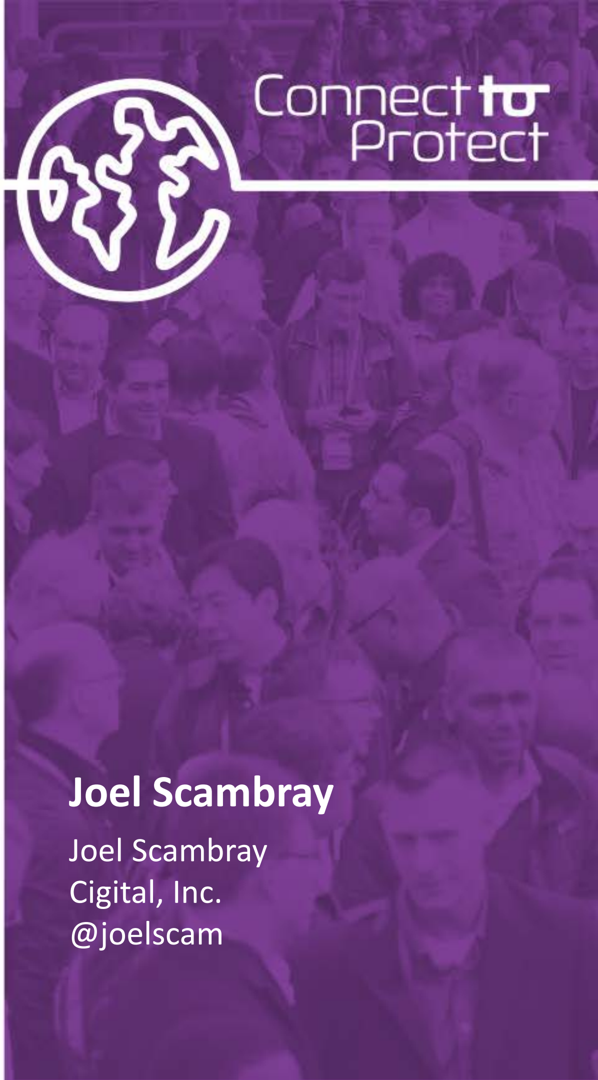
RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center



SESSION ID: CRWD-W05

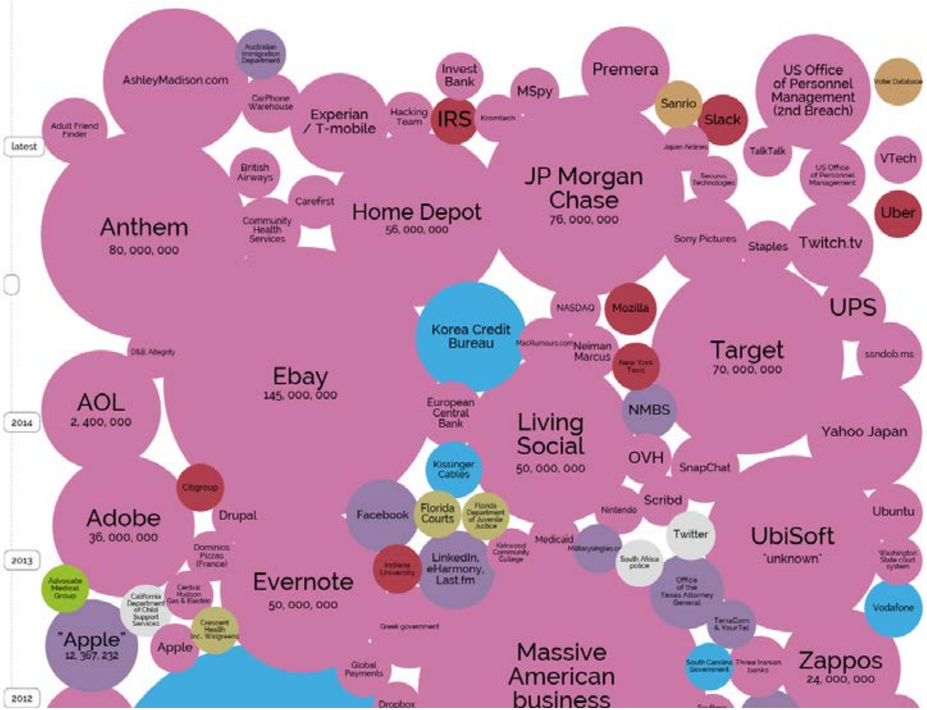
Data-Driven App Sec

Joel Scambray

Joel Scambray
Cigital, Inc.
@joelscam

#RSAC

App Sec is a Big Problem



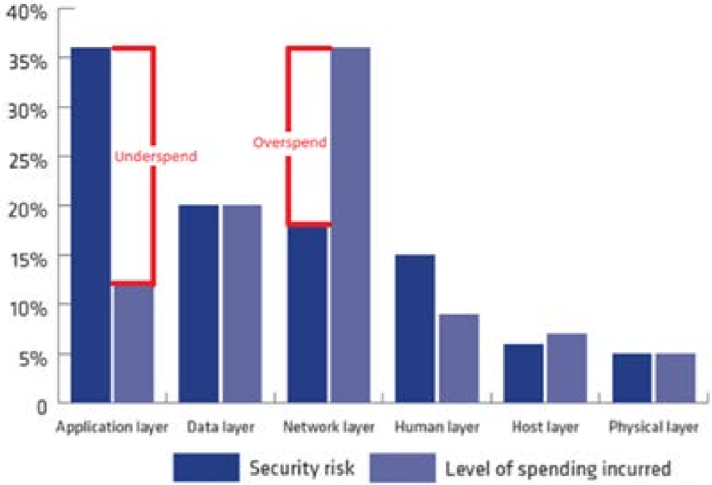
- ● accidentally published
- ● configuration error
- ● hacked
- ● inside job
- ● lost/stolen computer
- ● lost/stolen media
- ● poor security

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

What are we doing about it?

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

From SANS 2015 State of Application Security: Closing the Gap



The State of Risk-based Security Management: US and UK; 2013. Ponemon Institute. Pp 40.

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

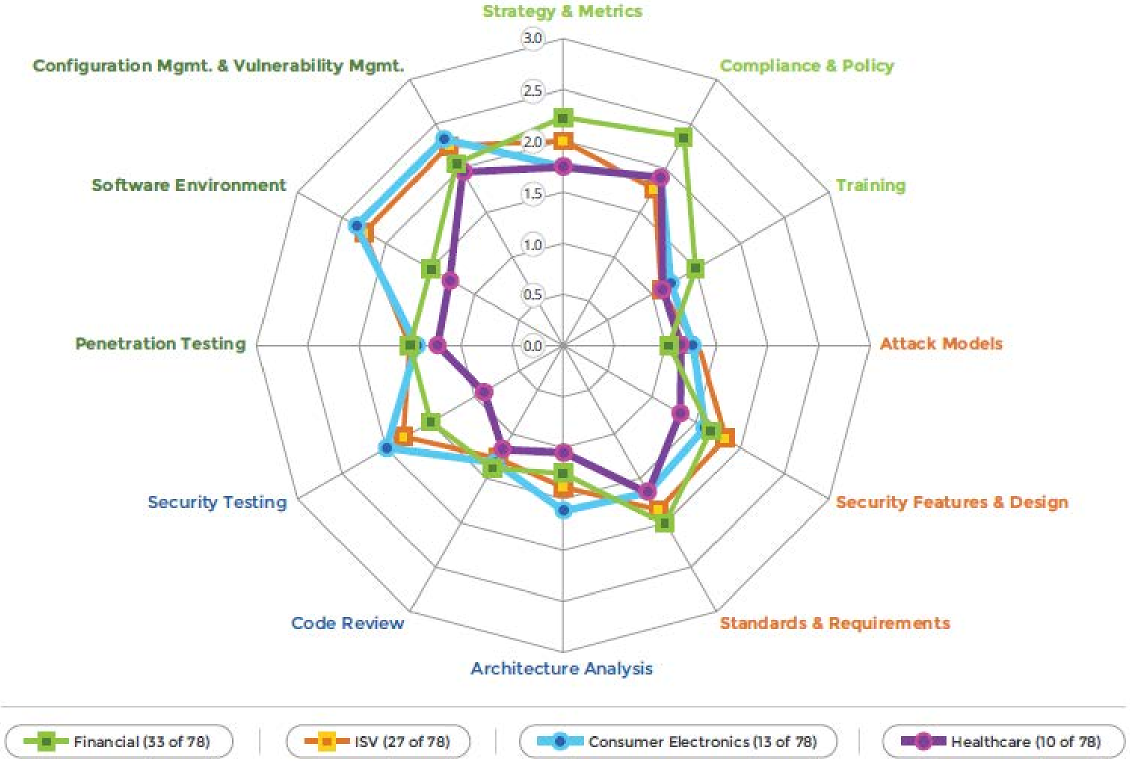
Over 70% of vulnerabilities exist at the application layer, not network - Gartner

It’s worse than it seems

It’s even worse than that

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

Source: bsimm.com



What are *you* doing about it?

- Who tracks software/app vulns distinctly?
- Who spends equally on app vs. IT sec?
- Who has an app sec program?
- What’s in it?

App Sec Activities: Just Do It!

The Maturity Curve

Do

Plan

Check

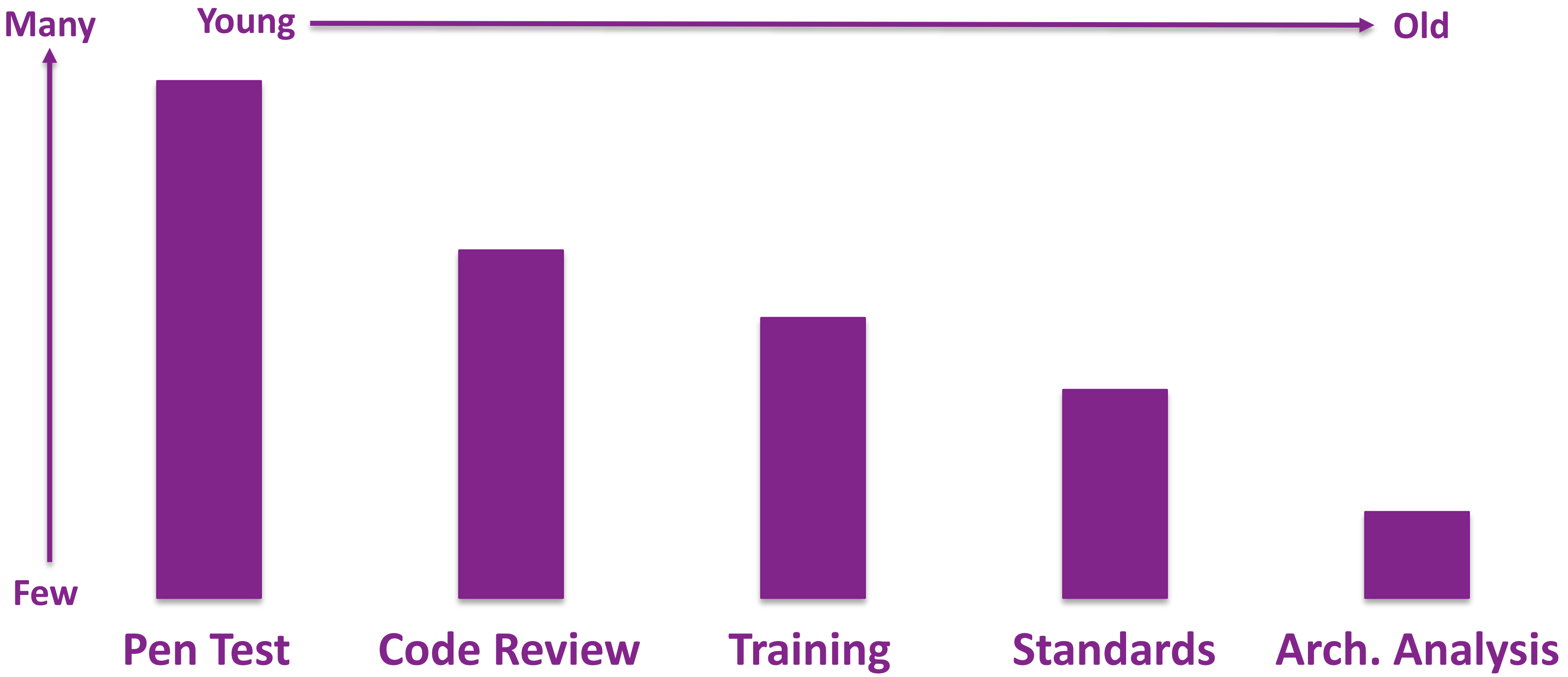
(repeat)

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

The Big 5


Many
Young
Old
Few
Pen Test
Code Review
Training
Standards
Arch. Analysis

The 6th Thing?

Big 5

- Organization
- Integration
- Metrics

} "Management"

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

Perennial Org Questions

- Infosec vs dev?
- Top down vs. bottom up?
- Which role makes the best leader?
- …and, where do I find qualified people?!?

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

Touchpoint	%
Legal	14
Vendor Management	7

Source: bsimm.com

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

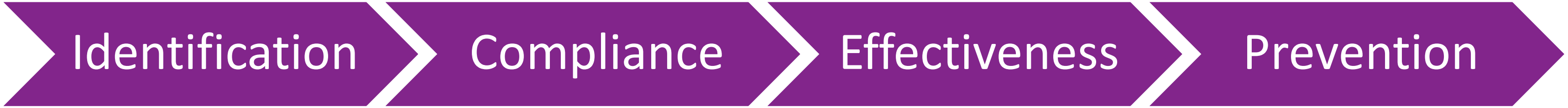
Metrics

Why?

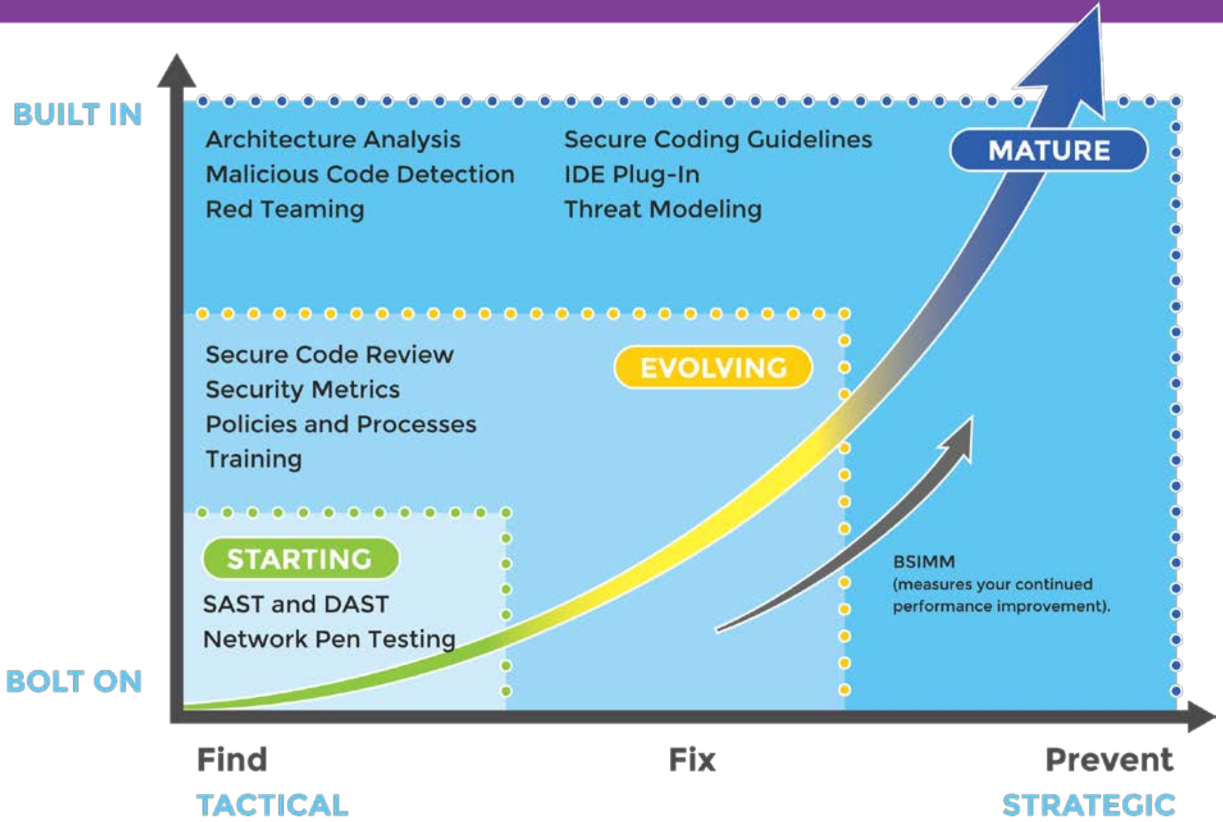
- Educate executives
- Publish for internal awareness
- Enforce the rules
- Drive budgets
- Evolve the program (portfolio view)

What

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



How will you complete the picture?



Architecture Analysis
Malicious Code Detection
Red Teaming

Secure Coding Guidelines
IDE Plug-In
Threat Modeling

Secure Code Review
Security Metrics
Policies and Processes
Training

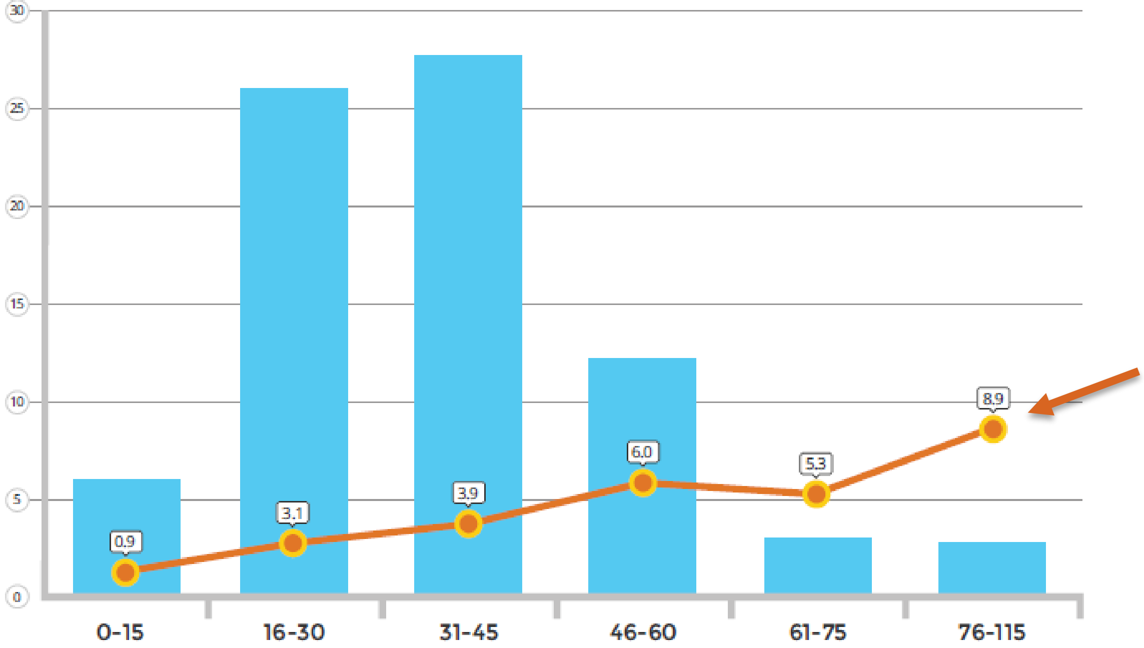
SAST and DAST
Network Pen Testing

BSIMM
(measures your continued performance improvement).

Cigital

More time = more maturity

# Firms



Avg Age of program

App sec “score” groupings → “Better?”

Source: bsimm.com

Sustaining the Investment

- Have an incident about every 2 years ☺
- Find a Champion (and a backup)
- Follow the maturity curve
- Get an independent measurement/benchmark

Just Do It!

- Assess apps
- Train developers
- Leverage results to drive:
  - The rest of the Big 5 (6)
  - Measurement and benchmark

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRWD-W05

Data-Driven App Sec

Joel Scambray

Joel Scambray
Cigital, Inc.
@joelscam

#RSAC