AppSec Current State
The Big 5 Activities

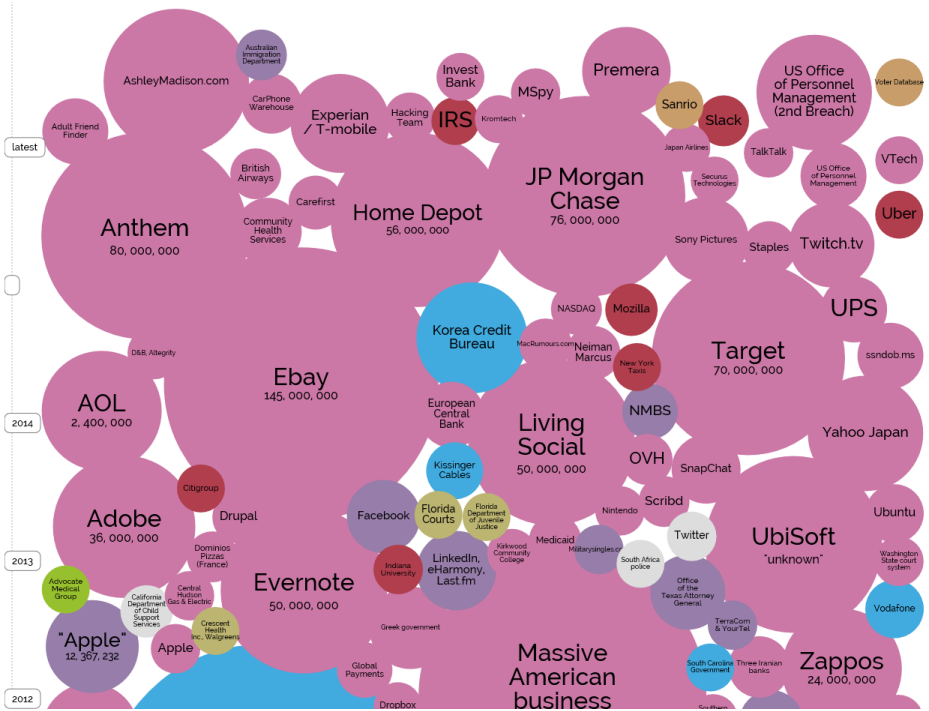
Aravind Venkataraman

Agenda

- AppSec need and current spend
- What are firms doing?
- Manage how?
- Integrate how?
- Measure how?
- Mature how?

Cigital

App Sec is a Big Problem

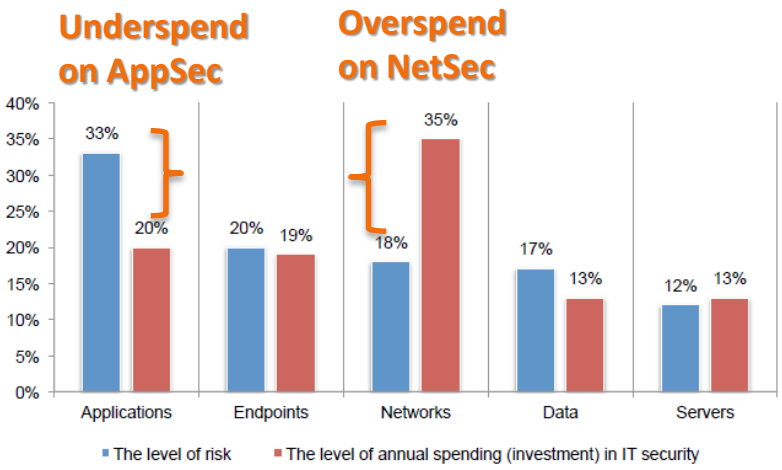


- accidentally published
- configuration error
- hacked
- inside job
- lost/stolen computer
- lost/stolen media
- poor security

Source: www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Cigital

What are we investing?



- "The Increasing Risk to Enterprise Applications," Figure 10, Ponemon Institute, Nov 2015

App Sec Spending	%
Inadequate	43%
Adequate	18%
> Adequate	3%
No opinion	18%

34% don't know what % of IT budget spent on app sec

-SANS 2015 State of Application Security, P 15

92% of reported vulnerabilities are in applications, not in networks – NIST

Over 70% of vulnerabilities exist at the application layer, not network - Gartner

Cigital

The Top 12 App Sec Things ‘Everybody’ Does

1. Identify gate locations and gather necessary artifacts, 84%
2. Identify PII obligations, 78%
3. Provide awareness training, 76%
4. Create a data classification scheme and inventory, 65%
5. Build/publish security features, 78%
6. Create security standards, 73%
7. Perform security feature review, 86%
8. Use automated tools along with manual code review, 71%
9. Drive tests with security requirements and security features, 85%
10. Use external penetration testers to find problems, 88%
11. Ensure host and network security basics are in place, 88%
12. Software bugs in ops fed back to development, 96%

Source: bsimm.com

Cigital

SANS Top-Ranked Activities

Defenders

Most useful security practices	Internal Apps
Penetration testing	54.2%
Application security training	61.8%
Identity/Access controls	56.5%
Dynamic analysis (vulnerability scanning)	45.8%
Application firewalls/Virtual patching	35.1%
Compliance reviews or audits	47.3%
Code review	43.5%
Threat modeling	31.3%
Static analysis (source or binary)	28.2%
Other	3.8%

Builders

AppSec Practice	Internal Apps
Risk and threat assessment	70.0%
Penetration testing	50.0%
Secure deployment standards and review	44.0%
Dynamic analysis (vulnerability scanning)	45.0%
Submit deployment processes for pen testing	36.0%
Static analysis (source or binary)	37.0%
Secure libraries/Frameworks	38.0%
Security assessment of third-party components	26.0%
Application integrity/Binary hardening	23.0%
Virtual patching	14.0%
Other	2.0%

Cigital

The Big 5

- Penetration Testing
- Code review
- Training
- Standards
- Architecture Analysis (incl. Threat Modeling)

Cigital

The 6th Thing?

Big 5

- Organization
- Integration

} "Management"

Cigital

Organization

Interpretations

- Make it formal + distributed
- Separation of duties scales better (governance/policy/execution)
- Deputize the devs: satellite correlates with better scores
- Tailor to your culture, structure

		Average			
Org Struct	Score	SSG	Sat	Devs	Ratio
Services	36	7	7	4,825	0.3%
Policy	41	10	16	8,630	0.3%
Hybrid S-P	46	16	16	2,300	1.4%
Bus. Unit	31	5	27	1,650	1.9%
Mangmt.	64	19	175	10,833	1.7%
Everyone	37	15	30	4,190	1.1 %

Source: bit.ly/gem-SSG

Cigital

Integration

% of App Sec Activities that depend on:

Touchpoint	%
Information Security	25
GRC	23
Defect Management	18
App Sec Portal	18
Incident Response	14
Project Management	14
Legal	14
Vendor Management	7

Source: bsimm.com

Cigital

Sidebar: Metrics

Why?

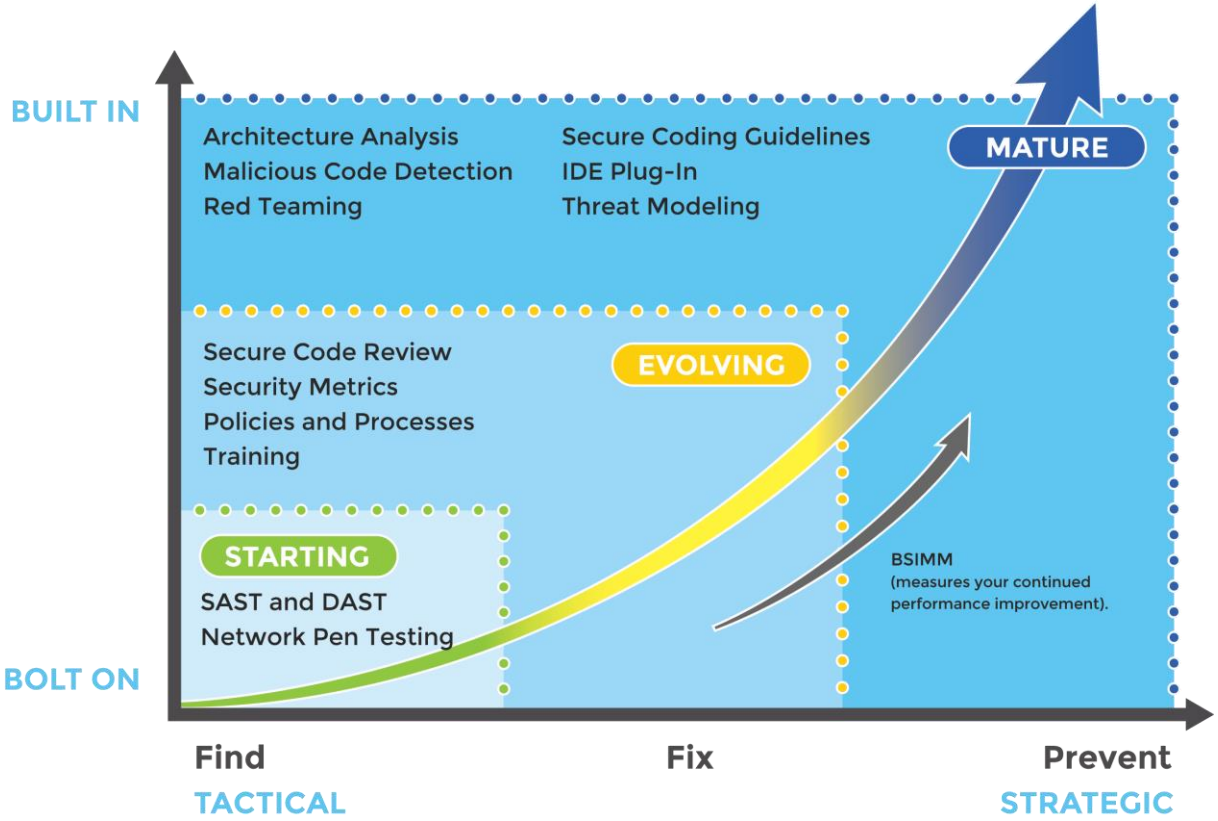
- Educate executives
- Publish for internal awareness
- Enforce the rules
- Drive budgets
- Evolve the program (portfolio view)

What

- The Big 5!
- 1st, 2nd order numbers
- Percent coverage (apps, devs…)
- Speed (time to fix criticals)
- $$$ (lower flaw density)

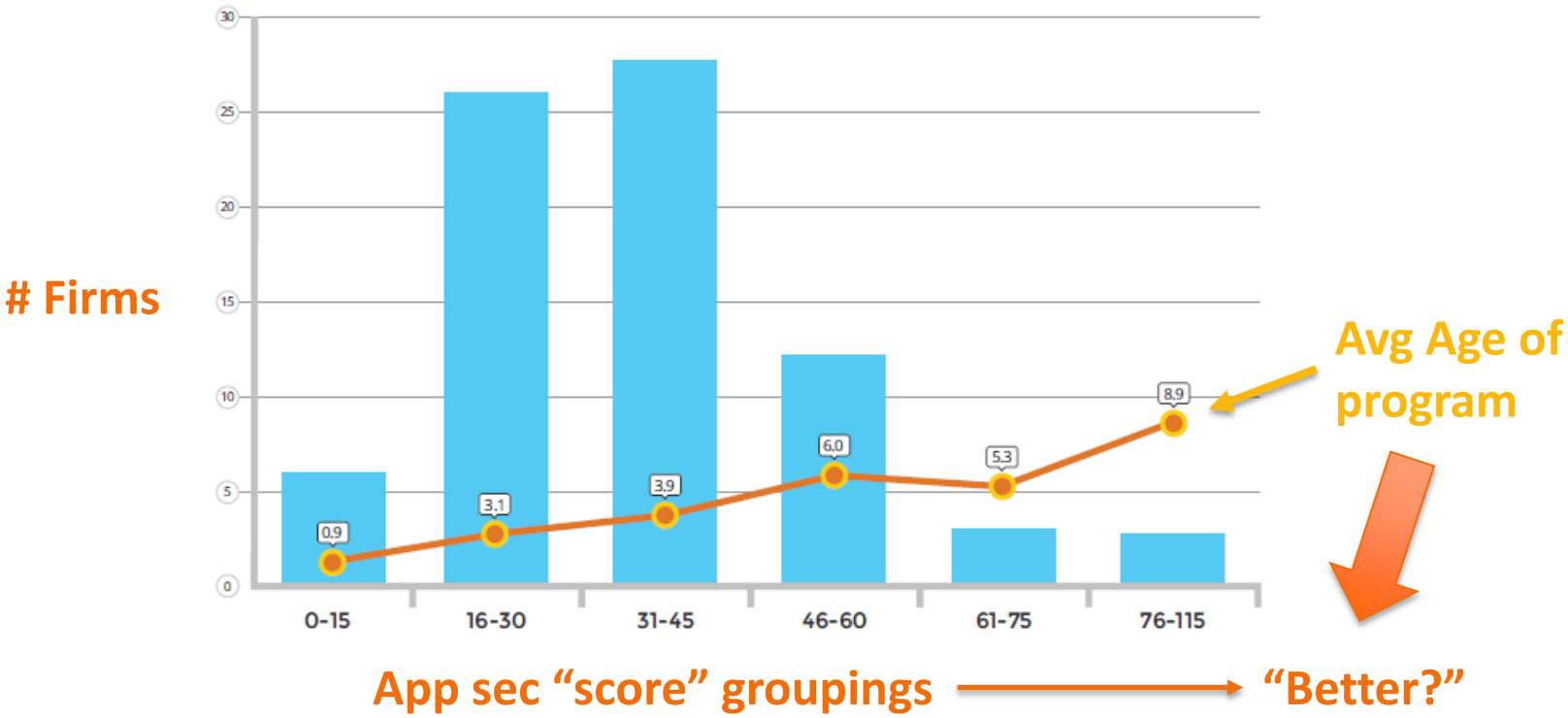
Cigital

How will you complete the picture?



Cigital

Start, Scale, *Sustain*



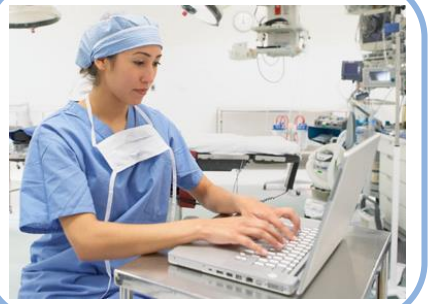
Source: bsimm.com

Cigital

Q&A

Backup Slides

It’s worse than it seems

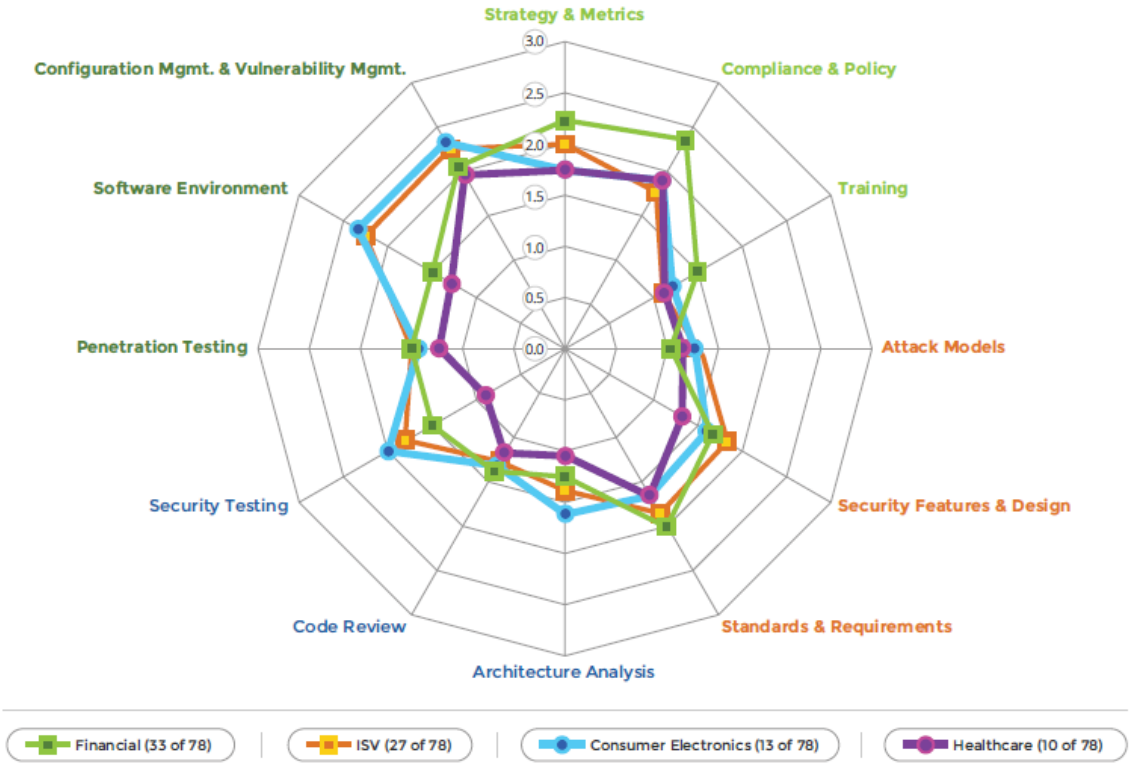


Cigital

It’s even worse than that

- Some industries have security maturity
- Others catching up
- Are you keeping up with peers?

Source: bsimm.com



Cigital

Other considerations

- Agile, DevOps, Continuous Integration/Development (CI/CD)
- “Special” tech, e.g. mobile, cloud, etc.
- WAF, RASP, IAST, etc.

Stick to the fundamentals! (adapt as needed)

More aligned: iterative + continuous = good for security too!

E.g. http://goo.gl/QSrIJc

Cigital

SANS: Who *tests* app sec?

Table 1. Who tests application security?

Answer Options	Response Percent
Internal security team	83.2%
External security consultants	29.6%
Quality assurance	22.4%
Development team	21.6%
Security-as-a-service providers	15.2%
Business unit owner	11.2%
Our commercial application vendors	5.6%
Other	3.2%

SANS 2015 State of Application Security

https://goo.gl/Q7liro

Cigital