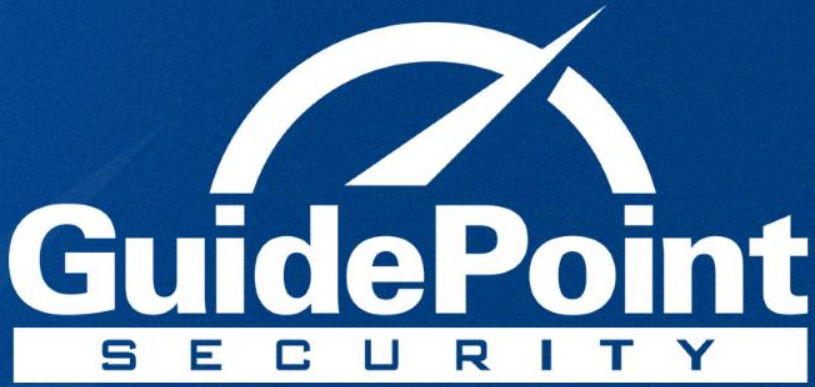


Lessons Learned from the Life of a Security Consultant

November 15, 2017

About Me

Seth Lucci

- Senior Security Consultant, Governance, Risk, Compliance Services (GRC) for GuidePoint Security
- Previously Government Contractor for the Office of the Chief Information Officer, NATO
- Extensive background in all things GRC

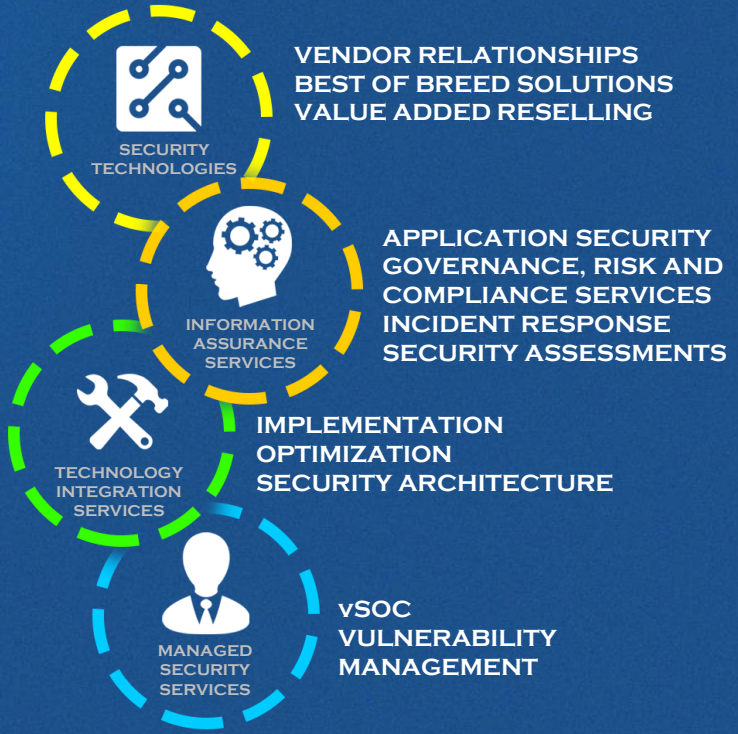
ABOUT GUIDEPOINT

GuidePoint Security

Leading Security Innovation

GuidePoint Security provides customized, innovative and valuable Information Security solutions that enable commercial and federal organizations to more successfully achieve their security and business goals.

GuidePoint ranked among the Top 3 Security Technology companies by the Washington Business Journal

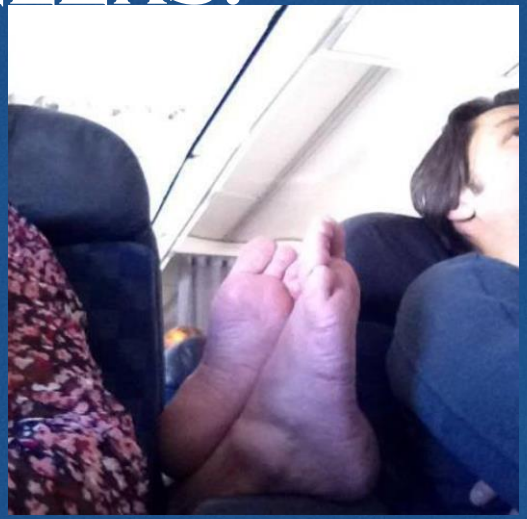


What this talk is NOT about

How to maximize your frequent traveler points

What this talk is NOT about

How to deal with inconsiderate travelers:



Source: @passengershame

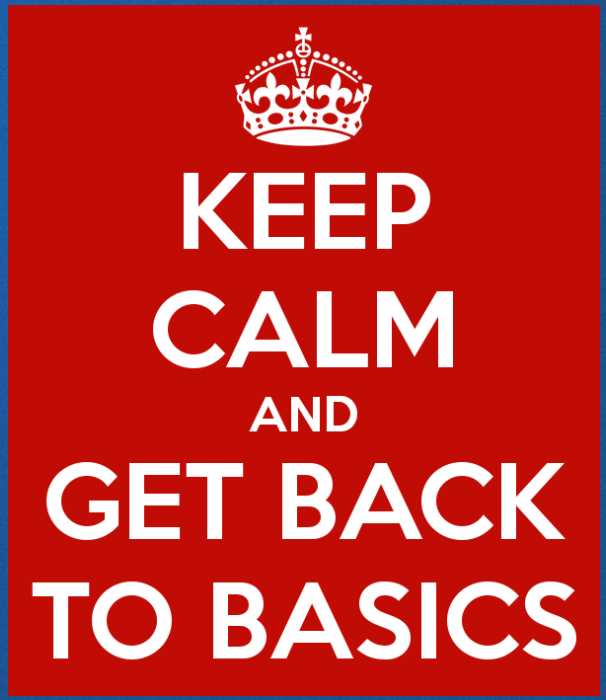
What this talk is NOT about

Clear up consultant lifestyle misconceptions

What are we here to talk about?

- Cyber Security!
- Three key observations:
  - Getting back to the basics
  - InfoSec Pressures
  - Changing Landscape

Getting back to the basics...



Just the basics… Vulnerability Management – Zero Day's aren't necessarily your biggest issue

vs.

Just the basics… Vulnerability Management

Source: 2016 Verizon DBIR

Just the basics… Vulnerability Management

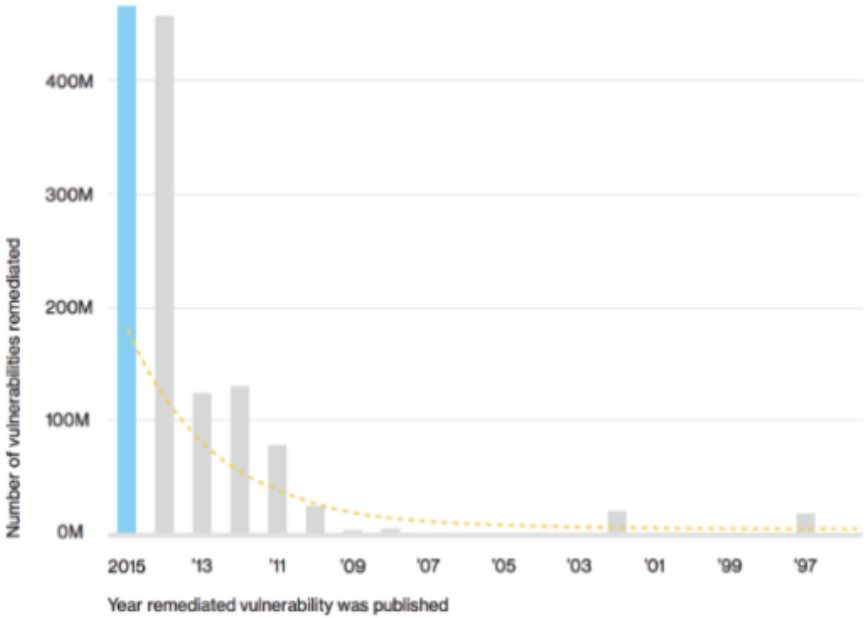


Figure 13.

Closure rate of CVEs by CVE publication date.

Source: 2016 Verizon DBIR

Just the basics… Secure Development

Starts with secure code training for developers
– Still terribly lacking
– Need to start with OWASP Top 10
– Five of the top 7 have been there since 2013!

Just the basics…

Source: owasp.org

Differences between 2004 and 2007

OWASP Top 10 2007	OWASP Top 10 2004
A1 - Cross Site Scripting (XSS)	A4 - Cross Site Scripting (XSS)
A2 - Injection Flaws	A6 - Injection Flaws
A3 - Malicious File Execution (NEW)	
A4 - Insecure Direct Object Reference	A2 - Broken Access Control (split in 2007 T10)
A5 - Cross Site Request Forgery (CSRF) (NEW)	
A6 - Information Leakage and Improper Error Handling	A7 - Improper Error Handling
A7 - Broken Authentication and Session Management	A3 - Broken Authentication and Session Management
A8 - Insecure Cryptographic Storage	A8 - Insecure Storage
A9 - Insecure Communications (NEW)	Discussed under A10 - Insecure Configuration Management
A10 - Failure to Restrict URL Access	A2 - Broken Access Control (split in 2007 T10)
<removed in 2007>	A1 - Unvalidated Input
<removed in 2007>	A5 - Buffer Overflows
<removed in 2007>	A9 - Denial of Service
<removed in 2007>	A10 - Insecure Configuration Management

OWASP - Top Ten 2013 – June 2013

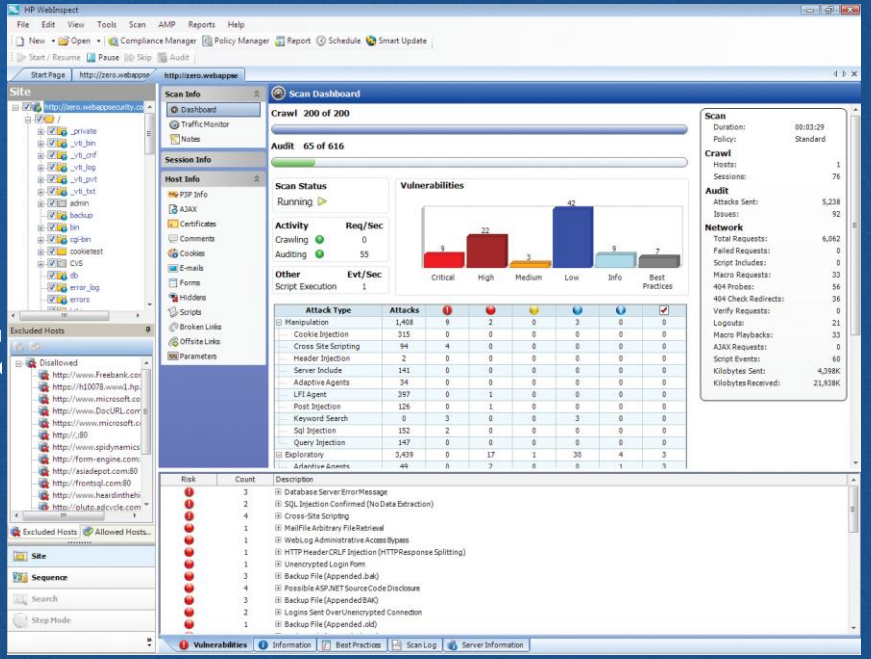
7

Top 10 2013	Top 10 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting
A4 – Insecure Direct Object References	A4 – Broken Access Control
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control	A7 – Insufficient Attack Protection
A8 – Cross-site Request Forgery (CSRF)	A8 - Cross-site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Unprotected APIs

Just the basics…
Secure Development

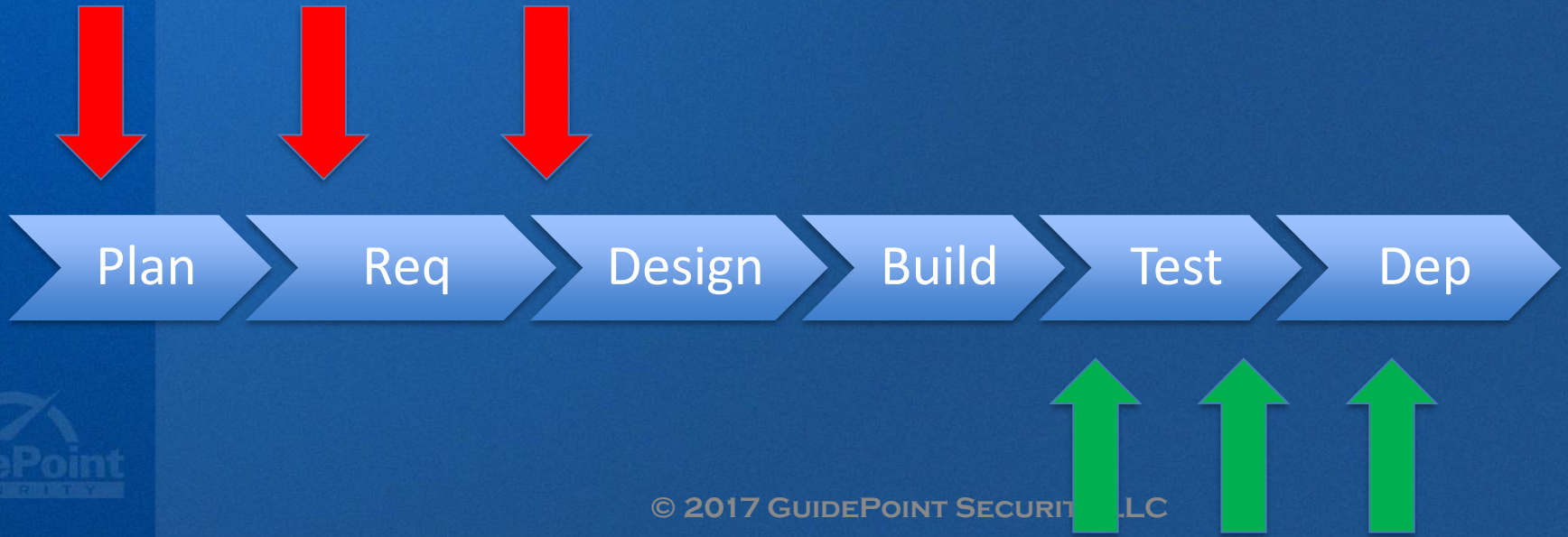
Organizations try to fix this with tools.

But don't get the expertise to run them or analyze the results.



Just the basics…
SDLC

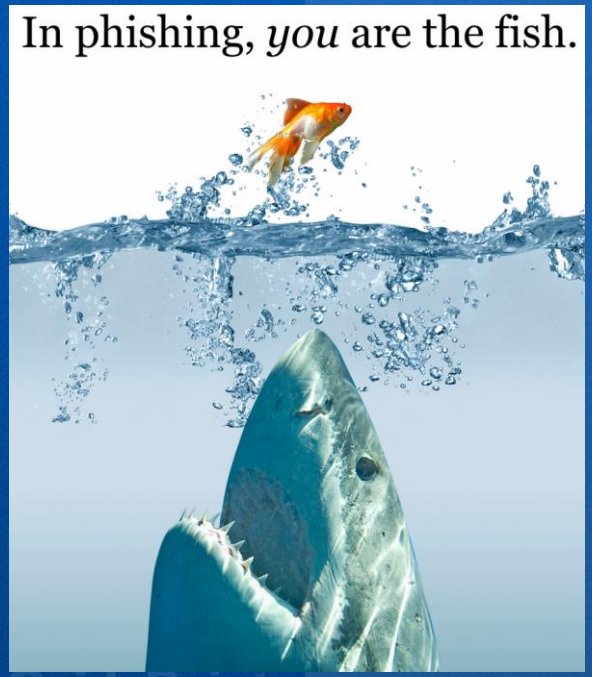
Security integration in the SDLC is happening too late if at all.



Just the basics…
Network Segmentation

The earth isn't flat and your network shouldn't be either.

Just the basics… Patching the Human Firewall



Source: www.uwec.edu

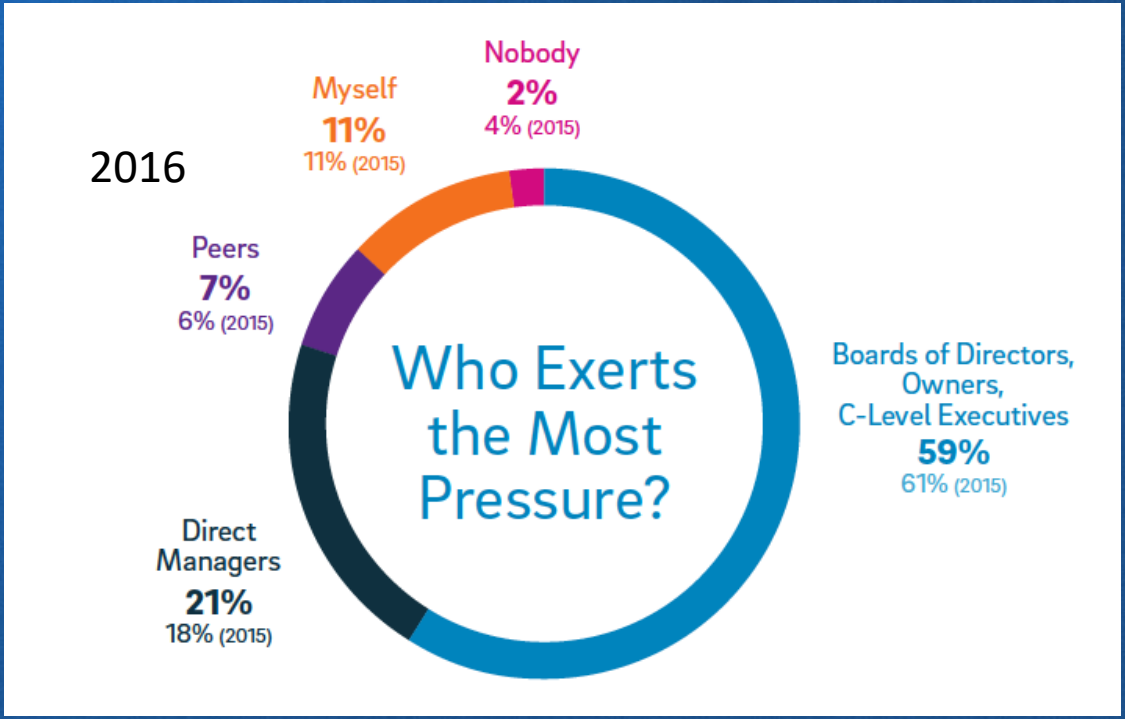
- Social Engineering / Phishing is working better than ever
- Users seem blissfully unaware of the value of data or their impact on data security

InfoSec Pressures

Under Pressure… Speed to Market

Source: 2016 Trustwave Security Pressures Report

Under Pressure… More Questions



Source: 2016 Trustwave Security Pressures Report

Under Pressure… Security Staff

Source: ISACA 2016 Cybersecurity Skills Gap

Under Pressure… Chasing the Silver Bullet

- Seen most often with technology solutions
  - Hardly ever accounts for the supporting people and processes

Changing Landscape

Changing Landscape… Regulatory / Contractual Expectations continue

Changing Landscape… Emerging Technology

EMERGING TECHNOLOGY: MOST PRESSURED TO ADOPT/DEPLOY

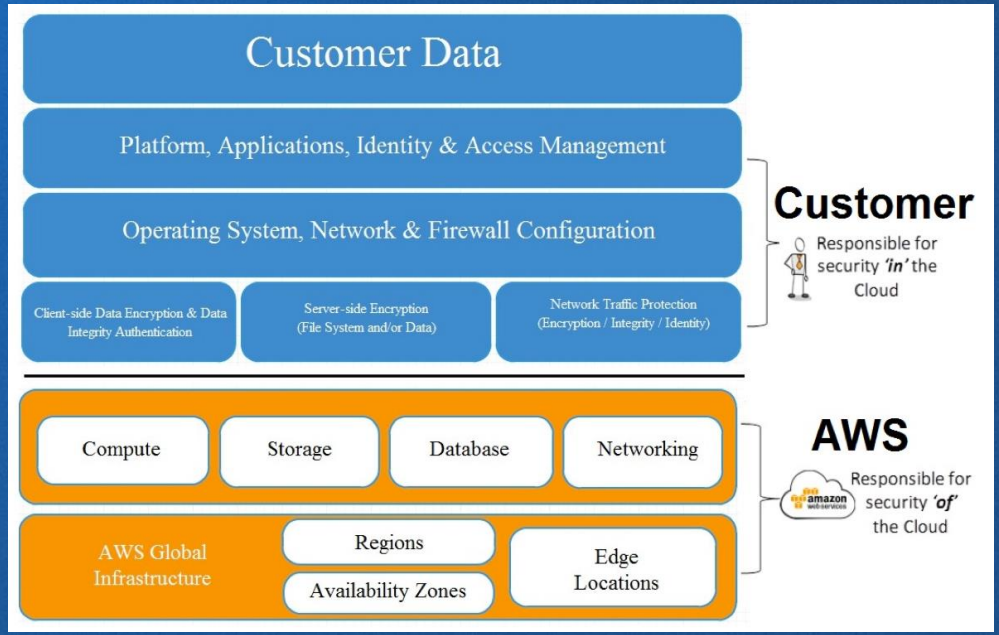
	2015 Report Overall		2016 Report Overall	United States	United Kingdom	Canada	Australia	Singapore
Cloud	47%	▼	44%	44%	49%	46%	37%	42%
Internet of Things (IoT)	N/A		17%	17%	17%	16%	16%	20%
BYOD	22%	▼	16%	17%	15%	15%	18%	13%
Social Media	9%	▲	10%	9%	8%	8%	19%	11%
Mobile Applications	15%	▼	7%	9%	7%	6%	6%	5%
Big Data	7%	▼	6%	4%	4%	9%	4%	9%

Source: 2016 Trustwave Security Pressures Report

Changing Landscape… Emerging Technology - Cloud

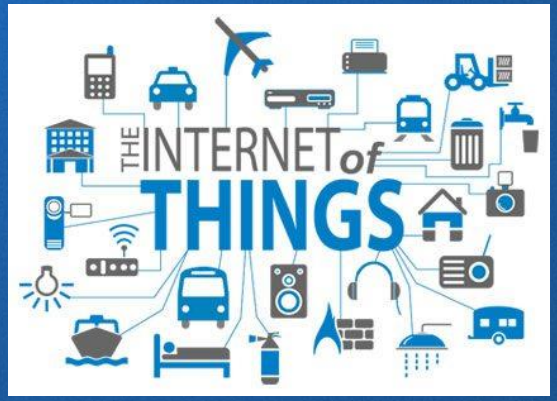
- Nobody understands the cloud!
- Cloud Computing Issues and Concerns
  - Business/Reputational Risk
  - Compliance – Legal/Regulatory
  - Privacy
  - Distributed/Multi-tenant security environment

Changing Landscape… Emerging Technology – Cloud



Source: https://aws.amazon.com/compliance/shared-responsibility-model/

Changing Landscape… Emerging Technology – IoT

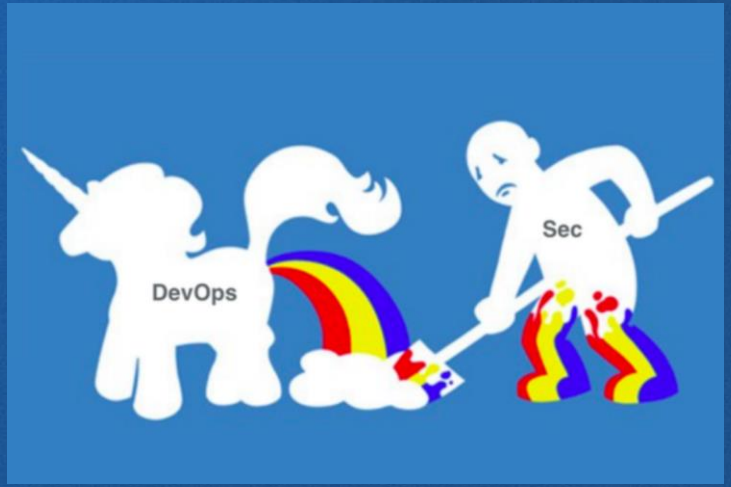


Already seeing security and privacy issues:

- Baby monitors / cameras
- Vehicle Hacking
- Medical Devices

Changing Landscape… Emerging Practice – Dev Ops

It doesn't have to be like this!



Source: Image attributed to Pete Cheslock at #DevOpsDaysAustin.

Conclusion

Back to the Basics – We have to catch up!	Pressure is Increasing – We have to stay grounded!	Changing Landscape – We have to get ahead!
• Vulnerability Management	• More Questions	• Regulatory / Compliance
• Secure Development	• Speed to Market	• Cloud
• SDLC	• Staffing	• IoT
• Network Segmentation	• Chasing the Silver Bullet	• Dev Ops
• Patching the Human Firewall		

Q & A

Contact:
Seth Lucci @
seth.lucci@guidepointsecurity.com or
Steve Jarosinski, Account Executive, Mid-Atlantic
@steve.jarosinski@guidepointsecurity.com
www.guidepointsecurity.com