CMS Case Study: SCAP-validated Vulnerability Management

C. Ryan Brewer
Chief Information Security Officer
October 27, 2009

AGENDA

- CMS – Context & Programs
- Legacy Information Security Program
- Back to the Basics…The Approach
- The How…
- Value Add
- Review

WHAT IS CMS?

- The Centers for Medicare & Medicaid Services
- 1977 united two largest federal health care programs Medicare & Medicaid
- Formerly Health Care Financing Administration (HCFA)
- Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA)

CMS PROGRAMs

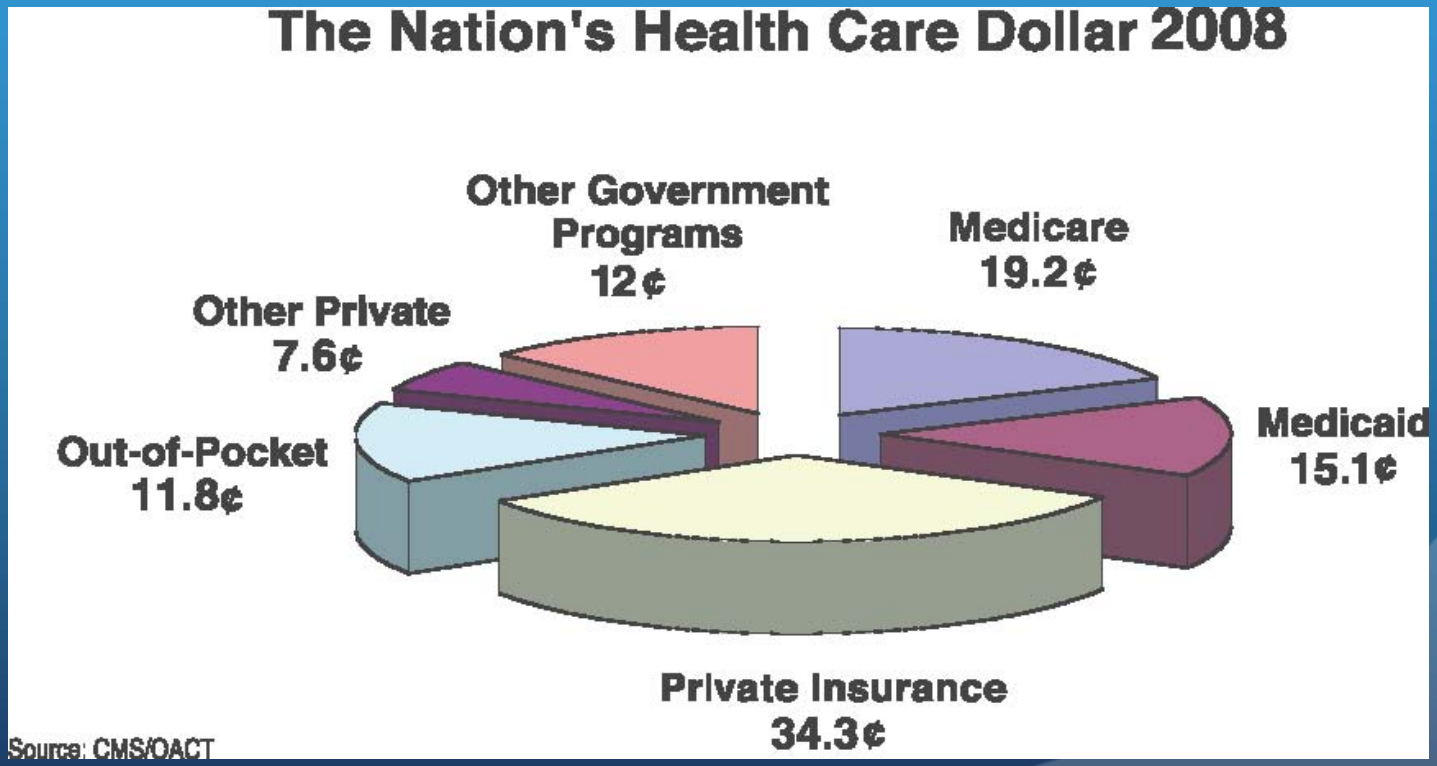
- Medicare: ≥65, disabled, End Stage Renal Disease
  - Part A – Hospital Insurance
  - Part B – Medical Insurance
  - Part C – Medicare Advantage – In lieu of A & B
  - Part D – Medicare Prescription Drug
- Medicaid: Low-income
  - CMS provides guidelines
  - States determine eligibility

CONTEXT

- Very large insurance provider >90 million beneficiaries
- ~21% of Federal Budget 2008 - $670 billion
- 15 million eligibility requests per week
- ~1.2 million providers
- >1.2 billion Medicare claims
- >1.0 billion prescription drug claims annually

CONTEXT

- Medicare & Medicaid = 34 cents of every dollar spent on health care in the US



LEGACY INFOSEC PROGRAM

LEGACY INFOSEC PROGRAM

- Compliance Based Approach
- Stove Pipe Approach to Monitoring
- Non-standardized metrics
- 2002 Security Model
  - Verbal vs. Validated
- Existing Culture

SO WHAT?

- What is Missing?
- Conficker helped me!
- Oh Yea….the Basics!

THE BASICS

- Step 1 - Know thy system
- Step 2 – Make sure you do step 1 really well (Don't fall for the thumbs up!)
- Step 3 – It's not sexy, but make sure step 1 is done really, really, well…

KNOW THY SYSTEM - RATIONAL

Risk = Threat X Vulnerability

- 2002 Security Model = Focus on Threat!
- 2009 Security Model = Focus on Vulnerabilities!
  - Too Many Threats to Focus on
- Make Vulnerability a Zero and then do the Math

KNOW THY SYSTEM – REAL WORLD

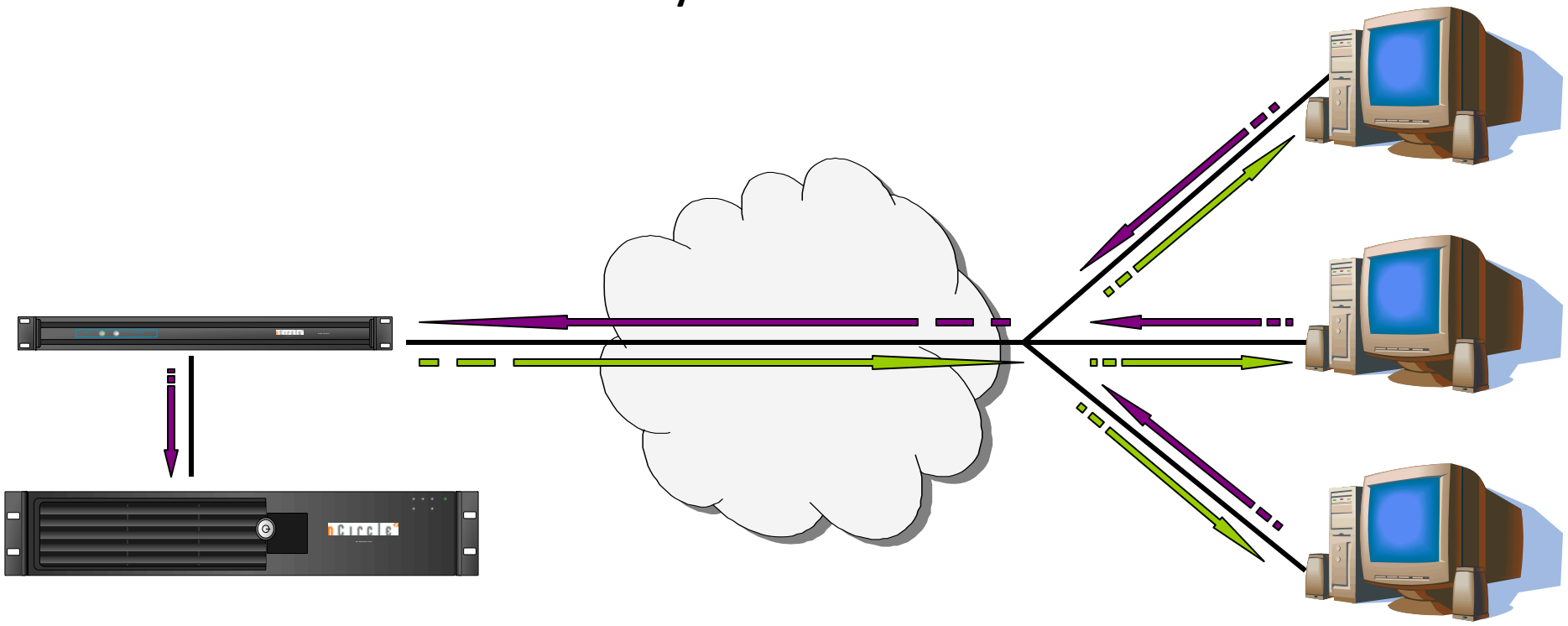
Enterprise Class Vulnerability Management

- Enterprise view into all IP enabled devices
- Apples-to-apples comparison
- Enterprise inventory
  - Who owns the IP?
  - Part of which network?
  - What is the current risk posture?
  - What business function does it support?
  - Are there others?

VULNERABILITY SCANNING 101

HOST DISCOVERY

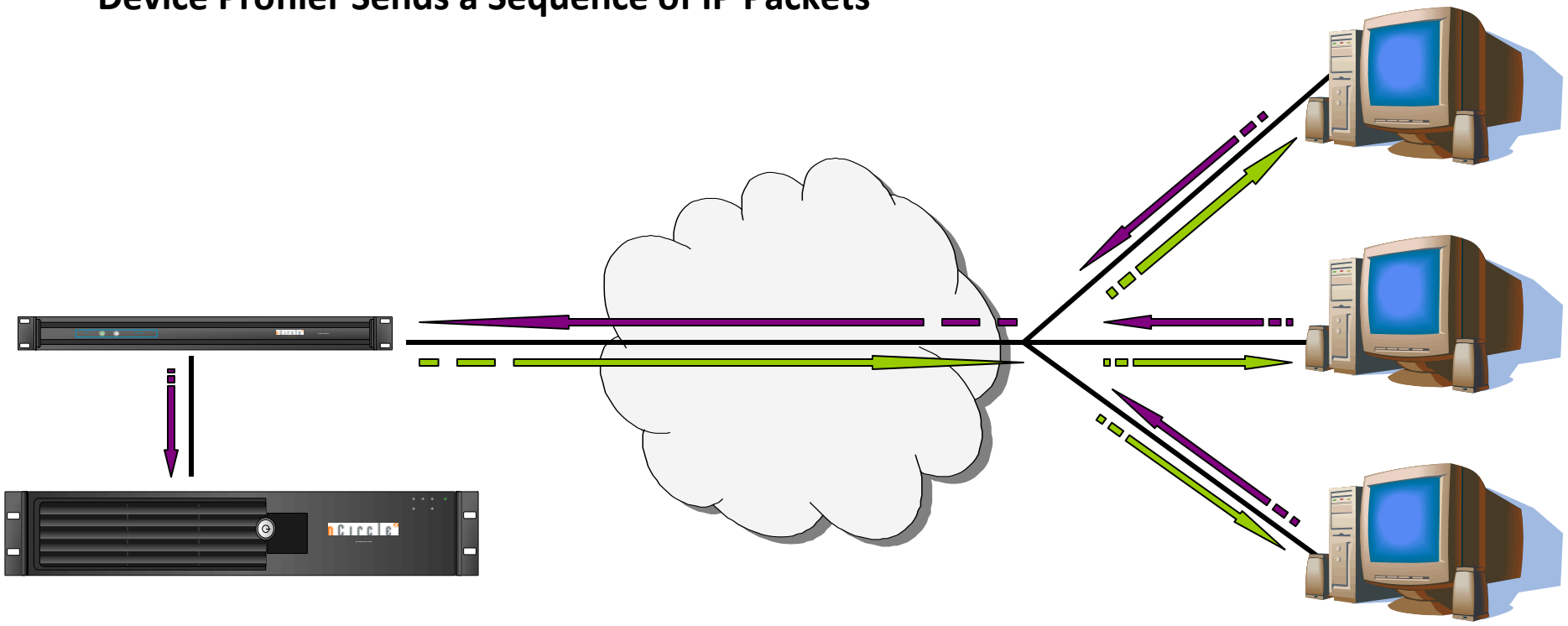
ICMP and TCP Checks are Performed by Device Profiler



Responses are Recorded and Further Analysis is Performed

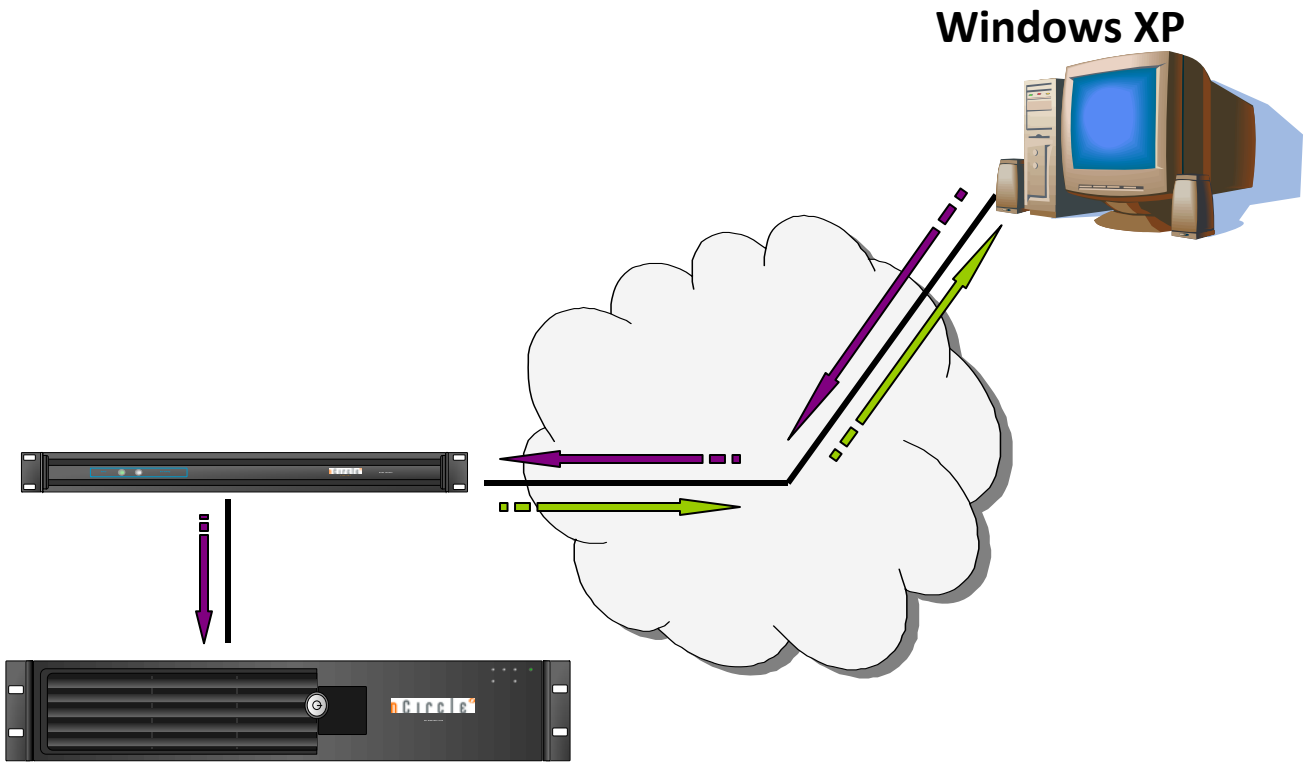
OS FINGERPRINTING

Device Profiler Sends a Sequence of IP Packets



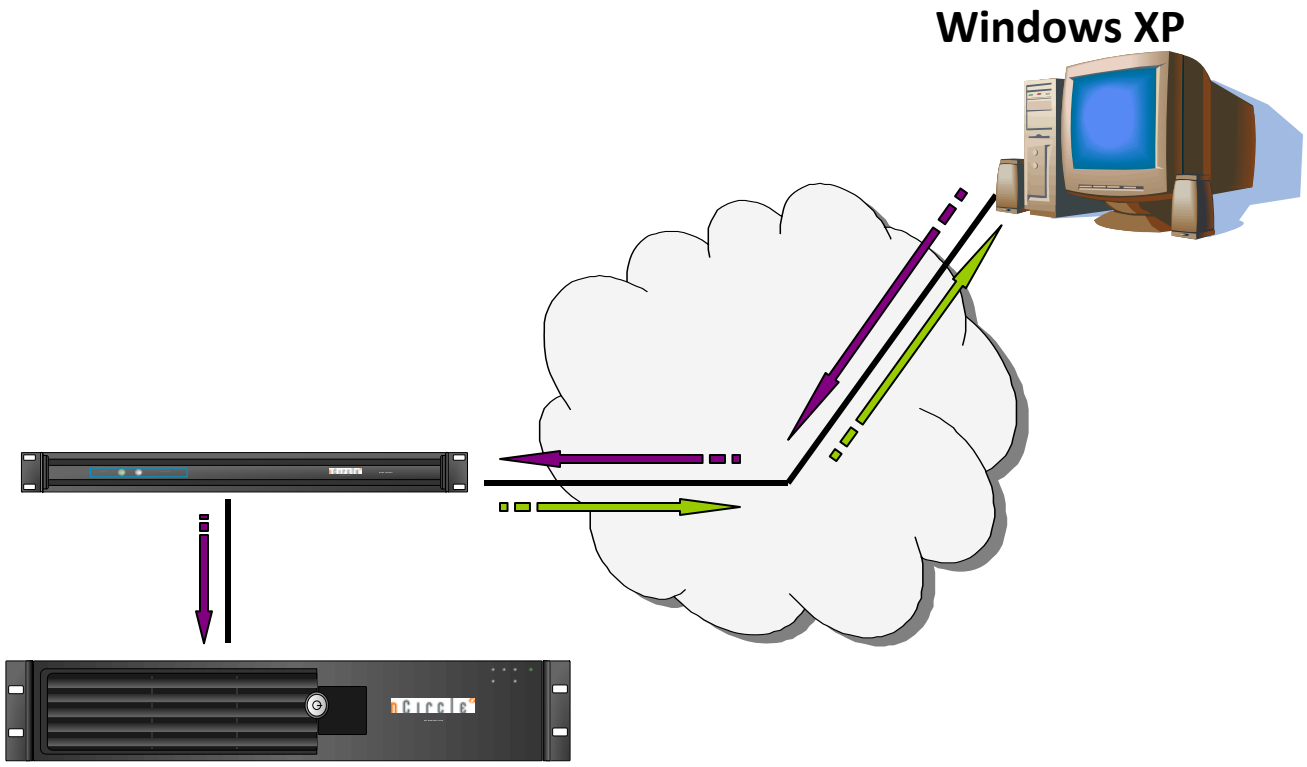
Hosts Respond with Characteristics Unique to Particular OS

APPLICATION & SERVICE DISCOVERY



Targeted Suite of Application Rules are Ran Against a Port

VULNERABILITY DISCOVERY



Vulnerabilities are Bound to Operating System and Application

HOW TO GET THERE

Our Approach to Vulnerability Management

HOW WE ARE GETTING THERE

1. Executive Support
2. Choose Thy Tools Wisely
3. Let Executives Drive the Change
4. KISS – Keep It Simple…

OUR BLUEPRINT

1. Get Executive Support
   - No Executive Support = Zero $$$
   - Explain the concept in layman's terms
   - Think Sparkly, Shimmering, and Glittery
   - Provide real world examples like our Conficker story
   - Address their fears – cost? resources?
   - Show a Value Add (more to come…)

OUR BLUEPRINT (cont.)

2. Select Thy Tools Carefully!
   - Continuous Scanning (Daily vs. Monthly)
   - Automated Scanning Ability
   - Auto Generated Reports and Emailed Reports
   - Executive Level Reports
     - Remember - Sparkly, Shimmering, and Glittery - Not spreadsheets!
   - Trending Data (Demonstrated Business Value)
   - Think ahead – SCAP Validated

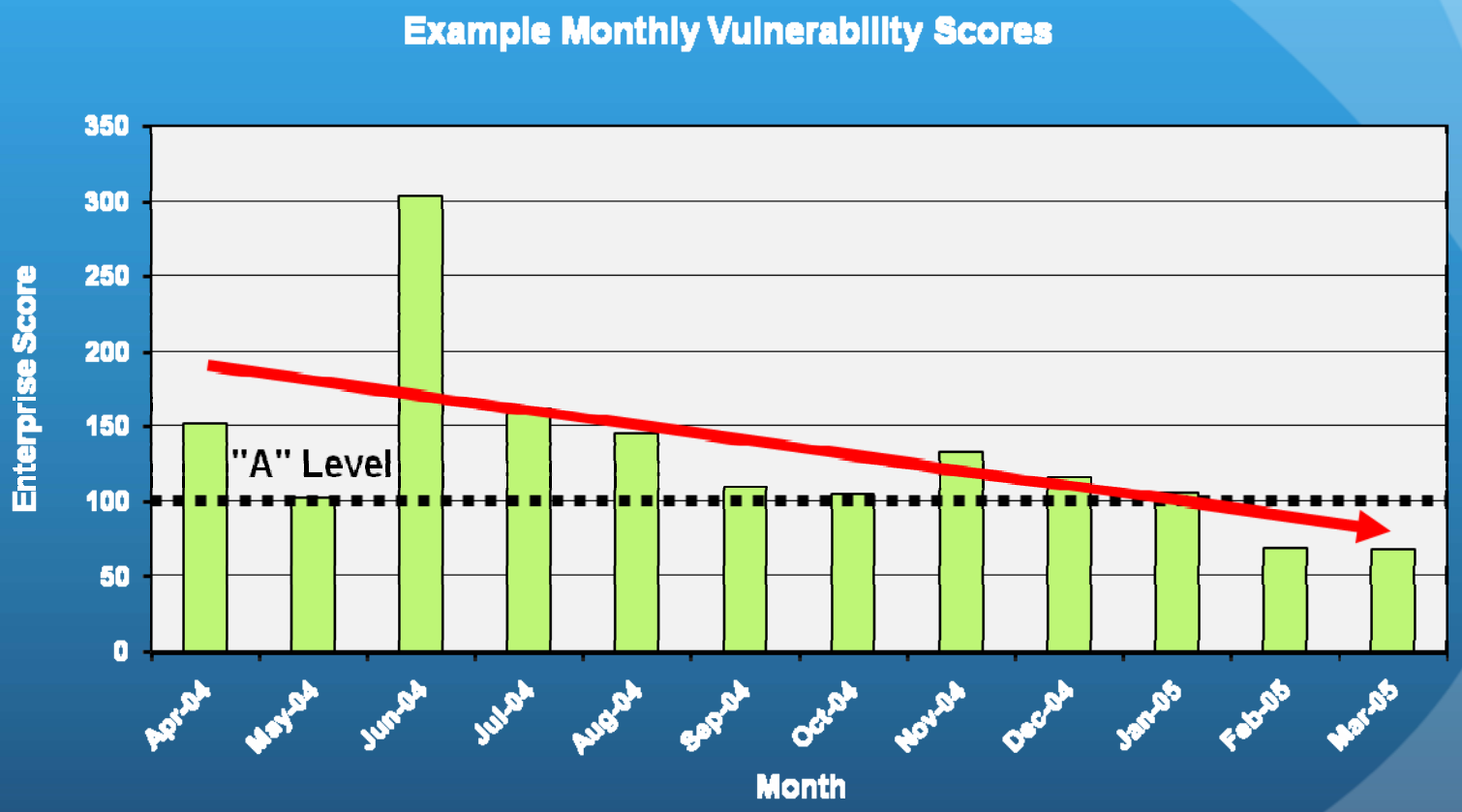
OUR BLUEPRINT (cont.)

3. Let Executives Drive the Change
   - Use non-technical language
     - We have a monthly scorecard – A, B, C, D, F
   - Use Executive Competiveness
   - Give them useful measurable information
   - Tie performance to standardized metrics

OUR BLUEPRINT (cont.)

4. KISS – Keep It Simple…
   - Apples-to-Apples
   - Be Accurate
   - Become A Trusted Source of Information
   - Be an Enabler – Help Them Improve
   - Transparency
   - Don’t let the way you’ve always done things be a barrier

DOES THIS REALLY WORK?



WHERE DOES SCAP COME IN?

- SCAP vulnerability scanner provides:
  - Standard vocabularies
  - Standardized measurement and scoring system
  - Automates security risk management
  - Exportable data in common language

VALUE ADD FOR MANAGEMENT & SECURITY

VALUE ADD FOR MANAGEMENT

- Agency level vulnerability mgt solution
  - Gives management an effective and easy to understand tool to measure risk
  - Establishes non-technical language (A-F grade)
  - Provides apples-to-apples comparison to level the playing field
  - Quantifies and measures staff/contractor progress on a standardized scale

VALUE ADD FOR MANAGEMENT

- Agency level vulnerability mgt solution (cont.)
  - Lowers cost of data calls, annual testing, and audits field work
  - Helps get ahead (proactive) of the curve
  - Guess what? People do what gets measured
  - Helps prioritize workload using existing resources

VALUE ADD FOR SECURITY

- Improved Situational Awareness
  - Ability to answer the simple question “What is on my network right now?”
  - Known risk posture of every system on a daily basis
  - Quickly analyze your exposure to publicized exploits for known vulnerabilities in real time

VALUE ADD FOR SECURITY

- Incident Response – In the "Know"
  - Know where every IP is located
  - Know who is the POC to "pull the plug"
  - Know its business value!
    - Is it really a concern that you need to make that 3am phone call to the CXO?

VALUE ADD FOR SECURITY

- Stop being the person who constantly sends out data calls!
- Less time for audit related compliance checks through automation
- Lowered cost of mitigation efforts because vulnerabilities can be prioritized

REVIEW

- CMS – Context & Programs
- Legacy Information Security Program
- Back to the Basics…The Approach
- The How…
- Value Add

THANK YOU

C. Ryan Brewer
CMS CISO