To People Who Want To Reduce Their Server Vulnerabilities

- But Can’t Get Started!

Tomomi Imamura / Todd Neidinger

Presentation for

IT Professionals Conference

June 6, 2019
Qualys has been around since 2015 so what’s new?

• Agent-based Vulnerability Management
• Small program (agent) installed on a host:
  • Lightweight (~3MB) agent
  • Utilizes less than 2% of CPU resources
  • No reboot is required
• Agent collects host data to identify vulnerabilities
• We have total 22,000 licenses - Available for UW Madison departments at no cost

https://kb.wisc.edu/vulnerability/internal/page.php?id=90843
DoIT Datacenter Deployment

Project timeline and milestones

- **Jan 2018**: Project Kick-off
- **Feb 2018**: Scope / Design
- **Mar 2018**: Deployment
- **Apr 2018**: Cryptocurrency Mining
- **May 2018**: API
- **Jun 2018**: Troubleshooting
- **Jul 2018**: Data Analysis
- **Aug 2018**: CMDB Integration
- **Sep 2018**: Risk Acceptance Process
- **Aug 2018**: Decommission Workflow
- **Sep 2018**: Metrics
- **Dec 2018**: Remediation
DoIT Datacenter Deployment

Core Team Members

- Tomomi Imamura (Cybersecurity, Project Lead)
- Michael Ippolito (DoIT Network Services)
- Jennifer Kuo (Cybersecurity)
- Jon May (DoIT SEO/Shared Infra Services)
- Dan Michalski (DoIT SEO)
- Todd Neidinger (DoIT SEO/Service Management)
- Victor Ponelis (DoIT SEO/Service Management)
- Kevin Schmidtke (DoIT SEO/Service Management)
- Chris Spencer (Cybersecurity)
**DoIT Datacenter Deployment - Key Challenges**

**Challenges**

- **Installation** issue: Symantec, AIX no auto-deployment, Vendor managed servers, unsupported OS versions (RedHat 5)
- **Connectivity** issue: Servers unable to communicate due to security configurations and SSL certificate
- **Data** issue: Long hostnames truncated, Dual entries due to snapshots taken, PeopleTools not showing up as installed software
- **Communication** challenge: Executives wanted to know progress and had remediation expectations, how to convey complexity of patching
- **Business workflow** challenge: Unable to “Show me the vulnerabilities of the servers maintained by Jon May”
- **Process** issue: What do we do with false positives? What if we cannot patch?

**Solution**

- Technologists worked through technical issues, escalated to management as needed
- Collaborative work: Opening tickets with Qualys support, Technologists worked through technical issues
- Collaborative work: Opening tickets with Qualys support, Technologists worked through technical issues
- Report to show progress with statistics, upward communication to Director-level to let them know that remediation effort is much larger effort
- API data feed with the Cherwell CMDB, cross-referenced with existing server owners and application information
- False positives tracking process, Risk Acceptance form/process
DoIT Datacenter Deployment - Success

We had these successes:

• Remediation efforts started taking place as we started sharing the Qualys data using the Cherwell dashboard.

• The “Urgent” severity level vulnerabilities have been reduced by 70% since the deployment.

• Leading to funding approval to purchase additional 20,000 Qualys Cloud Agent licenses - Available for UW Madison departments at no cost.

• Zero-day vulnerabilities – E.g. Oracle Critical Patch Update (CPU) and RDP BlueKeep. Notifying and monitoring the patching progress

• We now have metrics!
DoIT Datacenter Deployment - Success

High Severity Vulnerability History By Team

- CCI-Virtualization
- NS-App Admins
- NS-Voice-Legacy
- NS-WAN
- SE-AIX
- SE-DSA
- SE-Linux
- SE-Virtualization
- SE-Windows
- US-DS PCI
- None

Date: 9/16/2018 - 3/22/2019
Qualys CMDB Integration Overview

- DoIT Managed Servers
  - AIX (64)
  - Linux (380)

- Cloud Agents
  - Windows (427)

- Qualys Cloud
  - Asset Inventory
  - Vulnerability Data
  - Dashboards/Reports

- Qualys API

- WiscIT CMDB
  - Dashboards
  - Searches
  - Reporting
Qualys CMDB Integration Overview

Qualys Data

- OperatingSystem
- Patchable
- TimesFound
- PublishedDate
- FirstFound
- Diagnosis
- Software
- Solution
- Title
- Manufacturer
- Remote
- Vulnerability
- Consequence
- IsDisabled
- Vulnerability Type
- IsIgnored
- IPAddress
- LastLoggedInUser
- PCI
- Severity
Qualys CMDB Integration Overview

WiscIT Data

Description
TechnicalService
Environment
Title
EntityType
AdminTeam
Related
SupportInformation
UDDSS
Admin
CI's
Owner
Location
Stakeholders
Thank you!

Questions?

Tomomi Imamura  tomomi.imamura@wisc.edu
Todd Neidinger  todd.neidinger@wisc.edu