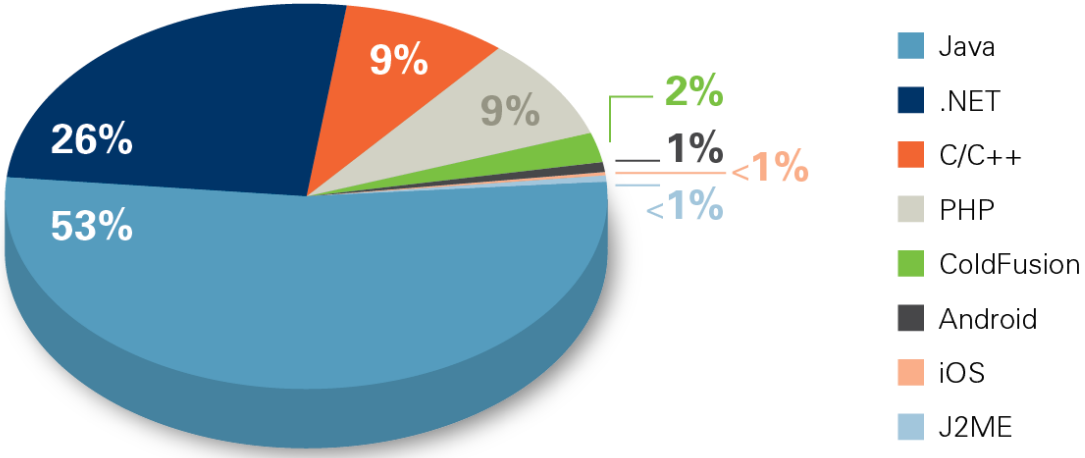
The Data Set

- Applications from over 300 commercial and US government customers
- Scanned 9,910 applications over the past 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

Applications by Supplier Type



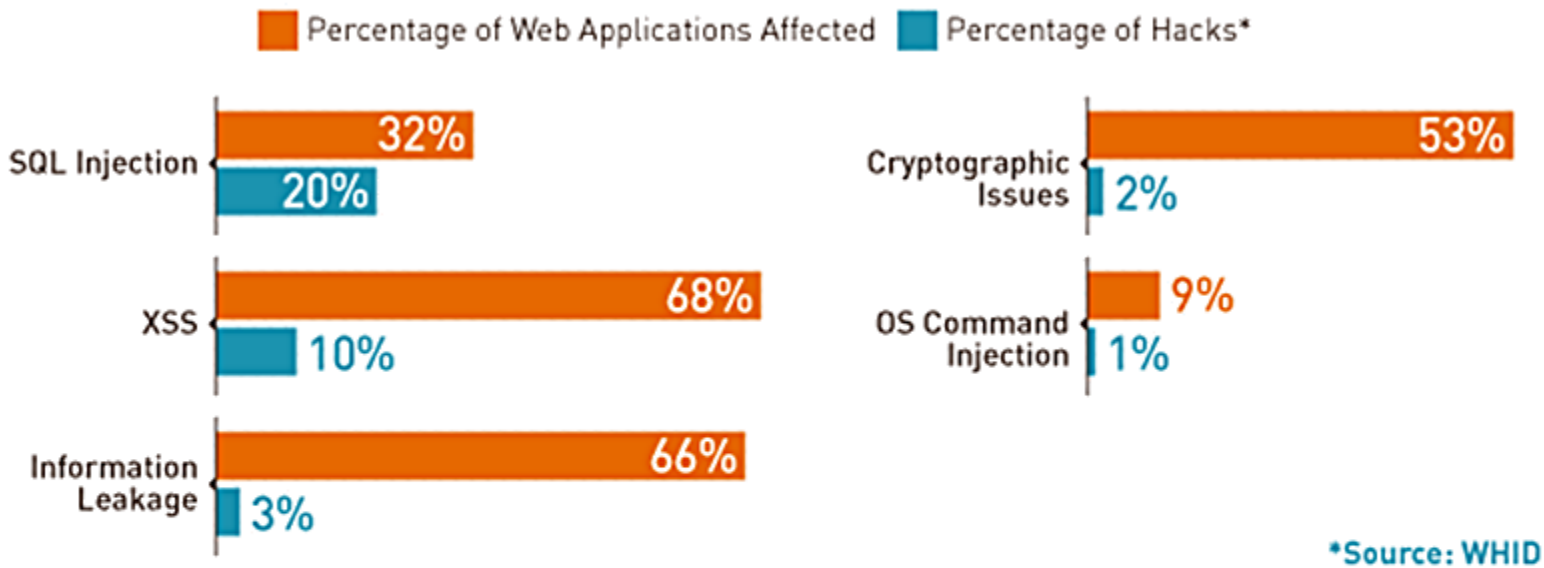
Applications by Language Family



Caveats

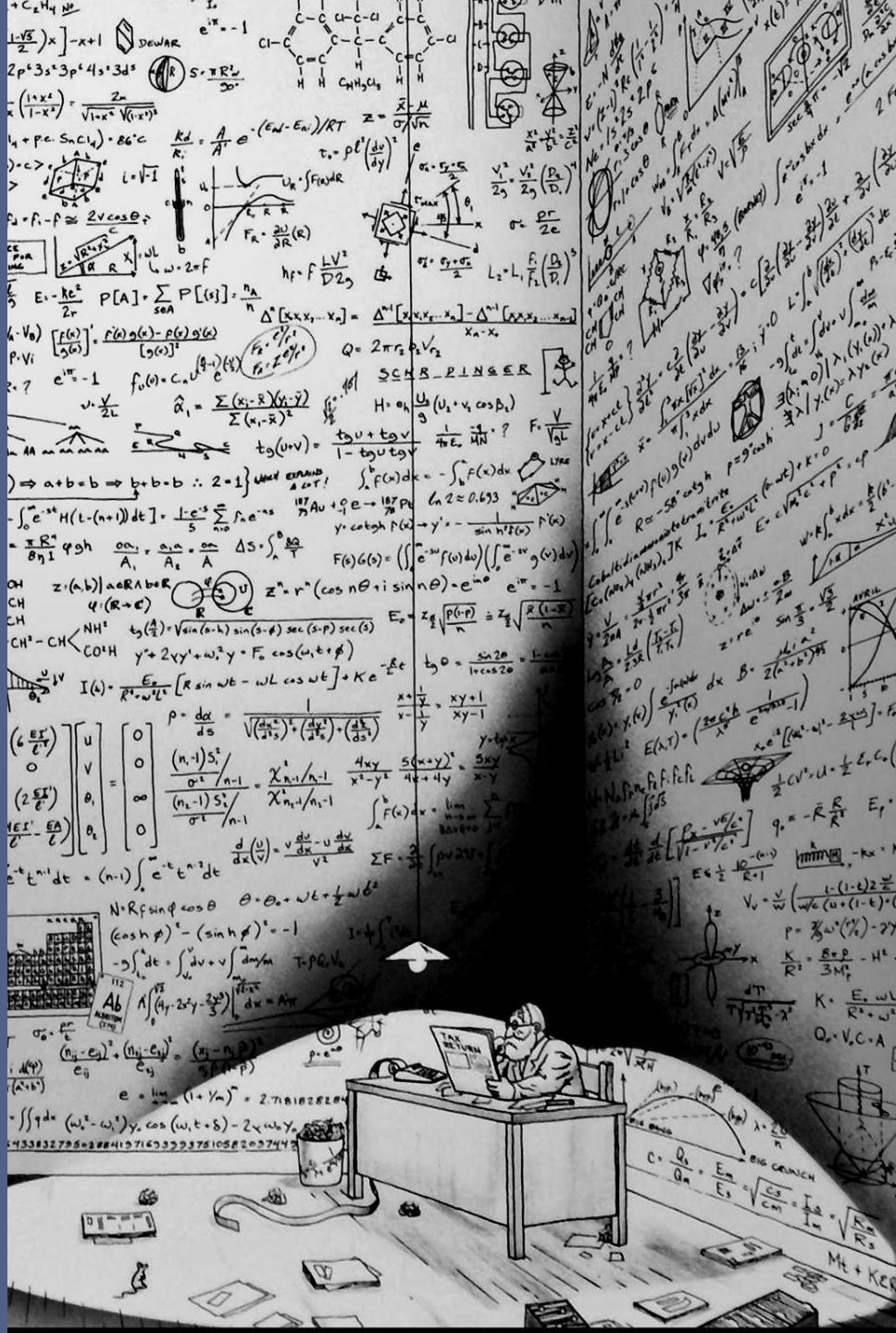
- Customer base is already security-conscious
- Bias toward business critical applications
- Applications are at inconsistent phases in the SDLC
- Not all flaws are necessarily easy to exploit
- Analysis technology is continuously being improved
- All security testing has False Negatives

THE LATENT VULNERABILITIES VS. THE ATTACKS

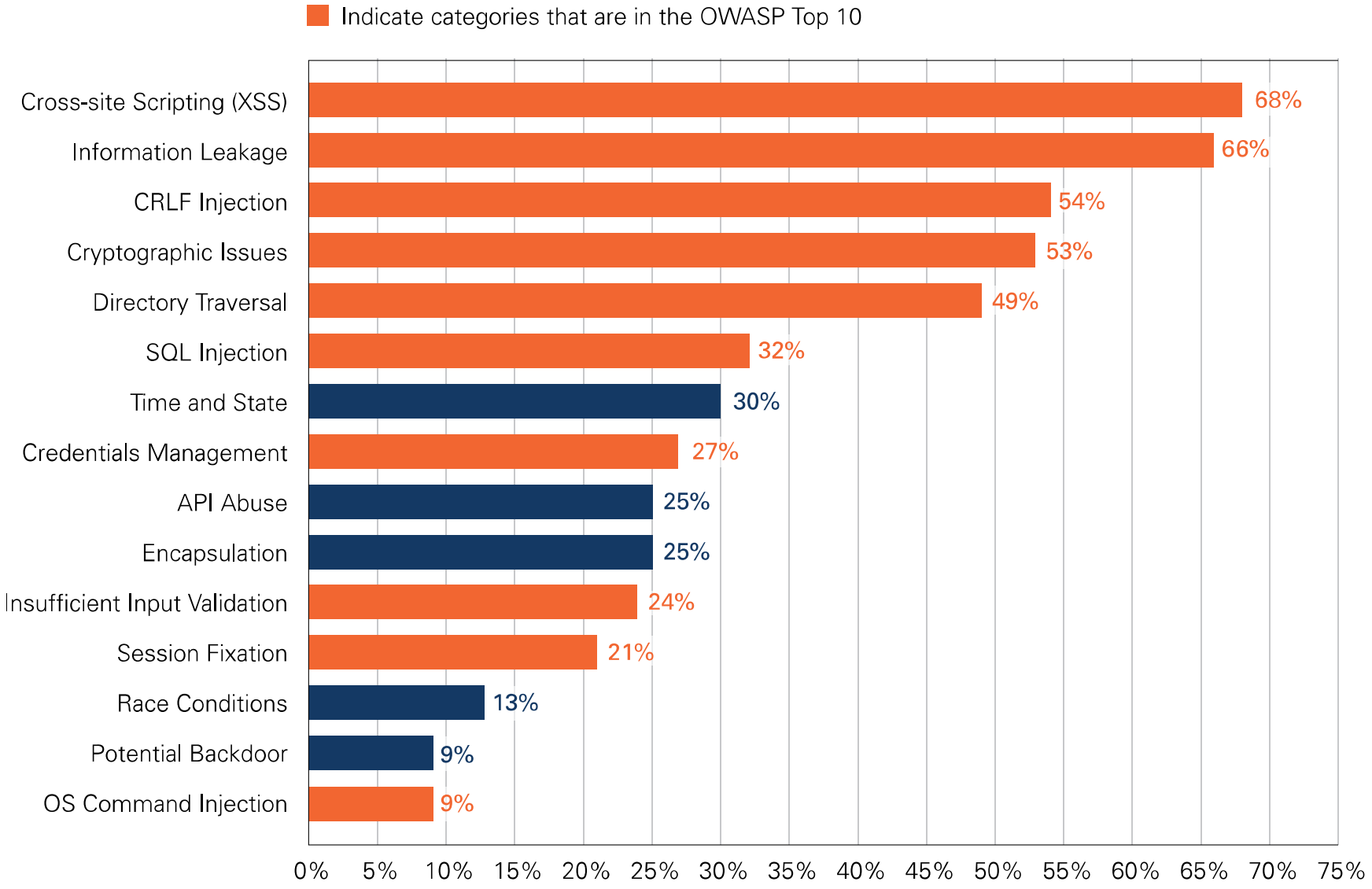


While other flaws such as XSS account for a higher volume of findings, SQL injection accounts for 20 percent of hacks.

LET'S TAKE A CLOSER LOOK AT THE NUMBERS

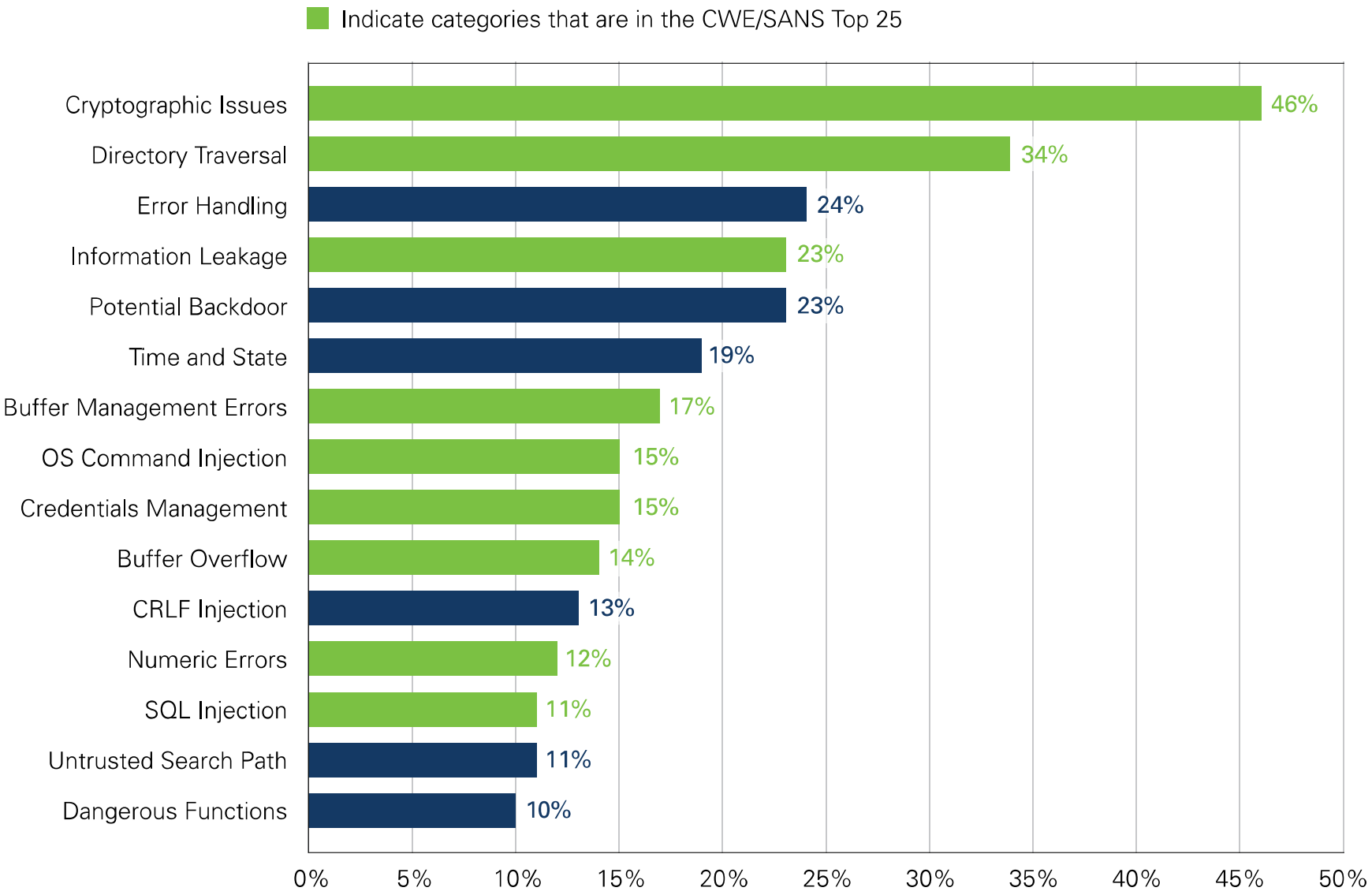


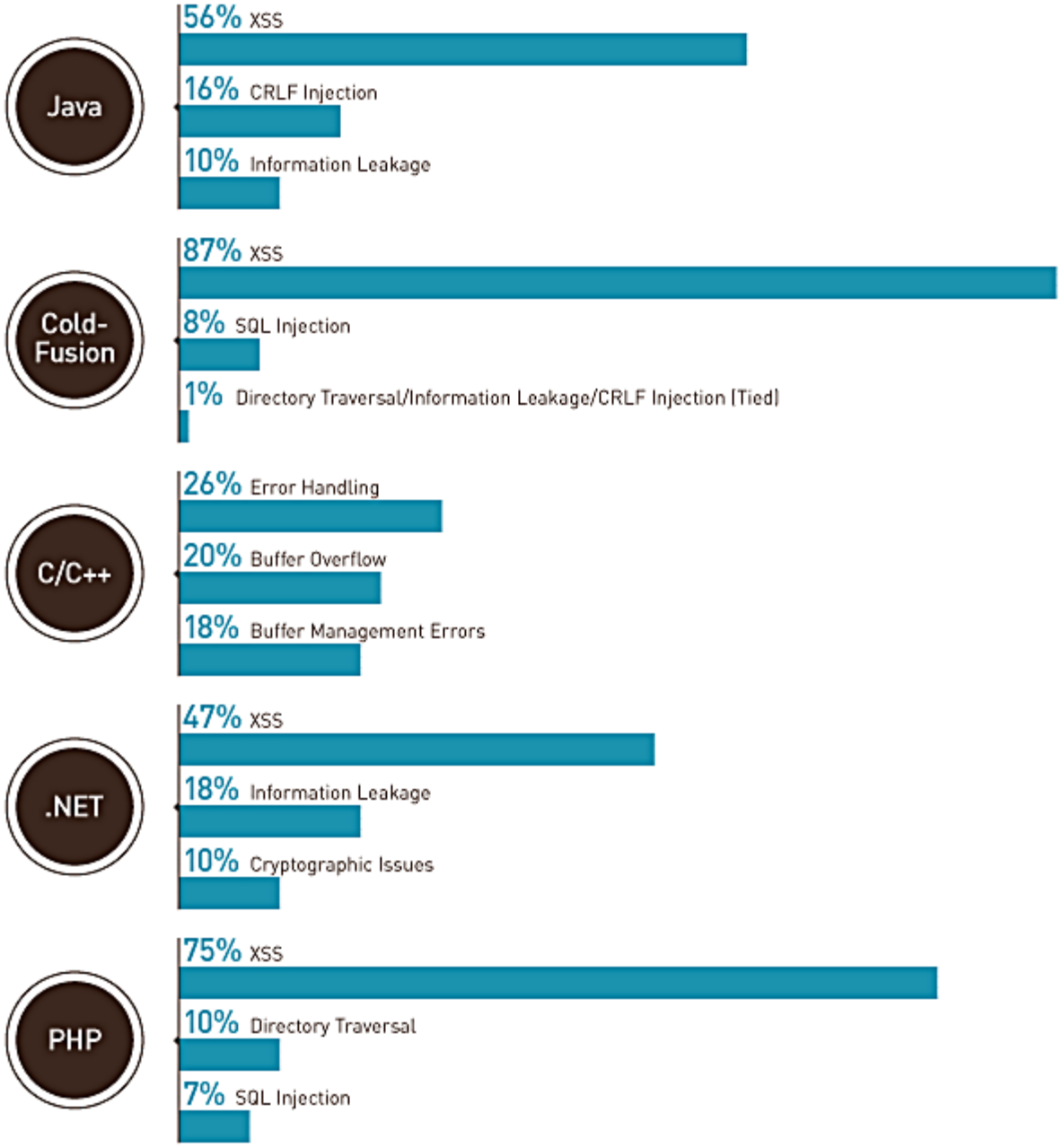
Top Vulnerability Categories
(Percent of Applications Affected for Web Applications)



Top Vulnerability Categories

(Percentage of Applications Affected for Non-Web Applications)

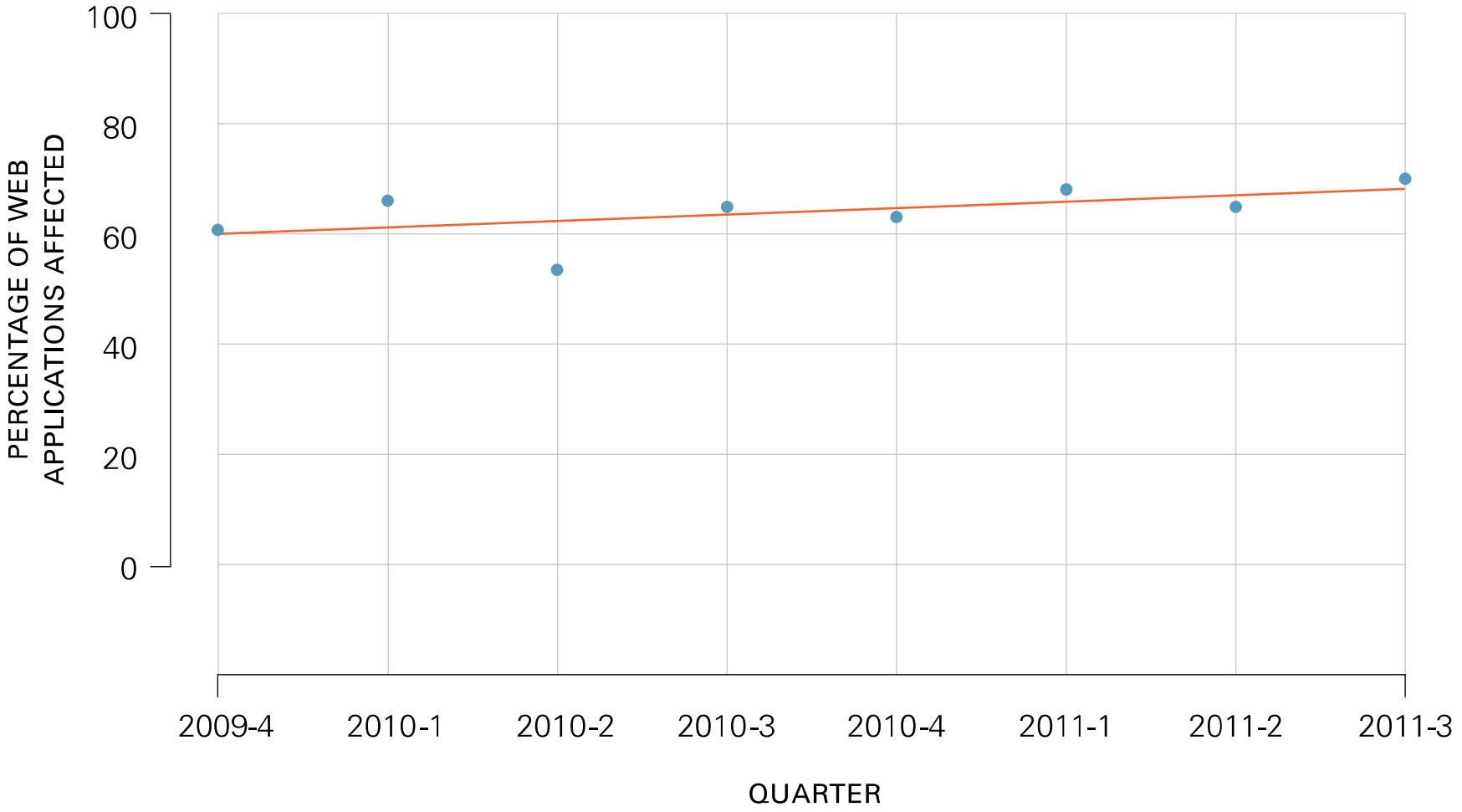



Java
56% XSS
16% CRLF Injection
10% Information Leakage
Cold-Fusion
87% XSS
8% SQL Injection
1% Directory Traversal/Information Leakage/CRLF Injection (Tied)
C/C++
26% Error Handling
20% Buffer Overflow
18% Buffer Management Errors
.NET
47% XSS
18% Information Leakage
10% Cryptographic Issues
PHP
75%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

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

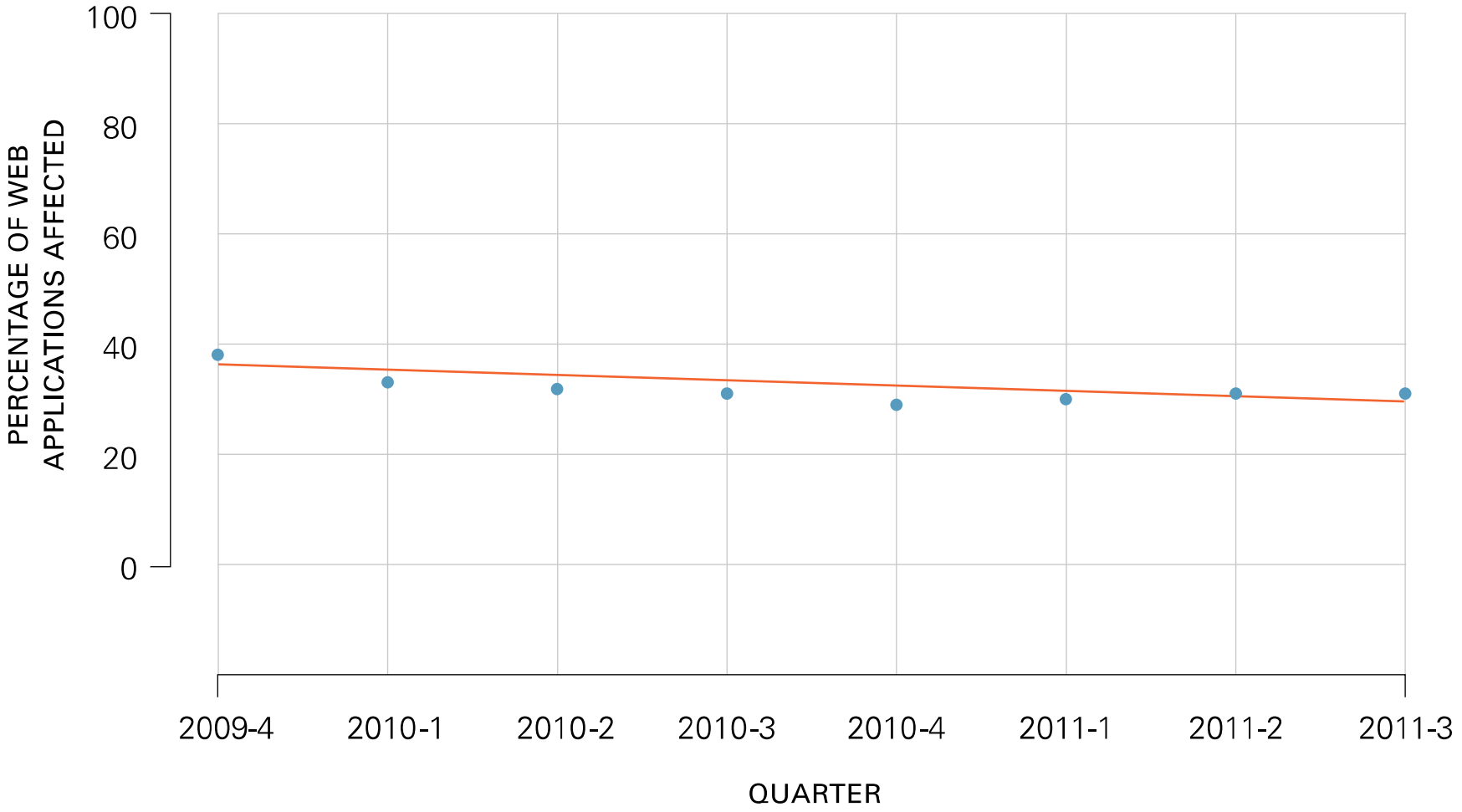
Quarterly Trend for XSS

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?

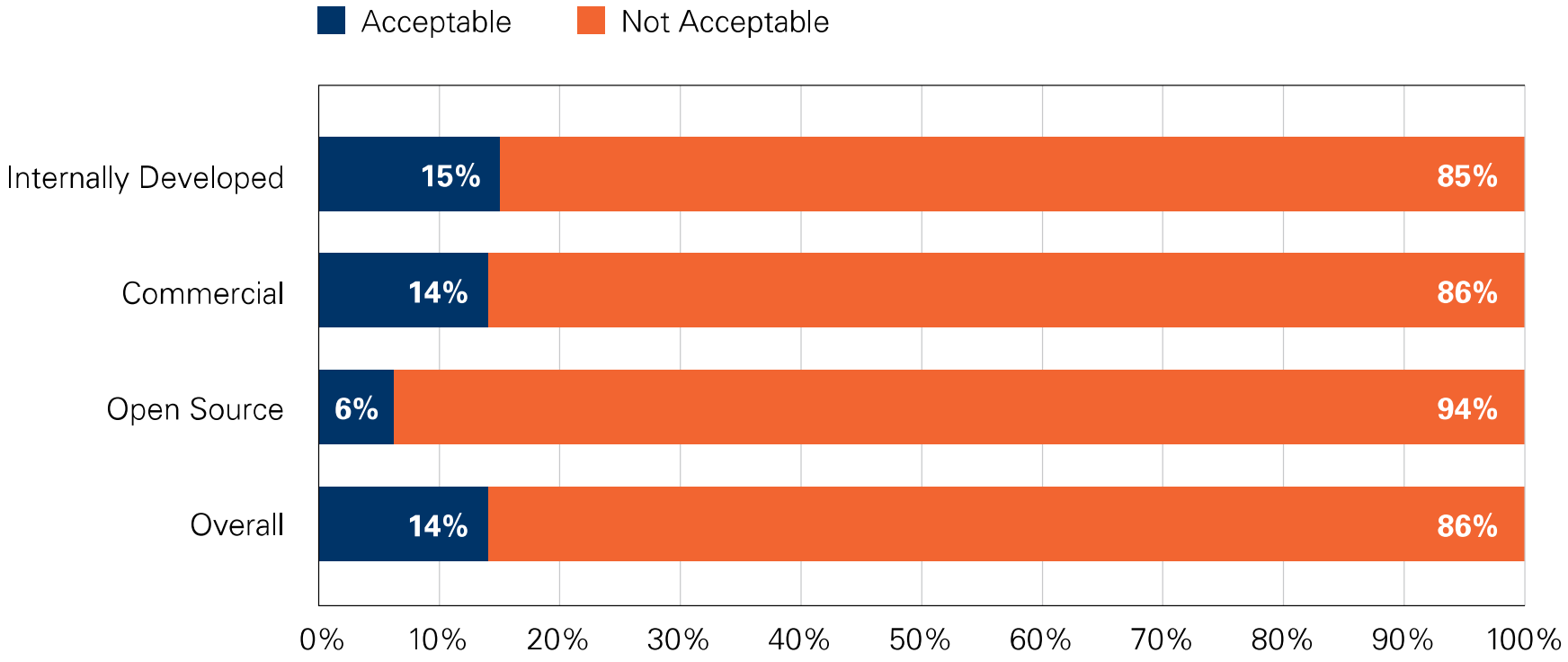
a) 34%

b) 57%

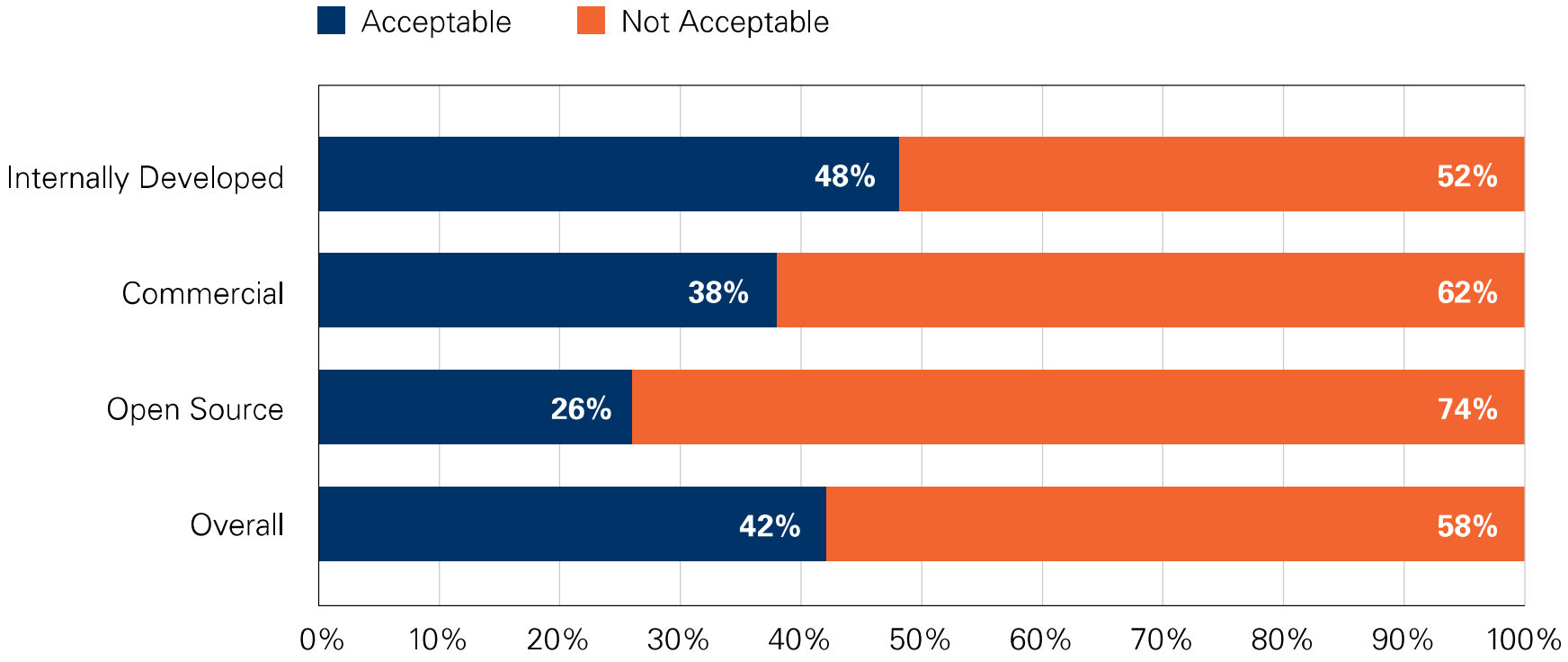
c) 86%

d) 99%

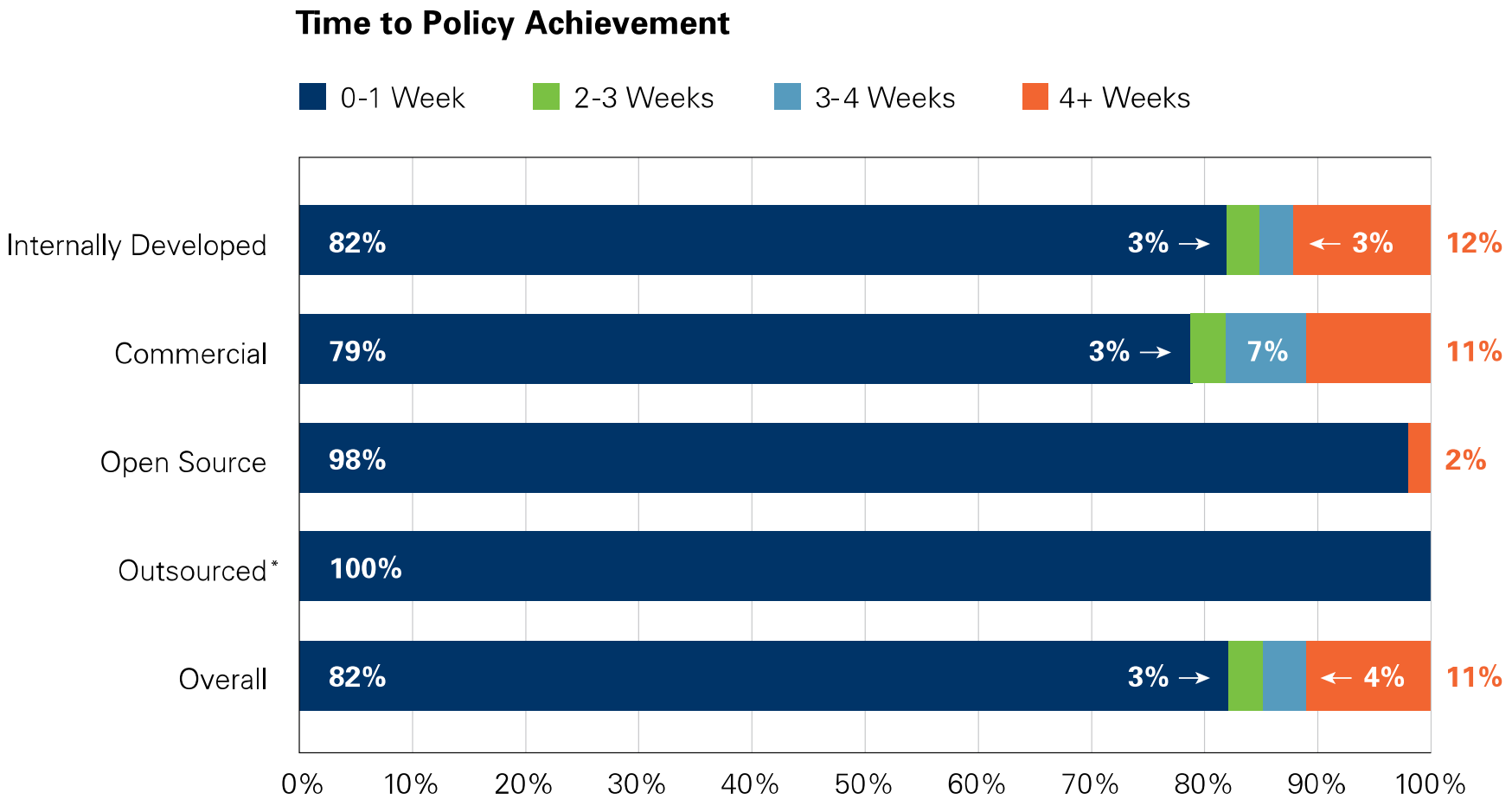
OWASP Top 10 Compliance by Supplier on First Submission
(Web Applications)



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

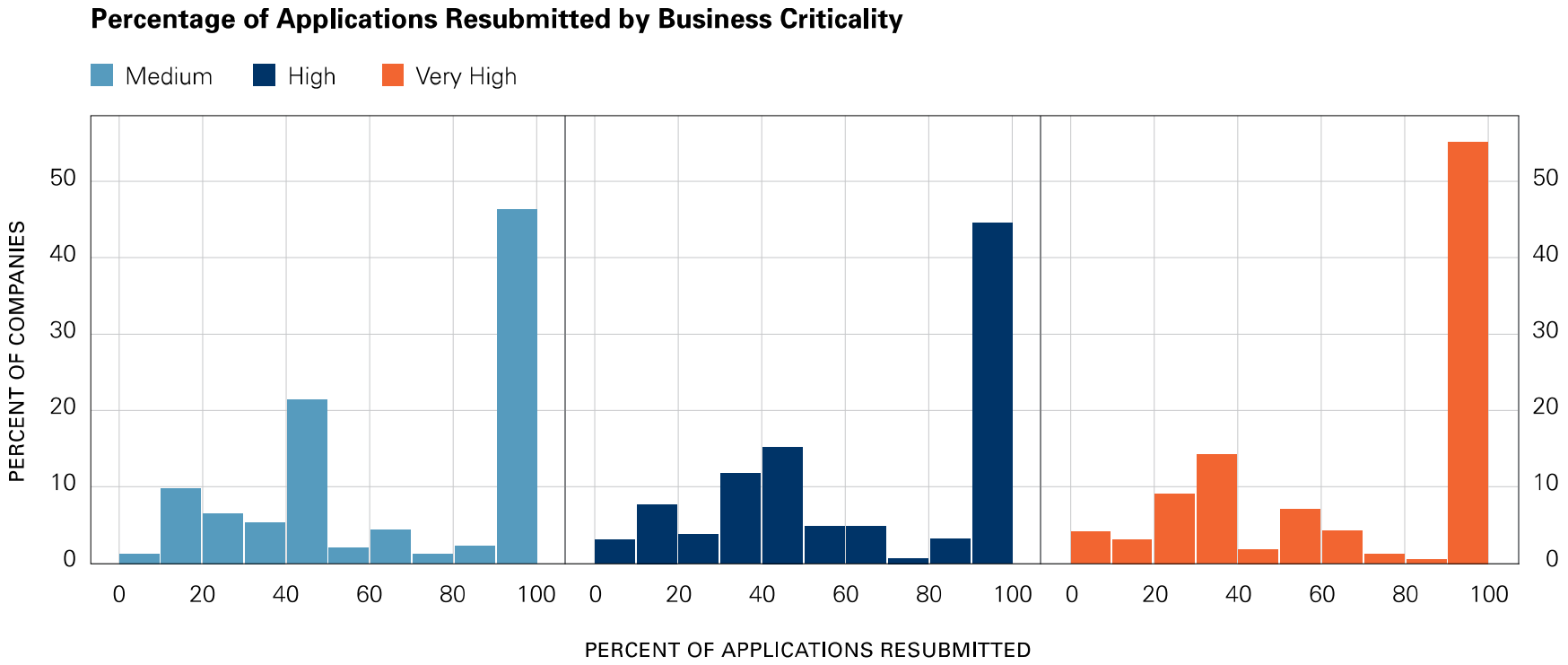


HOW LONG DOES IT TAKE APPLICATIONS TO ACHIEVE AN ACCEPTABLE RATING?



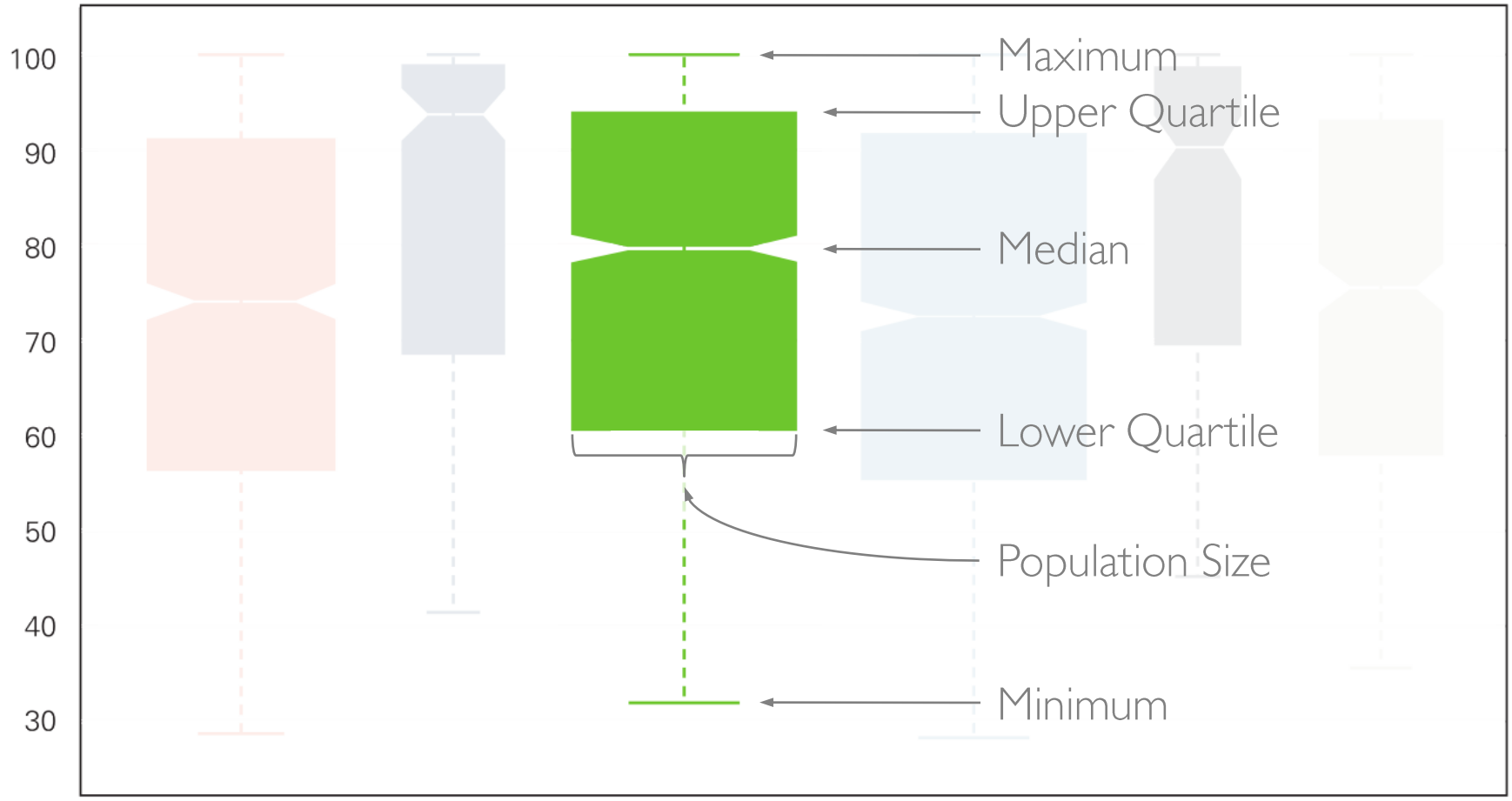
Development agility and application security are not mutually exclusive!

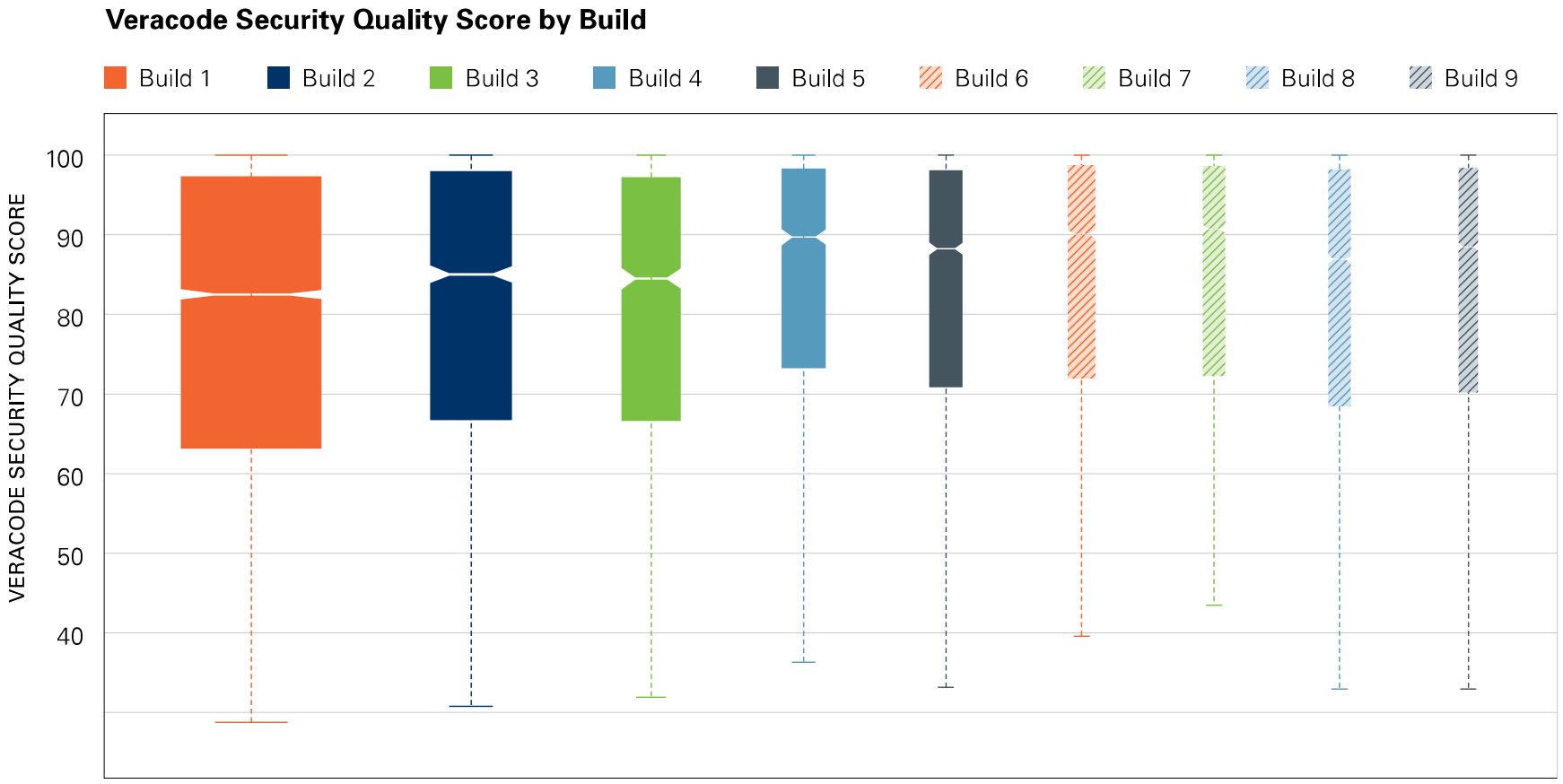
GREAT, BUT WHAT ABOUT ALL THE OTHER APPS?



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

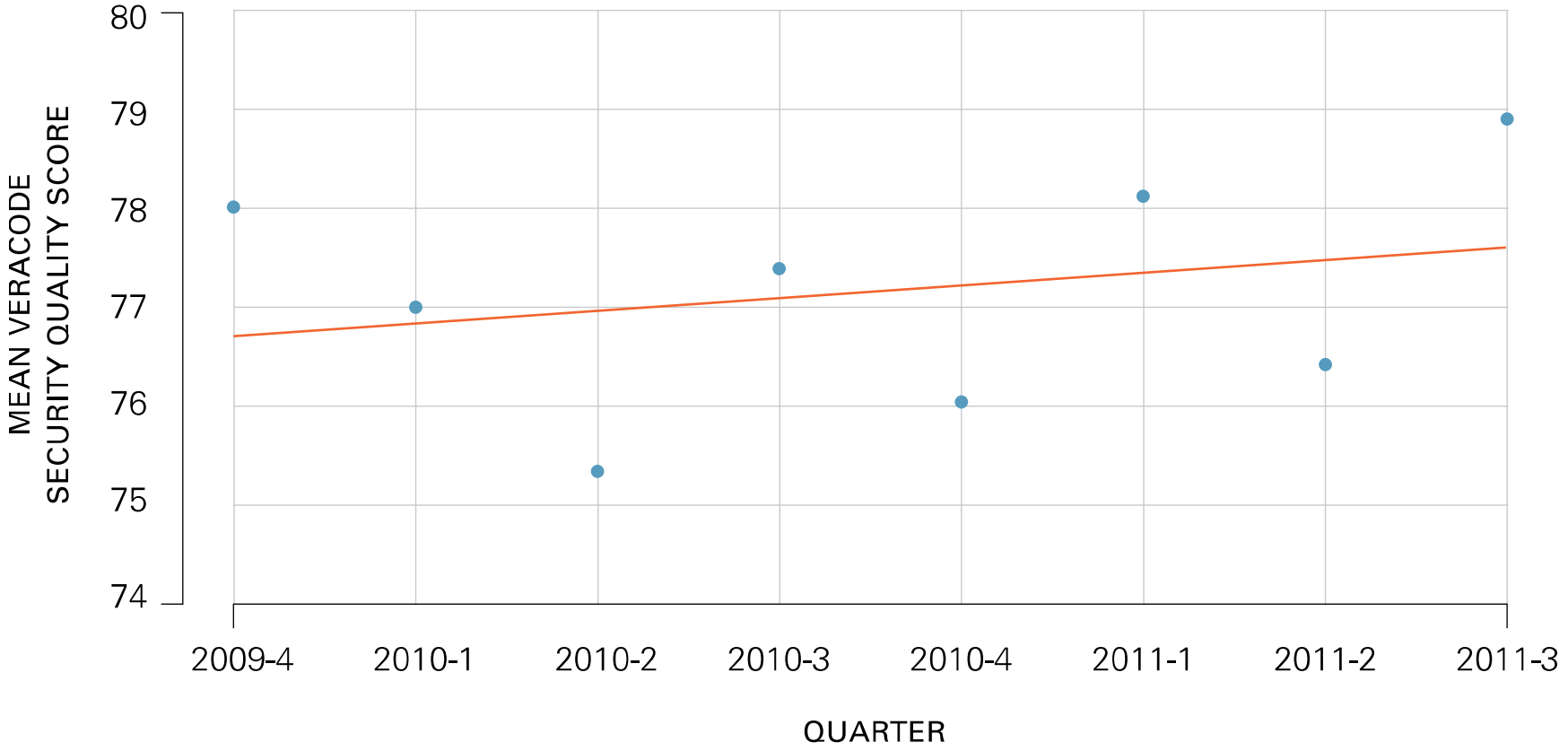
Refresher: Whisker Plots




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

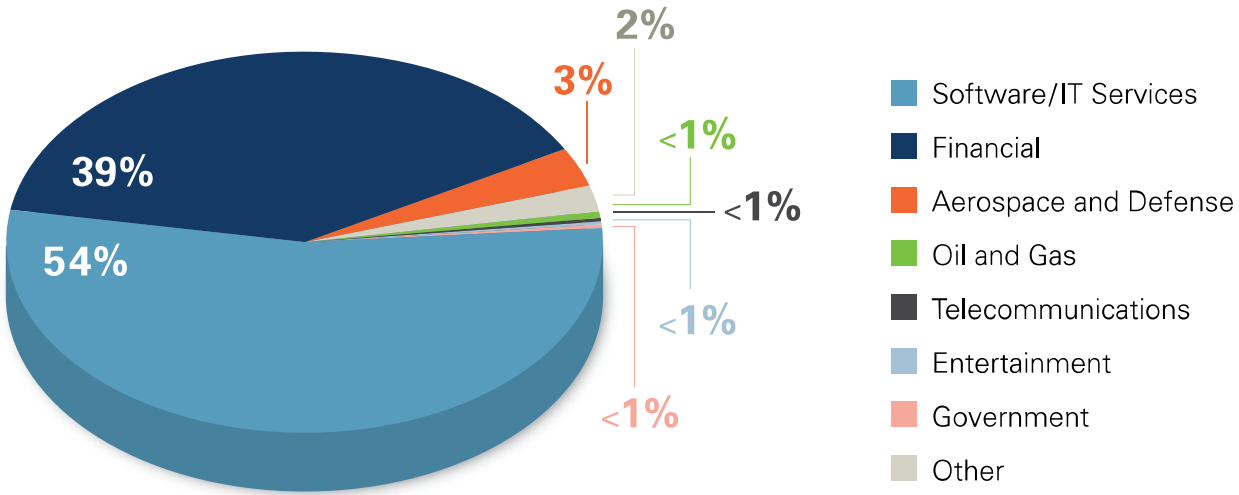
Veracode Security Quality Score Trend by Quarter

pvalue = 0.543: Statistically, the trend is flat.

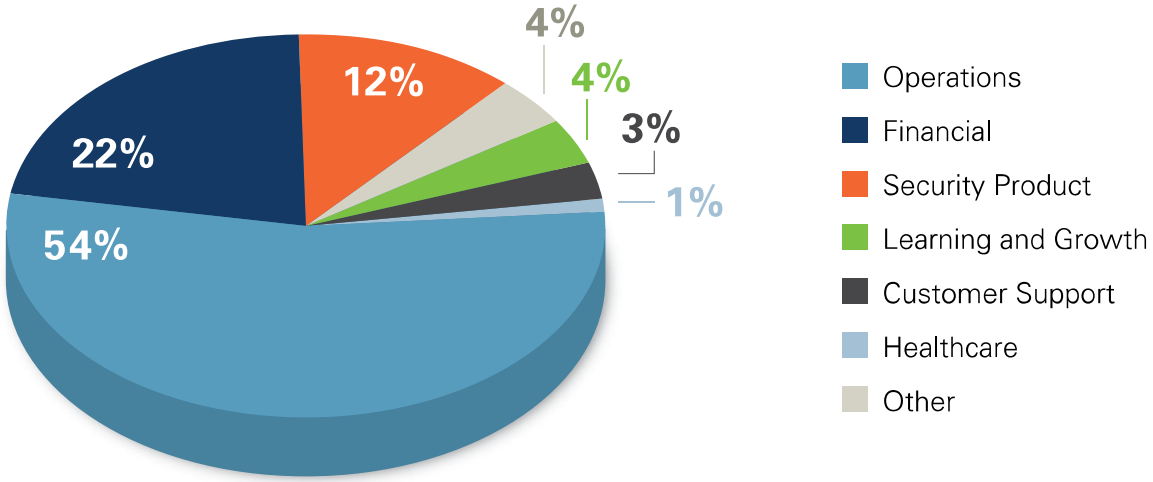


WHO IS HOLDING THEIR SOFTWARE VENDORS ACCOUNTABLE?

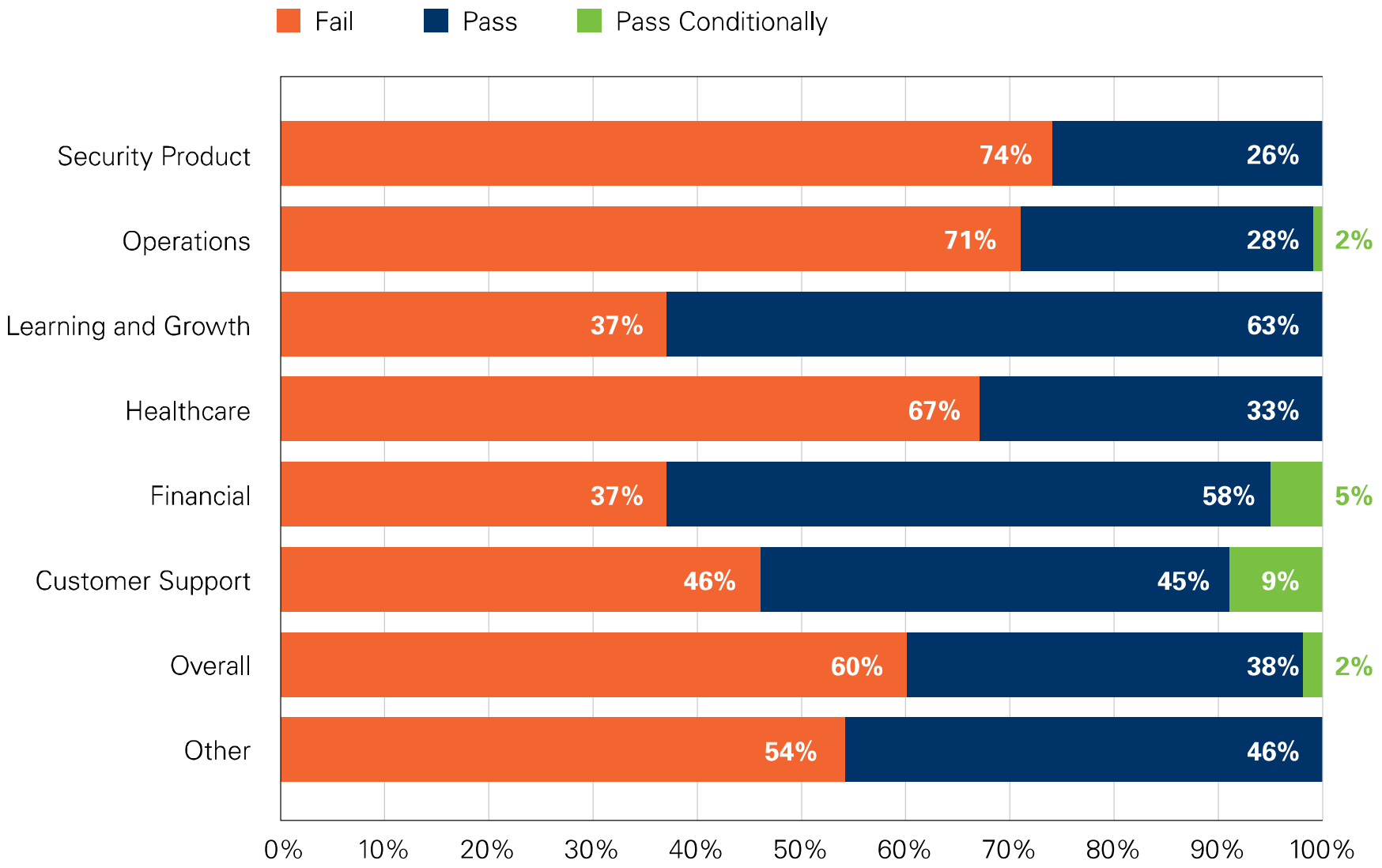
Requestor Type by Industry

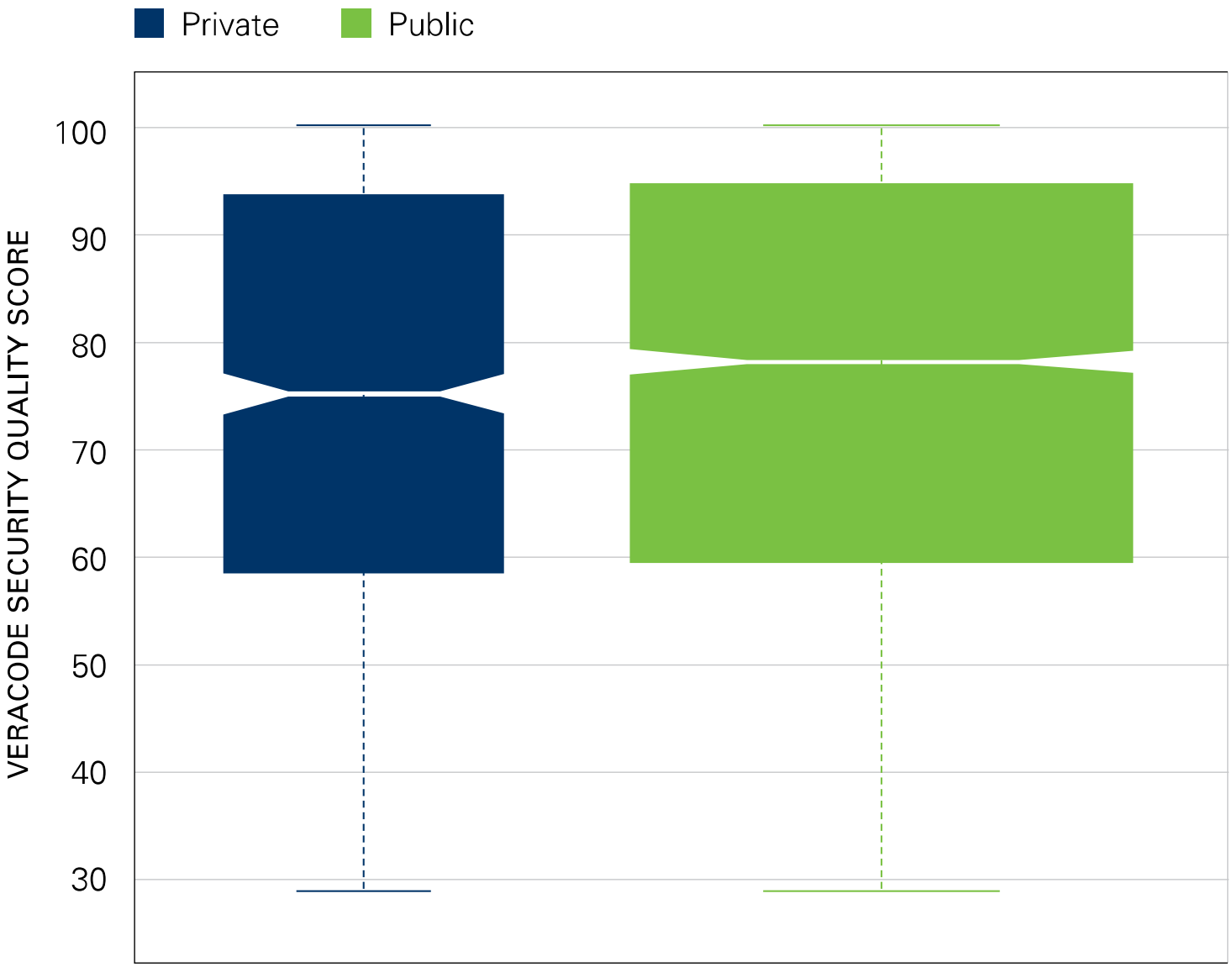


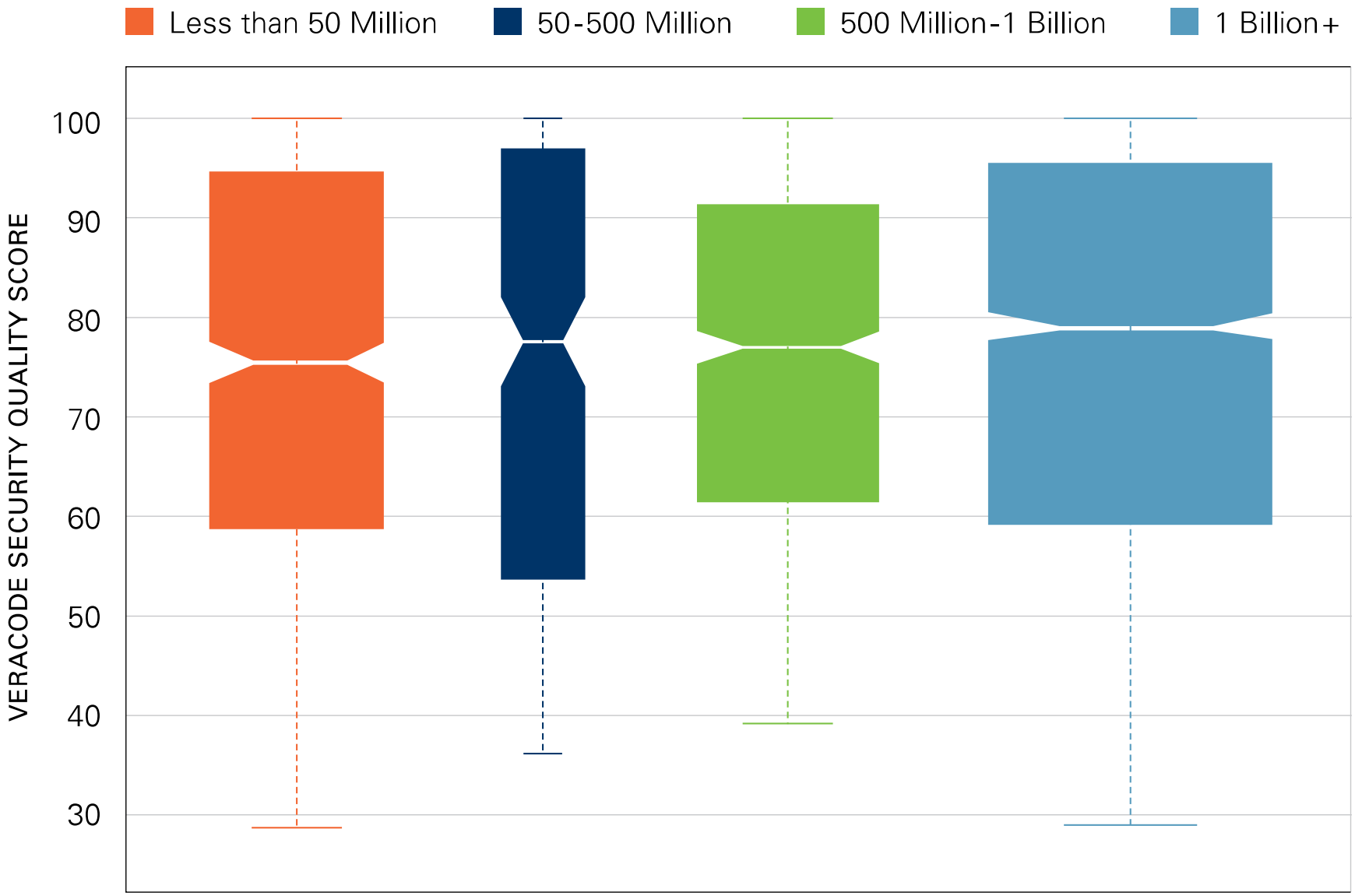
Third-party Assessments by Application Purpose



Performance Against Enterprise Policy by Application Purpose

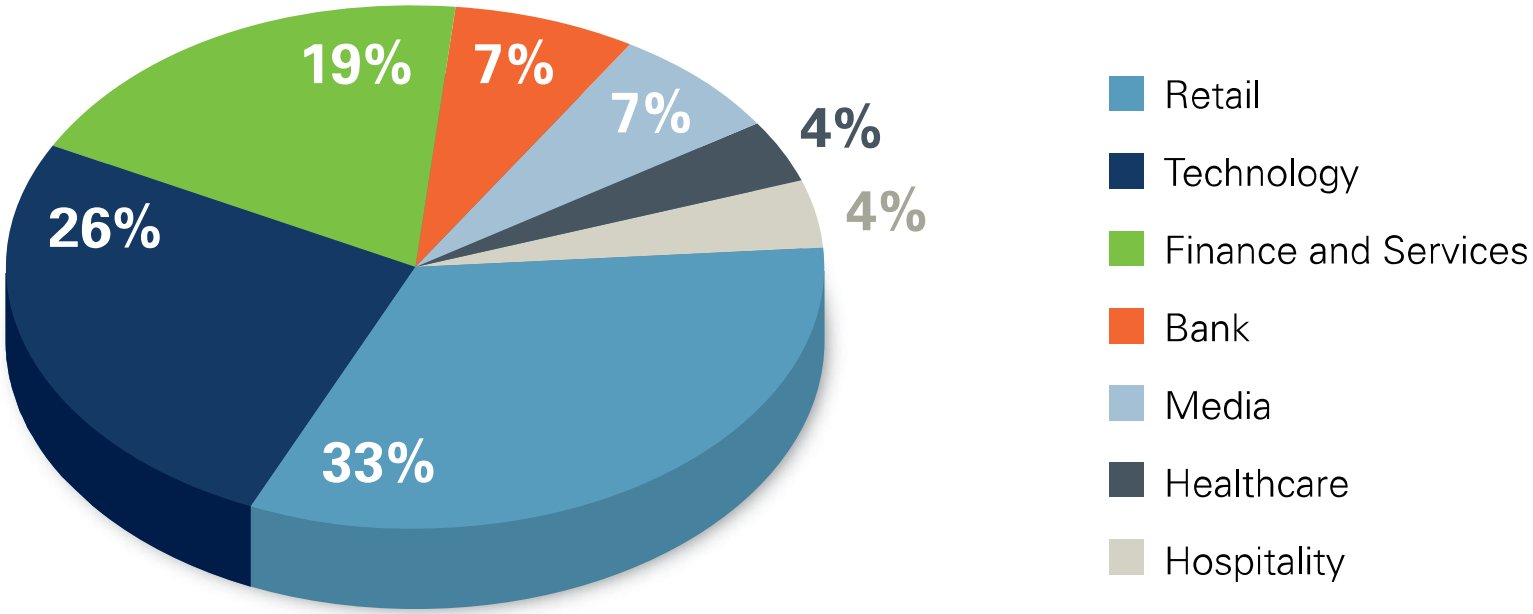



Private
Public
VERACODE SECURITY QUALITY SCORE
100
90
80
70
60
50
40
30


Less than 50 Million
50-500 Million
500 Million-1 Billion
1 Billion+
VERACODE SECURITY QUALITY SCORE
100
90
80
70
60
50
40
30

SO I HEAR YOU CAN RUN APPLICATIONS ON SMART PHONES?

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%

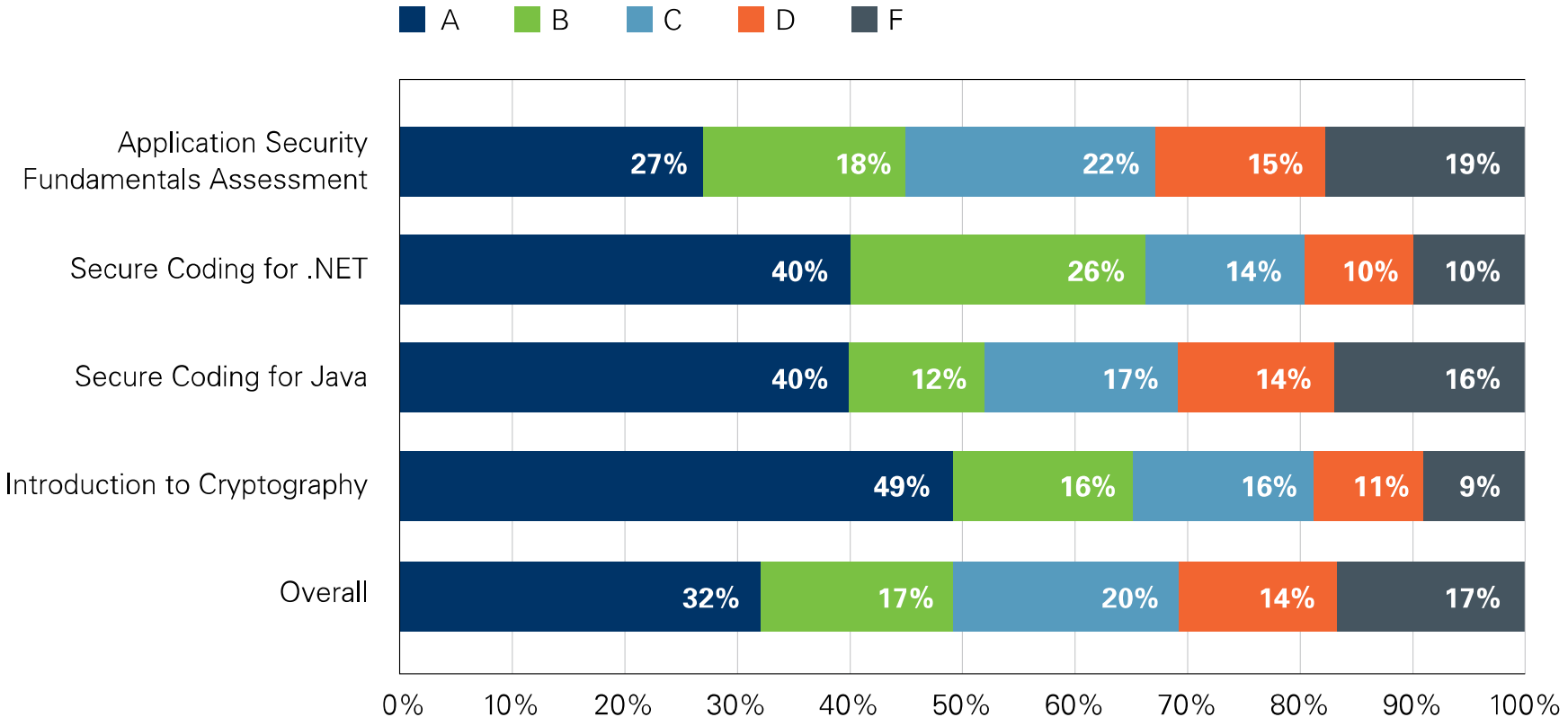
WHEN GIVEN AN EXAM ON APPLICATION SECURITY FUNDAMENTALS, OVER HALF OF DEVELOPERS...

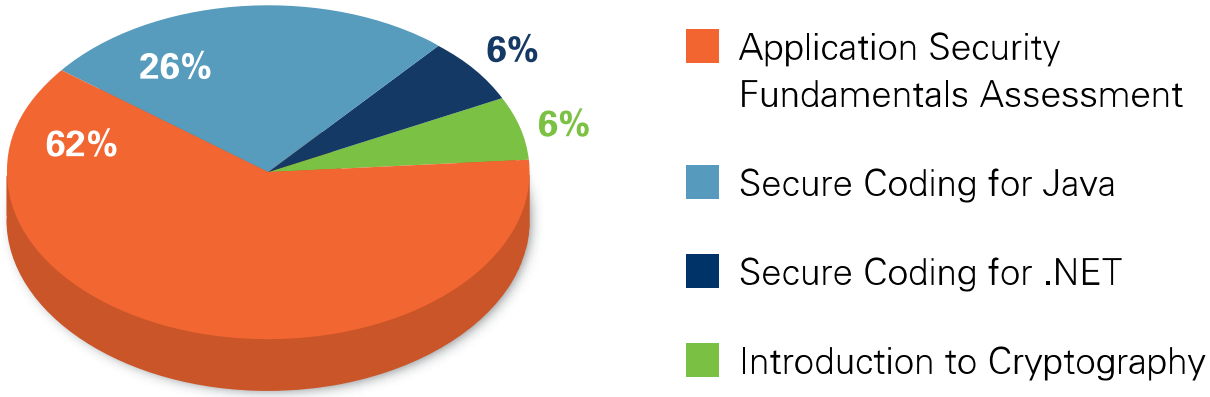
a) Receive an A

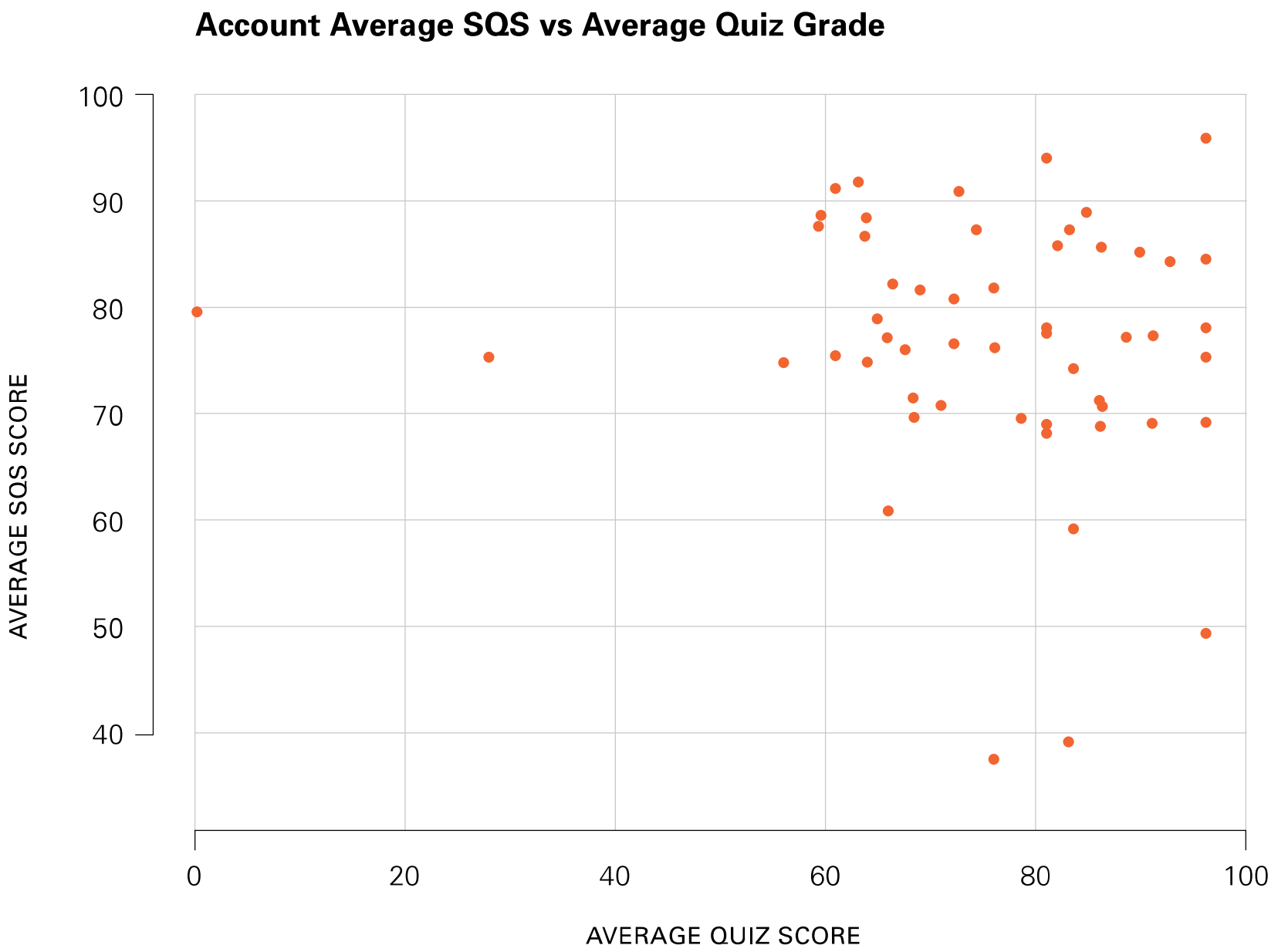
b) Receive a B or worse

c) Receive a C or worse

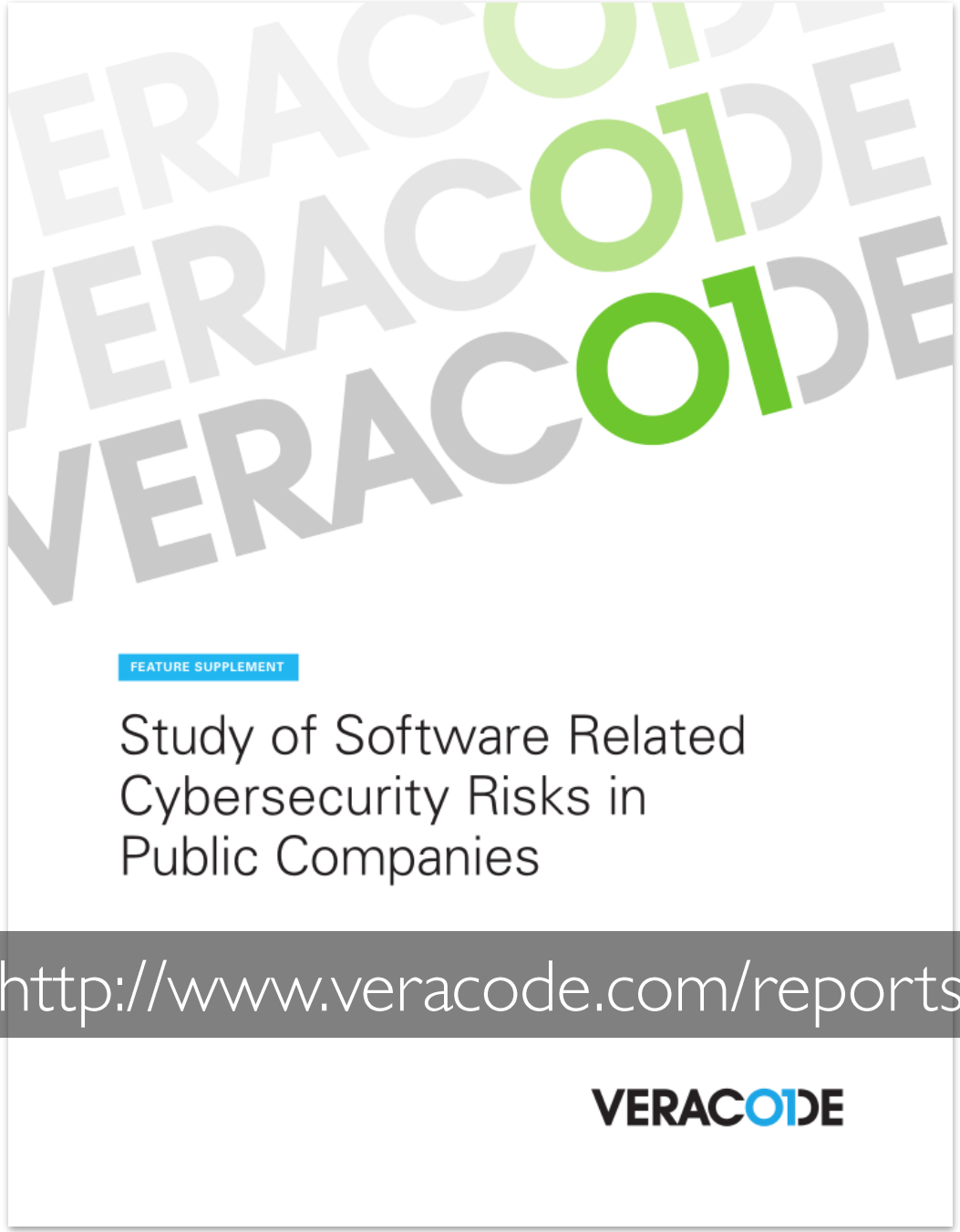
d) Fail (receive a D or F)


A
B
C
D
F
Application Security Fundamentals Assessment
27%
18%
22%
15%
19%
Secure Coding for .NET
40%
26%
14%
10%
10%
Secure Coding for Java
40%
12%
17%
14%
16%
Introduction to Cryptography
49%
16%
16%
11%
9%
Overall
32%
17%
20%
14%
17%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%


26%
6%
6%
62%
Application Security Fundamentals Assessment
Secure Coding for Java
Secure Coding for .NET
Introduction to Cryptography


Account Average SQS vs Average Quiz Grade
AVERAGE SQS SCORE
100
90
80
70
60
50
40
0
20
40
60
80
100
AVERAGE QUIZ SCORE

http://www.veracode.com/reports


FEATURE SUPPLEMENT
Study of Software Related Cybersecurity Risks in Public Companies
http://www.veracode.com/reports
VERACODE

QUESTIONS?


ceng@veracode.com


@chriseng