VERACODE

Application Security: Why Does It Take So Long?

Chris Eng
Tactical Edge
Bogota, Colombia
March 13, 2019

Software security is surprisingly difficult

- Poorly written software results in vulnerabilities that put customers and their sensitive data at risk
- We understand software vulnerabilities pretty well, but things aren't improving very quickly – why not?
- When we have a massive software security data set, we can extract some interesting learnings that may help us improve

My background

- Vice President of Research
- 20 years in application security: building, breaking, and defending software
- Leads all security research initiatives at Veracode
- Previously: US Dept of Defense, @stake, Symantec (via acquisition)

Who are you?

Developer

Security

Operations

Other

Context

All companies are software companies

Airbnb makes its money in real estate. But everything inside of **how Airbnb runs has much more in common with Facebook or Google or Microsoft or Oracle than with any real estate company.** What makes Airbnb function is its software engine…. It's a tech company.

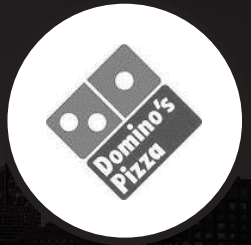
- Marc Andreesen, Investor

At its heart, **Tesla is a software developer dressed in a carmaker's robes…** This software focus affords Tesla a flexible and dynamic approach to updating its fleet, something that few, if any, other carmakers have been able to accomplish.

- Leah Niu, Motley Fool

Digital sport, as we call it at Nike, is incredibly important to us. We think it's going to be a bigger and bigger factor in terms of the experience that consumers have with the products that we create….**We are focusing more on the software side of the experience.**

- Mark Parker, CEO



Domino's has almost turned itself into a technology company that maybe just happens to sell pizza on the side. We look at metrics like orders per minute, actual transactions out to stores, and that can tell us what customers are ordering, in real time.

- Russ Turner, IT Manager

Apps Tied to Bottom Line

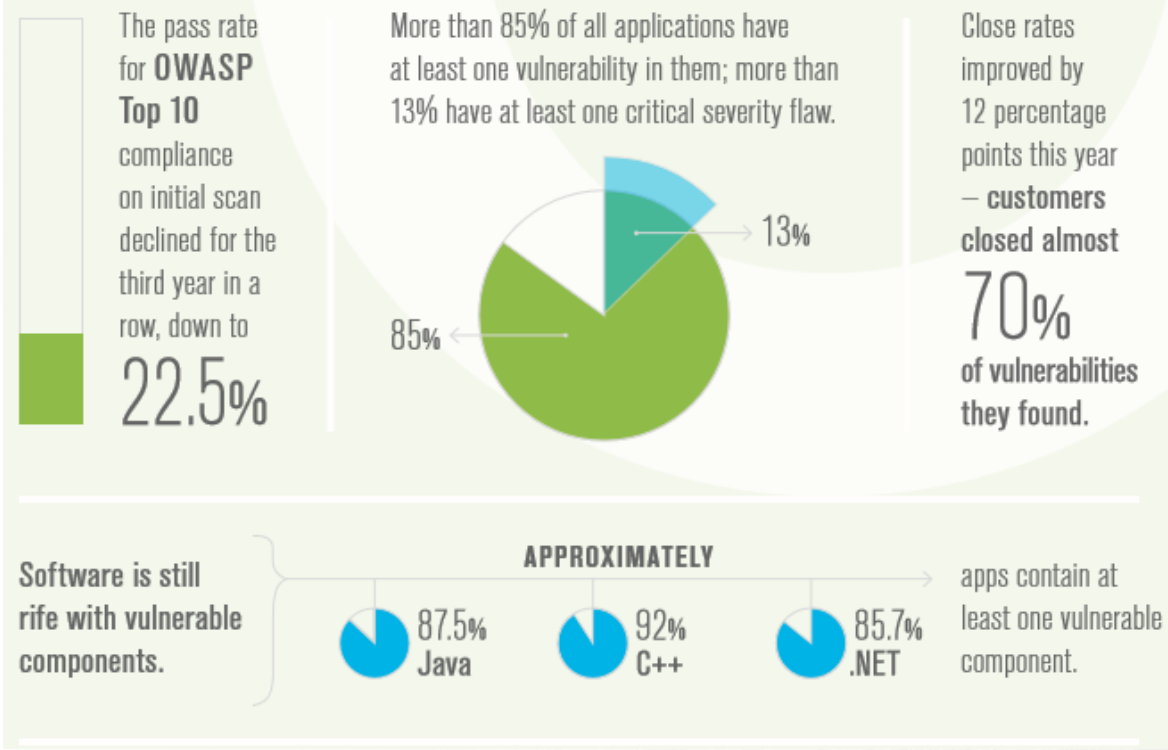
78% of enterprises believe that the shift to becoming a software-driven business will be a critical driver of competitive advantage. Over 40% say it is already affecting new product and service development. [1]

State of Software Security Volume 9

- Largest quantitative study of application security findings
- Based on data from over 700,000 application scans over a 12-month period representing 2 trillion lines of code
- Insights into industry performance, third-party component risks, vulnerability trends, and remediation rates
- Partnered with data scientists at Cyentia Institute to analyze the data set

So what's new?

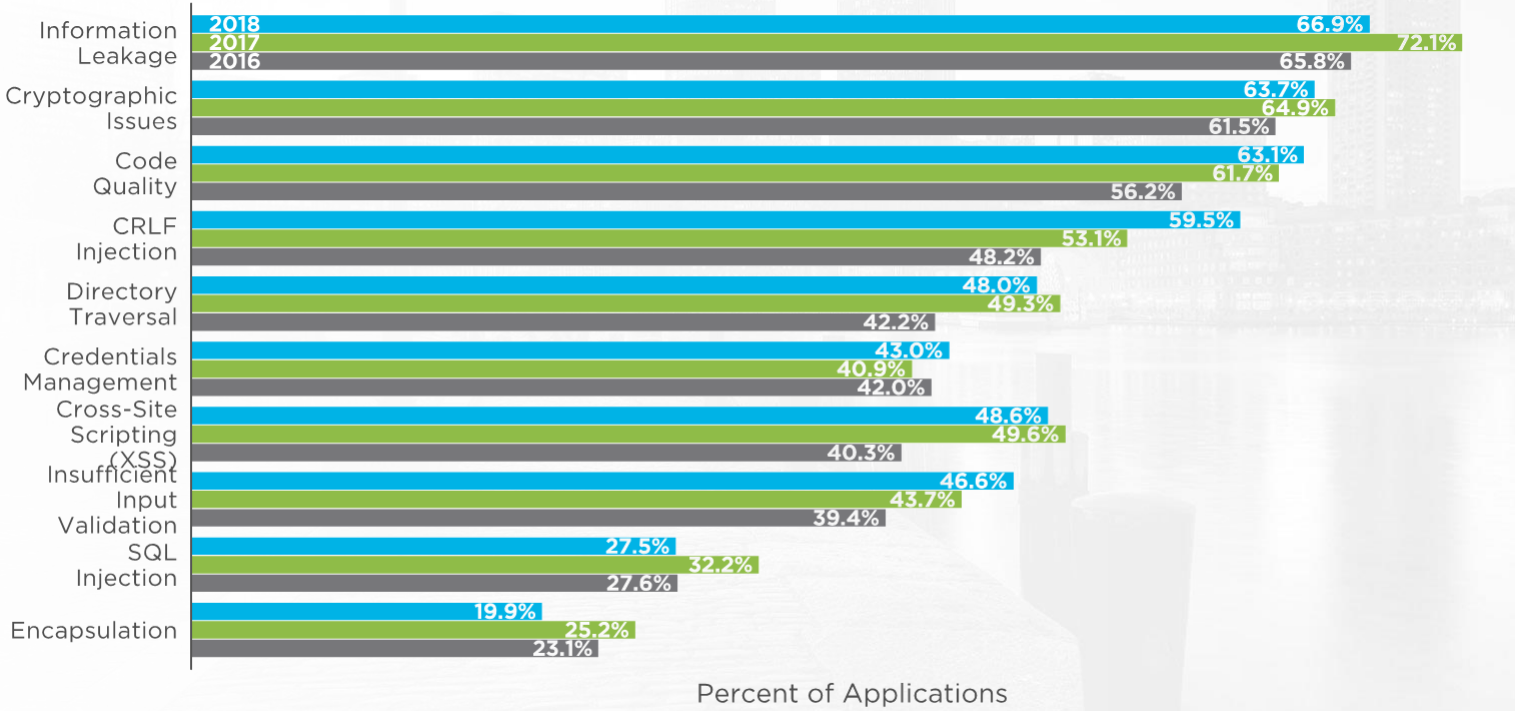
The more things change…



The most common vulnerabilities present in applications remained largely the same:

- SQL injection is still present in nearly one in three applications
- Cross-Site Scripting is found in nearly 50% of applications

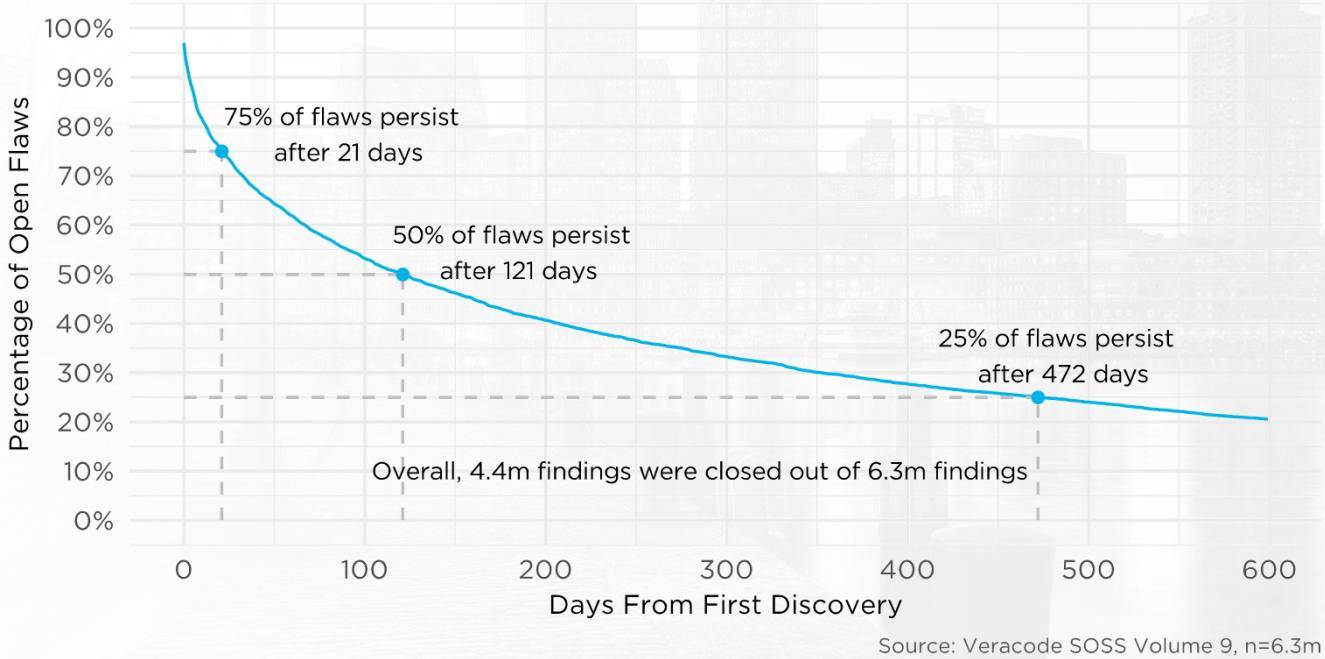
Prevalence of common flaw categories



Source: Veracode SOSS Volume 9, n=(2018:25.7k)

Focus on fixing

Flaw persistence



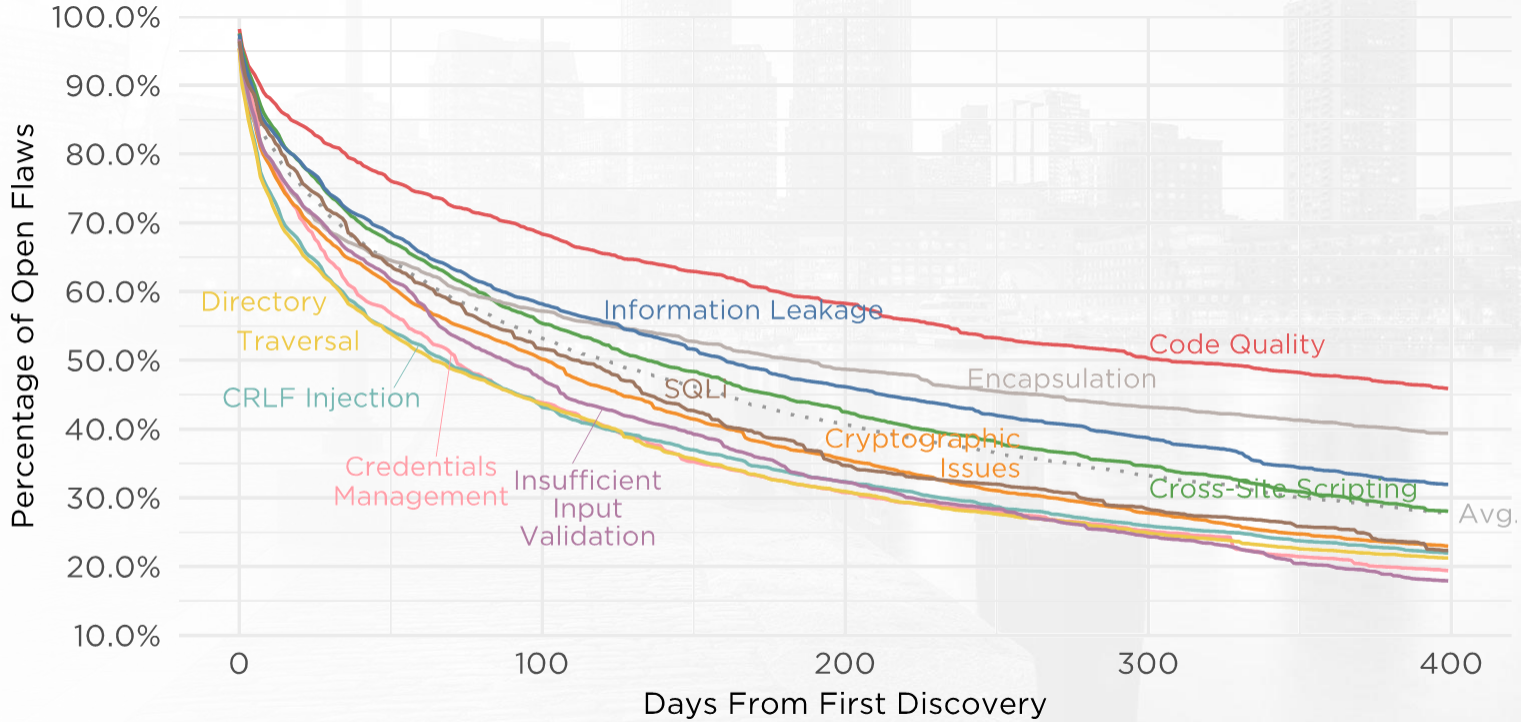
Source: Veracode SOSS Volume 9, n=6.3m

Flaw persistence analysis: the probability that a vulnerability will remain in an application over time

Overall flaw persistence interval

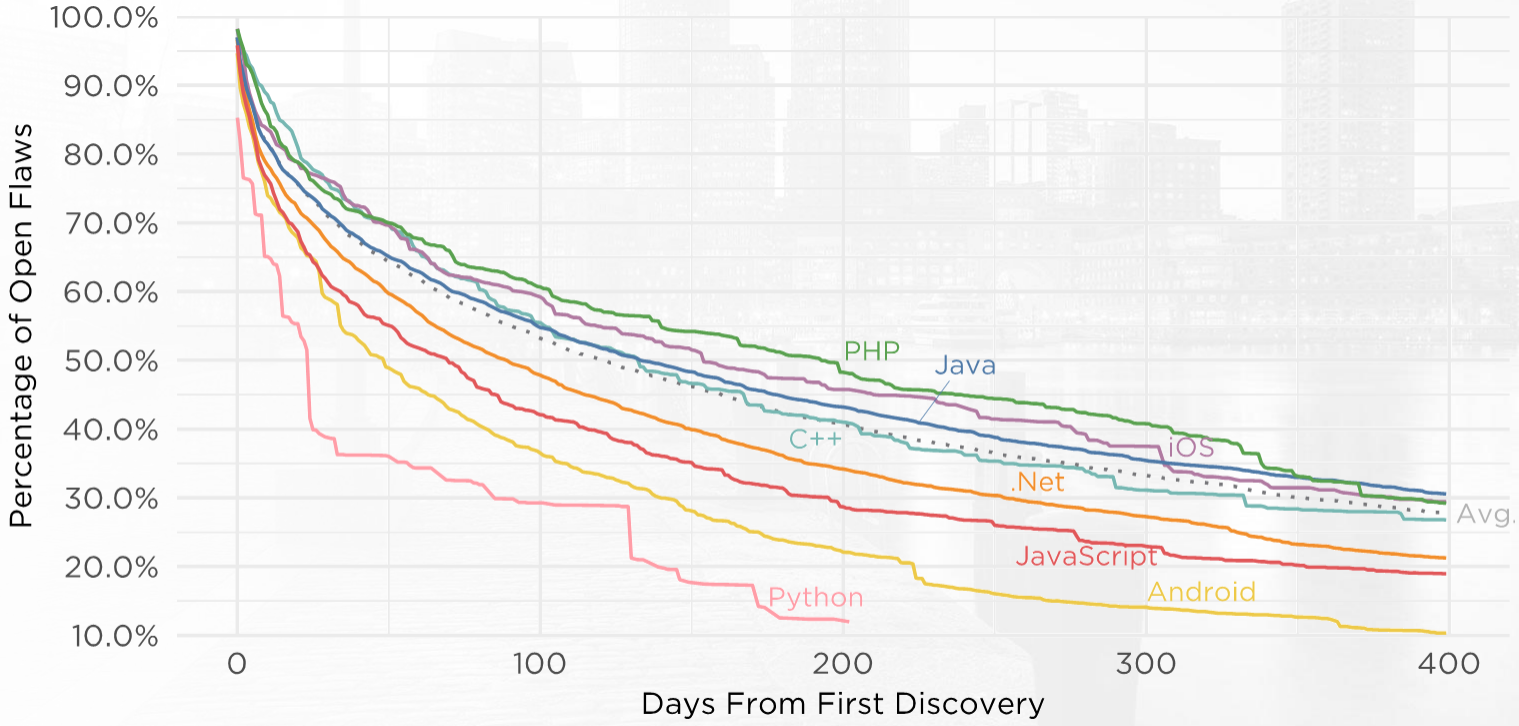
Source: Veracode SOSS Volume 9

Flaw persistence by flaw category



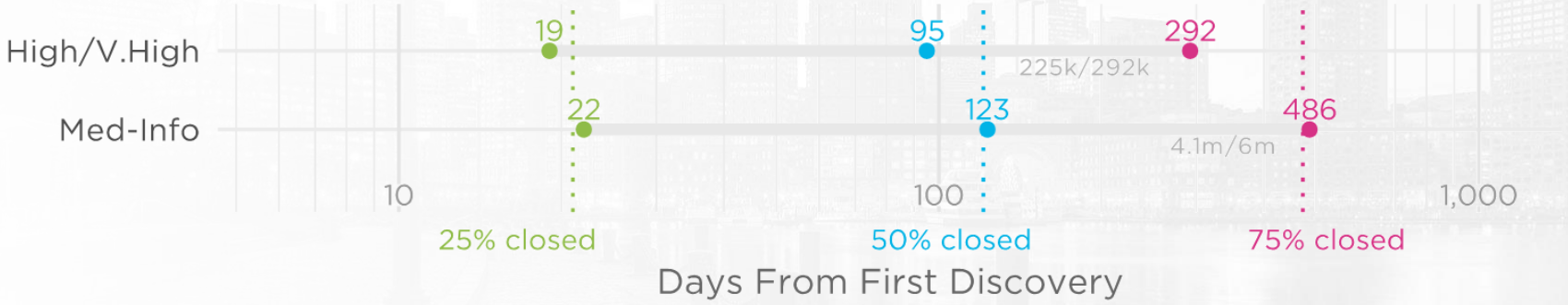
Source: Veracode SOSS Volume 9

Flaw persistence by language



Source: Veracode SOSS Volume 9

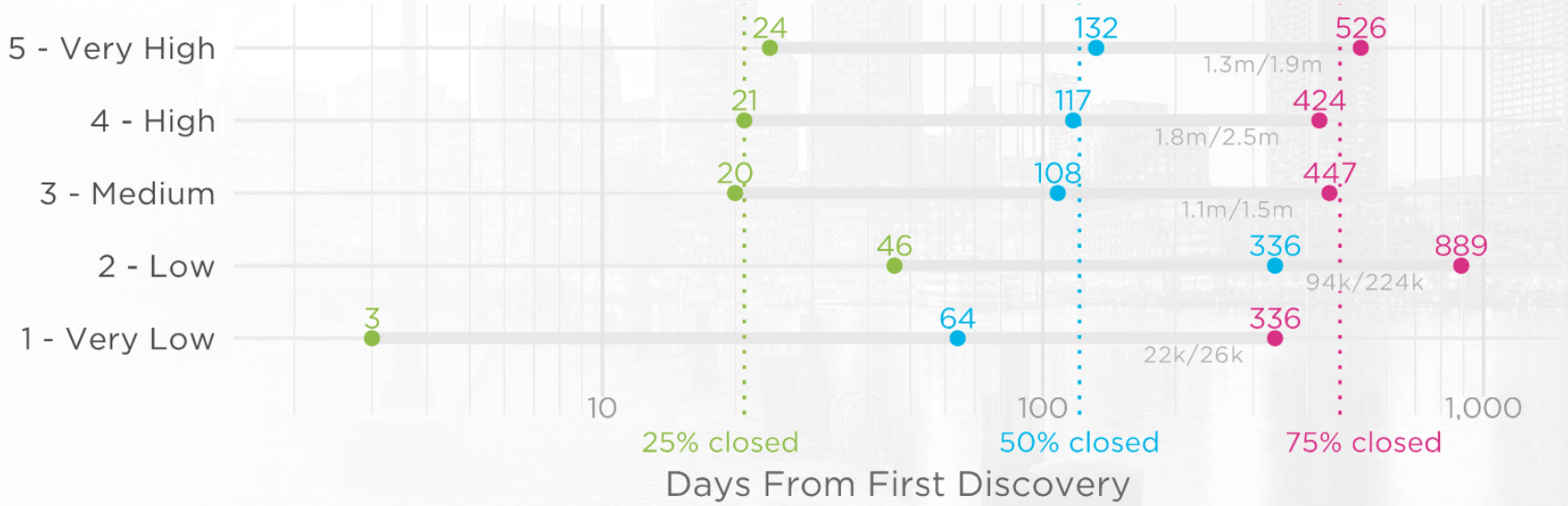
Flaw persistence by flaw severity



Source: Veracode SOSS Volume 9

You'd think higher severity flaws would be fixed faster
(but you'd be wrong)

Flaw persistence by app criticality



Source: Veracode SOSS Volume 9

You'd think flaws in business-critical apps would be fixed <u>much</u> faster
(but you'd be wrong)

The DevOps effect

What is DevOps?

DevOps is a **cultural and professional movement**, focused on how we build and operate high velocity organizations, born from the experiences of its practitioners.

– **Nathan Harvey**
Developer Advocate @ Google
(formerly VP Community Development @ Chef)

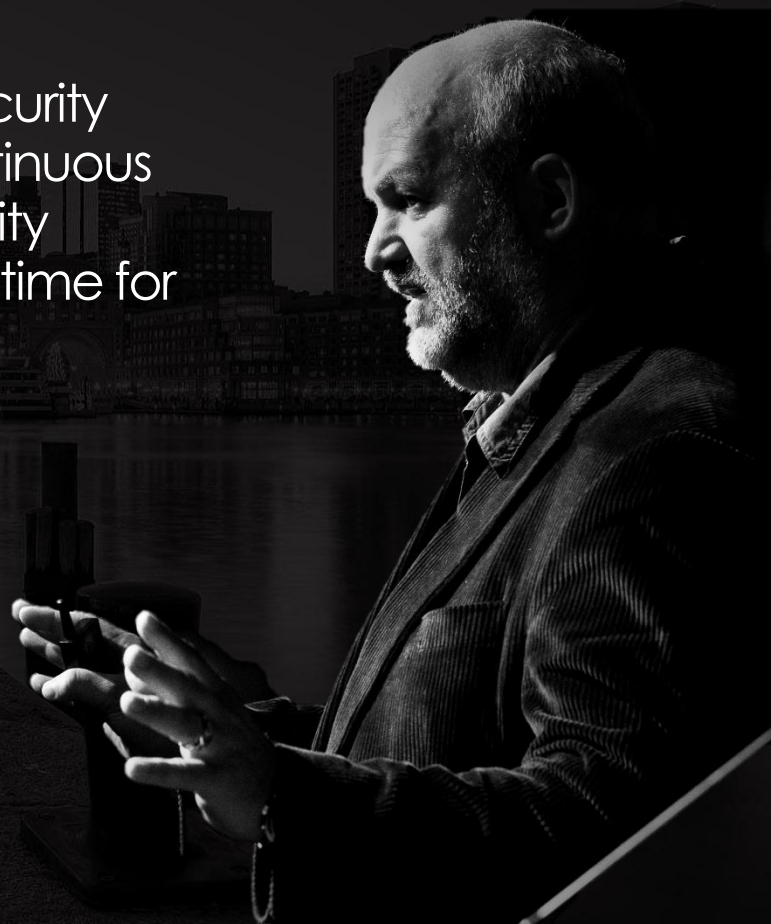
The evolving developer mindset

01

Security is **everyone's job** now, not just the security team's. With continuous integration and continuous deployment, all developers have to be security engineers... We move too fast for there to be time for reviews by the security team beforehand.

That needs automation, and it needs to be **integrated into your process**. Each and every piece should get security integrated into it... before and after being deployed.

– **Werner Vogels, Amazon CTO**
at AWS re:Invent 2017



DevOps is changing the way developers work

01

67%

Stated they actively work at an organization that practices DevOps; 50% are practicing continuous delivery

Source: Jenkins

46x

High performing organizations deploy code 46x faster their peers

Source: Puppet Labs

440x

High performing organizations commit changes 440x faster their peers

Source: Puppet Labs

34%

34% of developers say they build multiple times per day or during check-in

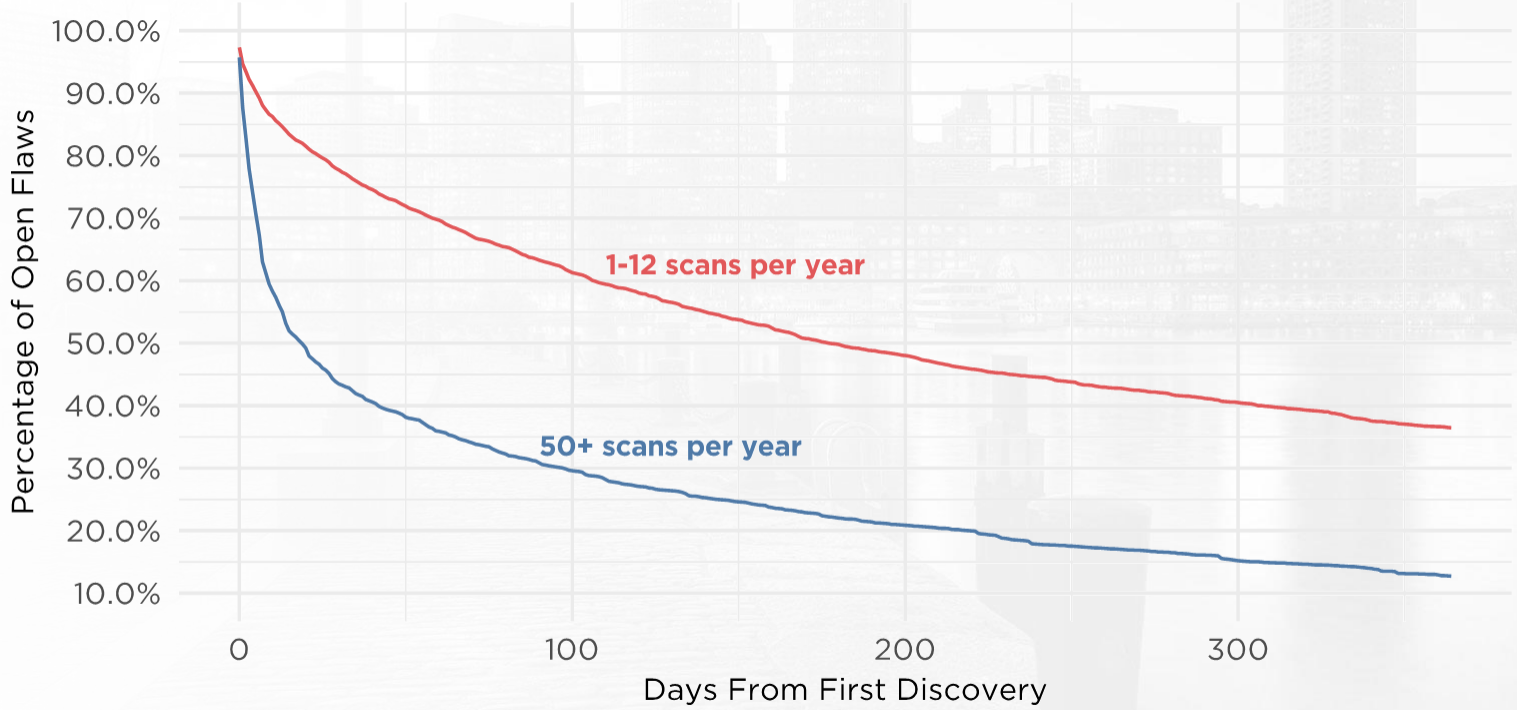
Source: Forrester

>1hr

High performing organizations have less than one hour of lead time to make changes

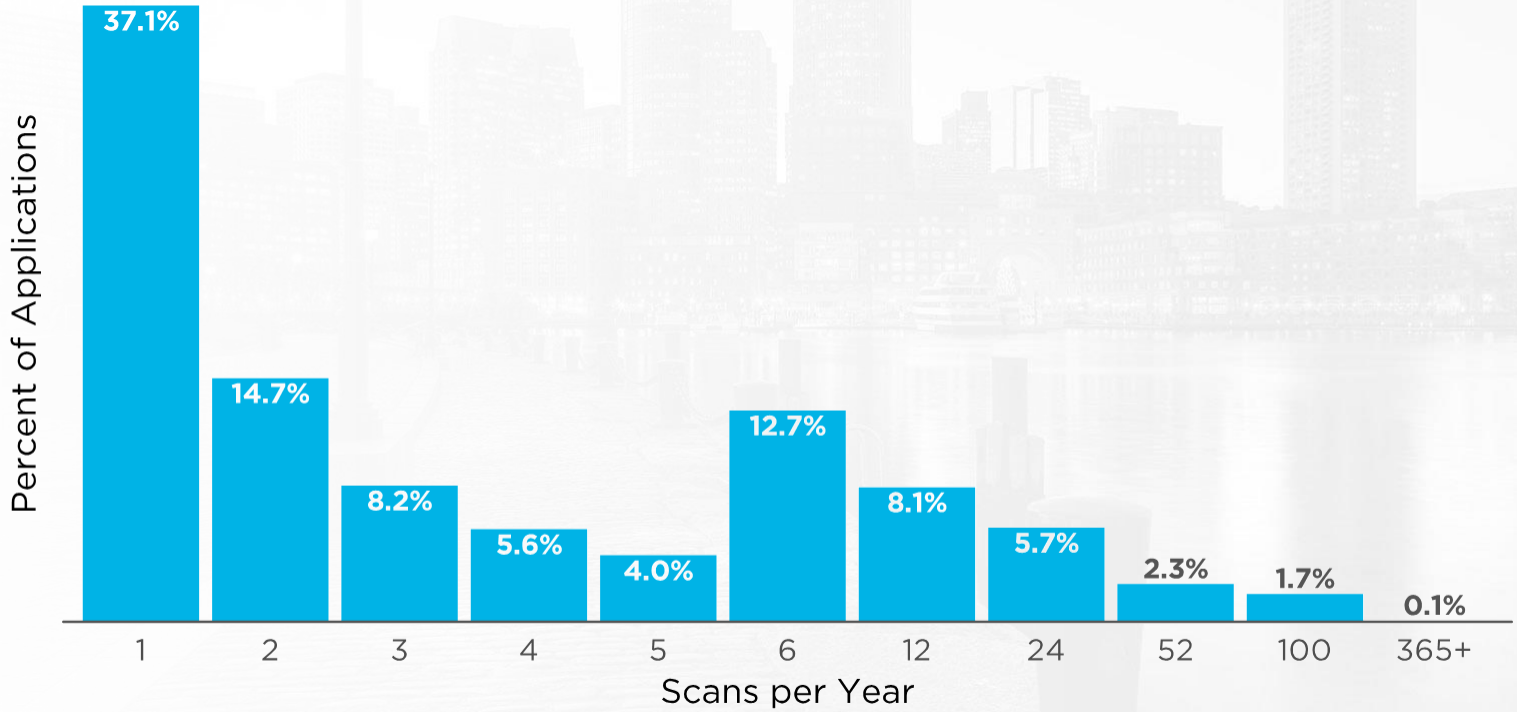
Source: Puppet Labs

Scan frequency as a proxy for DevOps



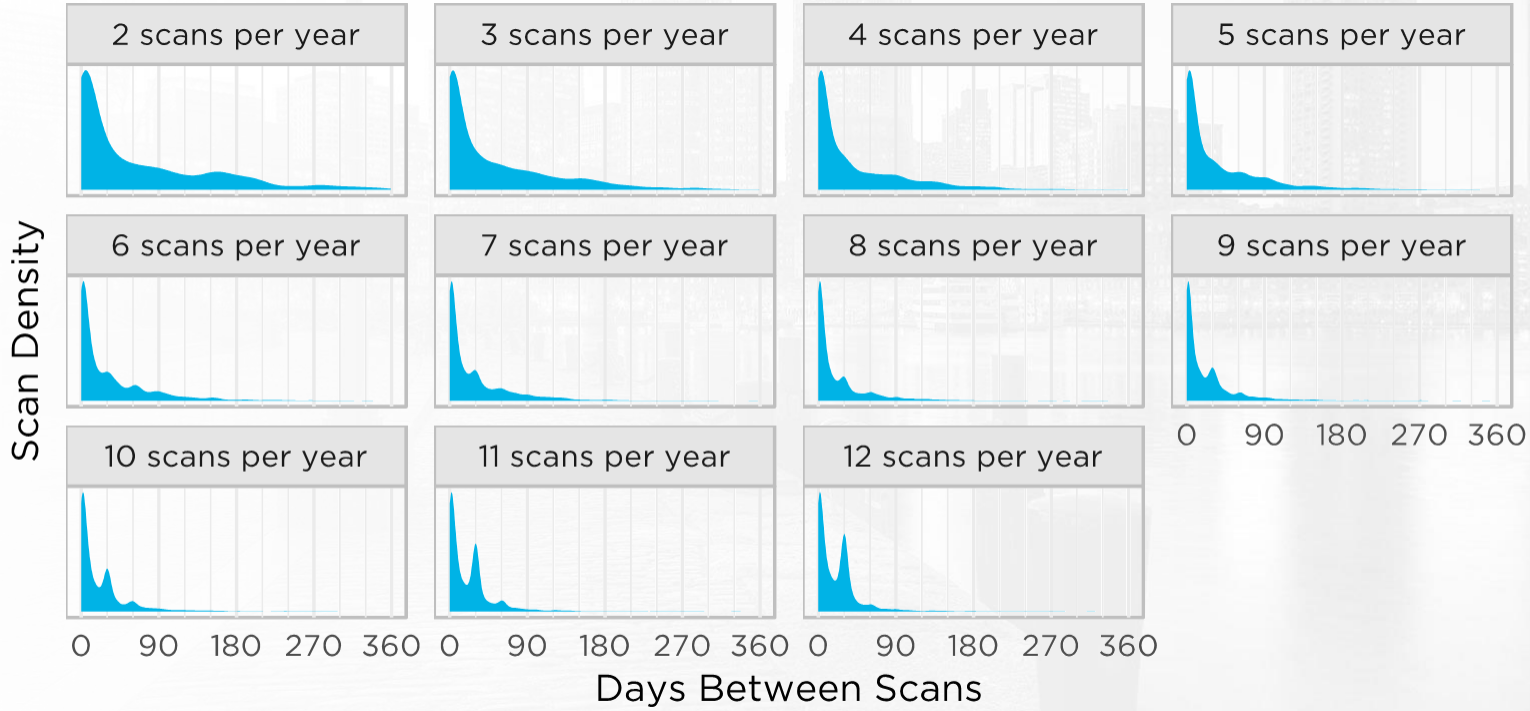
Source: Veracode SOSS Volume 9

Annual scan rates



Source: Veracode SOSS Volume 9, n=33.3k Static Scans

Days between scans based on annual rate



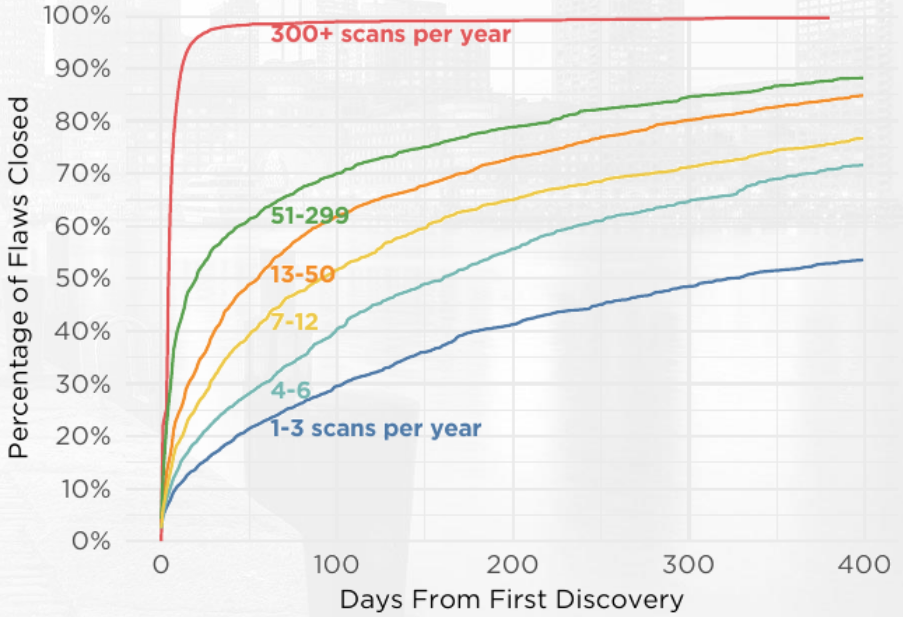
Source: Veracode SOSS Volume 9

DevSecOps increases fix velocity (?)

Organizations that adopt DevOps practices outperform their peers in how quickly they fix flaws; the most active DevSecOps programs fix flaws more than **11.5x faster** than the typical organization.

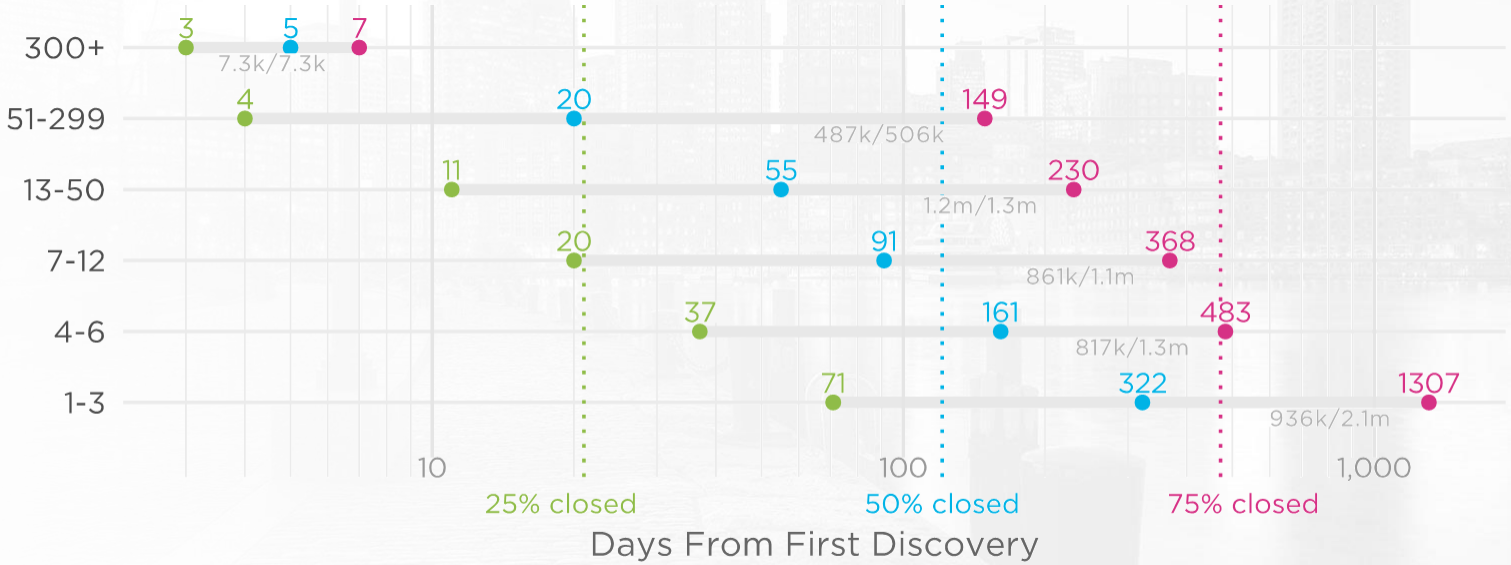
Flaws persist **3.5x longer** in applications only scanned 1 to 3 times per year compared to ones tested 7 to 12 times per year.

FIG. 43: Fix Velocity Based on Scan Frequency



Source: Veracode SOSS Volume 9

Same chart, with numbers

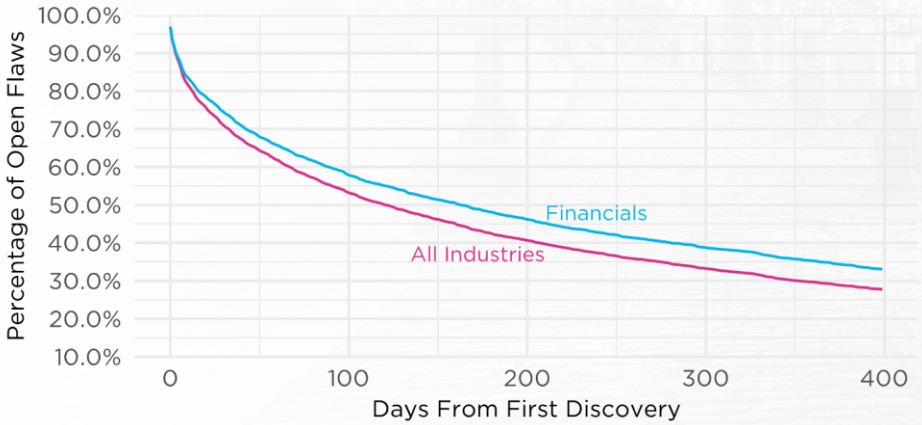


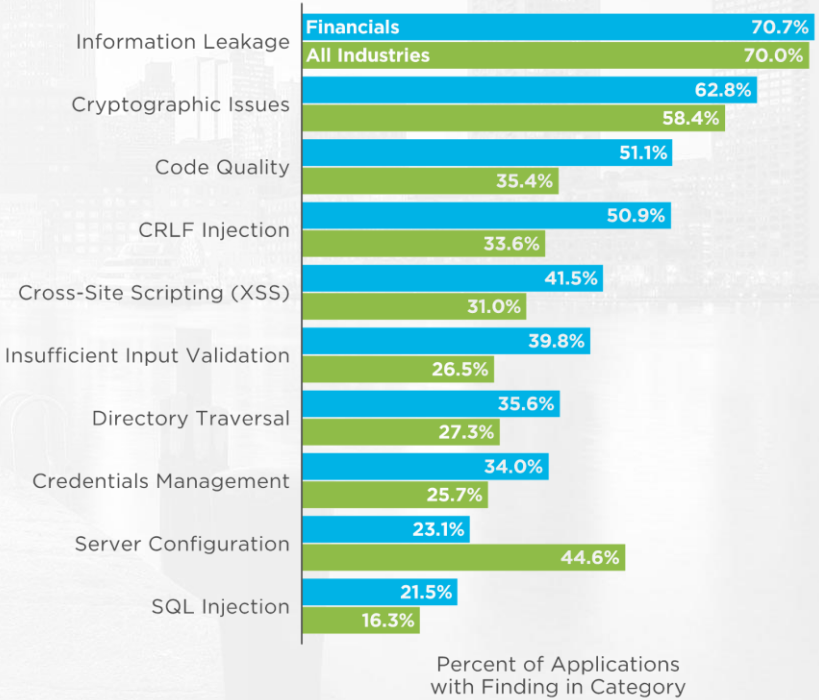
Source: Veracode SOSS Volume 9

Financial industry spotlight

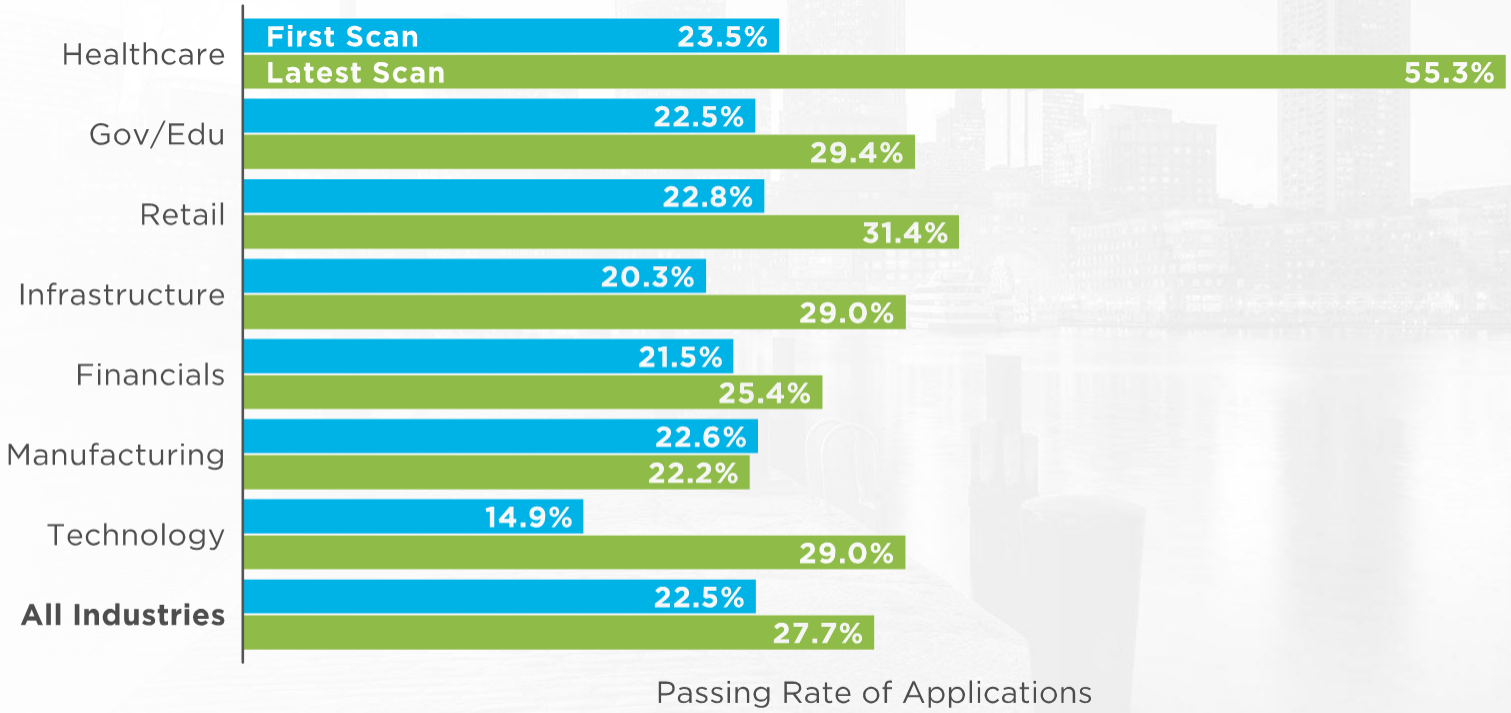
Financial industry overview

Source: Veracode SOSS Volume 9, n=25,790





OWASP pass rates by industry

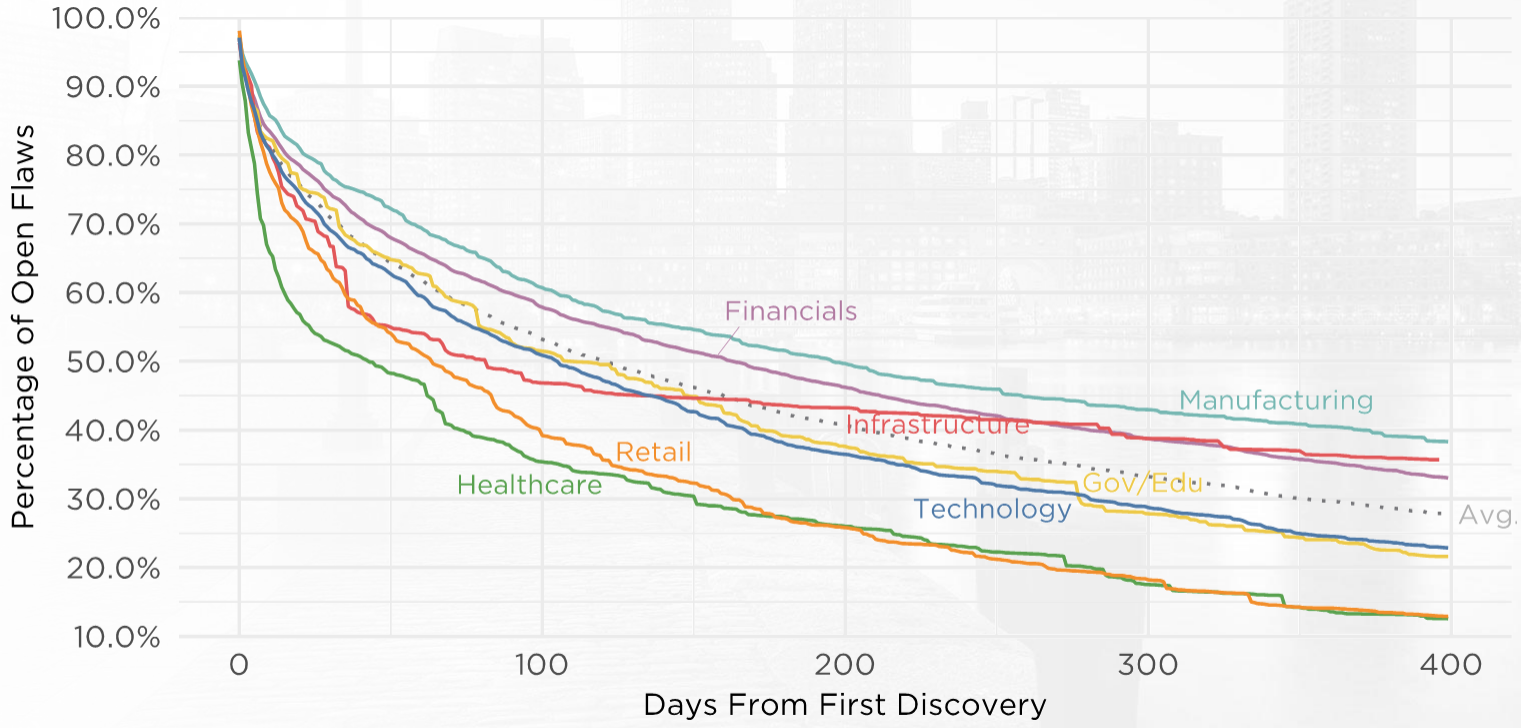


Source: Veracode SOSS Volume 9

Vulnerability categories by industry

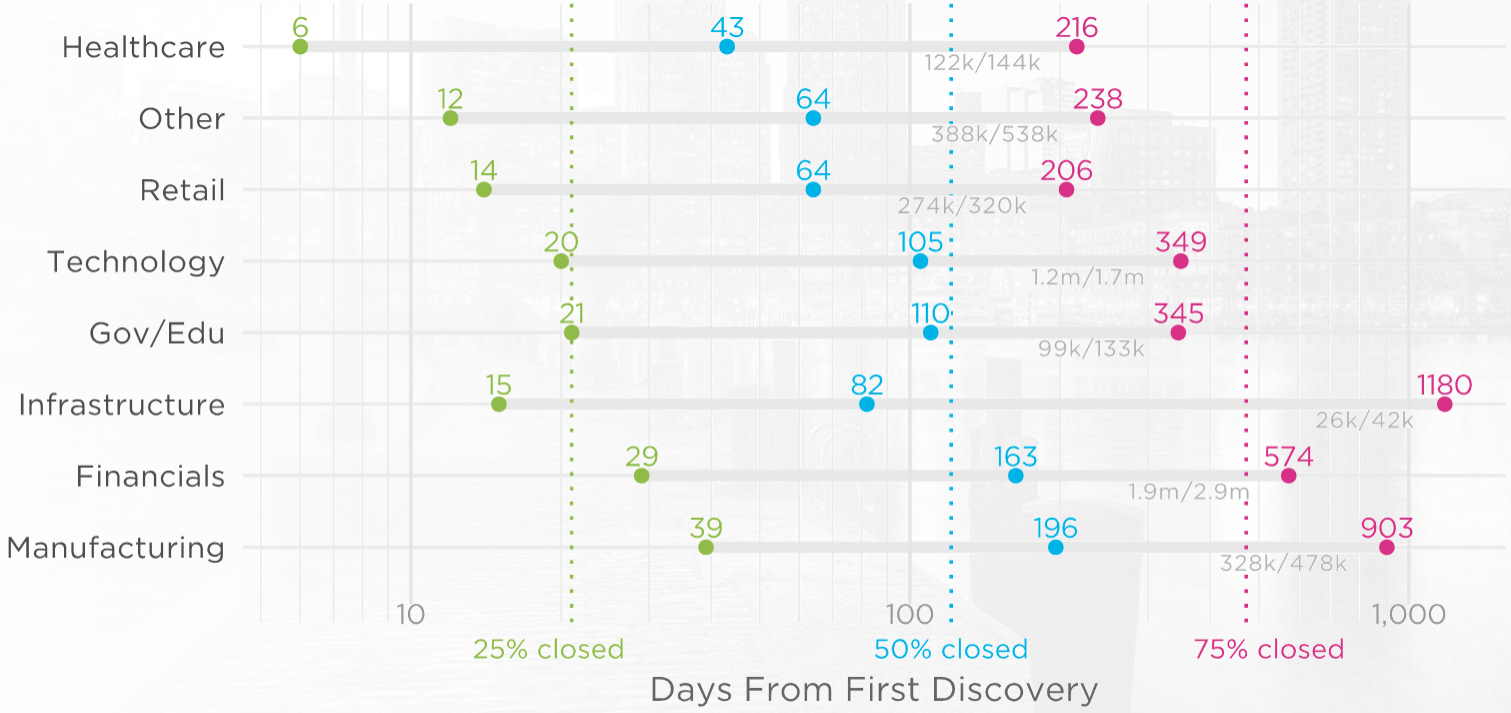
	Overall	Financials	Gov/Edu	Healthcare	Infrastructure	Manufacturing	Retail	Tech
API Abuse	12.3%	11.4%	10.7%	9.4%	6.5%	11.7%	9.8%	16.5%
Authentication Issues	3.3%	2.6%	0.5%	1.9%	5.2%	4.7%	2.8%	4.1%
Authorization Issues	3.5%	2.8%	1.7%	2.9%	2.5%	3.4%	2.7%	4.8%
Buffer Management Errors	3.5%	1.3%	0.2%	3.9%	0.7%	3.9%	1.4%	9.1%
Buffer Overflow	3.0%	0.7%	0.3%	4.2%	0.2%	3.4%	1.2%	8.9%
Code Injection	7.9%	6.6%	4.8%	6.1%	8.2%	6.2%	9.2%	10.3%
Code Quality	63.1%	62.7%	59.1%	59.4%	63.1%	61.6%	65.0%	64.2%
Command or Argument Injection	13.7%	11.0%	6.7%	14.2%	5.7%	12.3%	13.2%	19.4%
Credentials Management	43.0%	40.2%	34.8%	39.8%	38.2%	36.9%	43.4%	50.1%
CRLF Injection	59.5%	62.5%	50.5%	50.3%	59.1%	55.6%	59.1%	56.6%
Cross-Site Scripting (XSS)	48.6%	48.9%	58.8%	44.5%	32.7%	44.0%	47.2%	48.5%
Cryptographic Issues	63.7%	61.0%	41.7%	62.1%	47.9%	59.3%	64.3%	70.1%
Dangerous Functions	2.1%	0.5%		2.9%		1.8%	0.5%	6.4%
Directory Traversal	48.0%	43.5%	37.9%	47.2%	32.9%	49.6%	51.0%	55.5%
Encapsulation	19.9%	21.0%	17.3%	15.0%	12.5%	17.9%	18.9%	20.5%
Error Handling	7.7%	4.5%	1.9%	10.4%	2.7%	9.1%	4.9%	14.5%
Information Leakage	66.9%	67.3%	64.5%	63.8%	60.8%	61.7%	66.1%	67.8%
Insecure Dependencies	2.5%	2.3%	1.4%	2.9%	2.0%	2.7%	2.6%	2.7%
Insufficient Input Validation	46.6%	48.6%	50.4%	45.8%	45.4%	38.7%	46.3%	44.1%
Numeric Errors	3.1%	0.7%	0.2%	4.2%	0.2%	3.6%	1.1%	8.9%
Potential Backdoor	9.0%	5.8%	4.8%	12.6%	4.0%	8.0%	8.0%	16.4%
Race Conditions	8.1%	7.7%	6.1%	5.0%	3.0%	6.2%	6.2%	11.7%
Session Fixation	9.5%	10.6%	8.7%	7.1%	4.7%	9.1%	9.9%	8.4%
SQL Injection	27.5%	25.7%	24.0%	31.9%	13.7%	24.0%	31.5%	31.9%
Time and State	19.4%	17.2%	14.5%	19.3%	20.9%	17.8%	22.2%	24.1%
Untrusted Initialization	10.9%	8.6%	5.4%	16.8%	8.2%	8.2%	12.9%	15.5%
Untrusted Search Path	6.9%	4.8%	2.2%	9.7%	5.2%	6.5%	6.3%	11.3%

Flaw persistence by industry



Source: Veracode SOSS Volume 9

Flaw persistence by industry



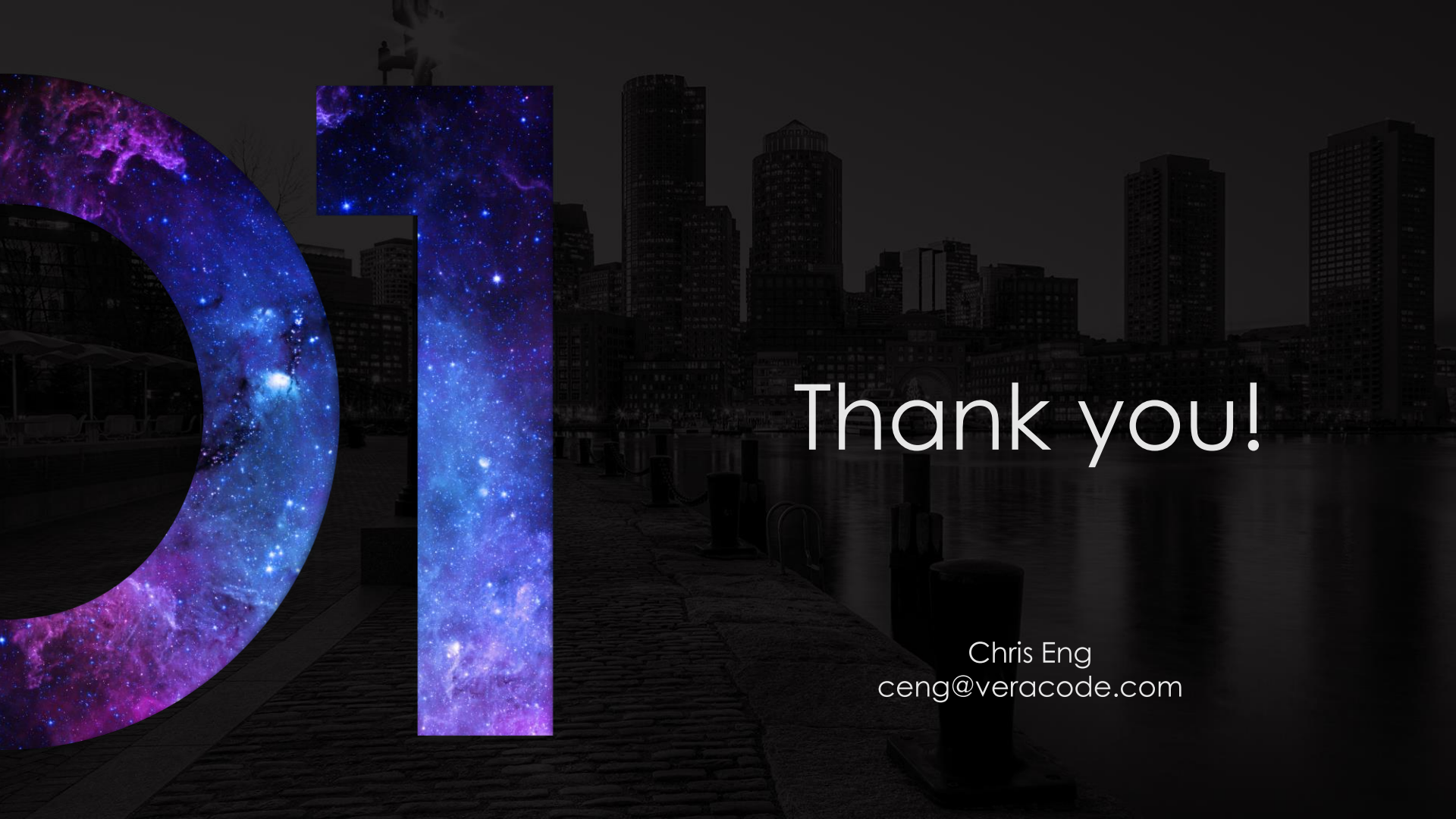
Source: Veracode SOSS Volume 9

Takeaways

- Organizations are getting better at fixing flaws, but there is still a long way to go
- Prevalence of the most common flaw categories is mostly the same year over year
- Several factors you'd logically expect to influence flaw remediation speed actually do not
- DevSecOps practices (specifically, scan frequency) correlate strongly with better fix rates

Suggested action plan

- Next you should:
  - Read the State of Software Security Report (http://veracode.com/soss)
  - Start talking to your peers in development/security about integrating application security in your development processes
- In the next three months you should:
  - Start training your developers on application security
  - Set achievable policies around vulnerability fix timeframes and measure developer compliance
  - Begin to inventory your applications to understand the risks associated with the use of third-party (e.g. open source) components
- Within six months you should:
  - Work with your development teams to implement application security into your development toolchain(s) – **figure out how to increase scan frequency**!


01
Thank you!
Chris Eng
ceng@veracode.com