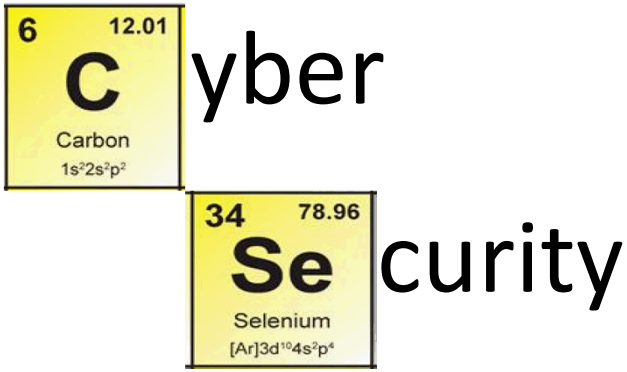
SAND2016-3757C

Exceptional service in the national interest

Sandia National Laboratories



yber

curity

Cyber Security Risk Management Pilot

Ted Lapina - tslapin@sandia.gov

Jeremy Baca – jeremy.baca@ppc.com

Jorge Hernandez – jgherna@sandia.gov

May 2016

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Agenda

Sandia National Laboratories

- Background
- Pilot Objectives
- Process Overview
- Restricted Access Implementation
- Remediation and Cybersecurity Management Tool
- Discuss Lessons Learned
- Questions

Background

- Production Operations is responsible for a low volume, full lifecycle manufacturing operation.
- We reside on the SNL campus and benefit form corporate support and protections.
- Our motivation is to seek innovative measures to enhance security within Production Operations, while leveraging corporate capabilities.

Pilot Project Objectives

Objectives based on needs of Production Operations

- Establish a cyber security baseline of Production Operations cyber assets
  - Subset of network attached devices
  - Web applications
- Establish ability to track and compare scans, over time, to quantify cyber security improvement.
  - A tool will be necessary to manage amount of data
- Establish an action plan to help improve overall cyber security posture.

Process Overview

- Identify needs / requirements
- Partner with appropriate stakeholders
  - Application Developers
  - Cyber Security Services & Technology
  - Engineering Infrastructure - Software Testing
  - Server Admins
- Receive formal approval
- Install Risk Remediation tool with help from vendor
- Determine proof-of-concept scan groups / Learn SW and optimal configuration
- Perform scans
- Upload and analyze scan data
- Establish action plan and implement mitigations

Restricted Access Implementation

Scan data is valuable to adversaries. Therefore we implemented restrictions to the tool and data.

Measures Taken

- Standard access management
- Two factor authentication
- Data repository only accessible via application service
- Application service blocked from Internet access
  - No push or pull allowed.
- Monitoring to ensure no external communication attempts
- Manual update process.

Cyber security in Risk Management Terms

Sandia National Laboratories

Threat Intelligence Sources

MITRE

metasploit

DShield.org

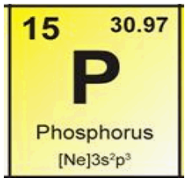
EXPLOIT DATABASE

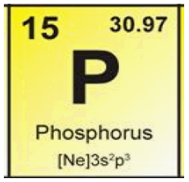
... Many Others

- Risk management assessments for C level executives
- Ability to prioritize threats for the purpose of assessing investments
- Correlation of the same information for IT professionals
- Multitude of ways to display information depending on the user
- Use of threat Intelligence data updated in real time

PPC Cyber Security Services

Sandia National Laboratories



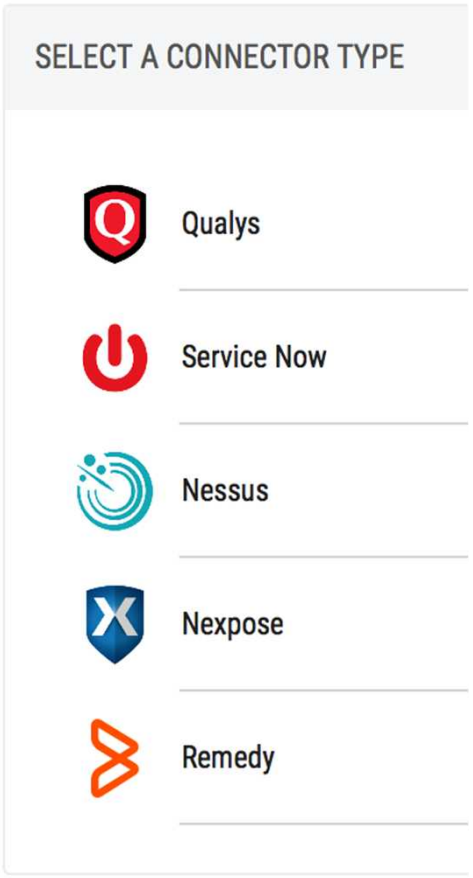


- SANS Certified Penetration testers and SANS Certified Forensics Analysts
- Ability to perform services in classified environments
- On-site deployment of server appliances
- Data encryption and user data rights
- Full on-site penetration testing
- Full on-site network and system forensics and mobile device forensics
- Training, Remediation and tool upgrades

ppc

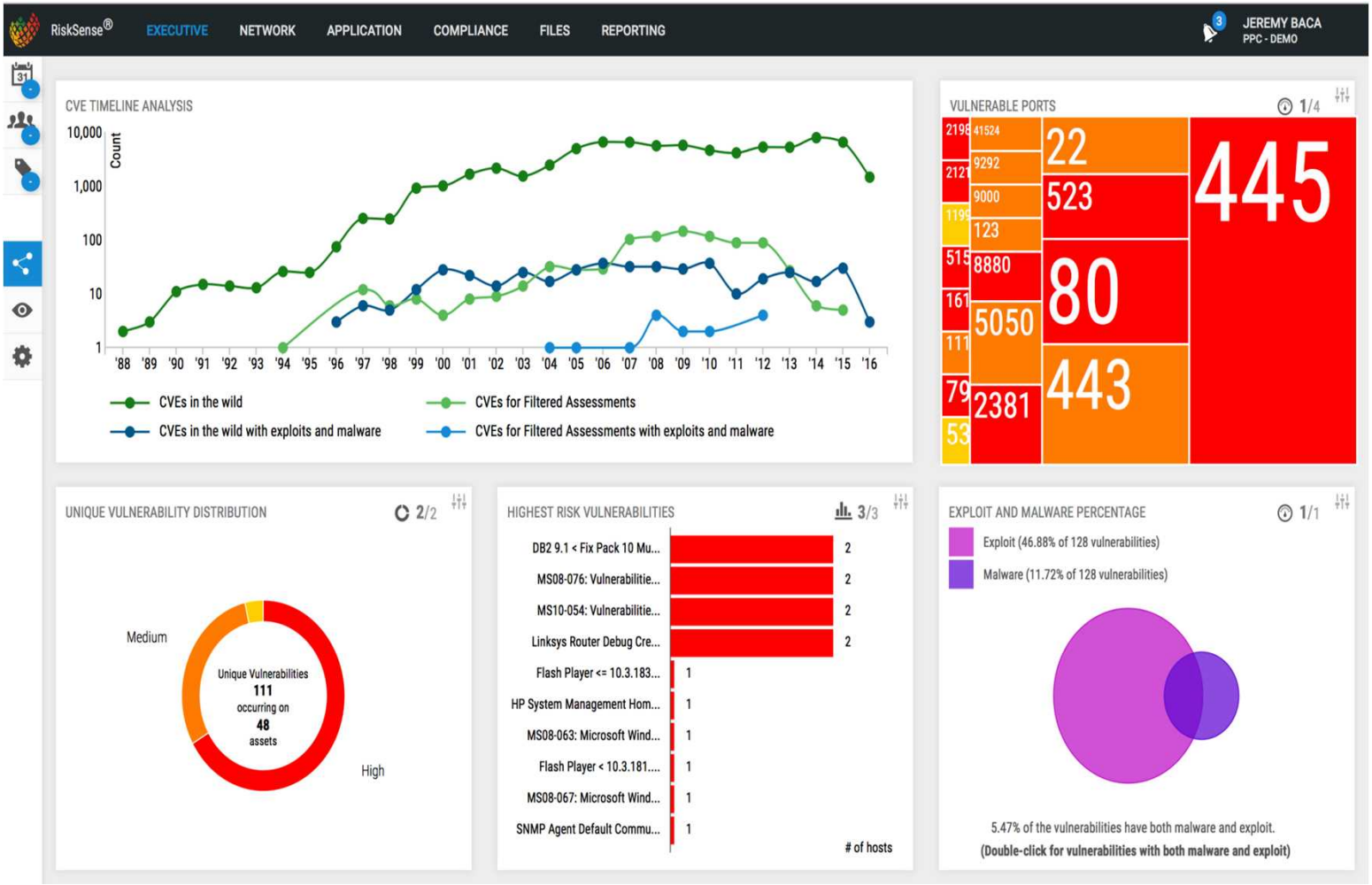
Remediation and Cyber Security Management

Sandia National Laboratories



- Compliant remediation management tools
- Integration with industry help desk tools such as Remedy and Service Now
- Ability to visualize security data by:
  - Asset type
  - Vulnerability
  - Risk
  - Exploit
  - Open sources
  - Malware
- Visualize Critical system vulnerabilities
- Differential analysis

Network Security Dashboard



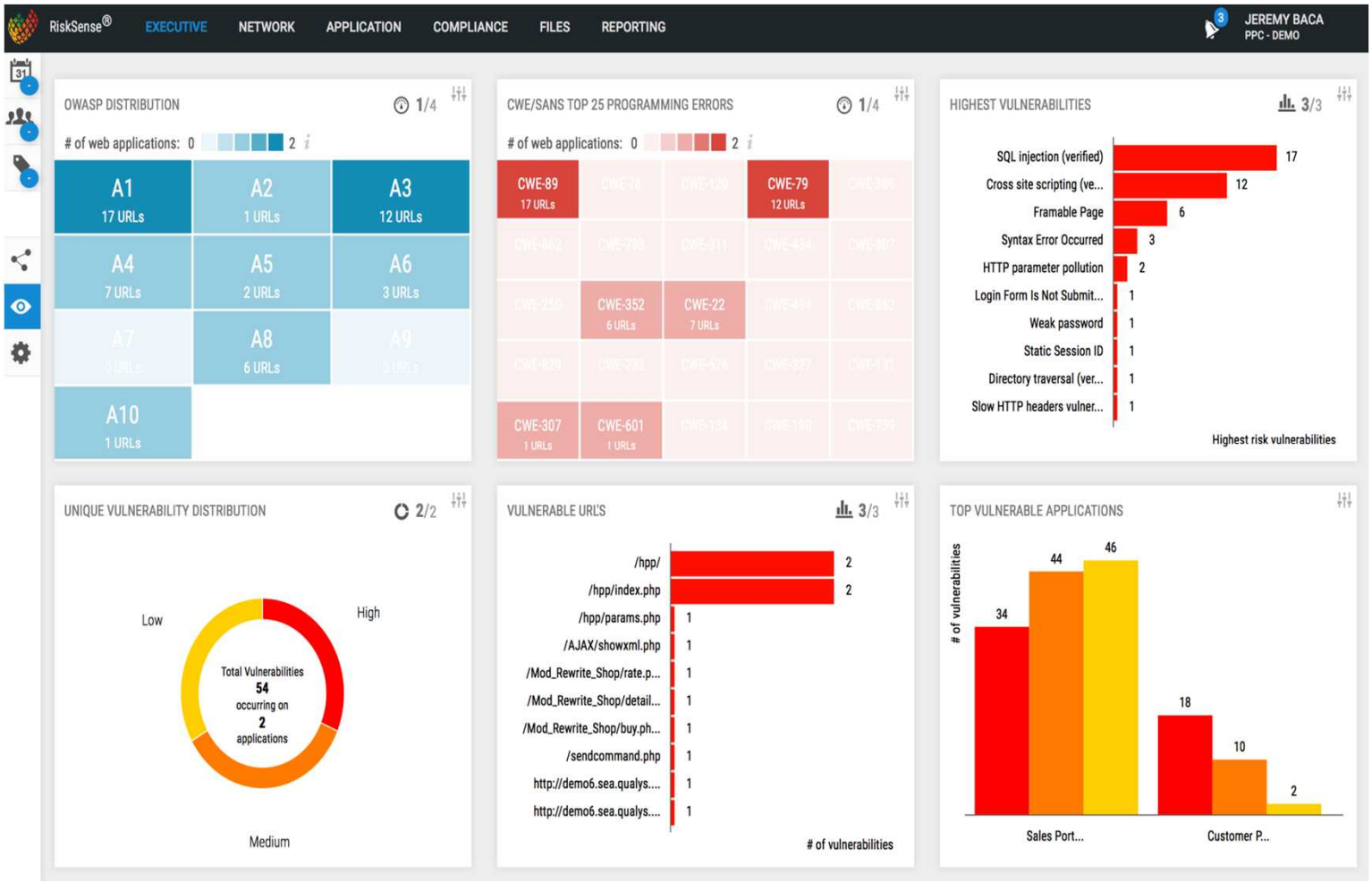
Asset Criticality and Vulnerability Distribution

Sandia National Laboratories

Name	IP Address	Asset Criticality	OS Name	Notes	Vulnerability Distribution			Tags
wujizmqlkflv.uxmbr...	1.0.36.42	5	Windows Server 2003	0	4	0	0	
mgtofnznqlkj.apvd...	1.0.36.34	5	Unix	0	4	0	0	
avoqjtjouslz.eoijls.r...	1.0.26.156	4	Unix	0	4	1	0	data center
auburqnjvbdn.srhre...	1.0.36.11	3	AIX	0	4	1	1	data center
gtbzewtcqpsw.tjwq...	1.0.36.5	3	Microsoft Windows Vista	0	0	0	0	
tunuygxwdllu.rwjfw...	1.0.36.24	3	Microsoft Windows Vista	0	0	0	0	Rescan
gscunllppywa.qgwb...	1.0.36.22	3	Microsoft Windows Vista	0	0	0	0	Rescan
udzyfqbsqiet.mjmid...	1.0.26.153	3	Microsoft Windows Vista	0	0	0	0	

Application Security Dashboard

Sandia National Laboratories



Aggregation of Vulnerabilities \ Threat data

Sandia National Laboratories

Network Scanners

... Many Others

- Use of a multitude of scanners and data
  - Nessus
  - Nexpose
  - Qualys
  - BurpSuite
- Automation of scans
- Network data
- Application data

Application Scanners

... Many Others

Compliance Management

Sandia National Laboratories

- NIST SP800-53 Rev 4, DISA, STIGs and thousands of others
- Adherence to existing and new standards
- Management of confidential information
- Management of proprietary information

Live Demo

Lessons Learned

Sandia National Laboratories

- Allocate plenty of time for due diligence, approvals, and setup.
- Time must be budgeted for performing manual software upgrades.
- False positives can be generated due to web application connectivity, performance issues. Use a second scanner to help ID false positives.
- Different scanners record host names in different formats. Without manipulation of the data there is the possibility of over reporting vulnerabilities for the same URL.
- Upload scans into a test client.
  - The system will allow you to upload the same scan twice.
  - There is no way to remove a scan.

Benefits Realized

Sandia National Laboratories

- Partnerships between mission and corporate
- Improved understanding of corporate protections
- Baseline captured
  - Reassured team and management of our security posture
  - Highlighted a few areas to improve
- Plan created for regular web application scans
- Capability to track and compare scans over time
- Web application scanning now part of SDLC
- Improved secure software development standards

Questions