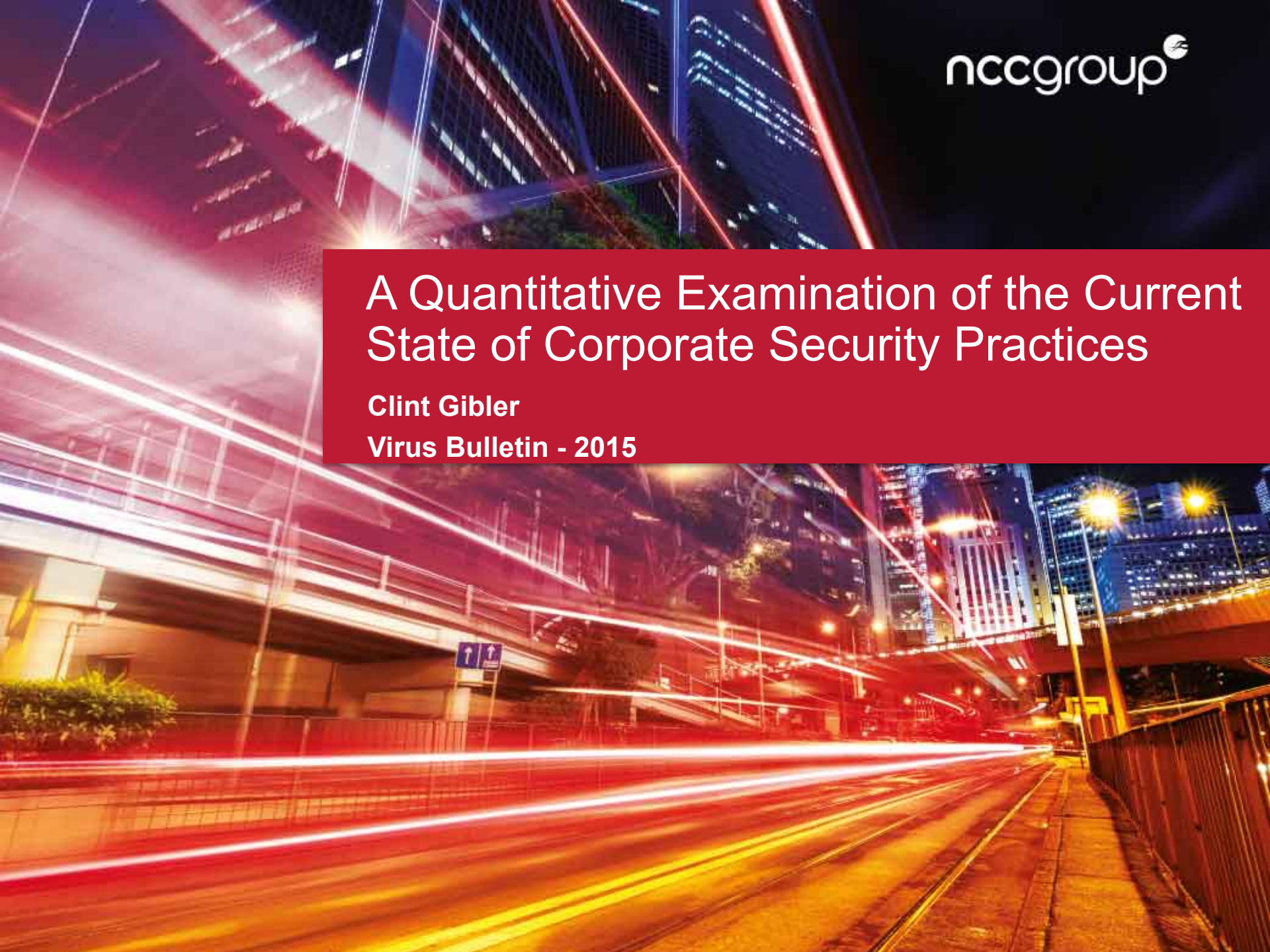


A Quantitative Examination of the Current State of Corporate Security Practices

Clint Gibler

Virus Bulletin - 2015

nccgroup

Anthem®
BlueCross®

TARGET

Goals of this work

- Give insight into vulnerabilities faced by real companies
- How quickly are vulnerabilities addressed?
- Highlight important areas for further security research

Agenda

Dataset and Methodology

Results

Demo

Who am I?

- NCC Group Domain Services
  - Software Security Engineer
- PhD from University of California, Davis
  - Focus in mobile security

Acknowledgments

- Carl Van Schie, NCC Group Managed Services

Dataset

- 100 companies across 10 industries
- Scan period - February 2014 – May 2015
- ~1,700 scans, >900,000 findings
- All findings have been vetted to be TP or FP
- Challenge:
  - Different # scans/scan frequency per company

Dataset

Industry			
Charities			
Energy & Utilities			
Financial Services			
Health			
IT			
Leisure & Media			
Public Sector - Education			
Public Sector - Local			
Retail			
Transport			

Dataset

Industry	Avg Scans / Company		
Charities	29.3		
Energy & Utilities	4.67		
Financial Services	22.6		
Health	2.56		
IT	24.6		
Leisure & Media	14.9		
Public Sector - Education	10.1		
Public Sector - Local	9.5		
Retail	10.1		
Transport	31.8		

Dataset

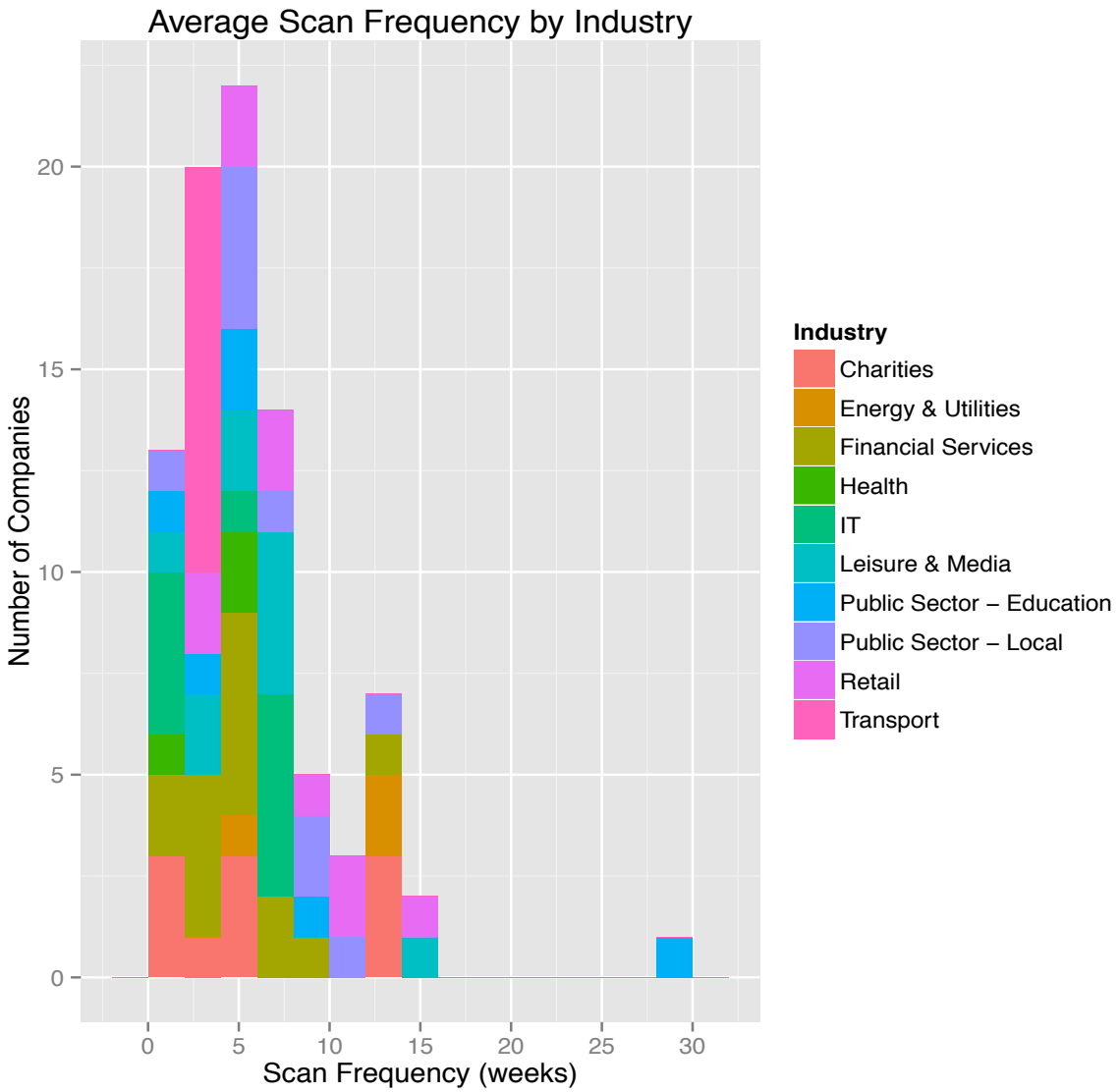
Industry	Avg Scans / Company	# Findings / company	
Charities	29.3	4,218	
Energy & Utilities	4.67	5,232	
Financial Services	22.6	8,011	
Health	2.56	1,580	
IT	24.6	8,480	
Leisure & Media	14.9	25,769	
Public Sector - Education	10.1	15,550	
Public Sector - Local	9.5	12,436	
Retail	10.1	4,431	
Transport	31.8	3,348	

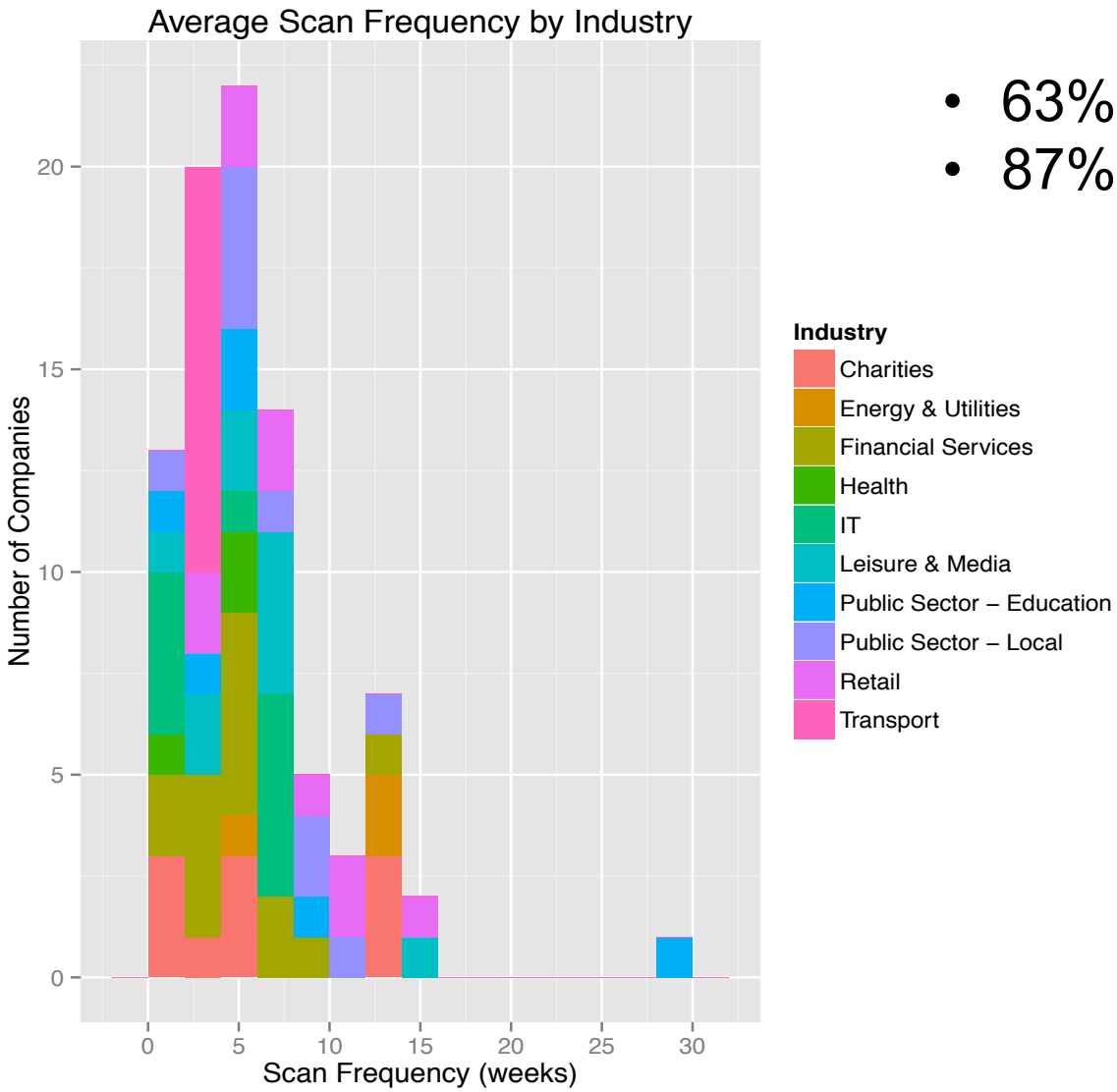
Dataset

Industry	Avg Scans / Company	# Findings / company
Charities	29.3	4,218
Energy & Utilities	4.67	5,232
Financial Services	22.6	8,011
Health	2.56	1,580
IT	24.6	8,480
Leisure & Media	14.9	25,769
Public Sector - Education	10.1	15,550
Public Sector - Local	9.5	12,436
Retail	10.1	4,431
Transport	31.8	3,348

Dataset

Industry	Avg Scans / Company	# Findings / company	% TP
Charities	29.3	4,218	51%
Energy & Utilities	4.67	5,232	11%
Financial Services	22.6	8,011	48%
Health	2.56	1,580	17%
IT	24.6	8,480	42%
Leisure & Media	14.9	25,769	16%
Public Sector - Education	10.1	15,550	23%
Public Sector - Local	9.5	12,436	23%
Retail	10.1	4,431	50%
Transport	31.8	3,348	23%


Average Scan Frequency by Industry
Number of Companies
0
5
10
15
20
0
5
10
15
20
25
30
Scan Frequency (weeks)
Industry
Charities
Energy & Utilities
Financial Services
Health
IT
Leisure & Media
Public Sector – Education
Public Sector – Local
Retail
Transport



- 63% <= 5 weeks
- 87% <= 10 weeks

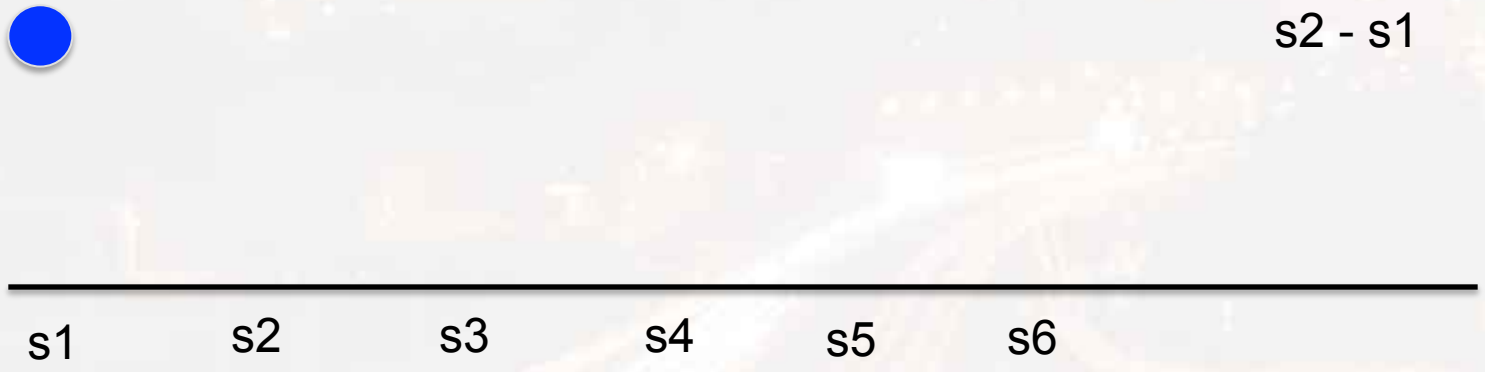
Methodology

- Categories
- Time to fix

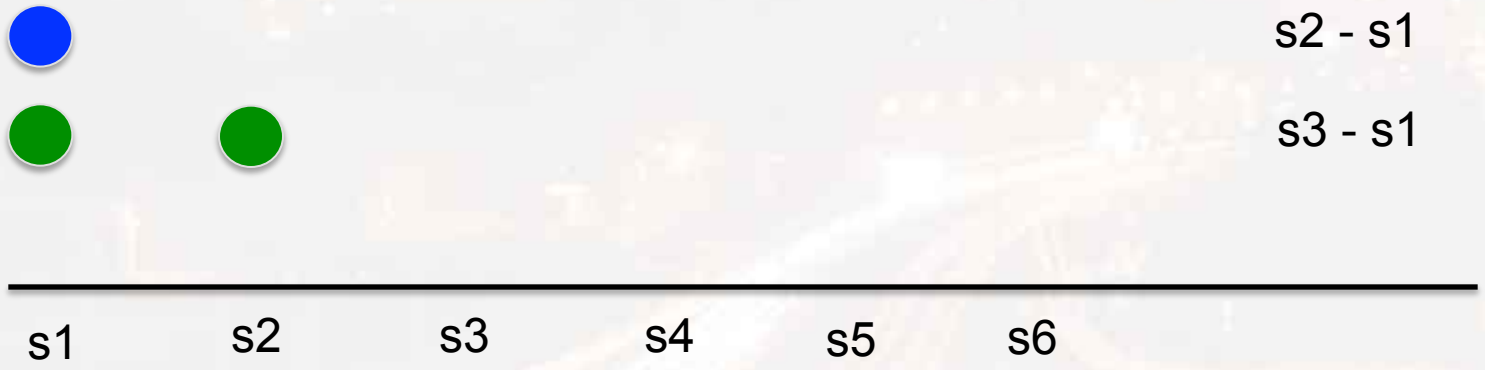
Categories

- Host
- Network
- Web Application

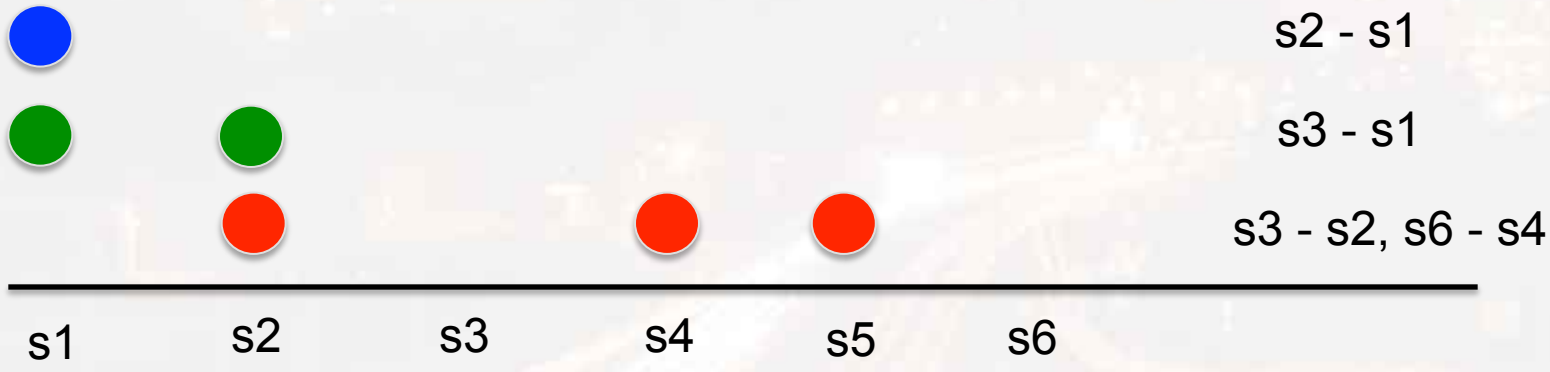
Time to Fix - Examples



Time to Fix - Examples



Time to Fix - Examples



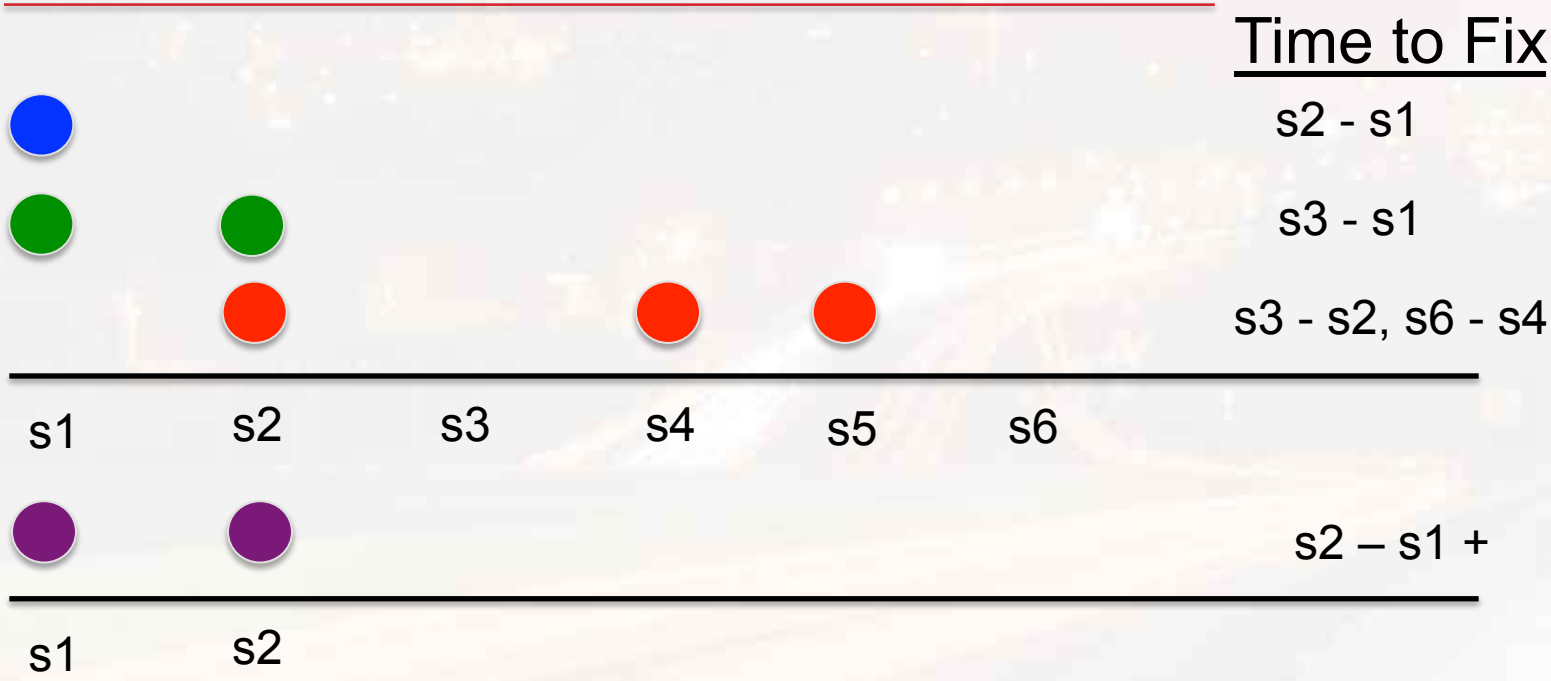
Time to Fix

s2 - s1

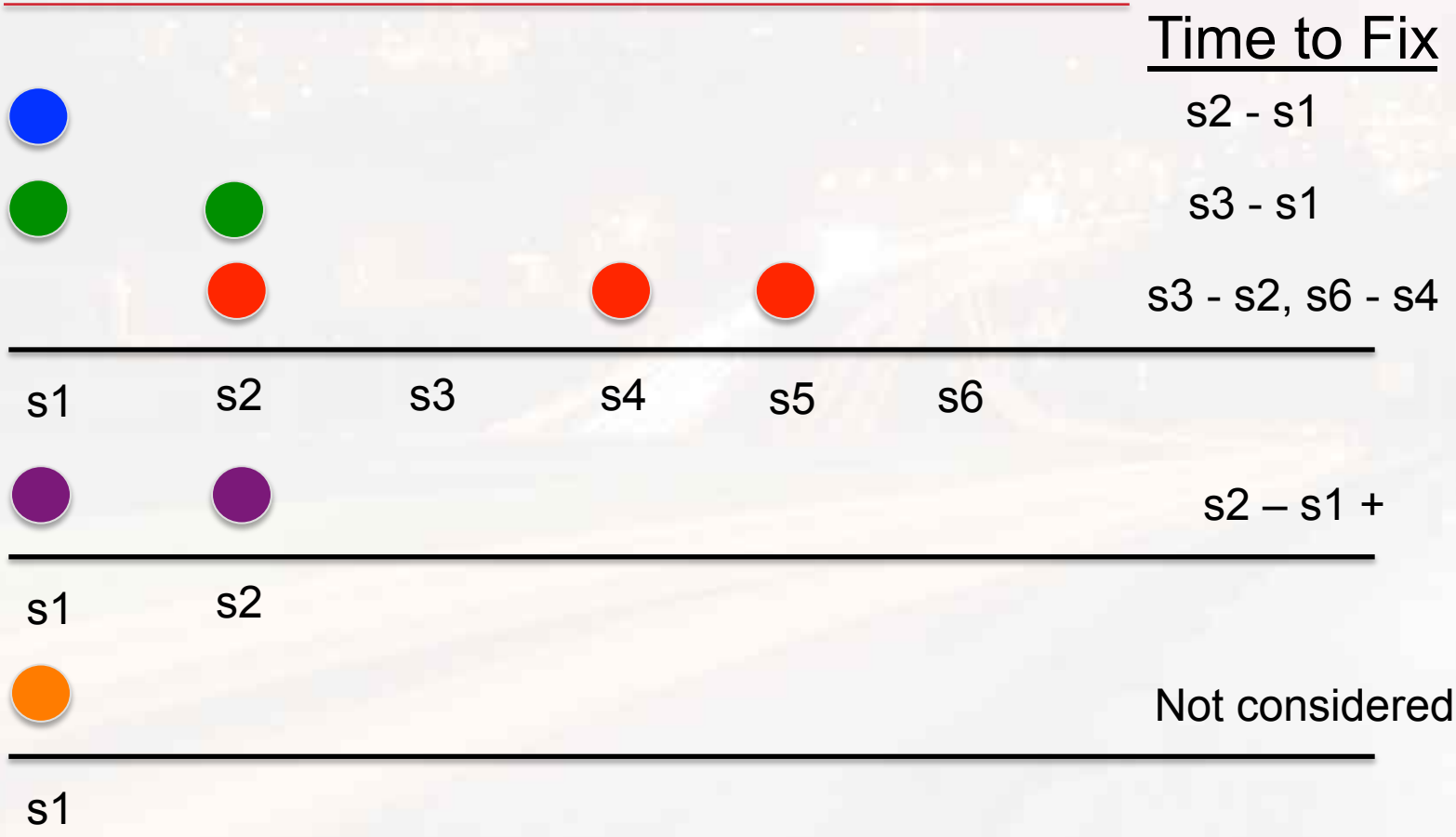
s3 - s1

s3 - s2, s6 - s4

Time to Fix - Examples



Time to Fix - Examples



Time to Fix - Caveats

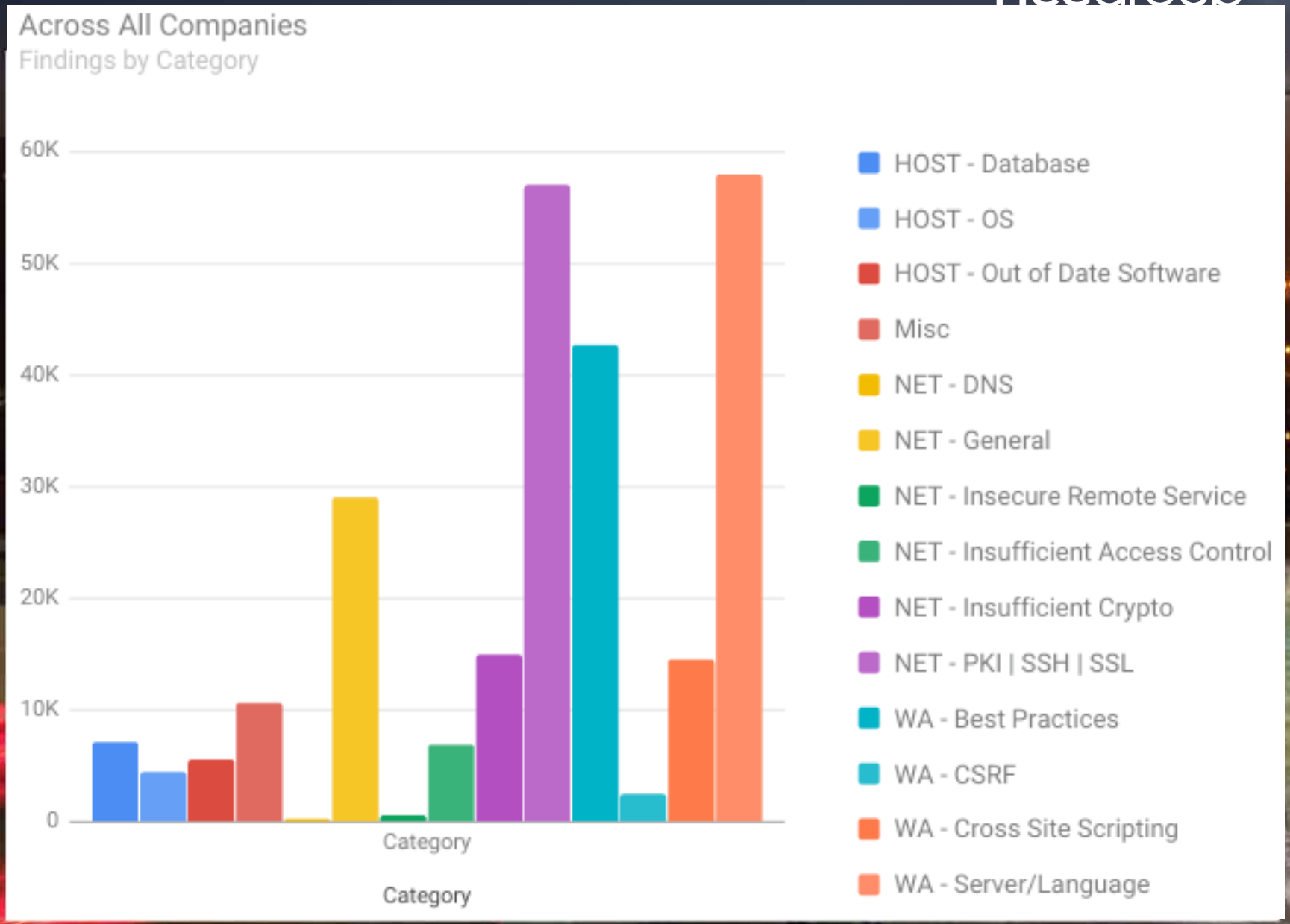
- Precision is inherently limited by scan frequency
- Different companies/industries have different # and frequency of scans

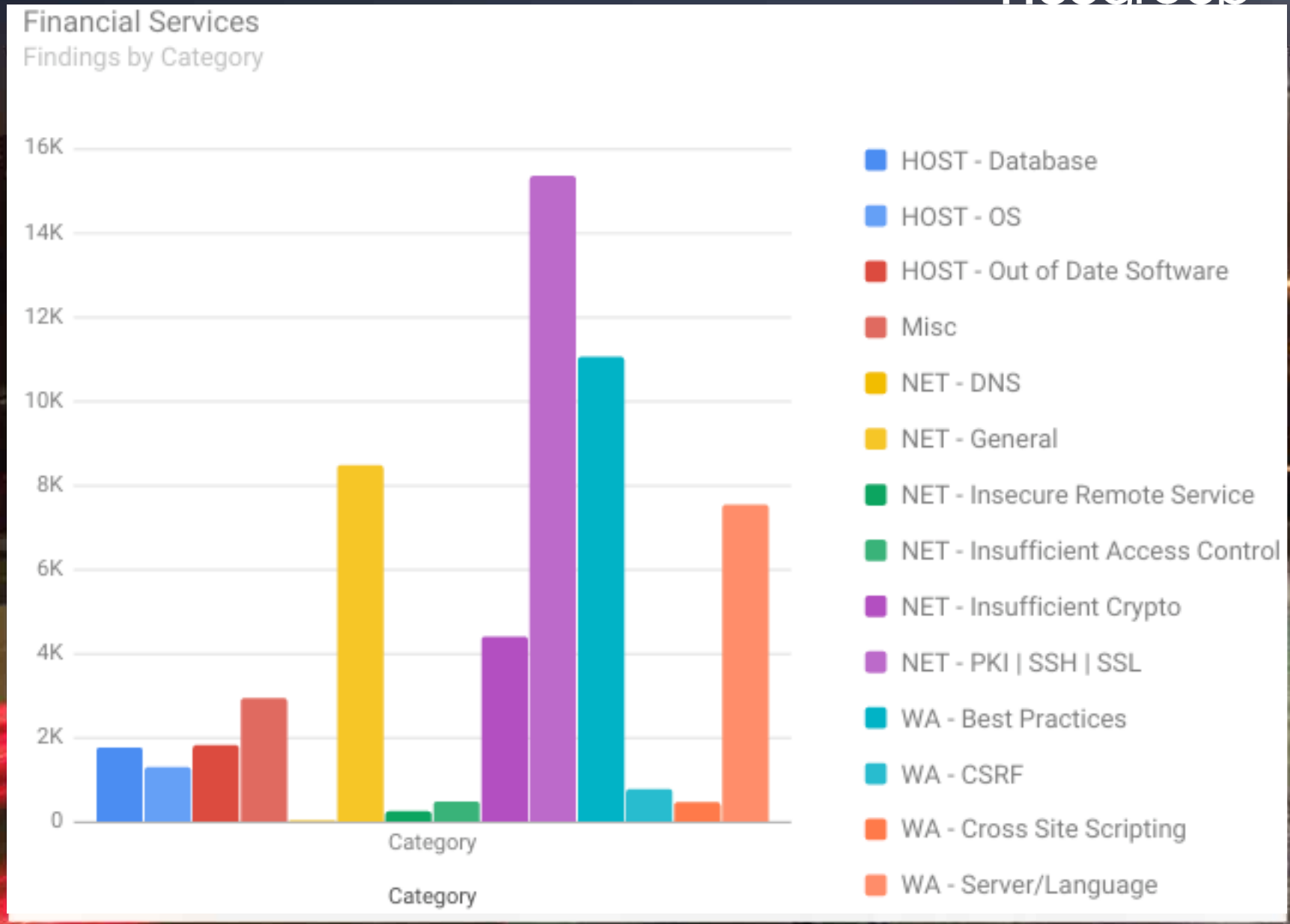
Evaluation

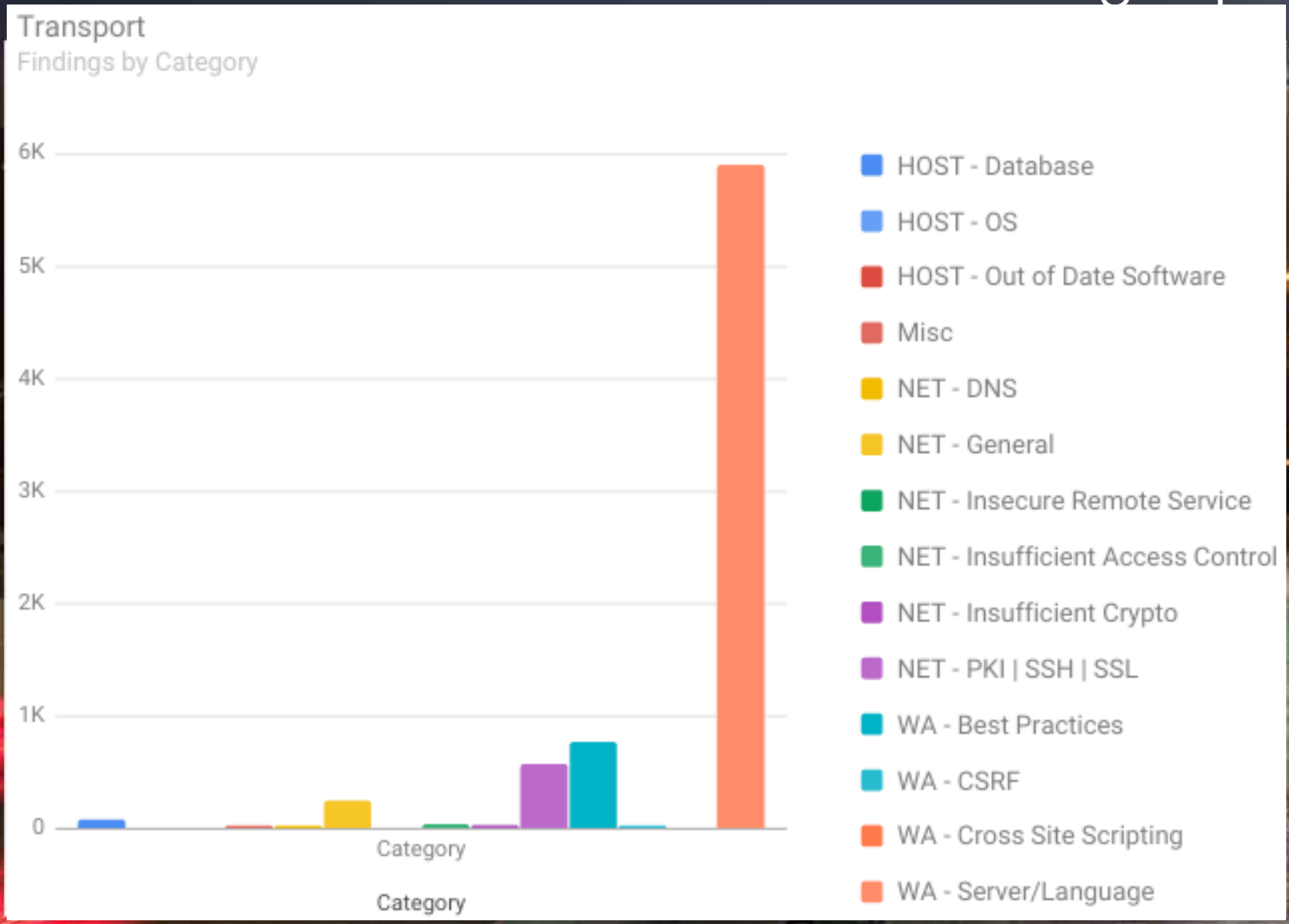
- What issues do we see in real companies today?
- How effectively are findings remediated?
  - 1) Time to fix and 2) Rate of fixing
  - Does it vary by:
    - Type of vulnerability
    - Industry
    - Severity
    - Remediation solution

Findings by Category

- Across all companies
- By Industry


Across All Companies
Findings by Category
60K
50K
40K
30K
20K
10K
0
Category
Category
HOST - Database
HOST - OS
HOST - Out of Date Software
Misc
NET - DNS
NET - General
NET - Insecure Remote Service
NET - Insufficient Access Control
NET - Insufficient Crypto
NET - PKI | SSH | SSL
WA - Best Practices
WA - CSRF
WA - Cross Site Scripting
WA - Server/Language

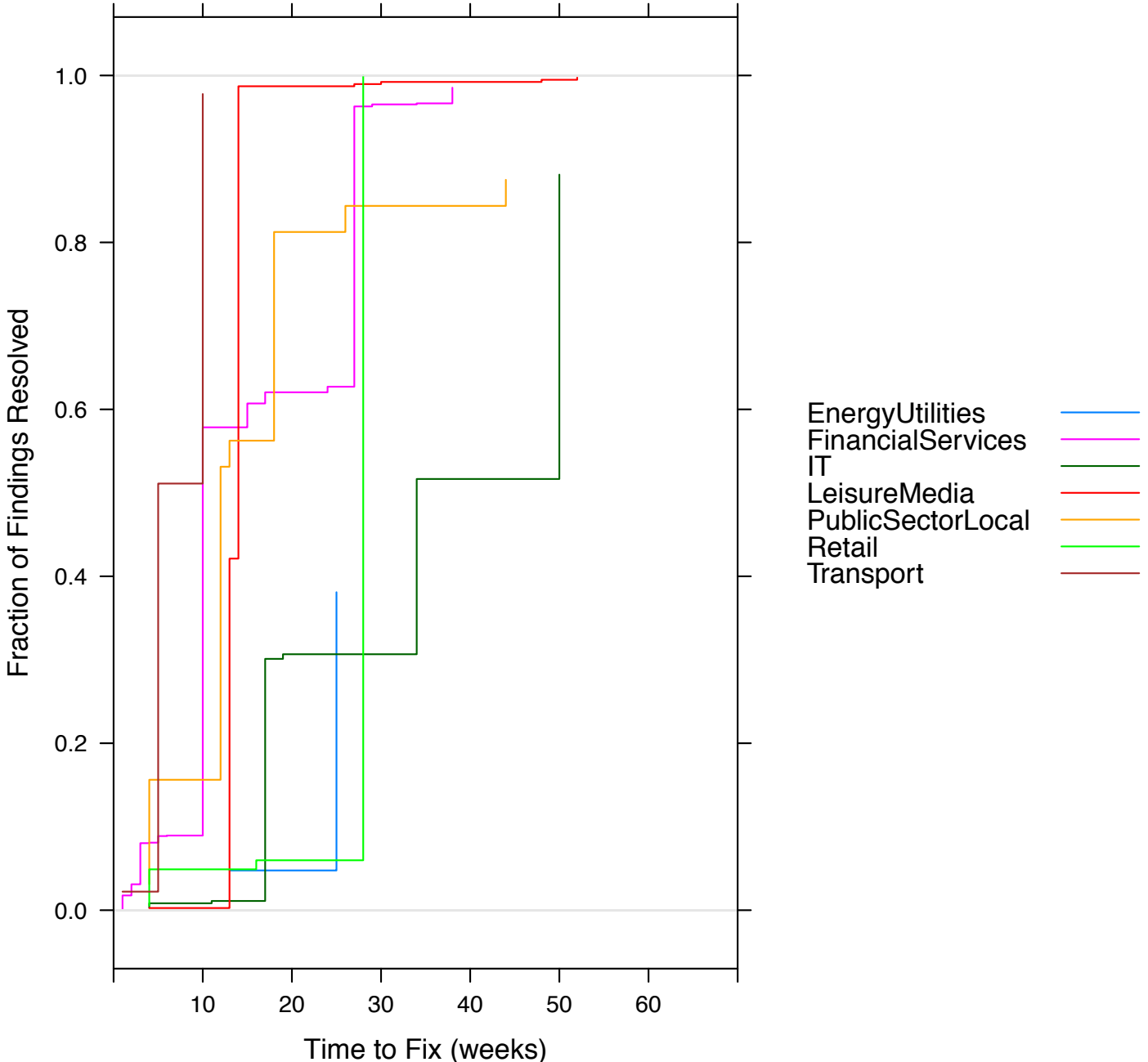

Financial Services
Findings by Category
16K
14K
12K
10K
8K
6K
4K
2K
0
Category
Category
HOST - Database
HOST - OS
HOST - Out of Date Software
Misc
NET - DNS
NET - General
NET - Insecure Remote Service
NET - Insufficient Access Control
NET - Insufficient Crypto
NET - PKI | SSH | SSL
WA - Best Practices
WA - CSRF
WA - Cross Site Scripting
WA - Server/Language


Transport
Findings by Category
6K
5K
4K
3K
2K
1K
0
Category
Category
HOST - Database
HOST - OS
HOST - Out of Date Software
Misc
NET - DNS
NET - General
NET - Insecure Remote Service
NET - Insufficient Access Control
NET - Insufficient Crypto
NET - PKI | SSH | SSL
WA - Best Practices
WA - CSRF
WA - Cross Site Scripting
WA - Server/Language

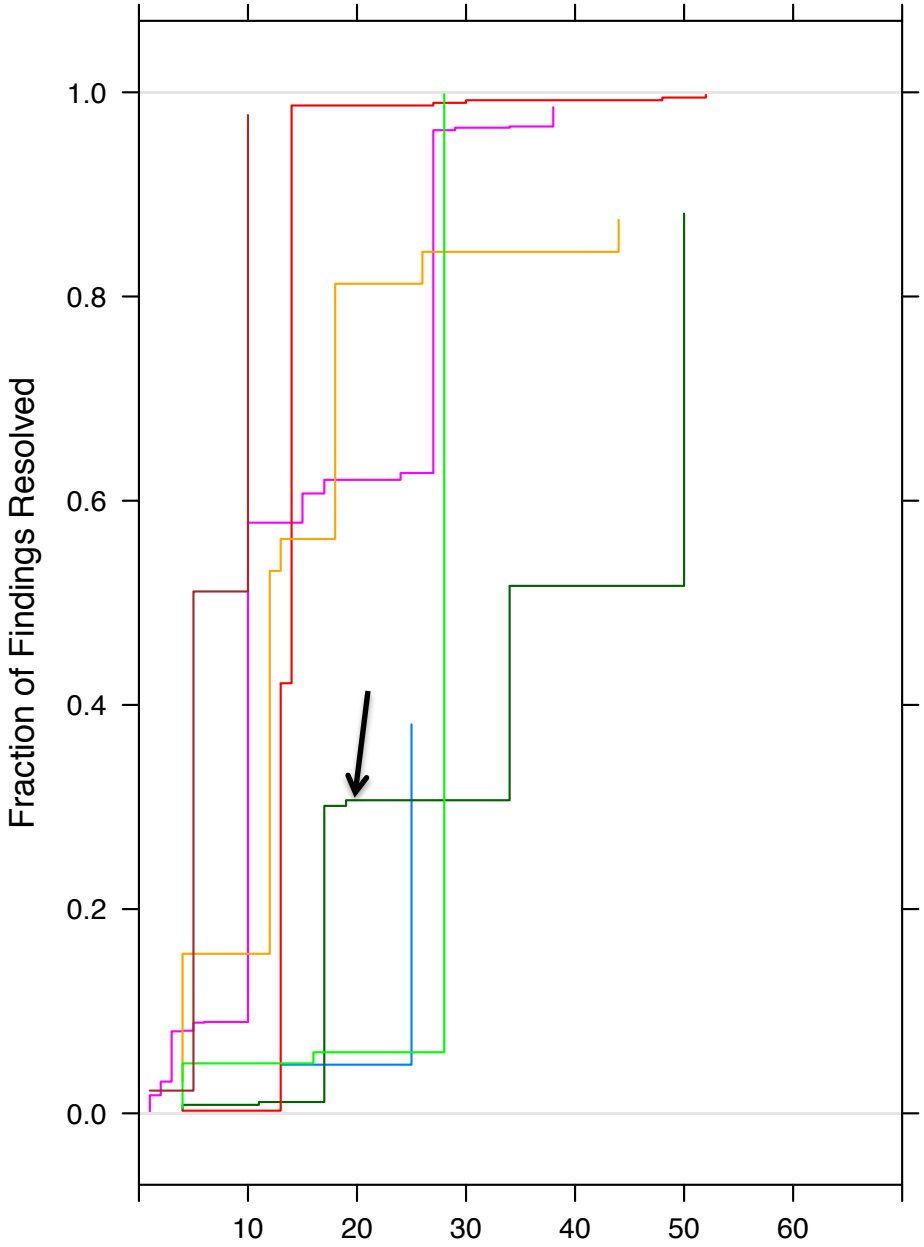
Time to Fix

- Category group
- Severity (CVSS)
- Remediation solution

Time to Fix by Category Group – Host

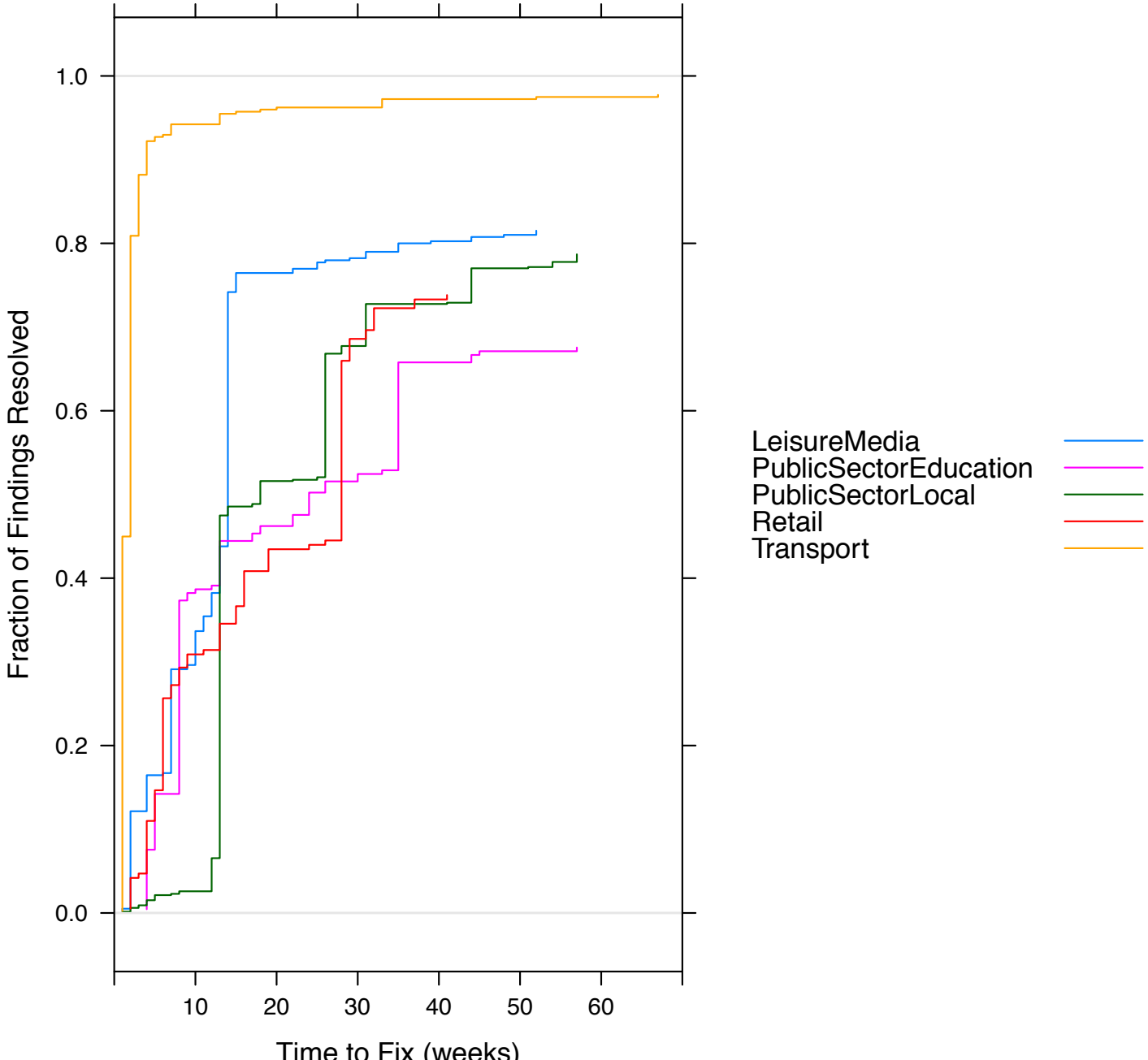


Time to Fix by Category Group – Host

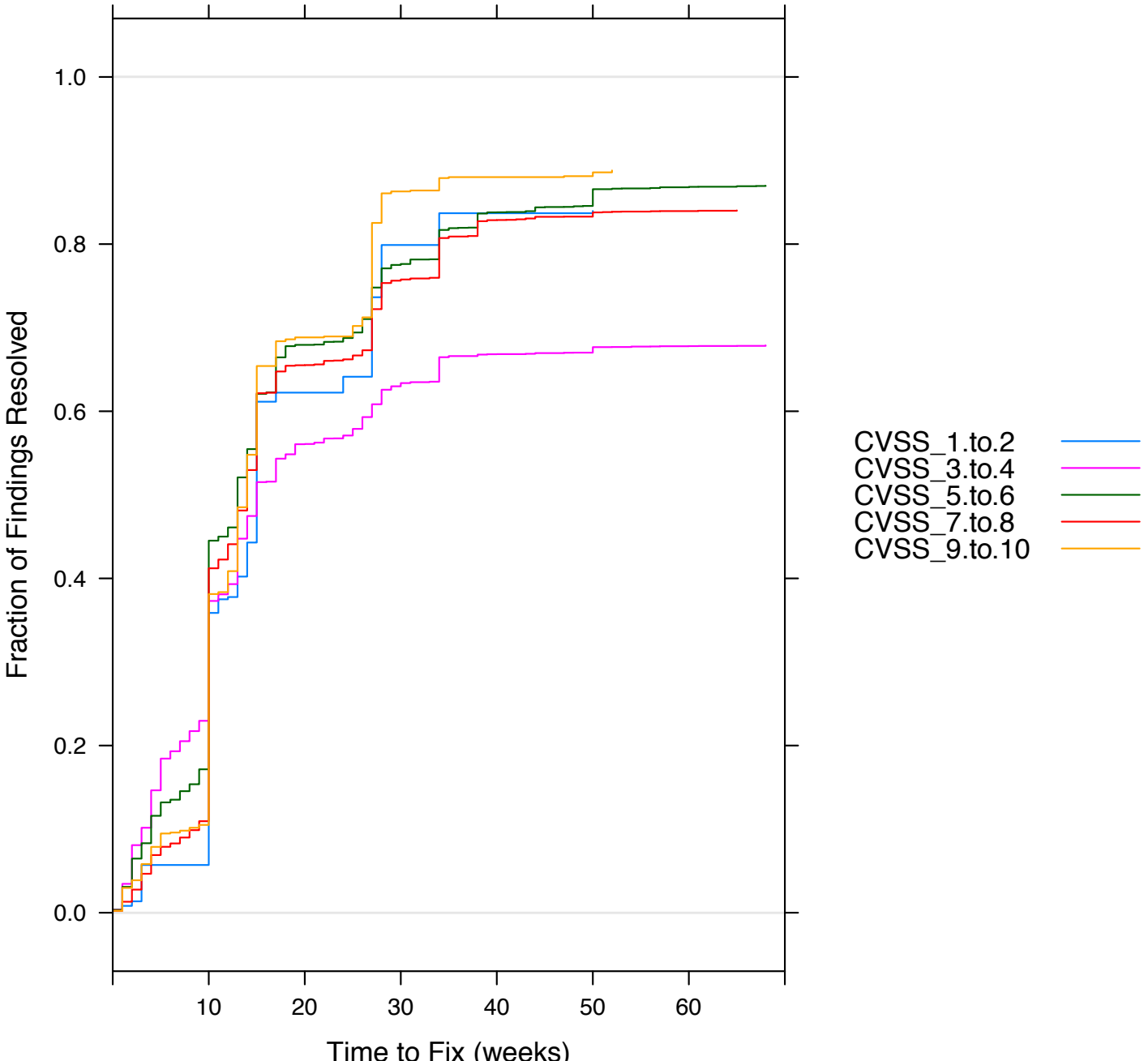


EnergyUtilities
FinancialServices
IT
LeisureMedia
PublicSectorLocal
Retail
Transport

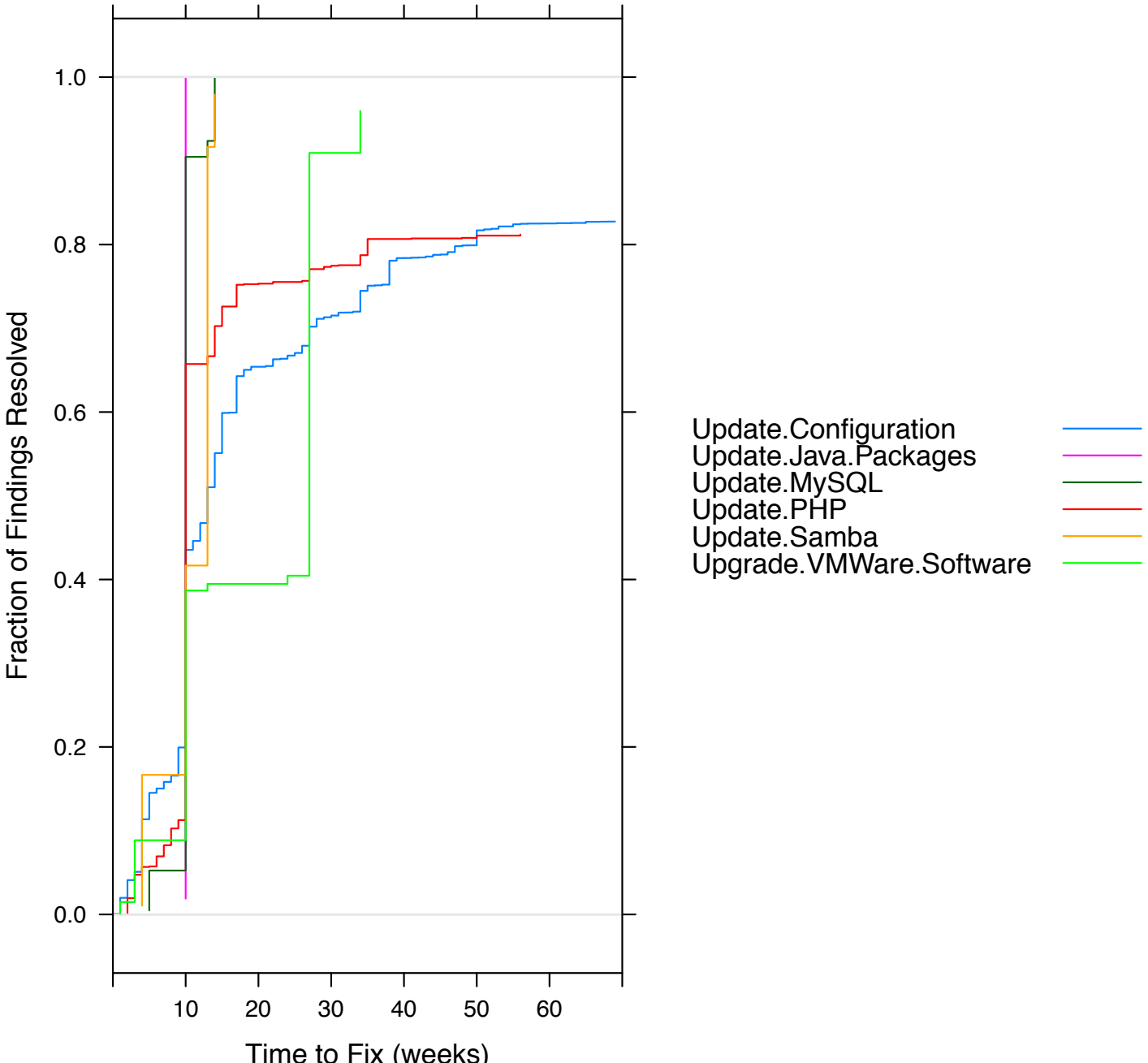
Time to Fix by Category Group – Web Application



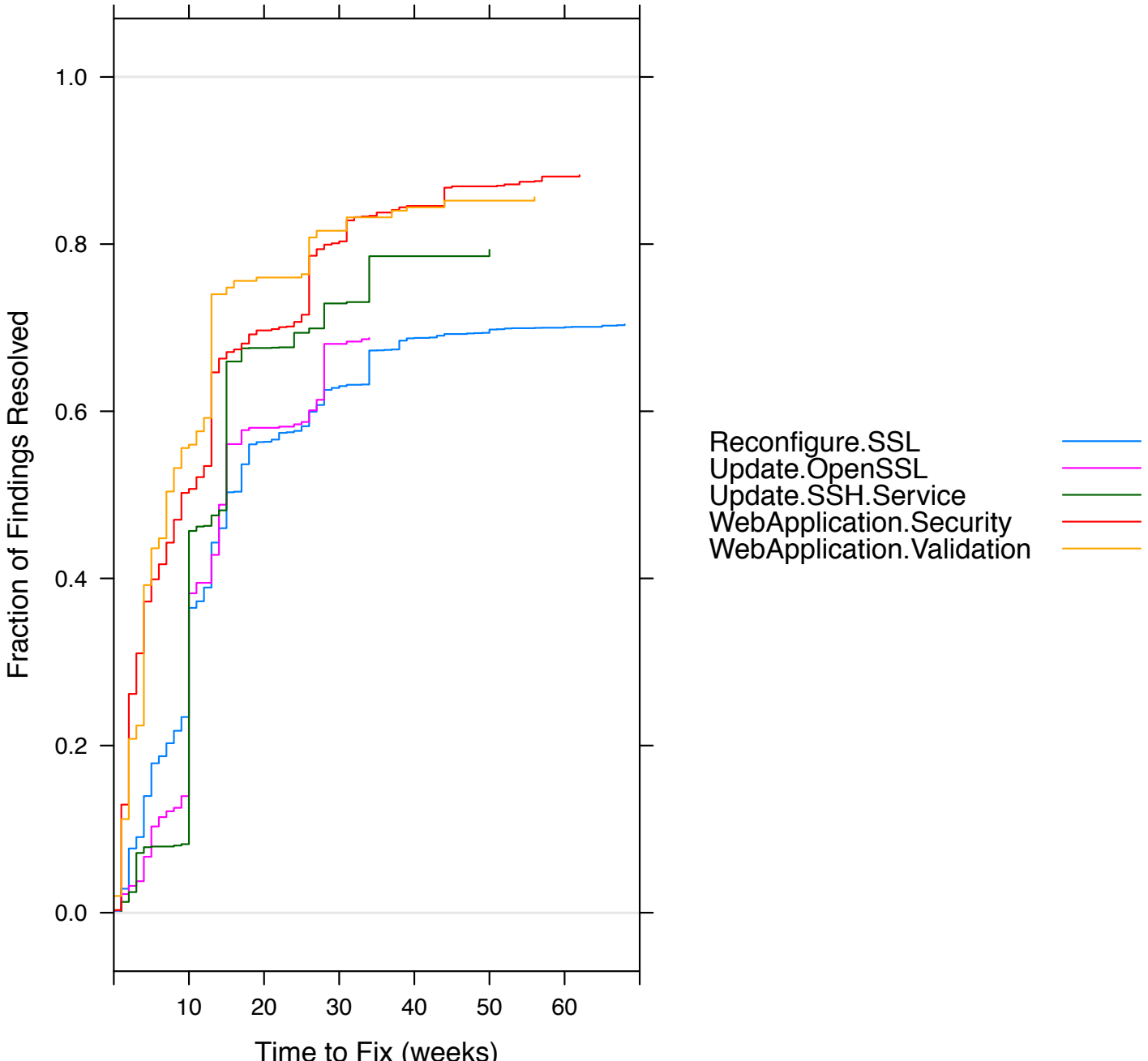
Time to Fix by CVSS Score – All Companies



Time to Fix by Solution Group – All Companies



Time to Fix by Solution Group – All Companies



Demo!

Key Takeaways

- Across all companies, most prevalent findings:
  - Web Application Server/Language
  - Network - PKI/SSH/SSL
  - Web Application Best Practices
  - General Network-related

Key Takeaways - Expected

- Managed services are valuable
  - FP rate by industry – 49%-89%
- Re: solution groups
  - Updating a language or package
    - Resolved quickly and at a high rate
  - Environment-specific solutions
    - Slower to be resolved and more likely to be left unresolved
  - Crypto-related (SSL/OpenSSL/SSH) lowest likelihood of being resolved (70%-80%)

Key Takeaways - Surprising

- Large percentage of findings addressed in 10-20 weeks
  - Tapers after 30 weeks, however some addressed past 50 weeks
- Does *not* appear to be a strong correlation between CVSS score and time to fix
  - But, higher CVSS findings resolved at a higher rate
- Up to 20%-40% disparity between industries of % fixed for web application and network findings

Thanks!

- clint.gibler@nccgroup.trust
- www.clintgibler.com
- @clintgibler