stratum//security

Innovative Risk Solutions

Discussion Topics

- Is it really worth investing in static analysis tools for your developers?
- Can you effectively deploy the tools and attain valuable results?
- What are the pitfalls?
- How do you succeed?

Why me?

- 10 Years of Application Security
- Built 3 consulting groups – AMS, Fishnet, Fortify
- Involved in countless assessments, trainings, etc…
- Experience deploying static analysis tools in 1000+ developer organizations
- Experience deploying static analysis in 3- developer organizations

Optimism & Cynicism

- Application security is crucial
- Single biggest opportunity to reduce organizational risk
- Why doesn't everyone agree?
- Stop talking to people who already are on your side
- Learn to communicate and sell

~~Success~~ Stories

- Large financial services organization
- Another large financial services organization
- World's largest and most capable military organization
- The ruler of the free world
- Taxes
- Department of Homeland Insecurity

Common Pitfalls

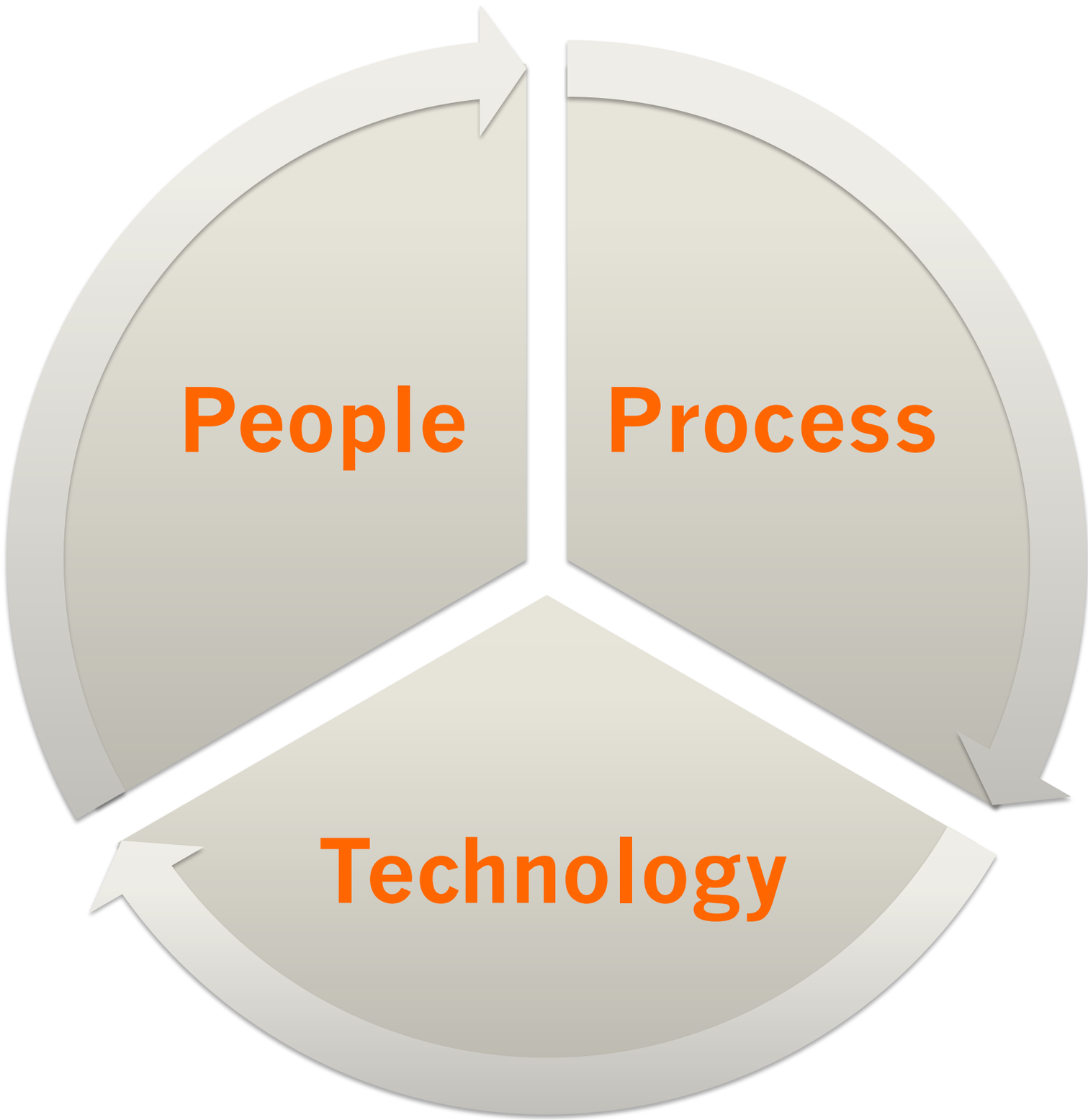
- Security group driven initiative
- No driver except good intentions
- Lack of a communications strategy
- Technology first
- Lack of a plan or goals
- Inability to integrate into SDLC

Typical Approach

1. Buy source code tool (HP, IBM)
2. Maybe 1-2 day training – how to run a scan
3. Ignore integration (i.e. build server)
4. Use only basic functionality
5. Don’t create testing procedure
6. Don’t create coding standards
7. Don’t create a process/feedback loop
8. No metric program
9. No success goals or incorrect goals

Lessons Learned

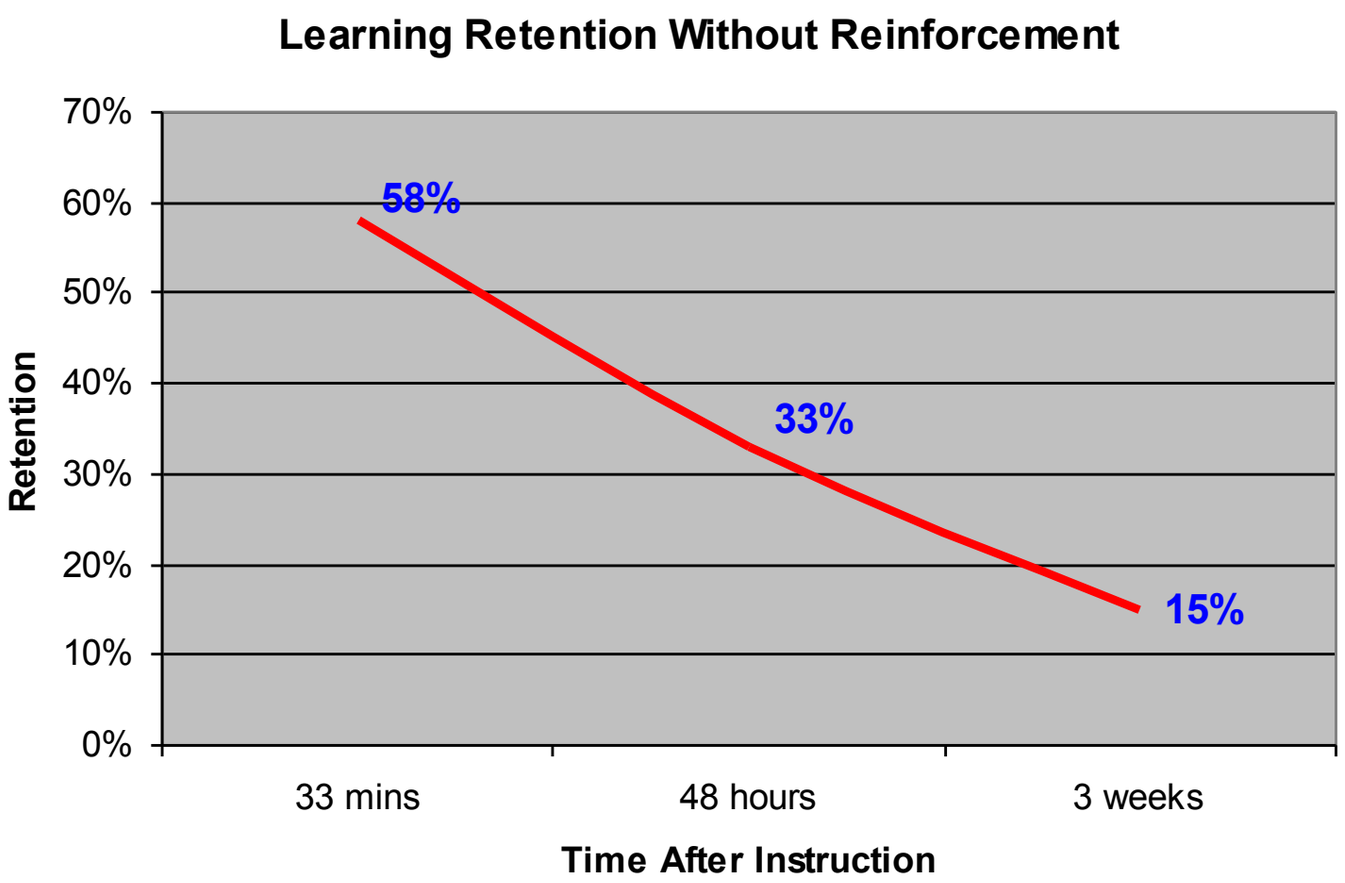
- Executive Mandate
- Case for Change
- Pilot
- Prioritize
- Measure
- Hands-on Training
- Mentoring
- Remediation
- Repetition
- On-going awareness


People
Process
Technology

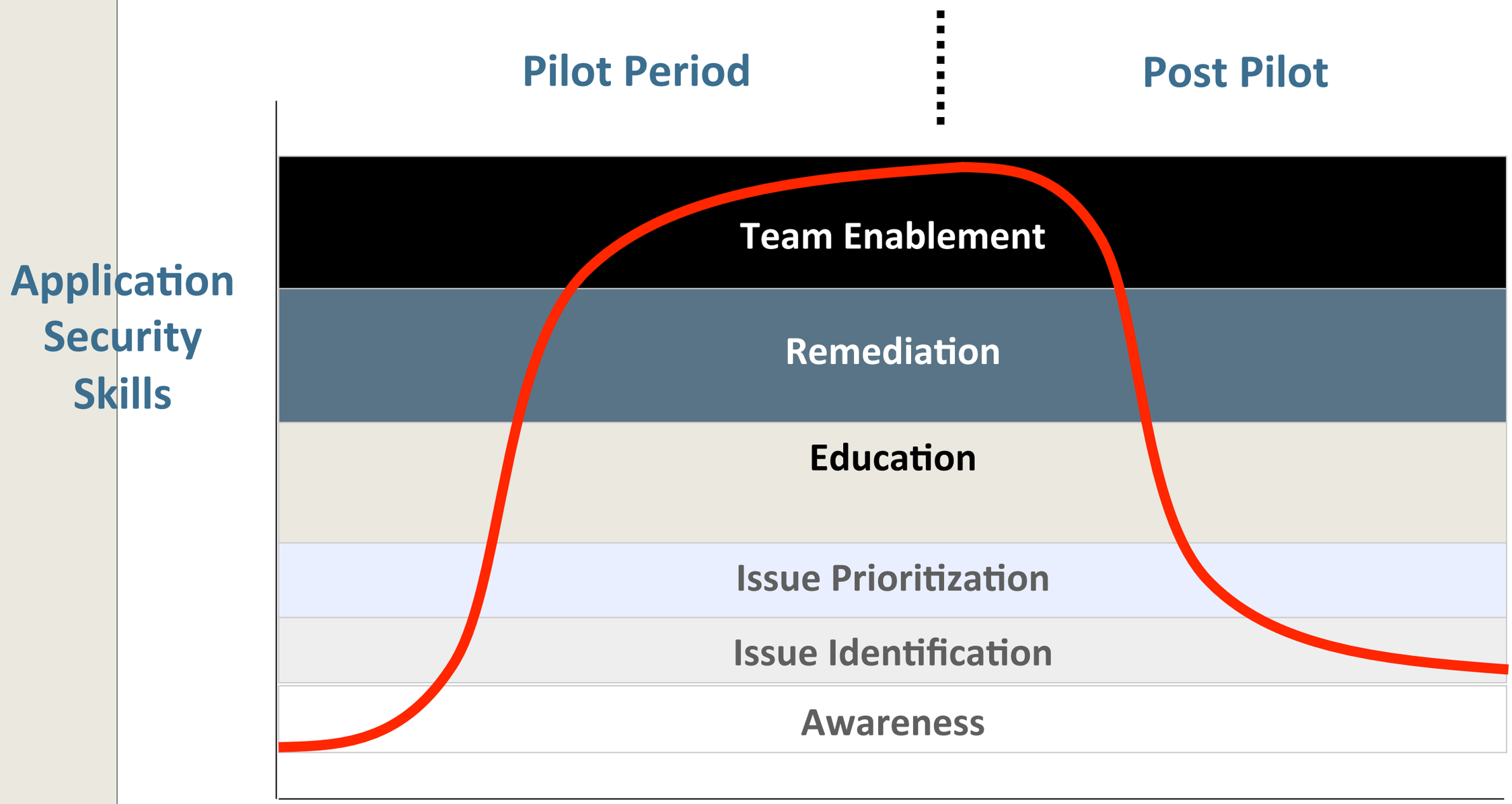
Knowledge Retention

"Most learners retain little from classroom instruction. About 33 minutes after a lecture is over, most students retain only 58 percent of what was covered in class, according to a 1998 study by the New York City-based Research Institute of America. By the second day, retention has fallen to only 33 percent. And after three weeks, all but 15 percent is forgotten."

Training Magazine, 1998



Post Pilot Regression



Without on-going awareness & education, the cycle cannot maintain itself and reverts back to new awareness level.

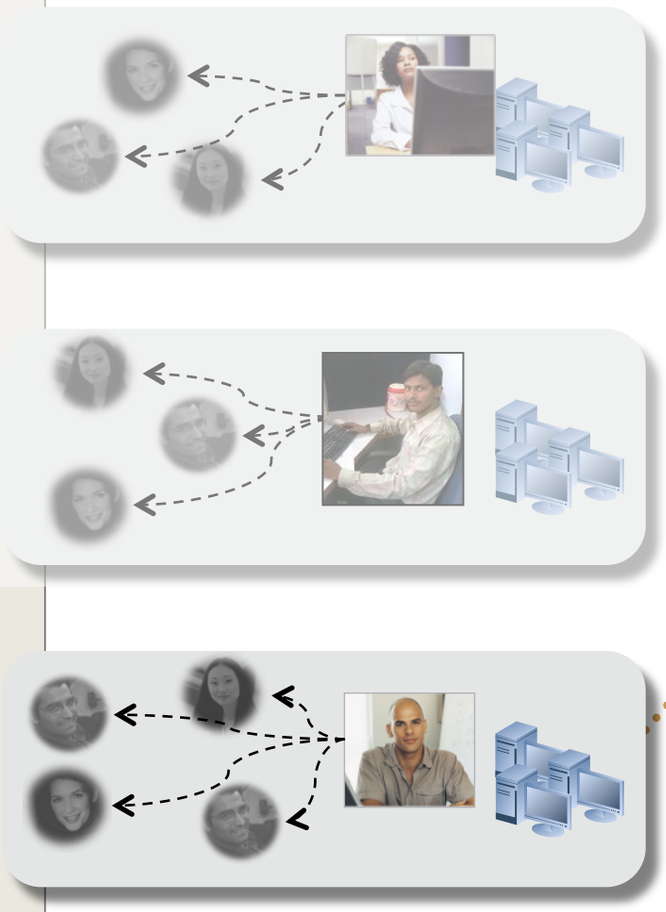
Marketing 101

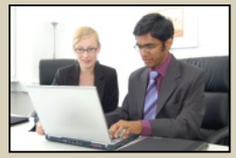
- Seriously, write a communications plan
- Stakeholders = customers
- Market segmentation
- Tailored messages with drivers
- Message frequency
- Delivery formats
- Repetition

Centralized - Security Team

Advocative (stealth)
Advisory / Consultative
Mandatory (Gate)

Development/QA Teams





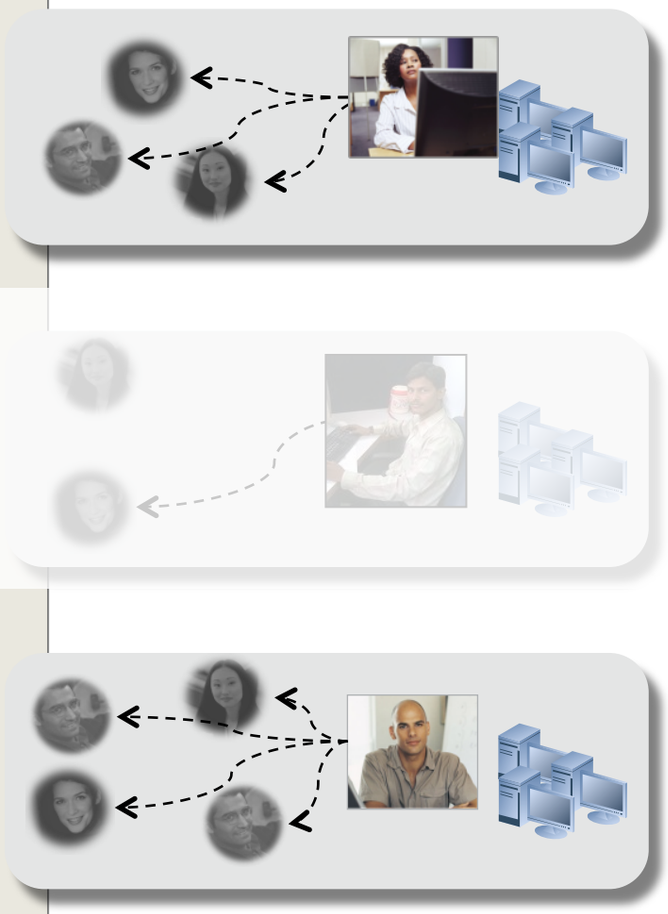
Risk/Information Security Team *(Software)*

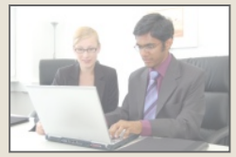
Information Security Team (Operations)

13

Distributed – Development

Development/QA Teams





Risk/Information Security Team *(Software)*

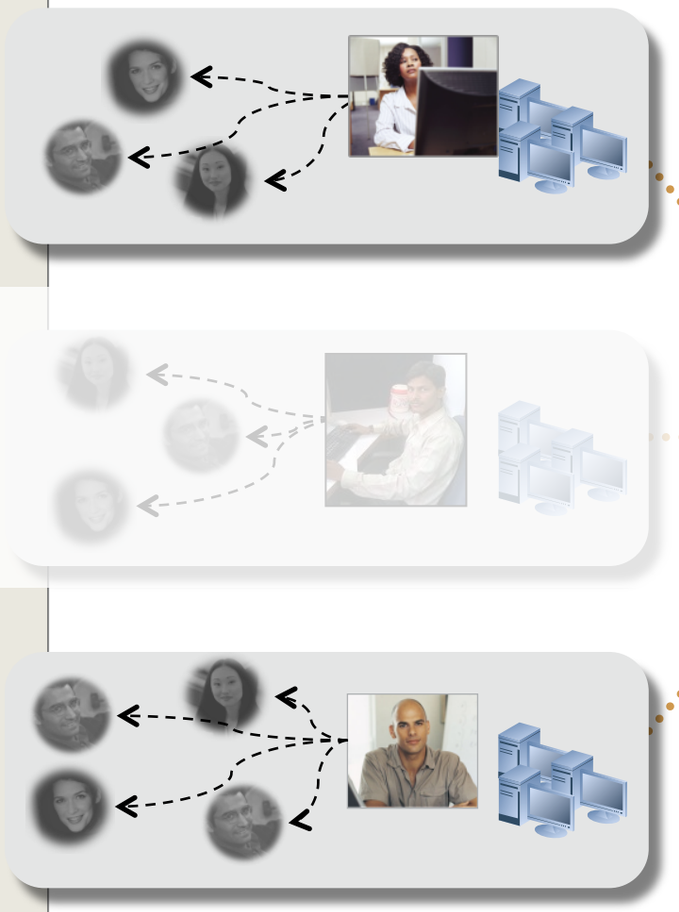
Information Security Team (Operations)

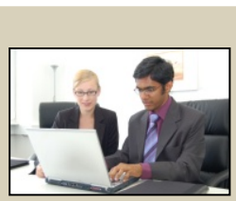
14

Operational – Integrated

Information Risk / Software Security
Development
Operational Security

Development/QA Teams





Risk/Information Security Team *(Software)*

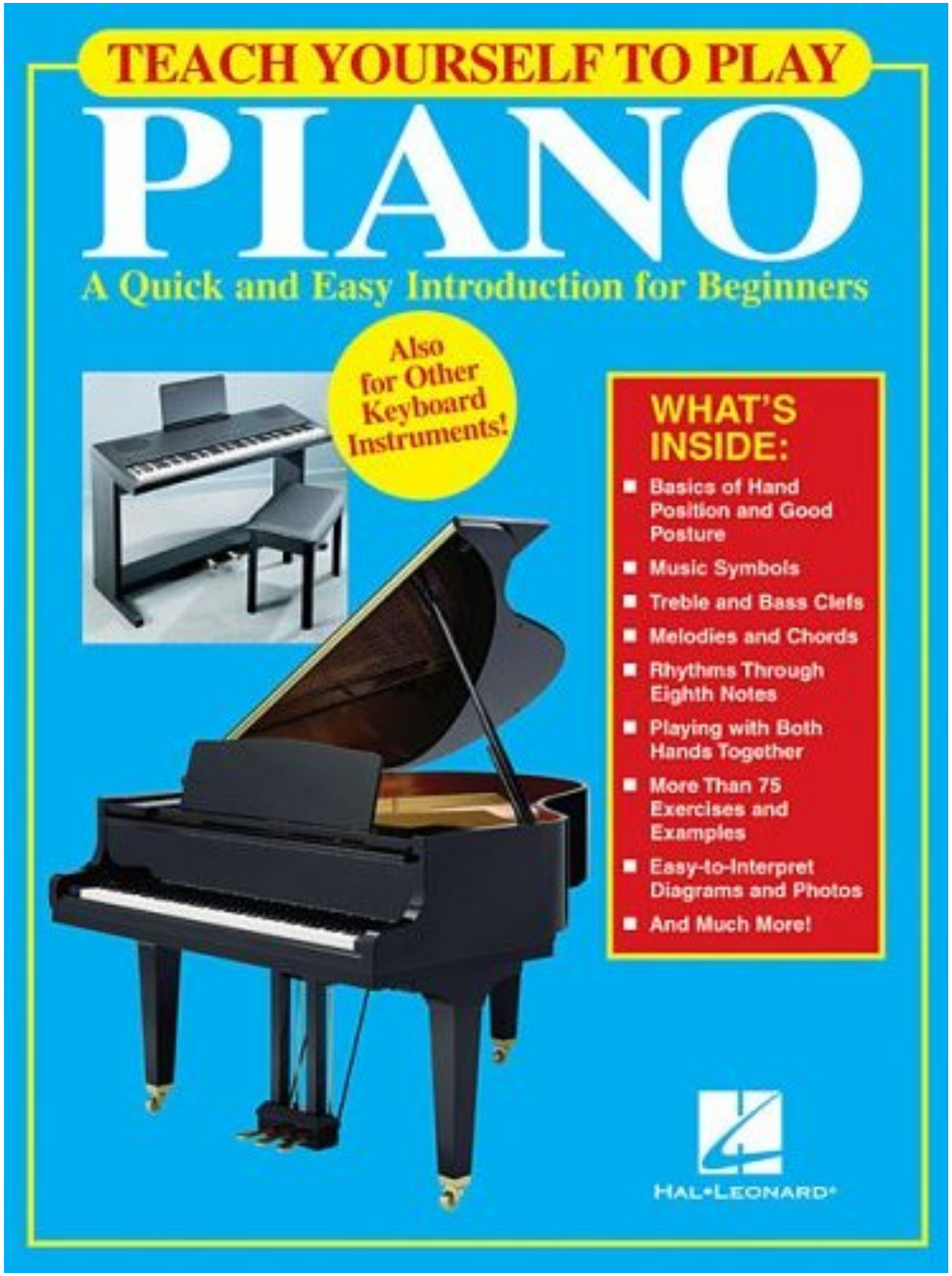
Information Security Team (Operations)

Required for "high-touch" pilot/PoC

15

If it was easy….

The reason I’m not a concert pianist is not because of lack of information



stratum//security

Stratum Security Introduction

- Information Security Consulting “boutique”
- Graduates of major infosec industry consulting firms
- Assessment, Compliance, Strategy, Program Development focus (not infrastructure)
- Consultants have at least 10+ years experience – no junior level resources
- Key differentiators:
  - Experience
  - Value
  - Satisfaction

Assessment Services

Stratum Security is an Information Security services firm headquartered in the Washington DC Metro area. Founded in 2005, Stratum Security provides services to clients worldwide. Our list of successful engagements include large multi-national enterprises to small start-ups in a wide array of industries including finance, insurance, retail, hospitality, education, health care, government, technology, energy, and telecommunications.

Stratum Security Corporate Headquarters
13800 Coppermine Road
Suite 302
Herndon, VA 20171

(703) 994-4167 office
(494) 993-3800 fax

Visit Our Web Site
www.stratumsecurity.com

Email Us
info@stratumsecurity.com