Vanguard Configuration Manager Implementation

Mike Wenger

Wisconsin Physicians Service

Madison, WI

7 Feb, 2013

Session Number 12794

SHARE in San Francisco 2013

Wisconsin Physicians Service

- WPS
  - Who We Are
  - Our Challenge
  - Our Opportunity

- What is VCM?

- Our Experience

WPS

- Major Health Insurance Provider in Mid-West

- Over 5 million Claims Processed Per Month
  - WPS Health Insurance
  - TRICARE
  - Medicare

Our Challenge

- Multiple Government Agency Security Compliance

- Audits Overwhelming
  - More than 18 Different Audits Annually
  - Most Comprehensive Used to Respond to All
  - Government Most Complex/Consuming
    - TRICARE - DIACAP Requirements (ATO)
    - Medicare – CMSR, Section 912, etc.

Our Challenge

- DIACAP Authority to Operate (ATO) Most Comprehensive
  - TRICARE Management Authority (TMA)
  - Annual Multiple Month Process
  - Significant Manual Effort
  - Significant Impact on Normal Operations

Our Challenge

- TMA Monthly Site CD
    - CA-Examine Based Scripts
    - Based on DoD/DISA STIGs
        - Department of Defense (DoD)
        - Defense Information System Agency (DISA)
        - Security Technical Implementation Guide (STIG)
    - Results Used for Other Audits, But Clumsy

Our Opportunity

- TMA Shifted Annual Certification to Contractors
  - Discontinued DIACAP ATO On-Site Visits
  - Switch to National Institute of Standards and Technology (NIST) Based Requirements
  - Annual Site Visits Replaced with WPS Assessment
  - WPS Executives Attest to Security Posture
    - Can Be Audited Anytime
    - Responsibility Now Ours!
  - Opened Prospect of Improving Internal Processes

Complete your sessions evaluation online at SHARE.org/SFEval

Our Opportunity

- Medicare Became Most Comprehensive Audit
  - CMS Minimum Security Requirements (CMSR)
  - Covers All of TRICARE National Institute of Standards and Technology (NIST) Based Requirements
  - NIST /CMSRs Tie Back To DoD/DISA STIGs
  - If We Focused on CMSRs, Results Available for All Audits
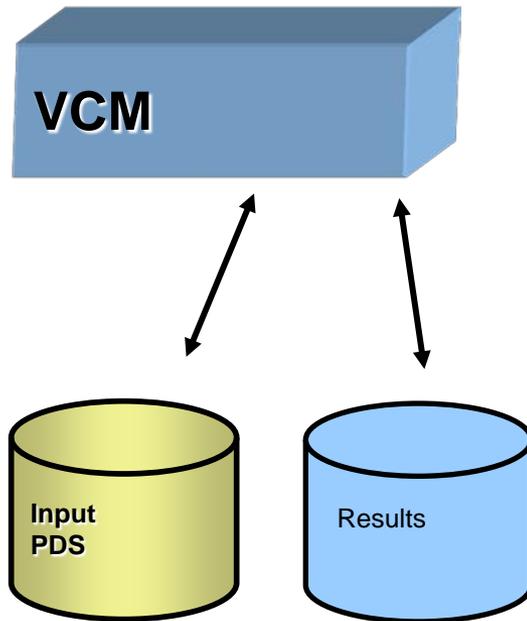
Our Opportunity

- Getting More Complex/Time Consuming!
  - With No TMA Monthly Site-CD, Manual Effort Unacceptable
  - Needed More Effective Technology
  - Researched Industry Options
  - Acquired VCM

Complete your sessions evaluation online at SHARE.org/SFEval

What is VCM?

- Vanguard Configuration Manager
  - Automated Vulnerability Assessment Solution
  - Assists in Passing a Security Readiness Review (SRR)
  - Tailored to DoD/DISA z/OS RACF STIG Checklist
  - Supports IBM OS/390 and z/OS RACF

Overview of Phases

Common Configuration *1*

Collection *1*

Execution *2*

Results *2*

Input PDS

RACF DB

Results

RACF DATA SECURITY MONITOR	
DATE: 03/13/99 TIME: 09-15:47 PAGE: 1	
SYSTEM REPORT	
CPU-ID	010191
CPU MODEL	3090
OPERATING SYSTEM/LEVEL	MVS/3.8
SYSTEM RESIDENCE VOLUME	SYRES01
SMF-ID	SMF1
RACF VERSION 2 RELEASE 1.0 IS ACTIVE	

1 ISPF

2 ISPF or Batch

VCM – Other features

VCM

Input
PDS

Results

1. History Processing
2. Compare Processing
3. Filter Processing

Our Experience – 'The Old Days'

- TRICARE - DIACAP ATO Process
  - Very Time Consuming
  - Used CA-Examine and SRR Scripts for 6 LPARs
  - Additional Week to Understand/Resolve Findings
  - Consumed Staff of Over 15 Techs and Security Staff
- Medicare Efforts Duplicated/Convoluted Effort
- High Risk of Missing Mitigation Requirements
- Potential Adverse Impact on Contracts/Future Business

Our Experience – Today

- VCM Runs Concurrently on All LPARs
  - 1-2 Hours Total
  - Findings Are Immediate and Clearly Described
  - Now Run Weekly for Proactive Scanning
- Reports Sent to Administrators For Resolution
  - Mainframe System Programmers
  - IT Security Personnel
  - Imported to Internal Central Vulnerabilty Data Base
  - Combined with Multi-Platform Reporting

Our Experience – Today

- Quarterly Submission Requirements Easily Met
- High Confidence Levels for TRICARE/Medicare Needs
- CMS May Require Monthly Scans
  - Not Possible with Old Method
  - Can Do Easy With VCM
- Reduced Staff Involvement from 15+ to 3
  - Old Process Required Manual Reviews
  - VCM Tailored to DoD/DISA STIGs
  - Reviews Automated

Our Experience – VCM Acquisition

- Internal Proof of Concept
  - Two Trainers for a Week
  - Installation/Configuration/Collection Very Smooth
  - Outstanding Results!
- Acquired/Continued Running
- Superb Support Since
  - Problems Fixed Within a Week
  - Some Immediate
  - New STIGs Supported Within a Month or Less
  - Updates Come as Single SMP/E PTF

Complete your sessions evaluation online at SHARE.org/SFEval

Wrap-Up

- Government Security Requirements Complex!
- Getting More So
- Lack of Appropriate Technology Costly
  - Staffing
  - Loss of Contract
  - Future Business Unlikely
- VCM Put WPS in Proactive Position
  - Minimized Staff Impact
  - Improved Security Posture
  - Well Positioned for Upcoming Changes

Complete your sessions evaluation online at SHARE.org/SFEval