



“We’ve been hacked! We did it!”



Transformation
through Partnerships

Rick Grandy
Lockheed Martin
Hanford Site

April 18, 2012

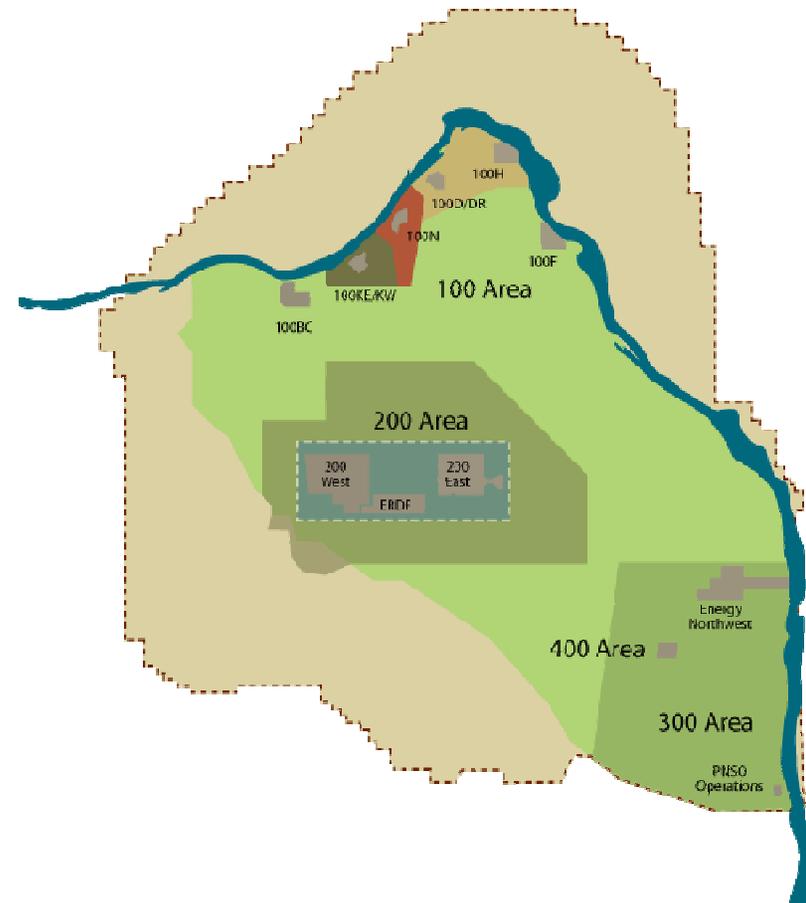
- Motivation
- What is Pen Testing?
- Establishing the Program
- Our Approach
- Pen Test Results
- Conclusion

“To make our customers extraordinarily successful in our unified mission of cleaning up the Hanford Site...”



Hanford Site IT Scope

- 586 square miles
- 8,000+ PCs
- 500+ servers
- 400+ applications
- 1,000+ miles fiber to 300 bldgs
- 12,500+ phones



Motivation

Why establish a Pen Test Program?

- Pen Testers found vulnerabilities my cyber team missed

Why establish an in-house team?

- Typical Pen Tests run for a week, APT-style attacks run for weeks and months
- Outstanding opportunity to grow my cyber team

Program Goal:

“Identify HLAN vulnerabilities and risks to ***provide management with an assessment of the general security posture*** of HLAN resources from an internal attacker perspective. Identify and validate technical weaknesses in HLAN security architecture, configuration, and/or controls relative to protection of HLAN system and information confidentiality, integrity and availability.”

What is Pen Testing?

- National Institute of Standards and Technology (NIST) Special Publication 800-115:
 - *Security testing in which evaluators **mimic real-world attacks** in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing **real attacks on real systems and data, using the same tools and techniques used by actual attackers.***

- Why Pen Testing?
 - Complements Assessments and Vulnerability scanning
 - Finds more “real world” risks
 - Many vulnerabilities found by scanners are not exploitable in the network environment
 - Pen Testing can use a “mosaic” of vulnerabilities to actually exploit (penetrate) a system
 - ***Pen Testing communicates the actual risk in a powerful way:***
 - Pen Tester to System Owner: “Let me show you screen shots from inside your application. Let me show you your information I took out of your system”
- Note: Pen Testing requires solid cyber security technical understanding and experience and disciplined processes to be effective and to minimize impact to the systems - ***it's not a game***

- Typical Pen Test Approach
 - Planning
 - Recon
 - Scanning
 - Exploitation
 - Report

Establishing the Program

- Very capable **people** that:
 - Are trained in Pen Testing & tools
 - Have solid domain knowledge and experience
 - Think like a hacker **but** are disciplined and thorough
- Solid **processes** in place
 - Pen Test Authorization (Scope, ROE, Trusted Agent, ...)
 - Templates for Pen Test Log, Final Report, ...
- Access to the right **tools**
 - Tool suite(s) that cover all phases of Pen Testing: Scanning, Exploit
 - Tools that enable the staff to be productive

- Develop Penetration Test Program Plan
- At least two staff trained and certified in Pen Testing
- Establish procedures for Pen Testing
- Acquire tools for Pen Testing
- Conduct Pen Test Pilot Exercise
- Develop FY 2011 Pen Test Schedule

- Some experience with Core Impact and WebInspect
- Selected Backtrack as primary distribution
 - Metasploit, nmap, ...
- Purchased for the team
 - Burp Suite Pro
 - High-end Windows laptops
 - VMware Workstation
 - Image snap software

- Plan and Procedure
- Templates (Pen Test Authorization, Pen Test Log)
- Pen Test Pilots
 - #1 was a table top exercise - validate procedures
 - #2 was against a server subnet
 - #3 was against a client subnet

- Selecting the right candidates:
 - Aptitude
 - Attitude
 - Experience: Windows/Unix/Network admin, programming
- Established a 4 person team
- Training selected:
 - SANS 560 - Network Penetration Testing and Ethical Hacking
 - SANS 542 - Web App Penetration Testing and Ethical Hacking

Our Approach

- No one on team had done Pen Testing
- If we can't exploit our network, is it because...
 - ... our network is very secure?
 - ... our Pen Test skills are very limited?
- If we demonstrate multiple exploits, is it because...
 - ...our team is very good?
 - ...our network is very insecure?

FY 2011 Q1

- Developed Pen Test program

FY 2011 Q2

- Focused on approach/items found by FY 2010 ST&E

FY 2011 Q3

- Focused on Personally Identifiable Information (PII)

FY 2011 Q4

- Focused on Pen Test team members' skills & more realistic attacks

- Start with a valid network account
 - Zero day attacks achieve PC compromise
 - Insider attacks have a valid account
- Seek “teachable moments”
 - Seek exploits that motivate change

- Partner with the IT staff
 - Don't trade Pen Test ego for IT staff cooperation
 - Exploit using non-privileged information
- Work together as a Pen Test **Team**
 - Not as a room of individual Pen Testers!

Pen Test #1

Pen Test Focus

- FY 2010 ST&E techniques and results

Pen Test Schedule

- Recon over whole period 2/7/2011 – 3/11/2011
- Exploits over a single Pen Test week

Results

Lessons learned

Screen Shots Removed

X Windows

Cold Fusion

JBoss

Server Power Down

Pen Test #2

Screen Shots Removed

PII in spreadsheet

Replicated accounts/pass-the-hash – DBMS w/PII

Meterpreter shell access to server with PII

Pen Test Focus

- Objective-focused target: PII

Pen Test Schedule

- Recon/Scanning/Exploitation 05/02/2011 to 06/17/2011

Analysis to identify likely (productive) sources of PII

- Shares on SAN, servers, clients
- Exchange public folders
- ftp servers
- Document Management System
- Key applications: Medical, HR, Finance, Security

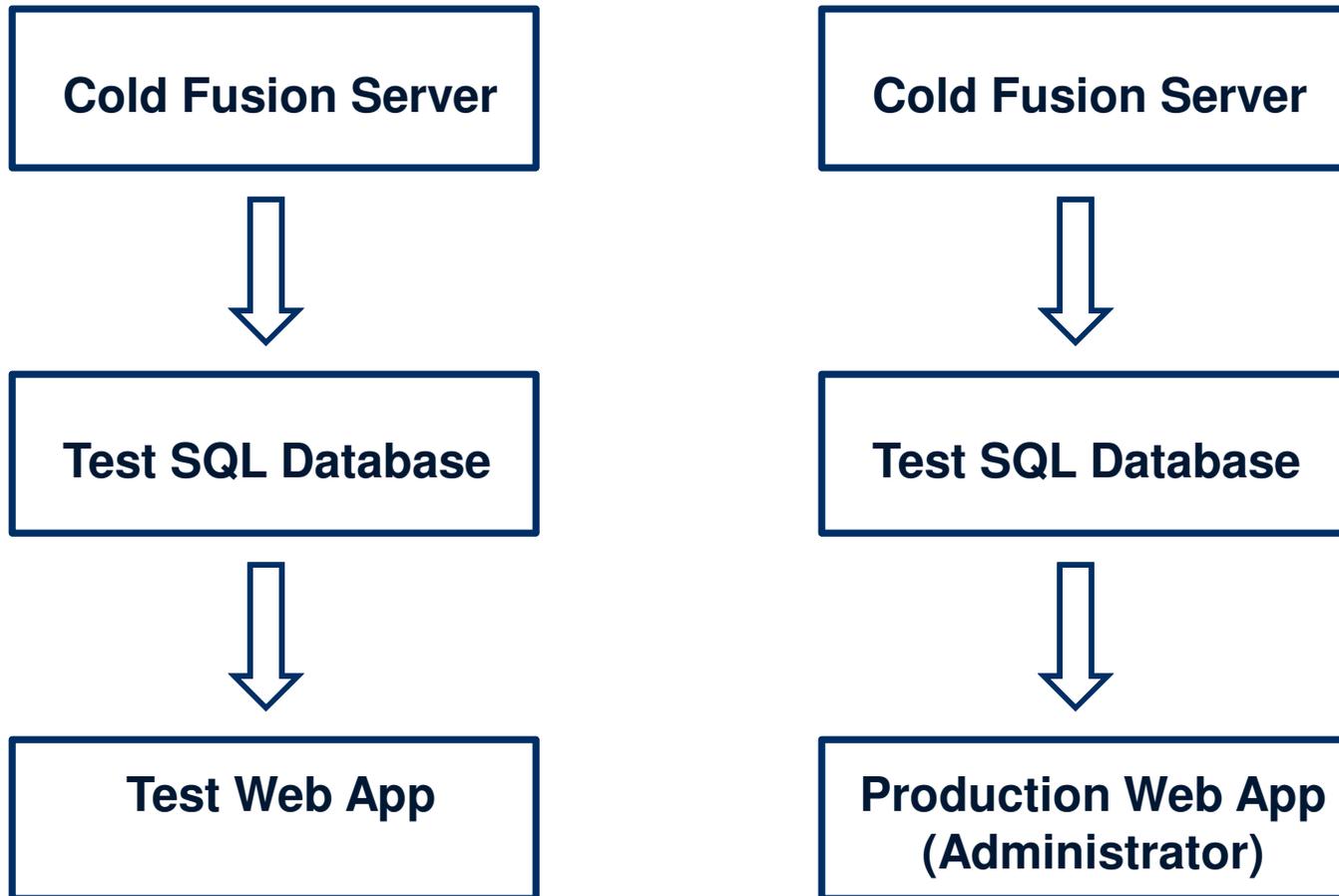
Pen Test #3

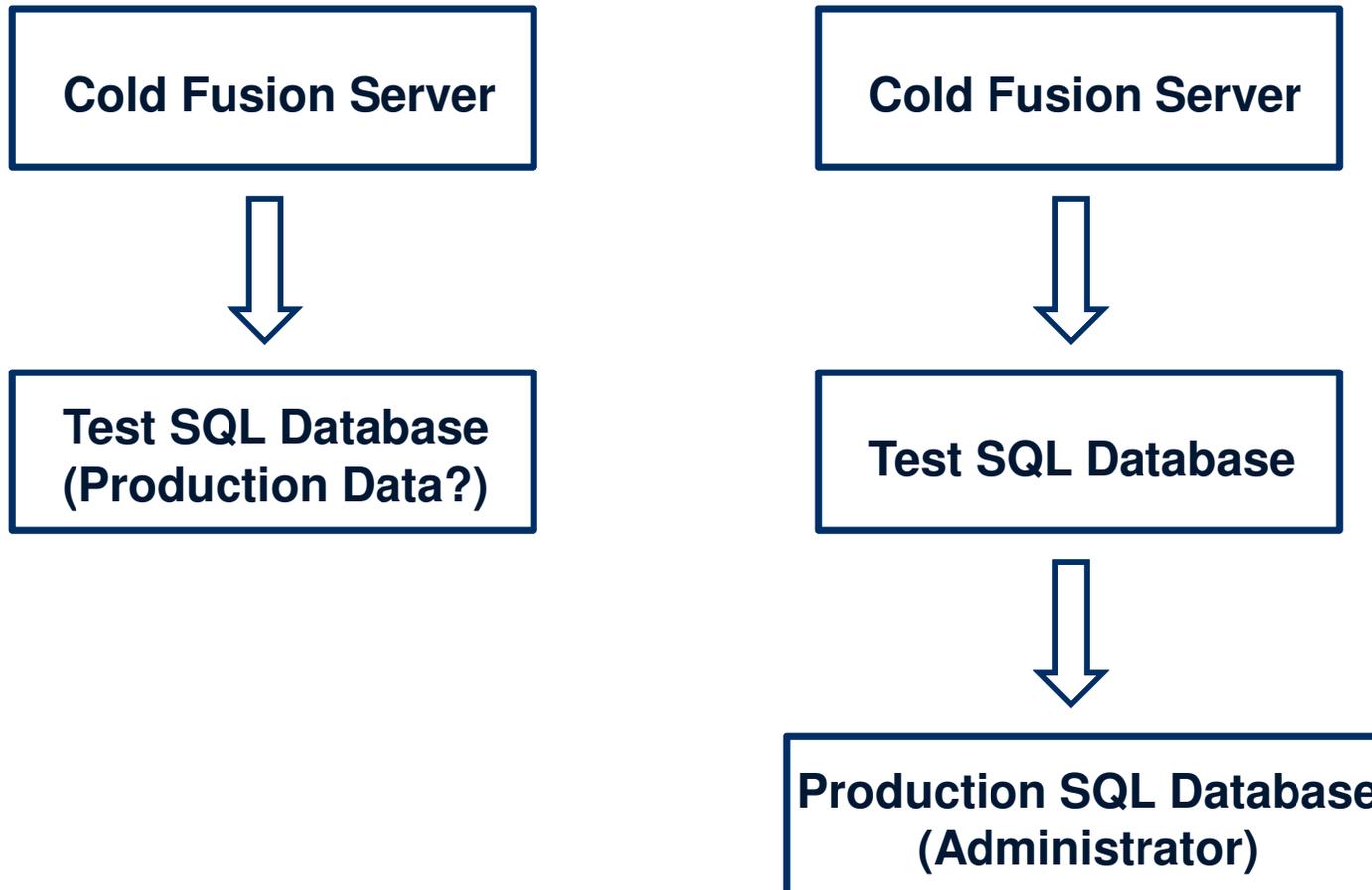
Q4 Pen Test Focus

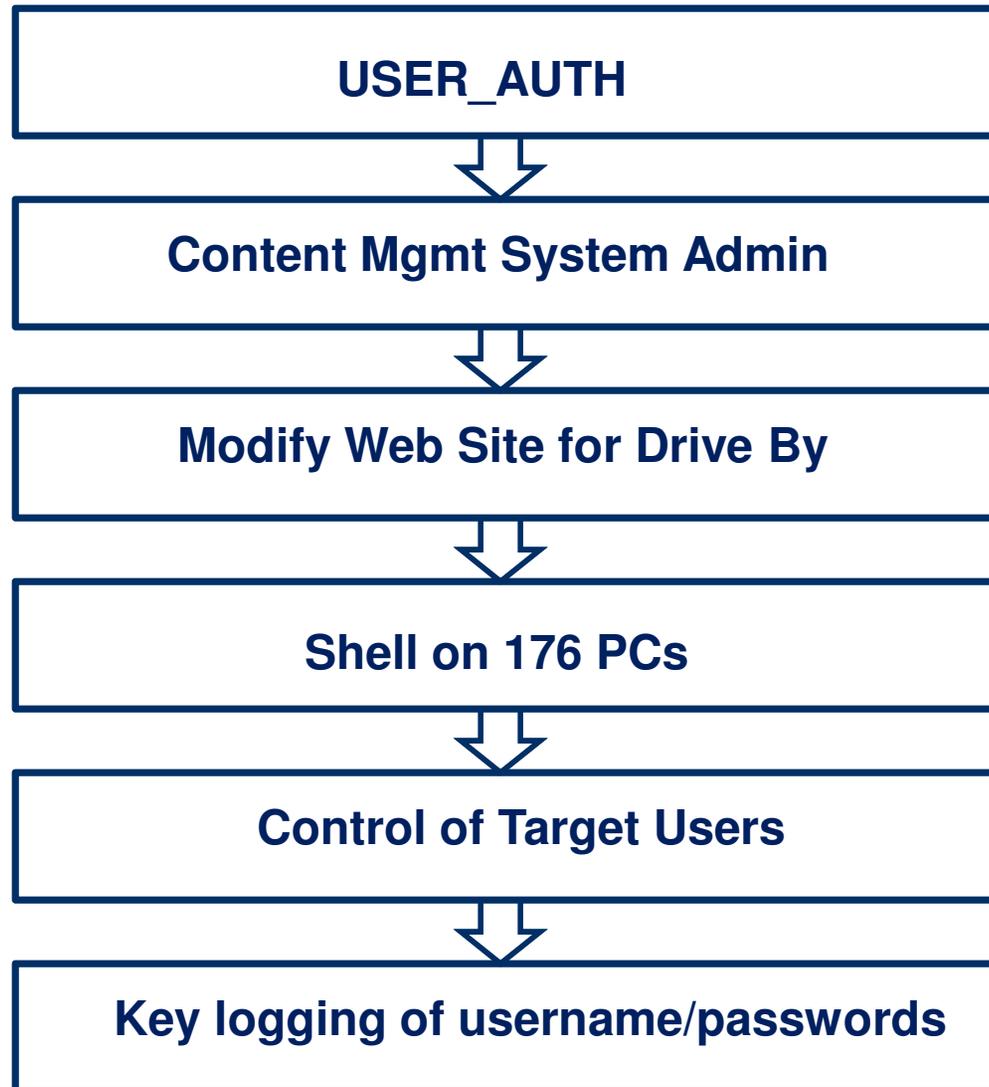
- Build Pen Test team members' skills
- More closely model attackers' behavior seen in DOE and other major breaches (RSA, ...)
 - Spear phishing email
 - Drive-by downloads from web sites
 - "Chained Exploits"
 - Focused on more sophisticated objectives
 - Multiple 'campaigns'

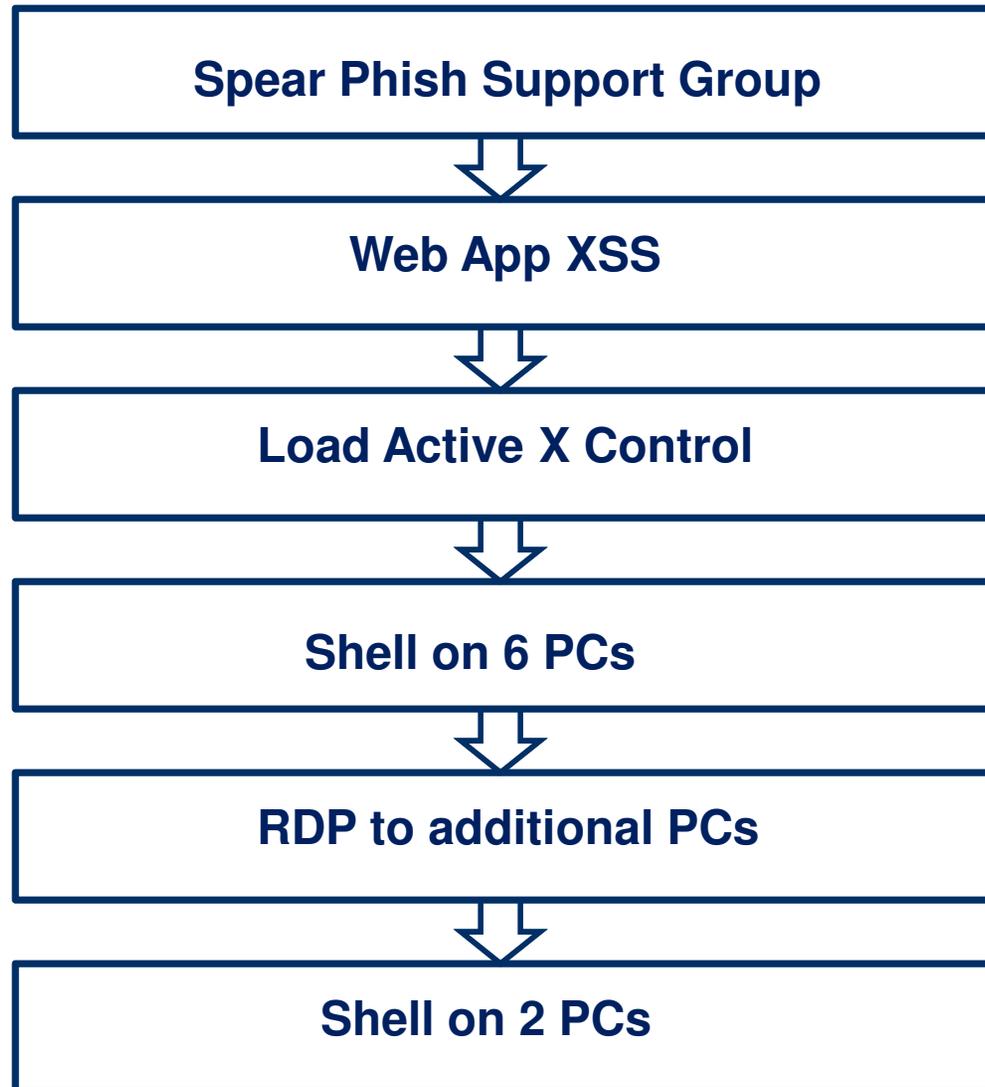
Q4 Pen Test Schedule

- Recon/Scanning/Exploitation: 07/25/11 – 9/17/11









Screen Shots Removed

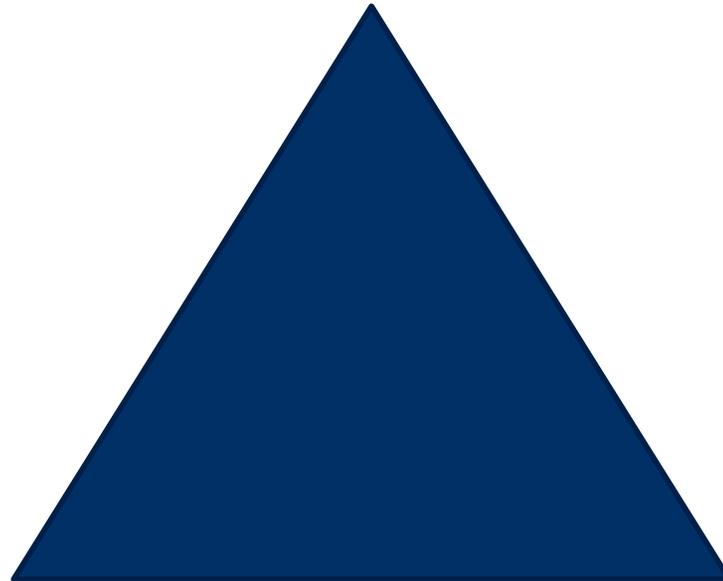
(various)

This Pen Test more closely paralleled the real-world attacks

- Use of spear phishing
- Use of drive-by downloads
- Compromise and control of multiple user PCs
- Undetected by Cyber incident or IT staff

Concluding Thoughts

**Security
Architecture**



Security Testing

**Incident
Management**

- Pen Tester aptitude, attitude, discipline and skills are key to success
 - Think like a tester...systematic, tedious, documented
- The importance of persistence
- The importance of indirect attacks/chained exploits

- Web-based applications are weak
 - Older web apps have poor security architecture and coding
 - Developers don't realize what proxies can do
- Very positive response from developers
 - Shifting focus to SDLC and security testing
- Beginning to think like a Pen Tester....you see your program very differently

- The Pen Testing program exceeded objectives
 - We found many weaknesses we would not have found otherwise ... including program weaknesses
- It's changed how we think about cyber security
- It's become an essential part of our “continuous monitoring”

Questions?