THE REVOLUTION IN INFORMATION SECURITY: WHAT YOU NEED TO KNOW NOW

FREDERICK SCHOLL
EXECUTIVE CONSULTANT
CARSON, INC.
www.carsoninc.com

615-739-1039

Changing Career Opportunities?

- Security Operations
  - SOC
  - Vulnerability management
  - Incident response
- Risk Management
  - Compliance
  - Assessment
  - Awareness training

New Security Opportunities

- DevOpsSec
- Systems security engineer
- Cloud security engineer
- Application security engineer
- Others?

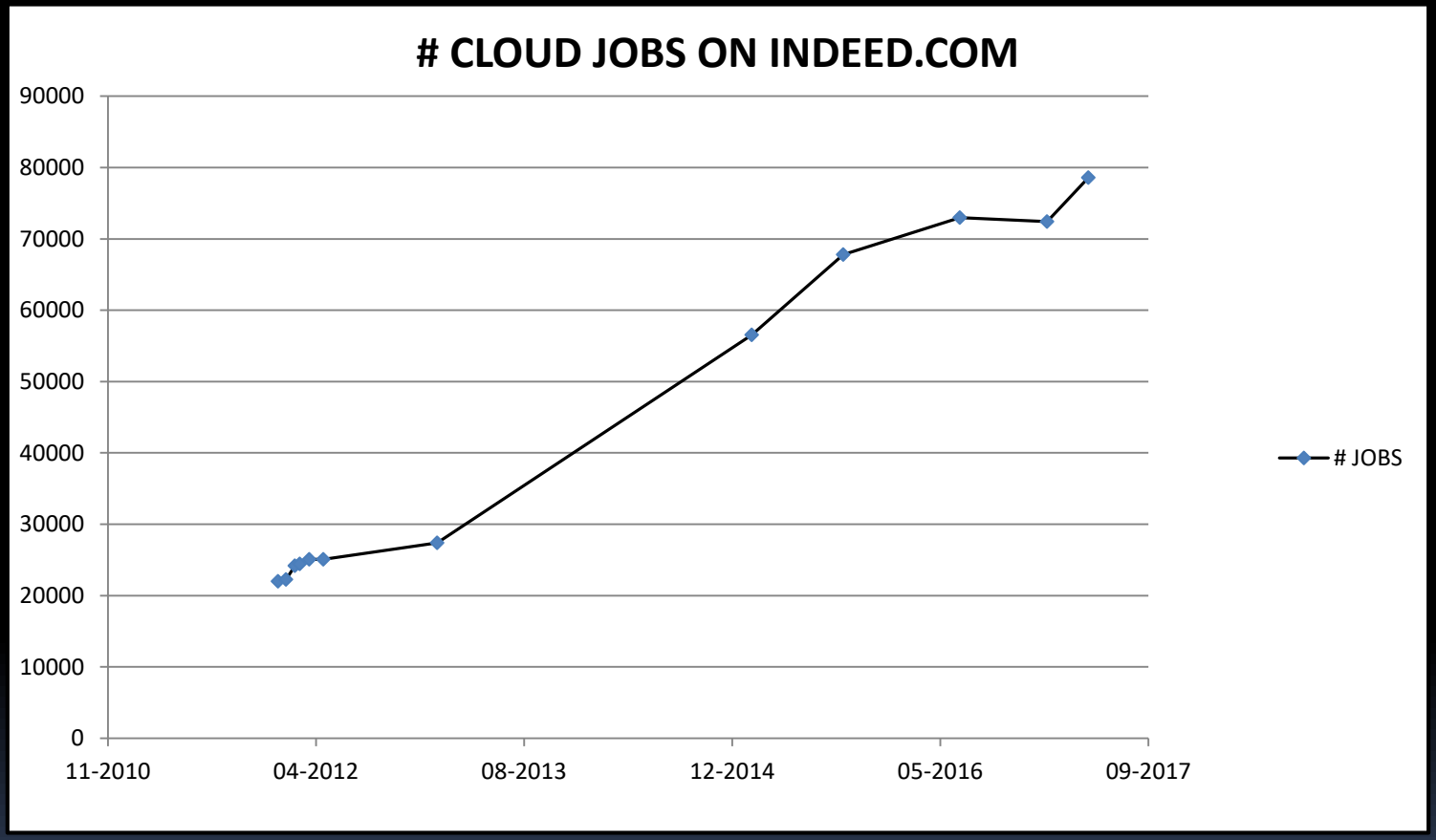
WHAT DO WE NEED TO DO TO KEEP UP?

Cloud computing?
Communications skills?
Systems engineering?
Software development?

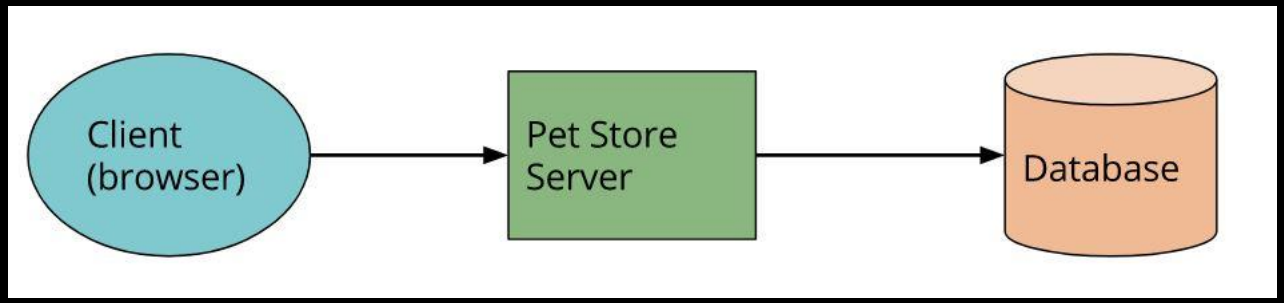
Discussion and brainstorming sessions

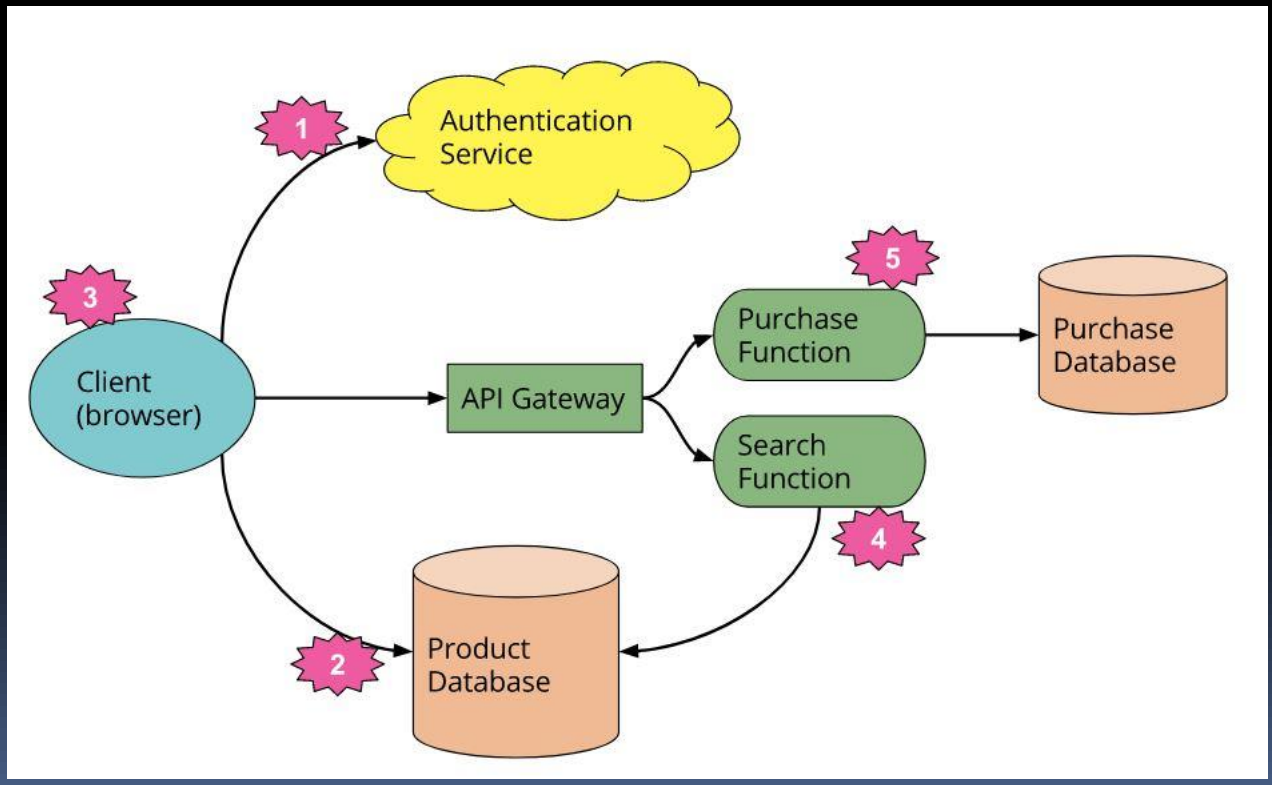
CLOUD

“Plastics”


CLOUD JOBS ON INDEED.COM
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
11-2010
04-2012
08-2013
12-2014
05-2016
09-2017
JOBS

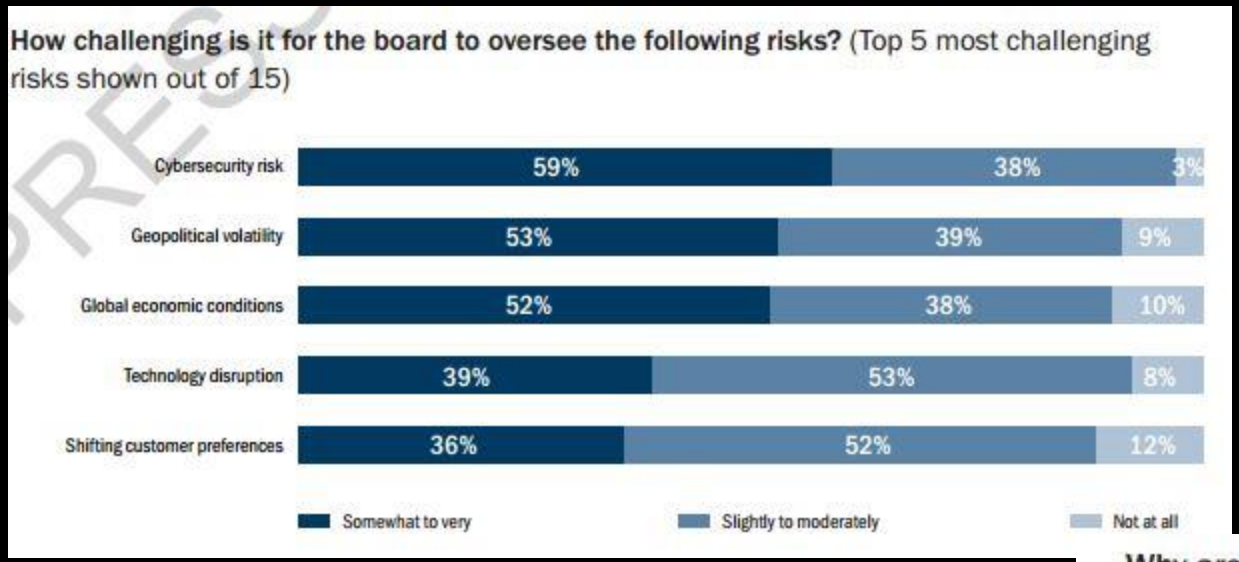
Cloud According to AWS

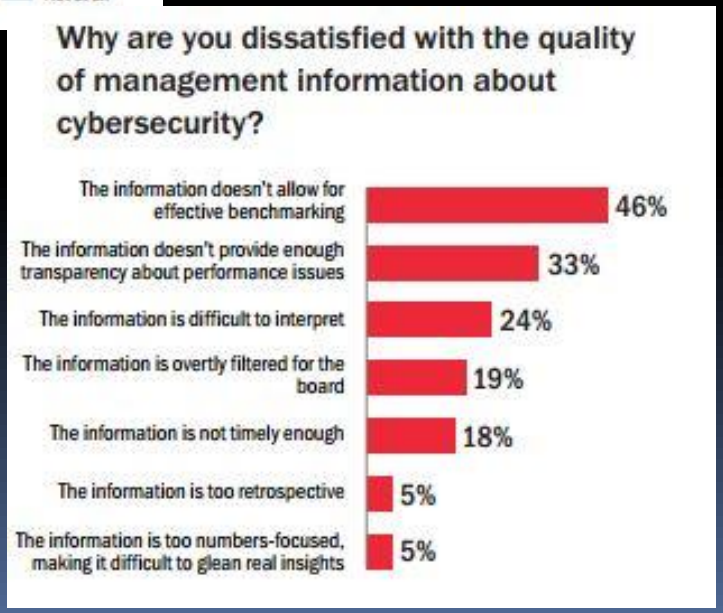

Client
(browser)
Pet Store
Server
Database


1
Authentication
Service
3
Client
(browser)
API Gateway
5
Purchase
Function
Purchase
Database
Search
Function
4
2
Product
Database

COMMUNICATIONS SKILLS

NACD Governance Survey 2016





SECURITY SYSTEMS ENGINEERING

*Compliance Sustainability**

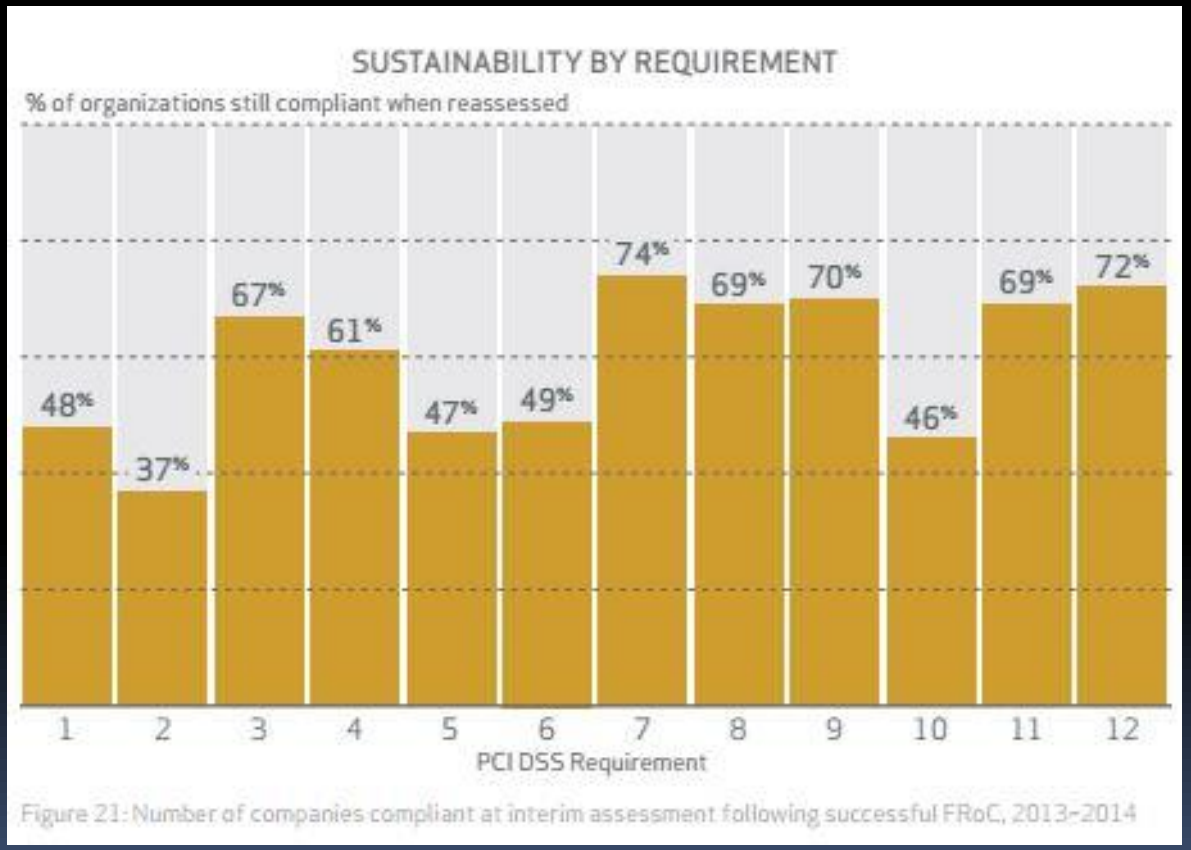


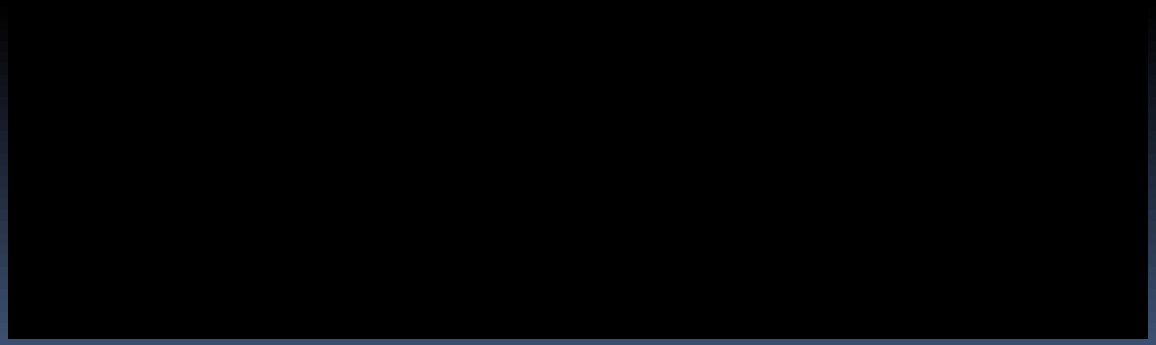
Figure 21: Number of companies compliant at interim assessment following successful FRoC, 2013-2014

* 2015 Verizon PCI Compliance Report

*Security as an Emergent Property**

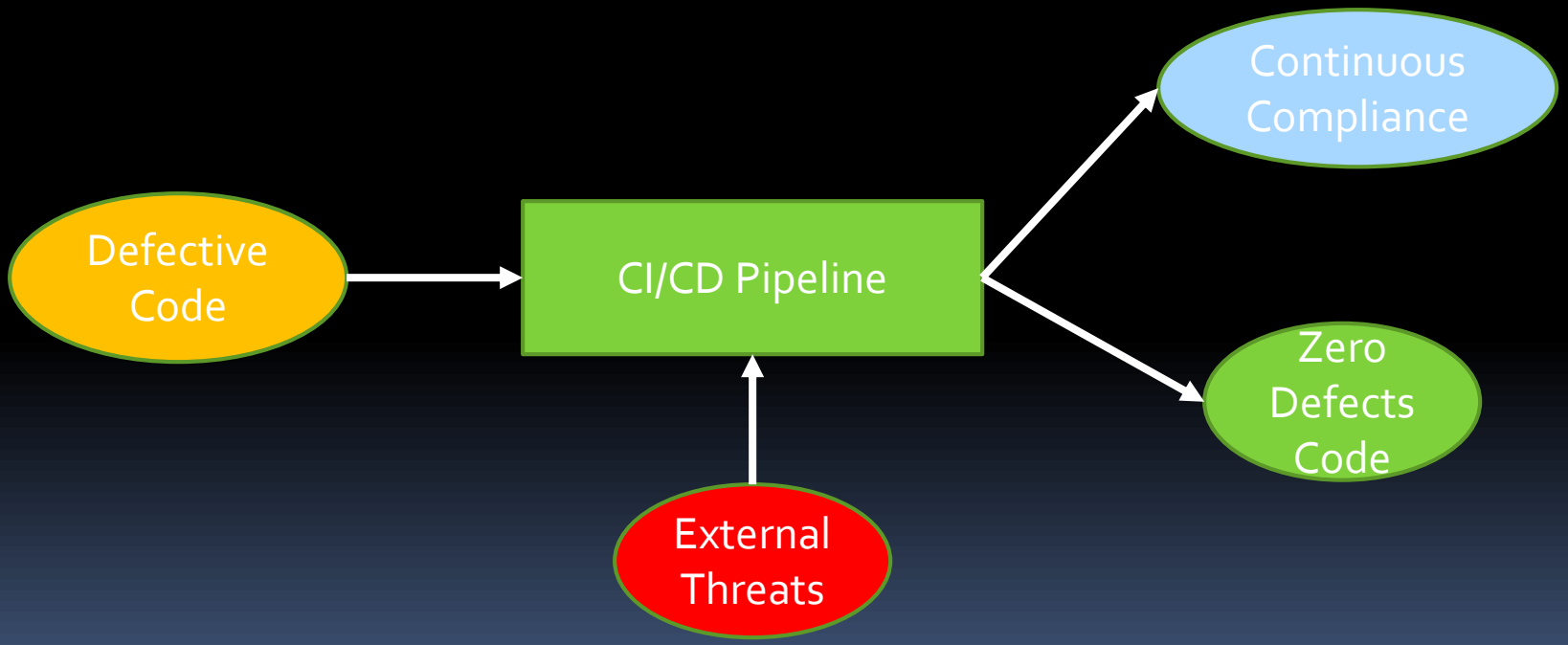
* NIST 800-160

A Few Cracked Plates…



SOFTWARE DEVELOPMENT

Agile/DevOps Manufacturing Line



Securing the DevOps Pipeline

NIST CSF Functions	Identify	Protect	Detect	Respond	Recover
CI/CD Processes					
Relative mitigation cost	1x	6.5x	6.5x	15x	100x
Agile/DevOps Lifecycle	Iteration 0	Construction iterations, 1-N	Construction iterations, 1-N	Transition (QA, staging, release)	Production
Security Activities	Threat model Compliance mgt.	Supply chain analysis Privileged access mgt. IDE security testing Library of user stories	Dynamic testing Static testing Penetration testing Manual code testing	Vulnerability mgt. Information radiator	Bug Bounties Web application firewall Security info. bus
Example Tools	Microsoft TMT Archer, Evident, Allgress	Blackduck CyberArk Veracode Under construction	Fortify Netsparker SAINT	Threadfix Splunk	HackerOne Barracuda Splunk

Threat Modeling With TMT

- Microsoft TMT (2017 Preview)
- Inputs: DFD
- Outputs: list of threats
- Features
  - Customizable
  - Considers everything to be malicious
  - Free!

STRIDE Model

Threat	Security Property We Want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation (logging)
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Resources

- www.martinfowler.com
- CSSLP: ISC2
- SANS DEV 534
- TMT 2017 Preview