Security Scoreboard in the Sky

OWASP AppSec Research

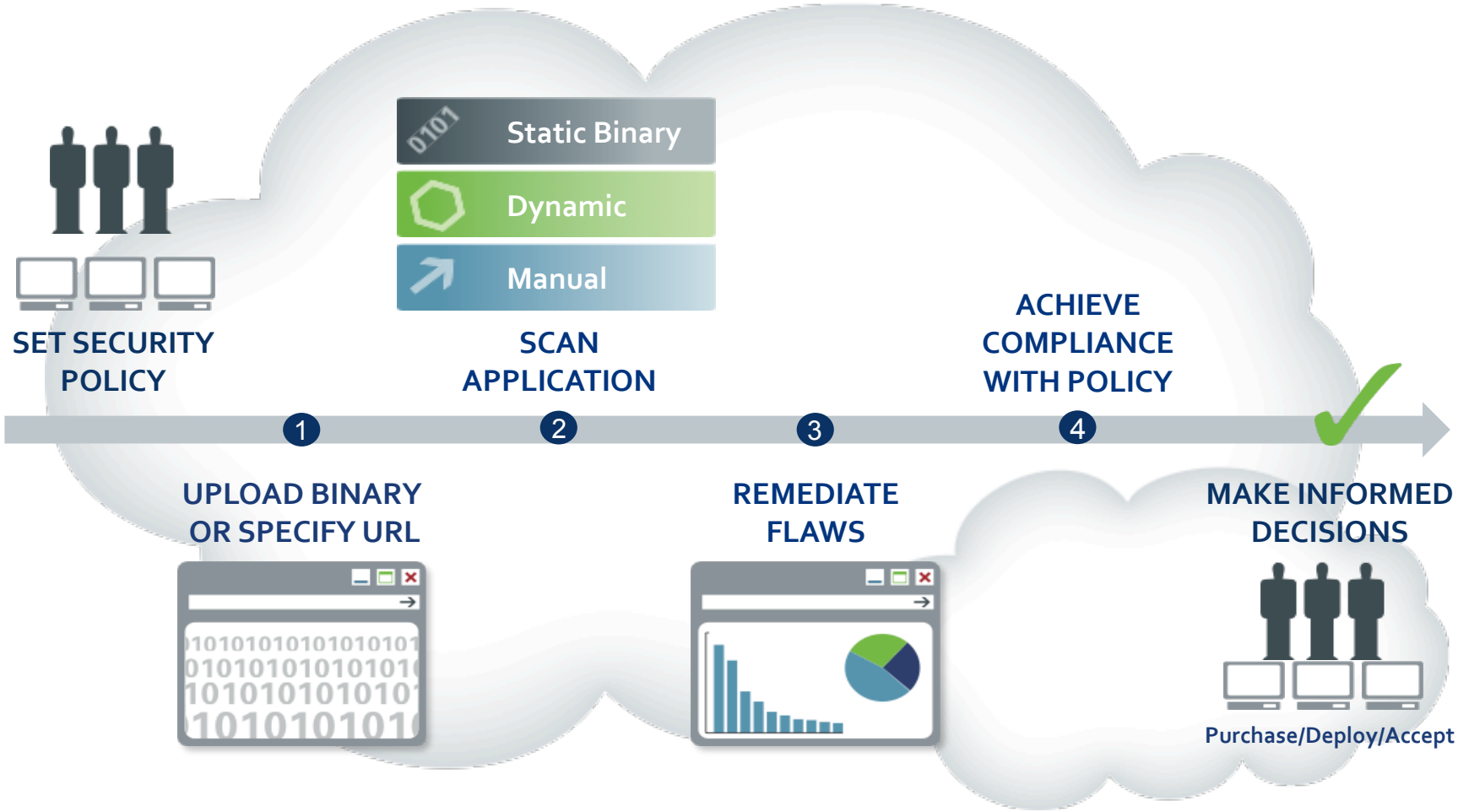
June 24, 2010

VERACODE

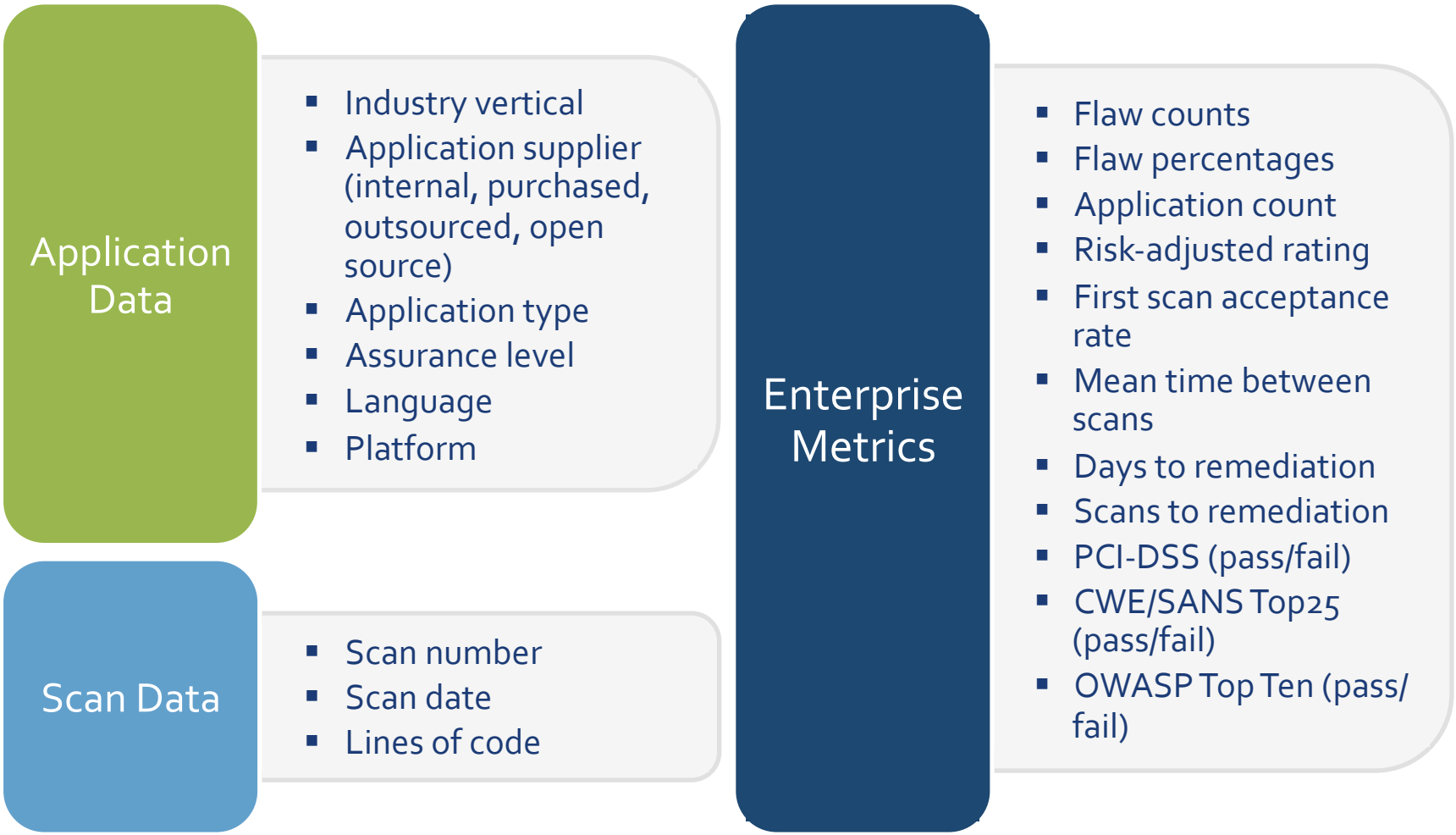
Bio

- Chris Eng
  - Senior Director of Research at Veracode
  - Responsible for incorporating security intelligence into Veracode's offerings
- Previously
  - Technical Manager at Symantec (through acquisition)
  - Technical Director and Consultant at @stake
  - Security Researcher, etc. at NSA
- Industry Involvement
  - Frequent speaker at security conferences
  - Contributor to various CWE, OWASP, WASC initiatives
  - Advisor, program committee for SOURCE Conferences (BOS, BCN)
  - Developed @stake WebProxy (any old timers out there?)

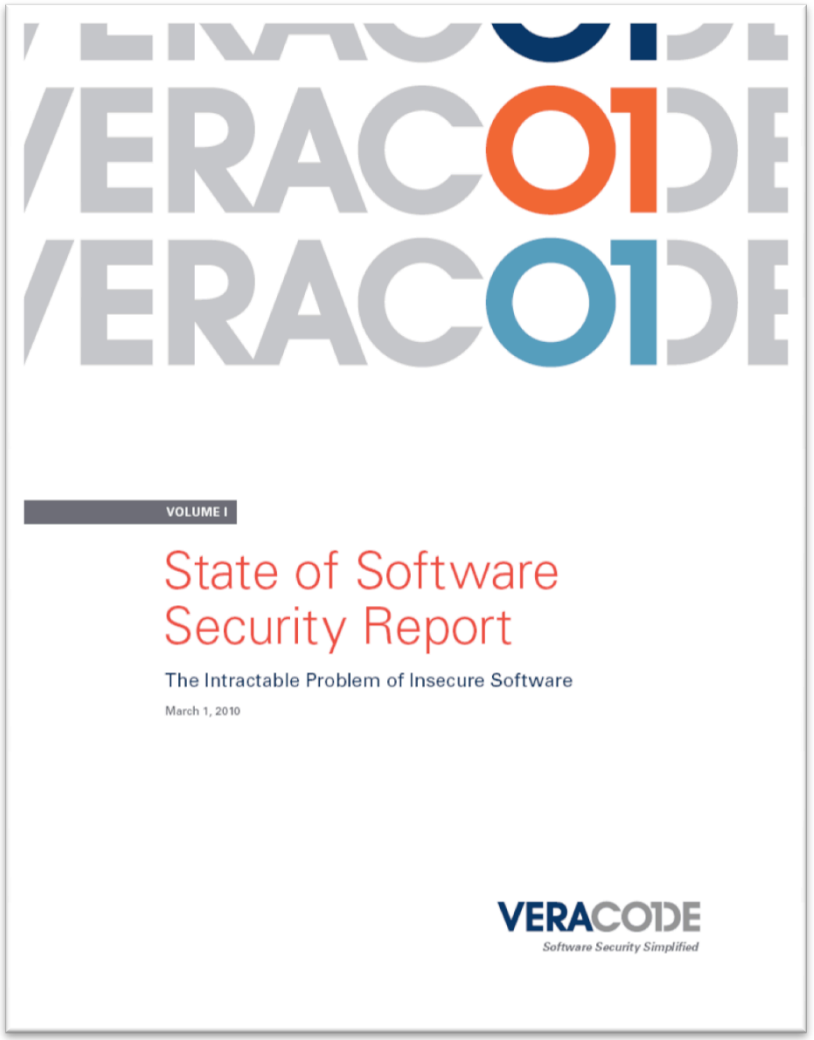
Application Risk Management Services Platform: Automating Security Acceptance Testing



Data Set and Available Metrics

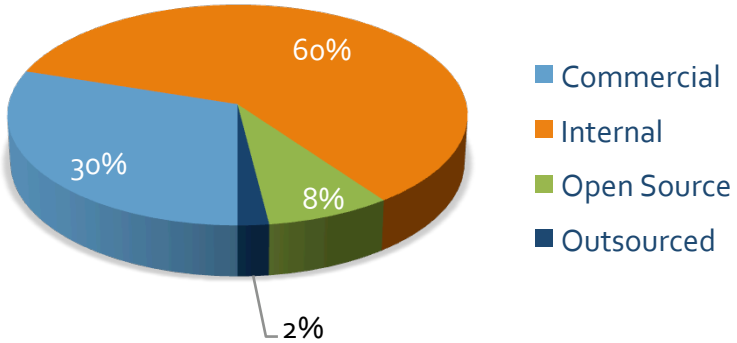


State of Software Security, Volume 1

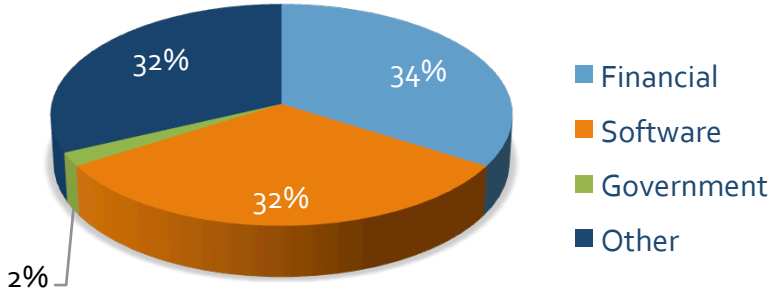


Sample Distribution

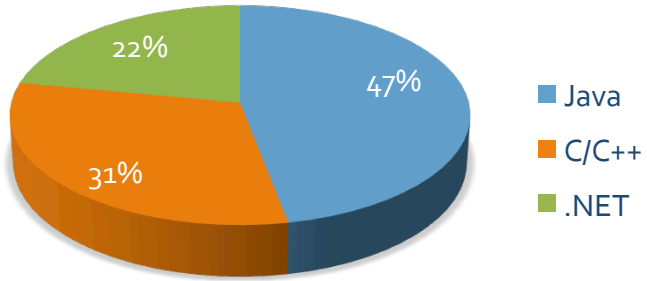
Applications by Supplier



Applications by Industry



Applications by Language



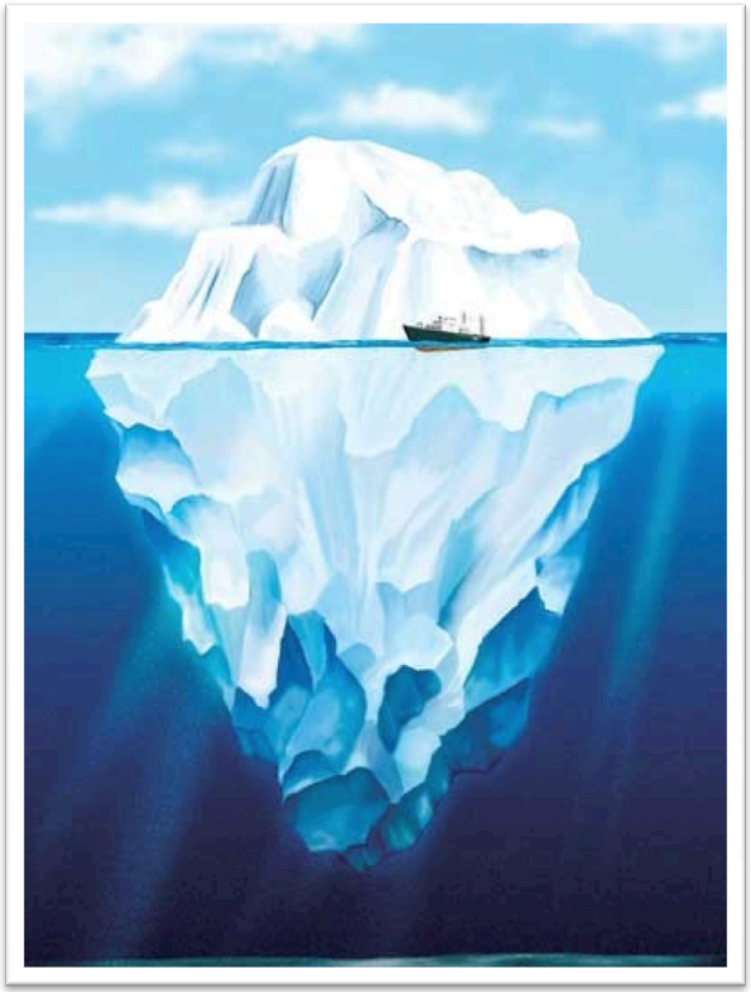
Statistically Significant Sample Size

- Sample size this large enable us to report findings with a reasonable degree of confidence:
- Type I Error
  - Probability of stating that something is FALSE when it is in fact TRUE: < 5%
- Type II Error
  - Probability of stating that something is TRUE when it is in fact FALSE: < 20%
- Margins of error for estimates of various metrics:
  - Flaw count: 10%
  - First scan acceptance rate: 15%
  - Veracode risk-adjusted rating: 10%
  - Remediation time: 10%

State of Software Security, Vol. 1: Observations

1. Most software is indeed very insecure
2. Third-party software is a significant percentage of the enterprise software infrastructure, and third-party components are a significant percentage of most applications
3. Open source projects have comparable security, faster remediation times, and fewer Potential Backdoors than Commercial or Outsourced software
4. A significant amount of Commercial and Open Source software is written in C/C++ making it disproportionately susceptible to vulnerabilities that allow attackers to gain control of systems
5. The pervasiveness of easily remedied vulnerabilities indicates a lack of developer education on secure coding
6. Software of all types from Finance and Government sectors was relatively more secure on first submission to Veracode for testing
7. Outsourced software is assessed the least, suggesting the absence of contractual security acceptance criteria

Most Software is Insecure



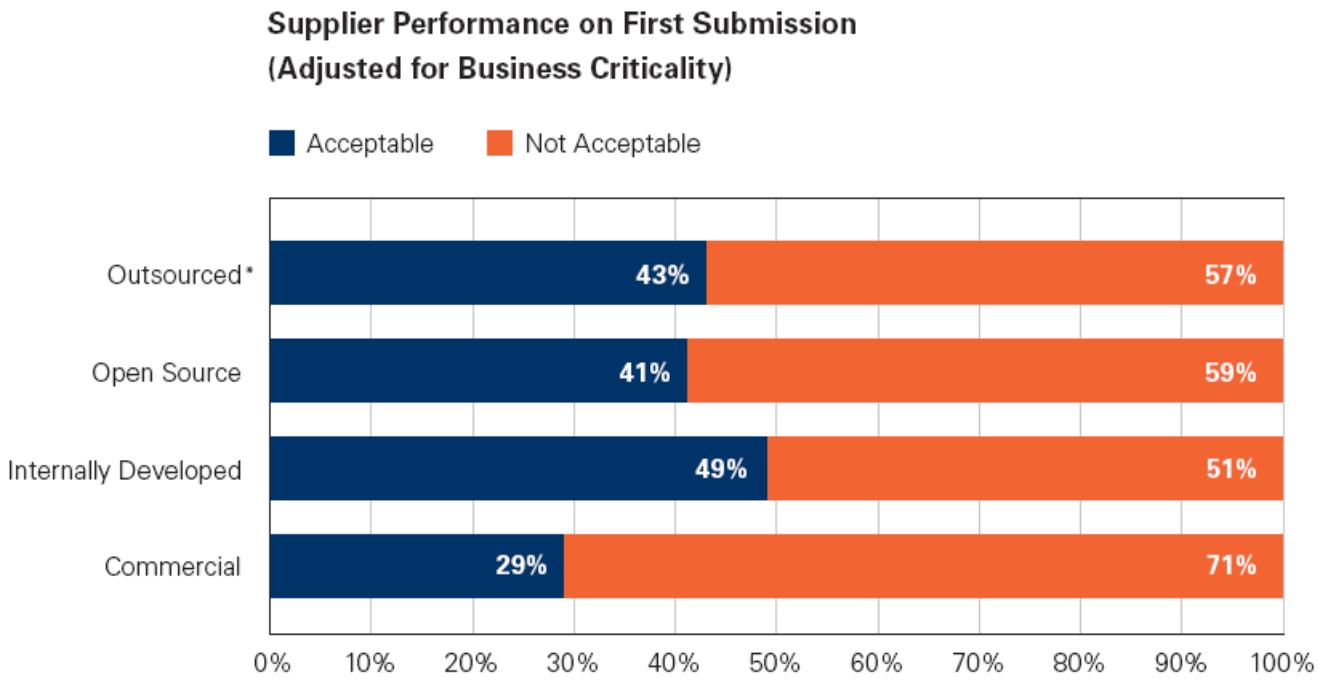
42%

58%

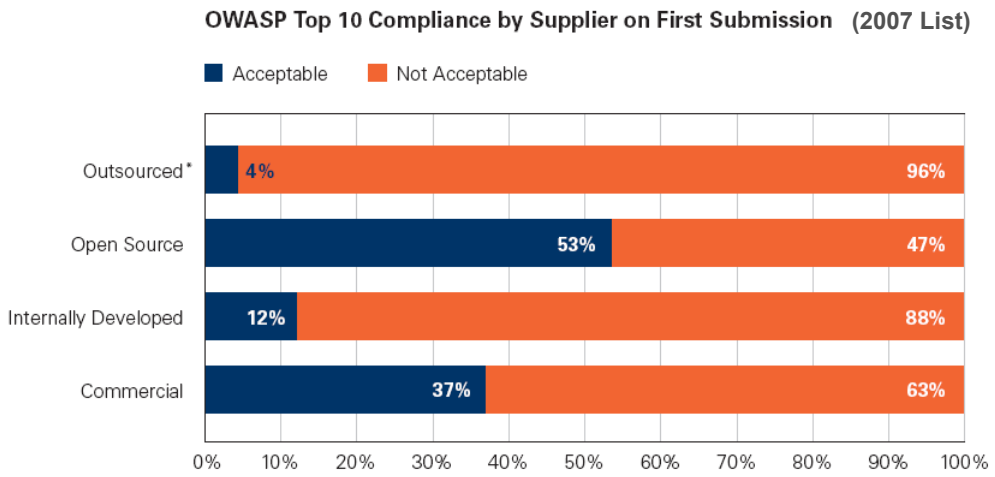
Veracode Risk-Adjusted Ratings

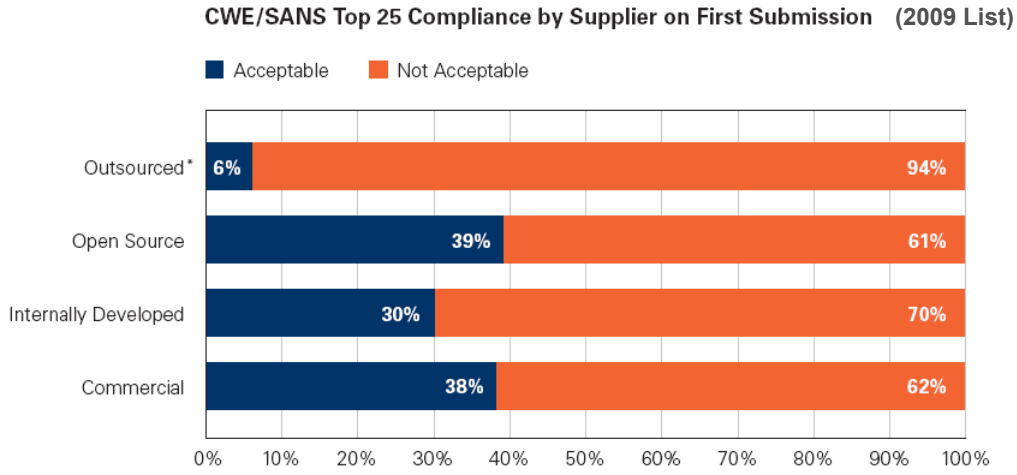
Assurance Level	Rating Based on Analysis Score	
VERY HIGH (AL5)	90-100 (no VH, H, M)	**A**
	80-89 (no VH, H)	**B**
	70-79 (no VH)	**C**
	60-69	**D**
HIGH (AL4)	80-100 (no VH, H)	**A**
	70-79 (no VH)	**B**
	60-69	**C**
	50-59	**D**
MEDIUM (AL3)	70-100 (no VH)	**A**
	60-69	**B**
	50-59	**C**
	40-49	**D**
LOW (AL2)	60-100	**A**
	50-59	**B**
	40-49	**C**
	30-39	**D**

Most Software is Insecure

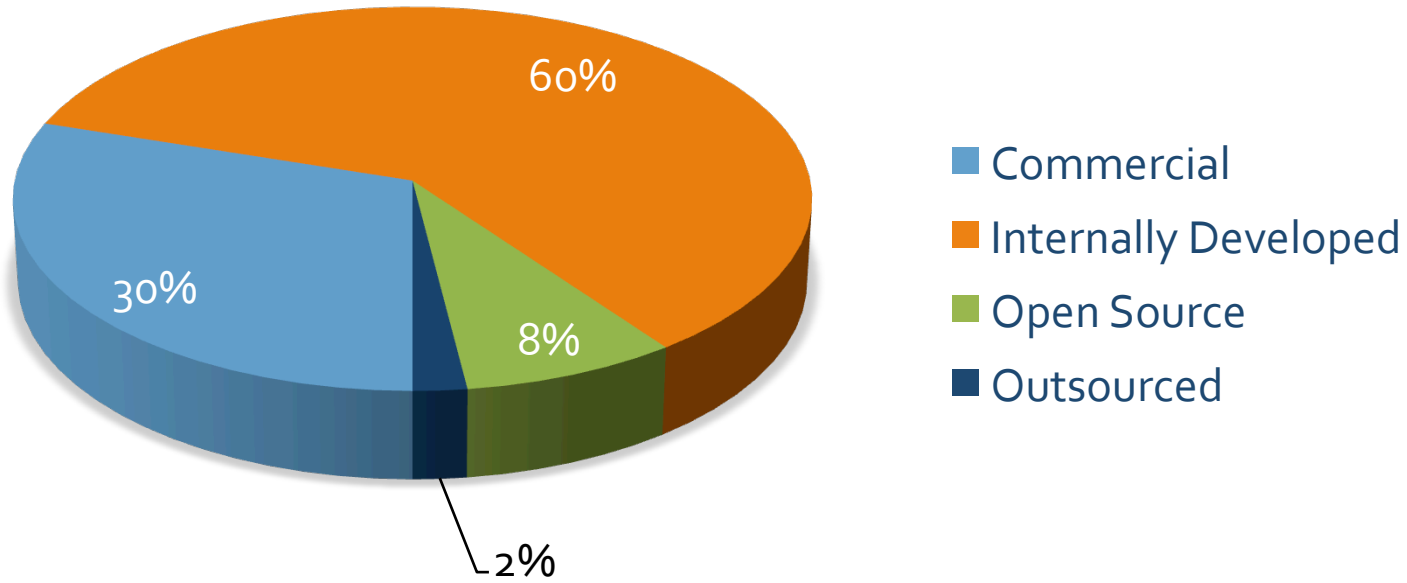


Most Software is Insecure

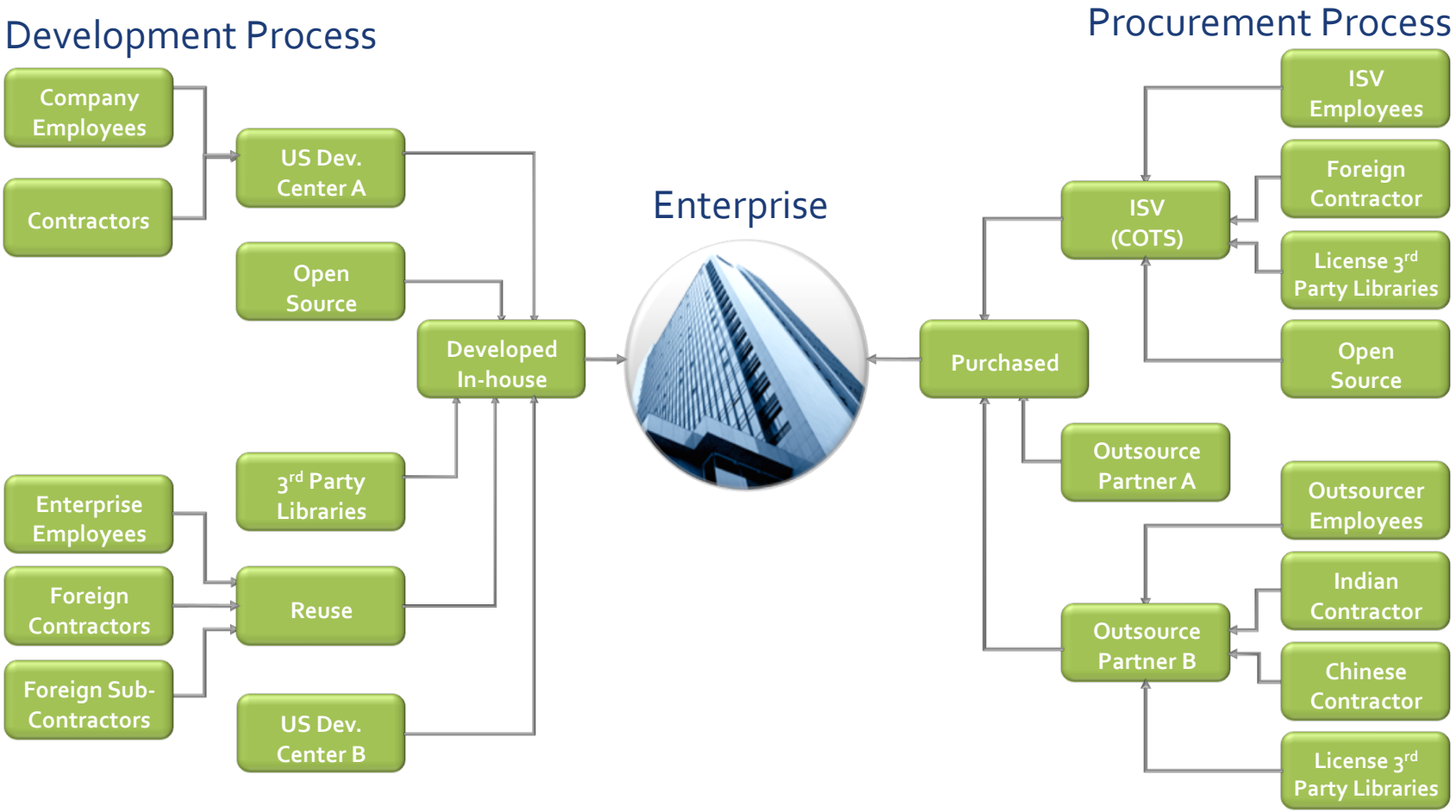




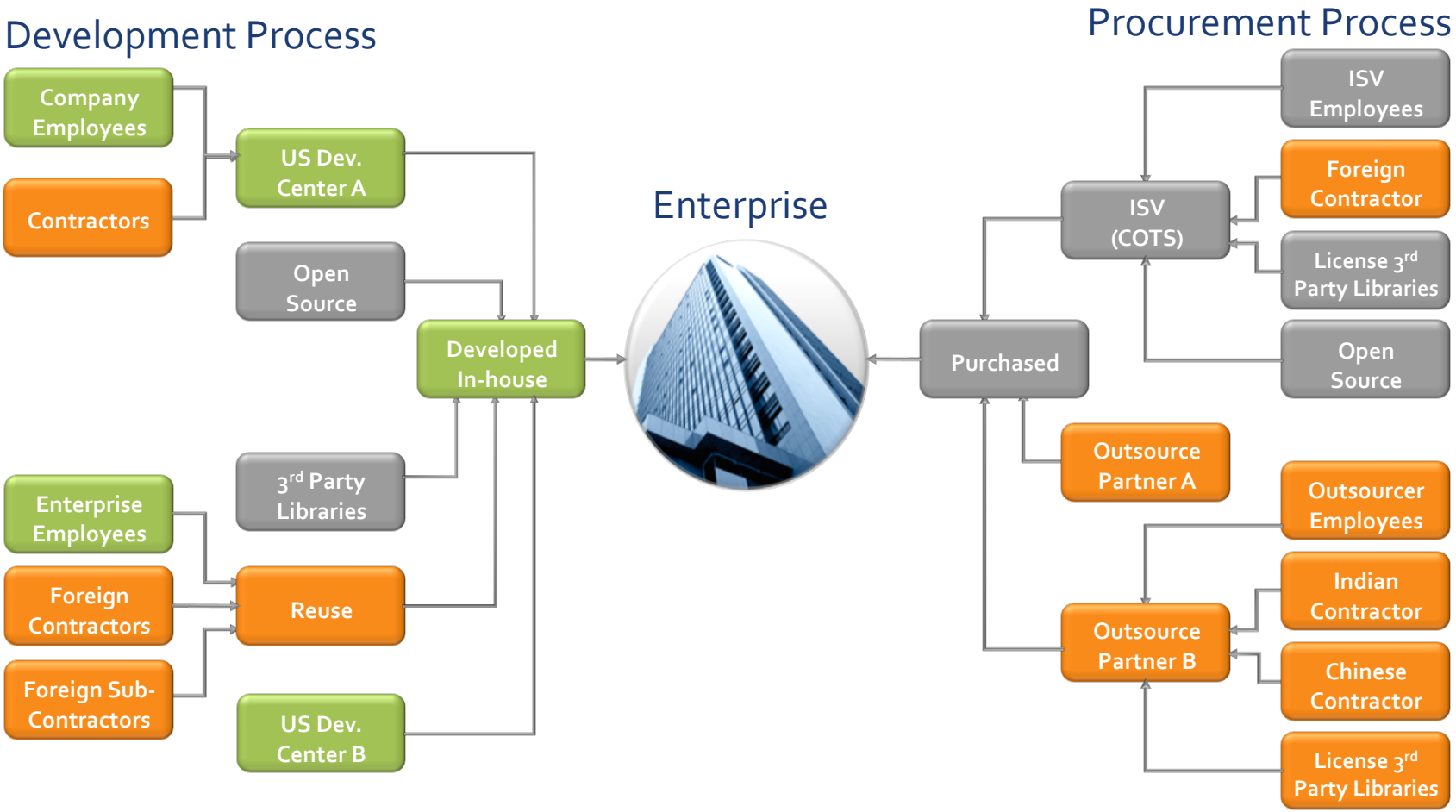
Third-Party Software Cannot Be Ignored



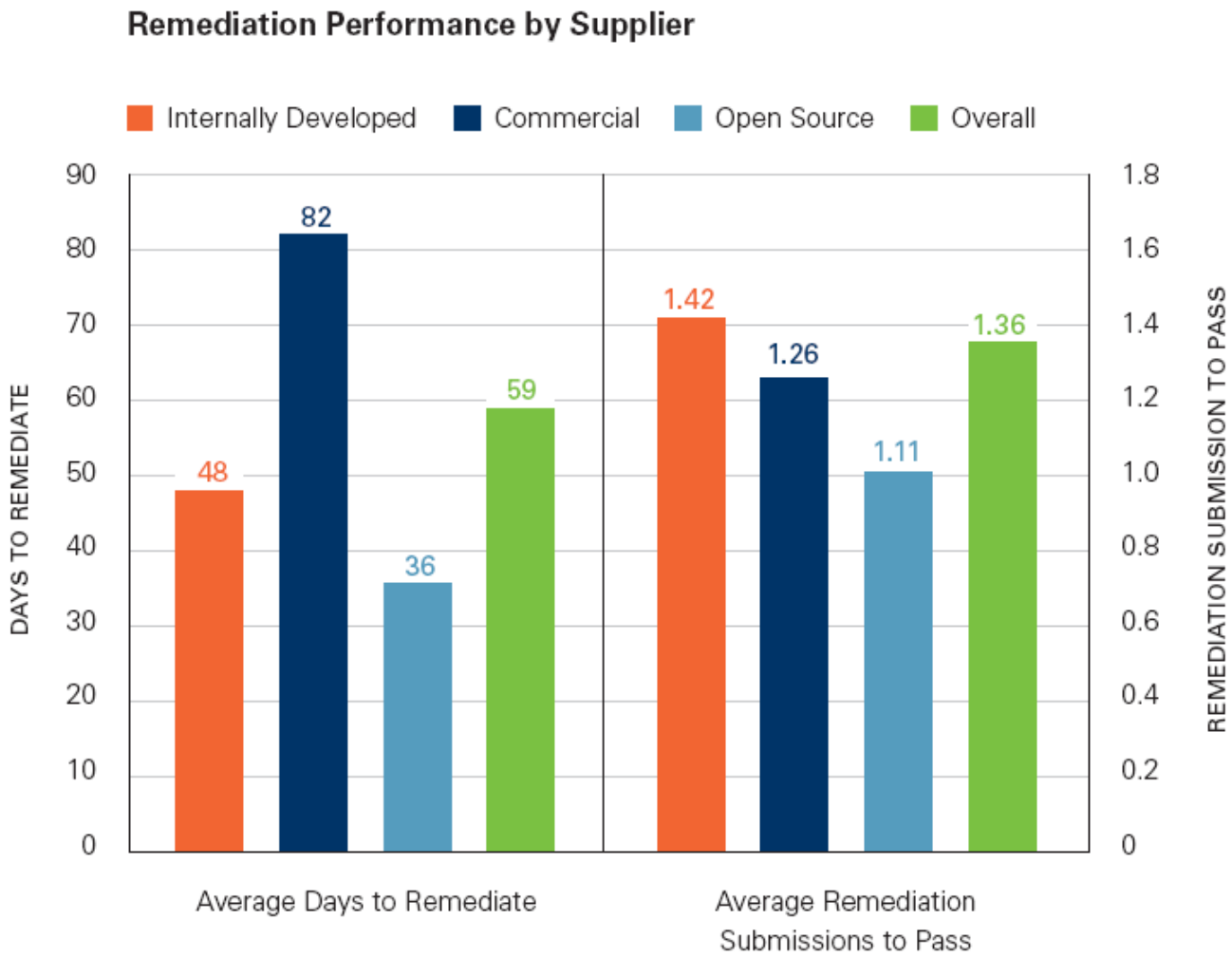
Third-Party Software Cannot Be Ignored



Third-Party Software Cannot Be Ignored



ISVs Slowest to Remediate; Open Source Fastest

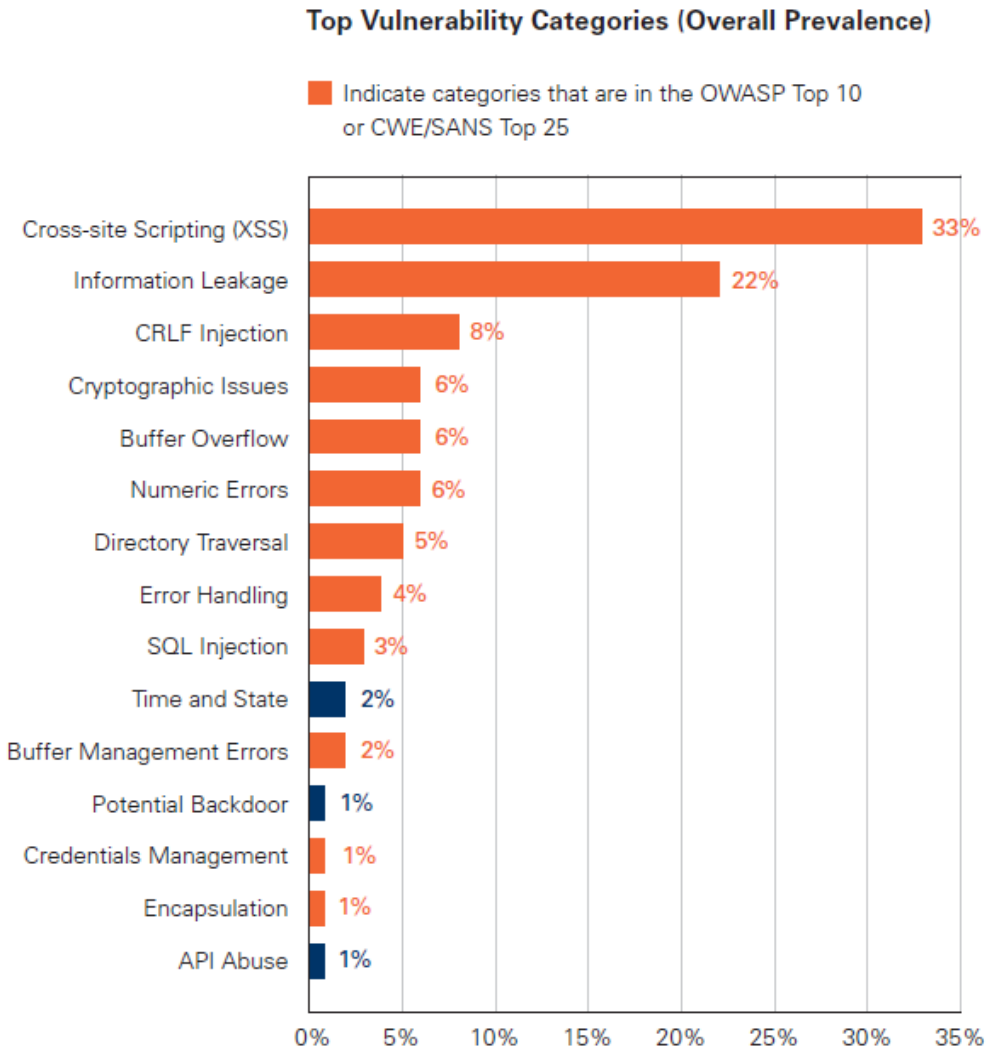


C/C++ Less Prevalent in Enterprises

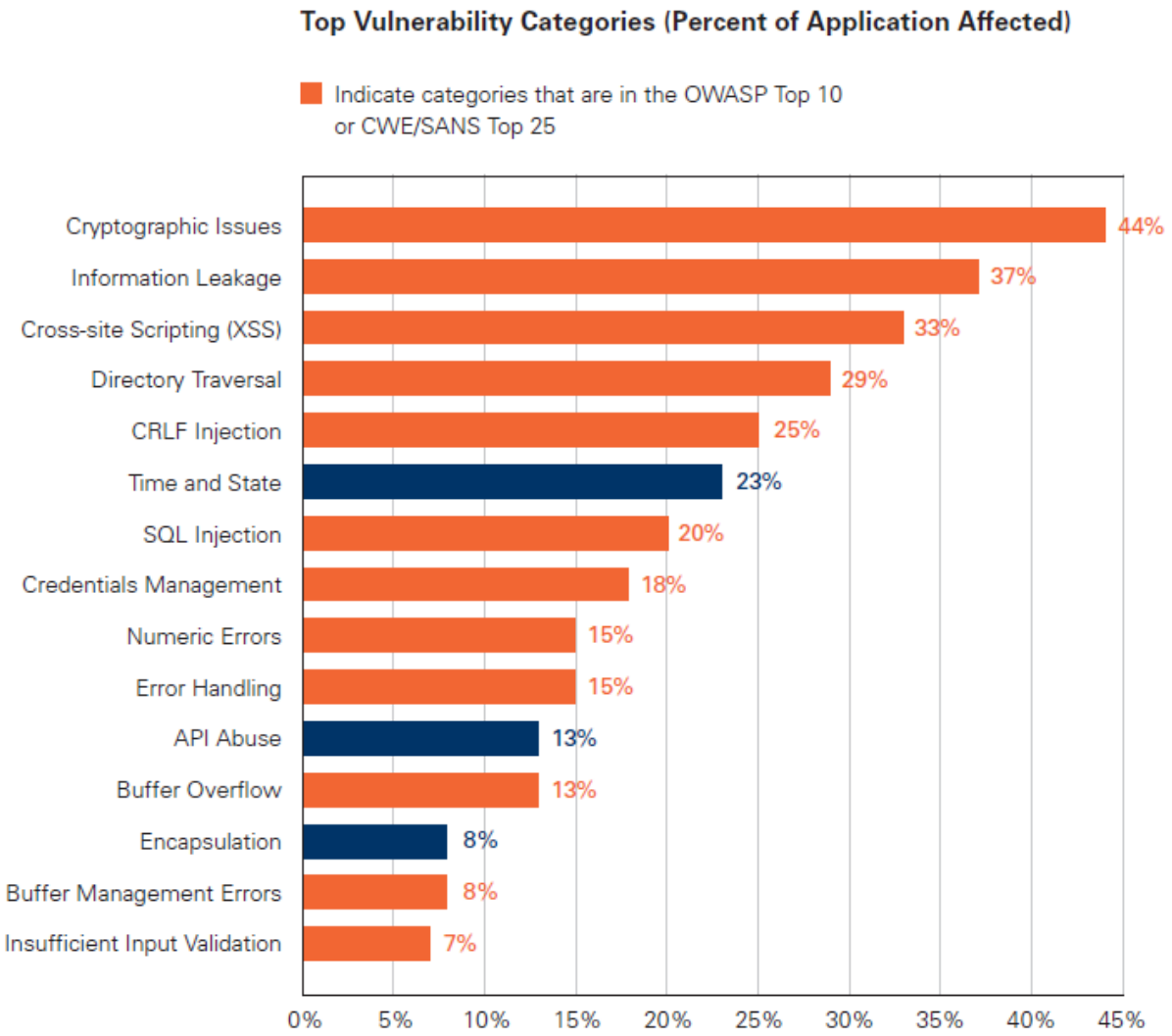
Supplier Application Profiles

	C/C++	Java	.NET
Internally Developed	22%	53%	25%
Commercial	44%	35%	21%
Open Source	45%	54%	1%
Outsourced* (Low sample size)	0%	67%	33%

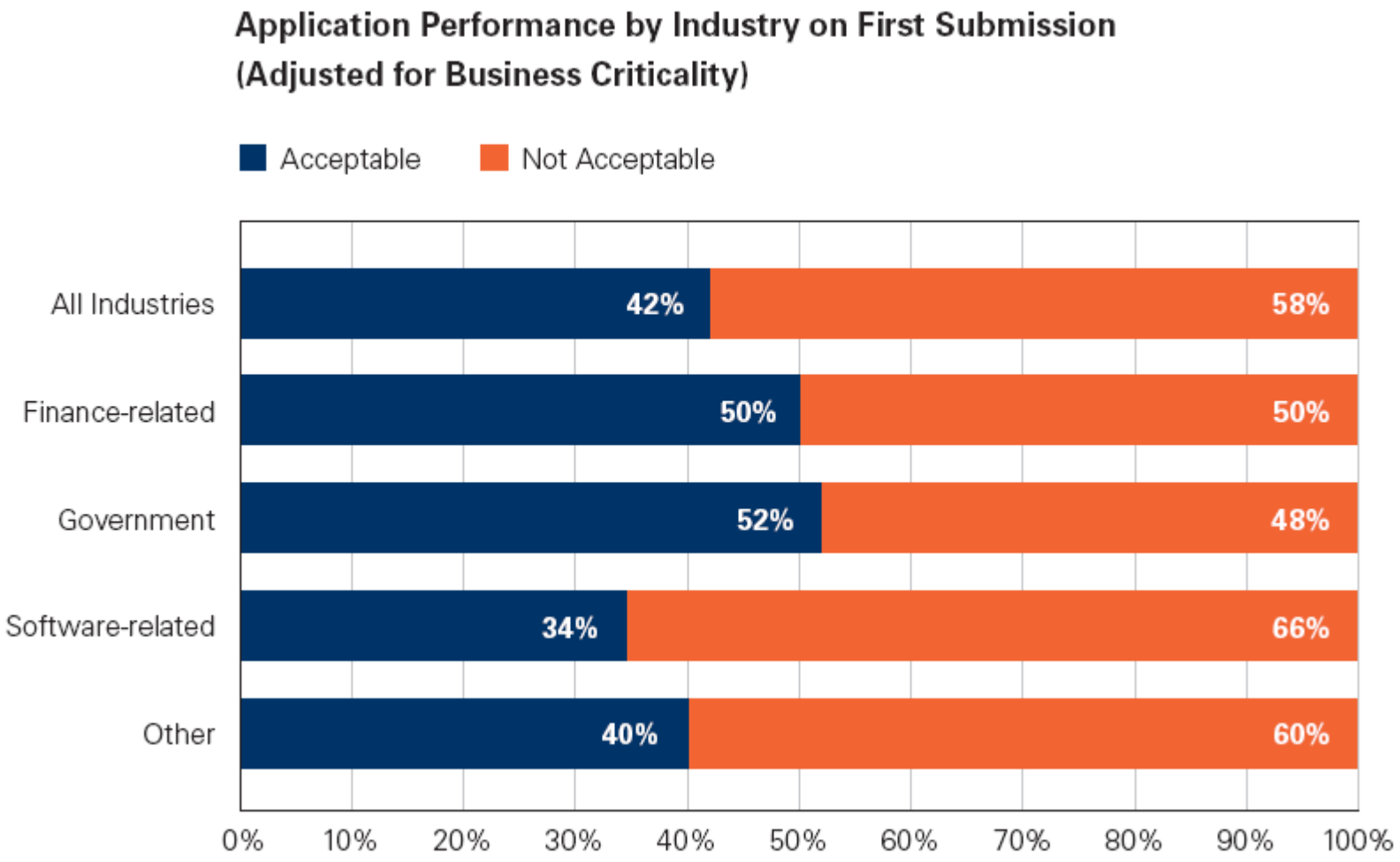
Easily Remedied Vulnerabilities Remain Pervasive



Easily Remedied Vulnerabilities Remain Pervasive



Finance and Government are Better

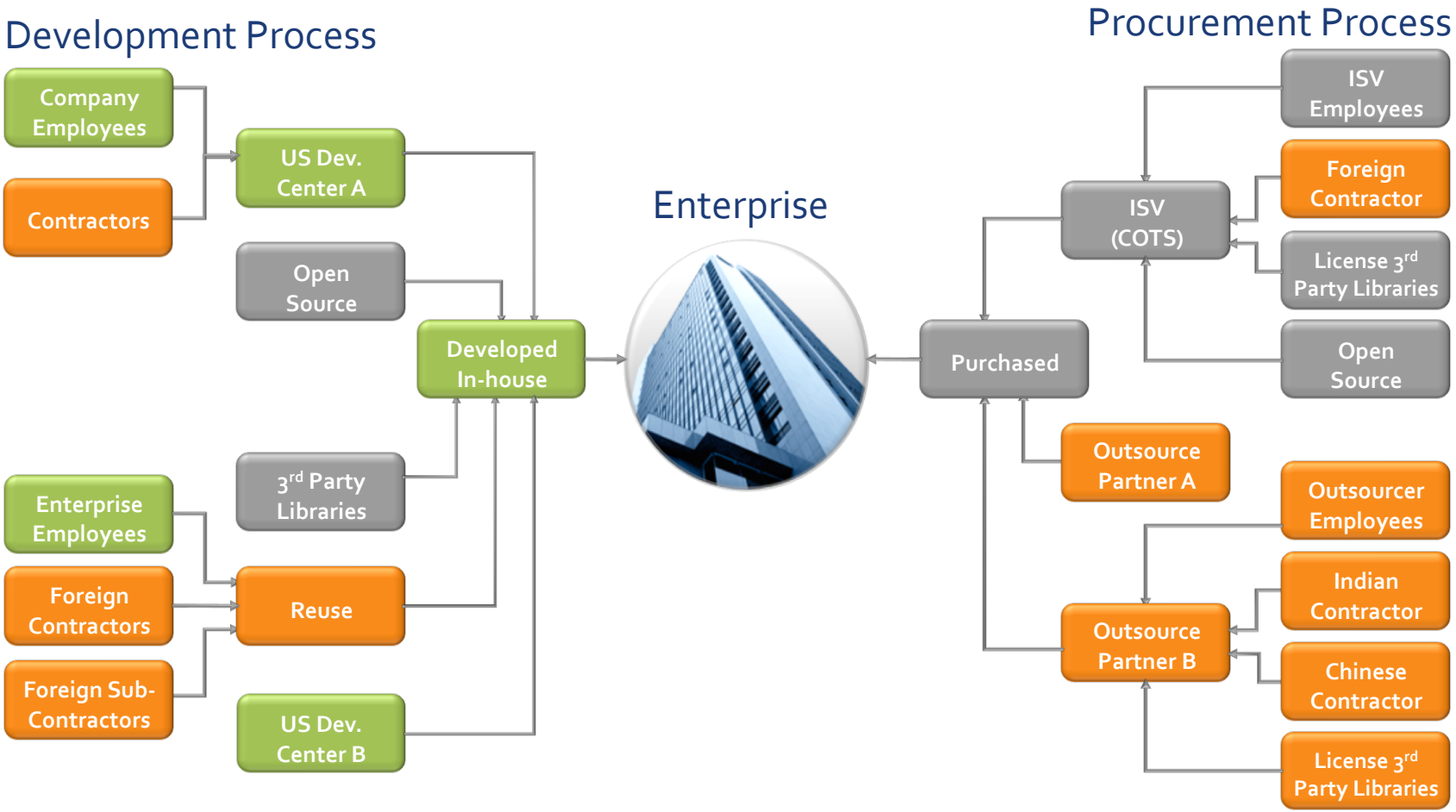


Finance and Government are Better?!

Vulnerability Distribution by Industry

Finance-related		Software-related		Government	
Cross-site Scripting (XSS)	35%	Cross-site Scripting (XSS)	19%	Cross-site Scripting (XSS)	53%
Information Leakage	21%	Information Leakage	17%	Information Leakage	12%
CRLF Injection	5%	Numeric Errors	11%	CRLF Injection	6%
Cryptographic Issues	5%	Buffer Overflow	8%	Buffer Mgmt Errors	4%
Directory Traversal	3%	Cryptographic Issues	6%	SQL Injection	3%

Outsourced Software is Assessed the Least



More Resources

- Download the report, plus other whitepapers, webcasts, and educational resources
  - http://veracode.com/resources
  - Volume 2 due out in July/August timeframe
- Veracode ZeroDay Labs Blog
  - http://veracode.com/blog
- Contact info
  - Email: ceng@veracode.com
  - Twitter: @chriseng
  - Phone: 781.425.6040