Correlating Security Data Using SCAP Standards

Panel Discussion: Department Of State & Environmental Protection Agency

John Streufert, CISO Department of State

Panel Members

Mary Stone Holland, Director, Office of Computer Security, Bureau of Diplomatic Security, DoS

Dr. George Moore, Chief Computer Scientist, Office of Information Assurance, Bureau of Information Resource Management, DoS

Marian Cody, CISO,
Environmental Protection Agency

Paul Green, President & CEO, G2

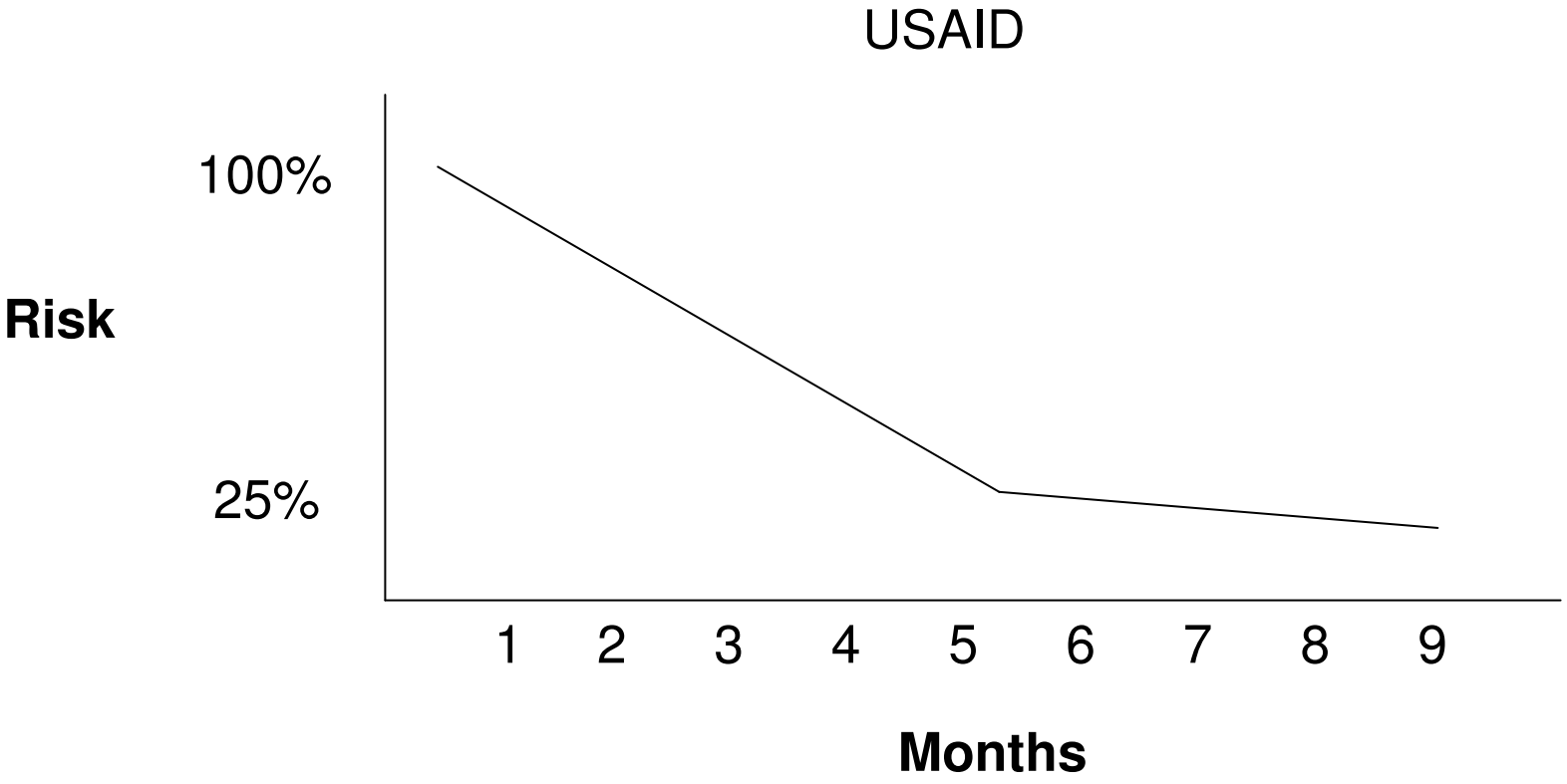
Moderator: Calvin Reimer, Chief, Evaluation and Verification Division, Office of Computer Security, DoS

Eight Strategies to Becoming Best of Class Using SCAP Data

John Streufert
Chief Information Security Officer
US Department of State
September 19, 2007

Why?

- Correlation of IT Security Data Yields Fast Results – SCAP is the best tool yet



How?

1. Respond to the unique data needs of each customer
2. Build a support structure to help ISSO's solve their problems
3. Use weighted percentages as incentives to correct the worst problems first
4. Provide letter grades to assessable business units
5. Structure the "pre-game" warm up
6. Use bureaucratic jujitsu – focus on those with the most to lose
7. Organize public competitions for continuous improvement
8. Structure continuous improvement efforts in 90 day increments

1. Respond to the unique data needs of each customer

- ISSO's and system owners need highly detailed summaries of specific vulnerabilities SCAP can provide, but
- Ambassadors and Assistant Secretaries want to know their relative risk in comparison to the rest of the organization

Conclusion:

- Individual vulnerabilities need to be presented to the owner
- The relative risk needs to be aggregated and presented to higher management.

Reference: The One to One Field Book: The Complete Toolkit for Implementing a 1 to 1 Marketing Program, Don Peppers and Martha Rogers, Ph.D Currency-Doubleday Press (1999)

2. Build a support structure to help ISSO's solve their problems

- When individual technicians see the a specific problem, the fastest overall change comes from showing them a way to fix it themselves. (SCAP Baseline Feature)
- The best experience USAID had was a scanning tool that had an automated link between a specific vulnerability and self-help for a solution.

3. Use weighted percentages as an incentive to correct the worst problems first

IT Security managers find a “target rich” environment of problems to fix.

USAID and State are structuring the use of SCAP scanning tools to highlight data on the worst problems first

Tweaking of SCAP uses weighted percentages and other math to lift up high risks and diminish lower risks

4. Provide letter grades to assessable business units

- The leadership of federal organizations have come to associate status of IT Security with letter grades and stoplight charts used in the President's Management Agenda
- If SCAP data can be summarized, entire business units can get continuous feedback on their progress

5. Structure a “pre-game” warm up

- ISSO’s are your customers -- angering them is counterproductive.
- False positives occur, and improperly assigned devices found in scanning take on-site technicians to sort out.
- Give time for the learning curve to work
- Do not share grades outside the immediate organization for at least six months.

6. Use bureaucratic jujitsu – focus on those with the most to lose

Throw the weight of the organization into the IT security problem

- Send the grades to the senior manager
  - Send a copy to the technical team
- "Sell" the change to the leaders by noting how IT security attacks can disrupt, damage and diminish the budgets of the primary mission
- At early phases, do not escalate problems until all local attempts to support improvement are tried

7. Organize public competitions for continuous improvement

- All best of class organizations promote and reward leaders based on results
- “Good IT Security Culture” recognizes leaders and “publicly encourages” those who are lagging
- After six months compare all organizations head to head

8. Structure continuous improvement efforts in 90 day increments

- Over several years this approach works has worked best:
  - Visualize the top 50 problems
  - Select the top 5 with highest benefit to lower risk
  - Organize teams to pursue those initiatives with a 90 day check point
  - Reset the playing field for the next game
  - Set aside some resources for long term improvements and training

Standards Based Security
The EPA Story

Building a Culture of Compliance

Marian Cody
Chief Information Security Officer,
U.S. Environmental Protection Agency

Challenges to Building a Culture of Compliance

- **Lots** of standards
- **Lots** of IT devices
- **Lots** of organizations
- **Lots** of miles between physical locations
- **Lots** of different management styles
- **Lots** of compliance reporting

Management with limited understanding of security control specifics

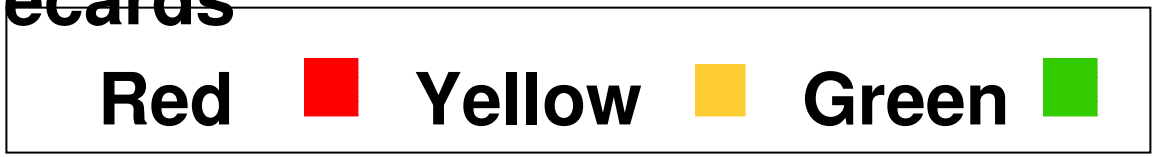
EPA's Strategy

Create an integrated suite of automated security solutions based on federal (SCAP) standards.

- **Implemented at the hardware/software level but viewable at the enterprise level**
- **Supported by PERFORMANCE Reporting**
- **Geared to MANAGEMENT**
- **Based on REAL data**
- **Reflecting REAL operational status**
- **Using REPEATABLE processes**

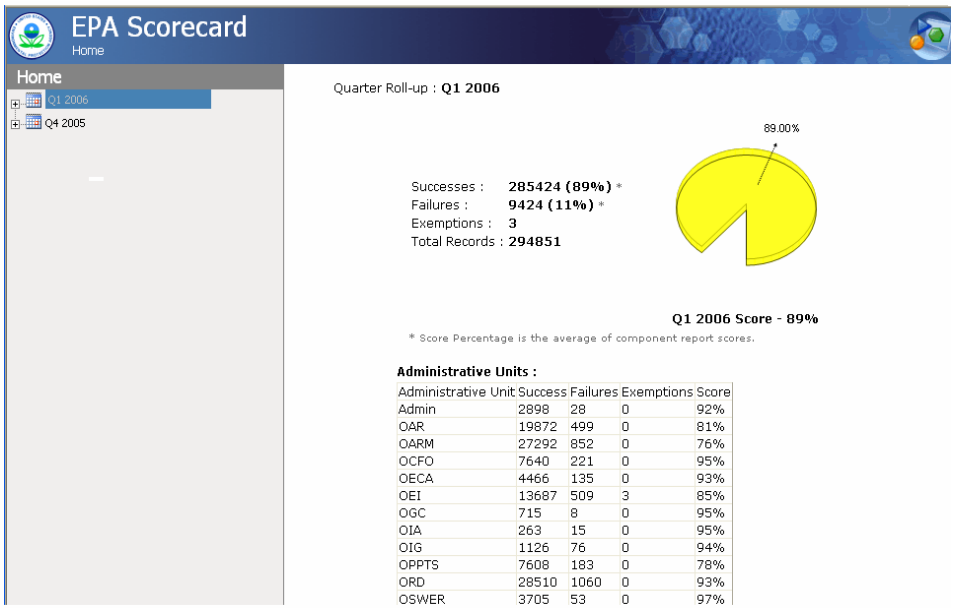
How Did We Do It?

- Selected an automated Compliance Tool
- Tested it ourselves to make sure it worked
- Began deployment amid great resistance
- Found success in two offices – within days their compliance issues were solved – which was shared with their peers
- Provided time and training to ease into the system – about 9 months
- Communicated first at the staff level
- Added Management Level Quarterly Scorecards



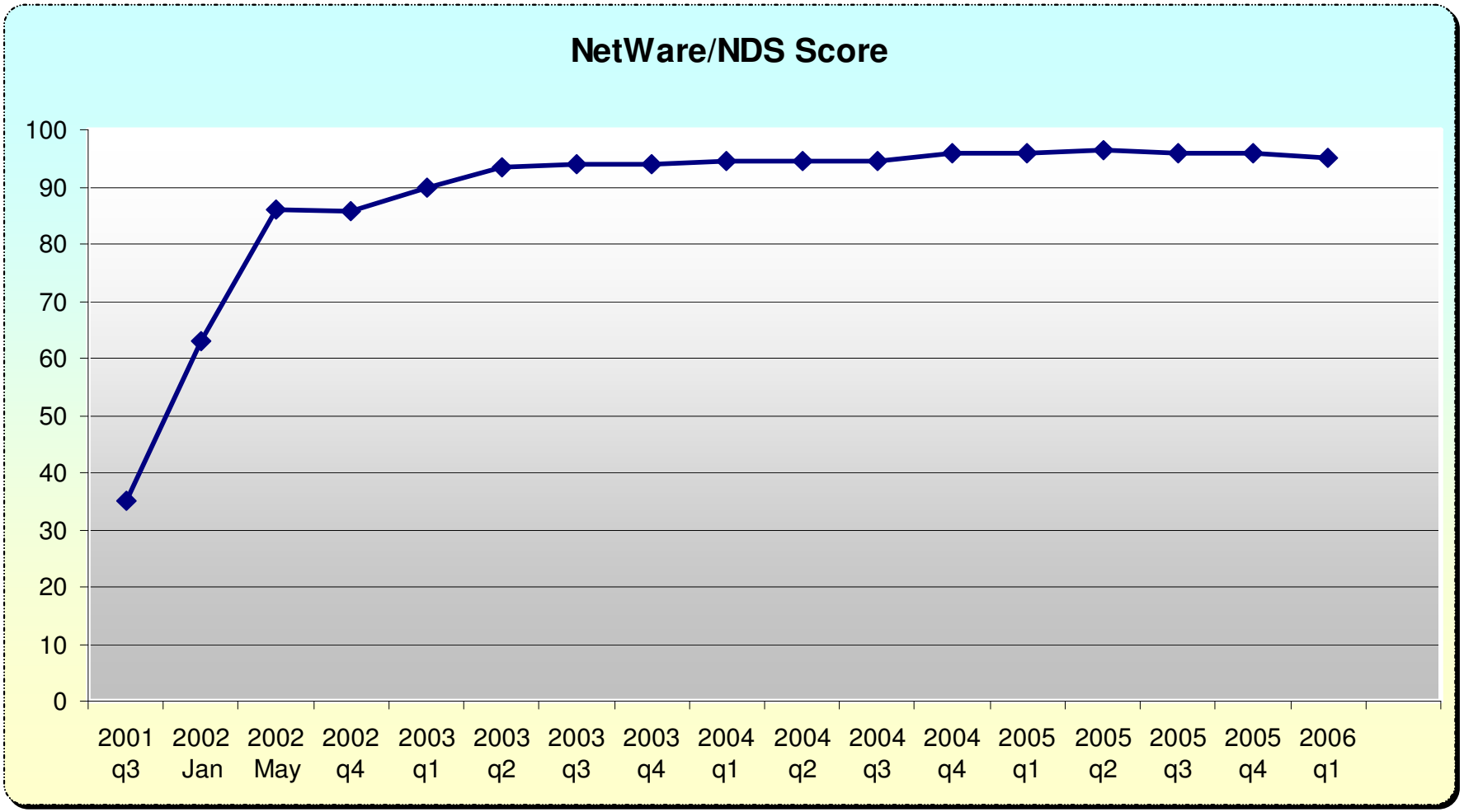
Explicit Scoring & Publishing

- 90% + = Green
- 75-89% = Yellow
- >75% = Red



- Allowing success in the face of operational realities
- Enhancing communication despite technical complexity
- Fostering healthy competition

Did It Work?


NetWare/NDS Score
100
90
80
70
60
50
40
30
20
10
0
2001 q3
2002 Jan
2002 May
2002 q4
2003 q1
2003 q2
2003 q3
2003 q4
2004 q1
2004 q2
2004 q3
2004 q4
2005 q1
2005 q2
2005 q3
2005 q4
2006 q1

Building a Culture of Compliance

- **Automated Standards-Based (SCAP) Tools**:
  - Regular and reliable security checking
  - Built on repeatable processes
  - Standard metrics
  - Remediation information
  - Results useful to technicians and management alike
- **Giving Management**
  - Regular, understandable communications
  - Greater understanding of risks
  - Real data upon which to make management decisions
  - Ability to provide technical direction

What's Next?

- Expanding the scope of management reporting to capture results from other security management tools – e.g., patch management, vulnerability scanning, and anti-virus monitoring
- Interfacing test results into ASSERT for Agency security reporting
- Converting to SCAP compliant tools

Standards Based Security the Department of State Story

- History of Compliance Management at DoS
- Bringing Agency-unique issues in to focus
- Circumstances leading to SCAP adoption
- Areas under repair
- On the horizon

MH

Increased Accountability is Critical to Improving IT Security

- The Honorable Karen Evans, noted speaker here, shared the following with Congress*: "…agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure."*

MH

Department of State – Challenges & Success of Compliance Management

- Customized security configuration documents were comprehensive but hard to implement globally

- DS built a custom compliance scanning tool to validate settings and security

MH

Bringing Agency-unique security issues in to focus

- Global nature of our networks makes it important to standardize and an oversight challenge
- System Administration by local personnel makes it more important to “lock down” the configuration
- Roles & Responsibilities agreement to balance security responsibility among Security Oversight bureau and the CIO’s Information Assurance office

MH

Circumstances Leading To SCAP Adoption

- New Technology Arriving Faster Than We Can Produce Word Documents
- Realignment of Resource Use
- Updated Commercial Compliance & Vulnerability Scanning Tools
- SCAP Facilitates Network Security Perspective From Multiple Tools

MH

Diversity of Data Sources

- Inventory Sources
- Vulnerability Scanners
- Certification Information
- Patch & AntiVirus Status

- Each of these have different models and don't store / report information the same way
- Need to identify "systems of systems", groups of individual IT resources that have value together

GM

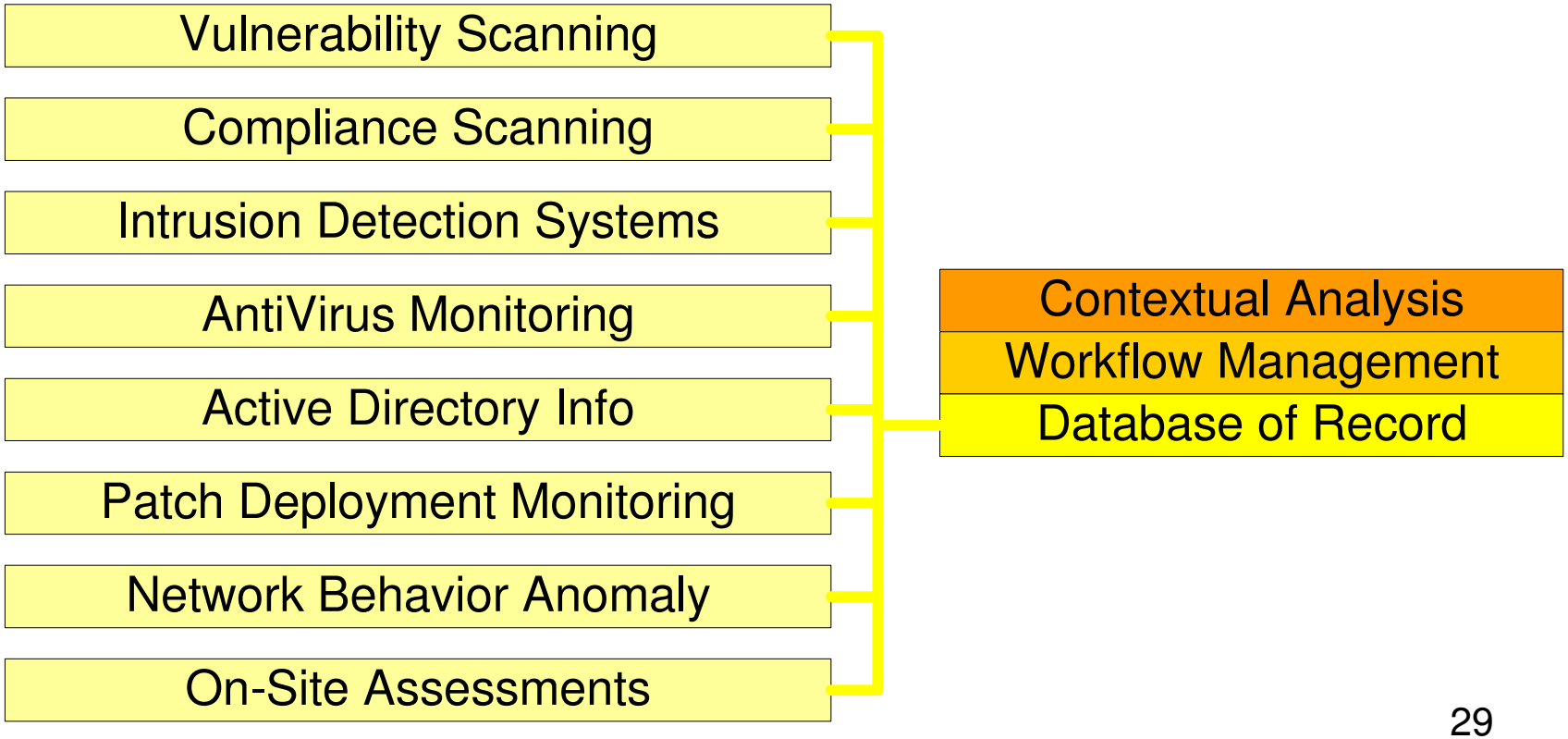
Steps in Progress

- Advanced Security Scoring Method That Helps Prioritize Response And Ensures That Risk Is Measured & Reported Fairly
- Need For ‘Common Remediation Enumeration’ – What Repeatable Fixes Will Provide Measurable Results
- Security-enabled Console To Enable System Owners / Managers To Track Progress
- Migrating To FDCC-compliant Checklists

GM

Transition To Better Situational Awareness

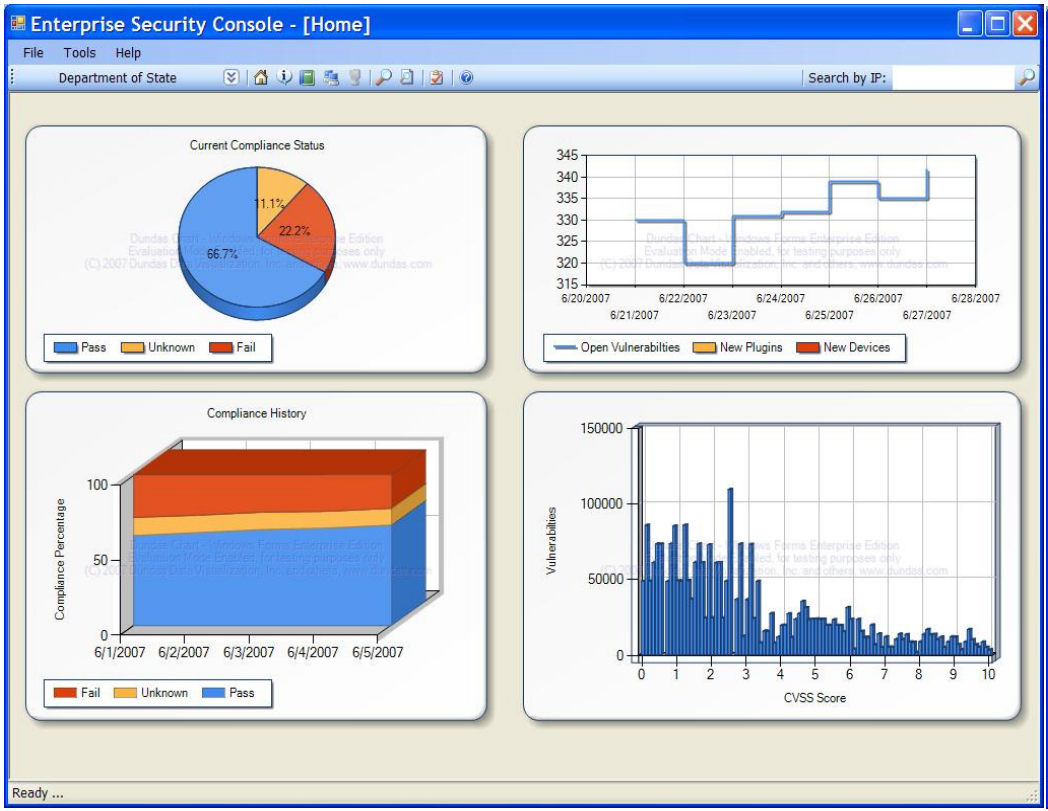
Get Good Risk Info to the Right Managers to Enable Remediation and Tracking

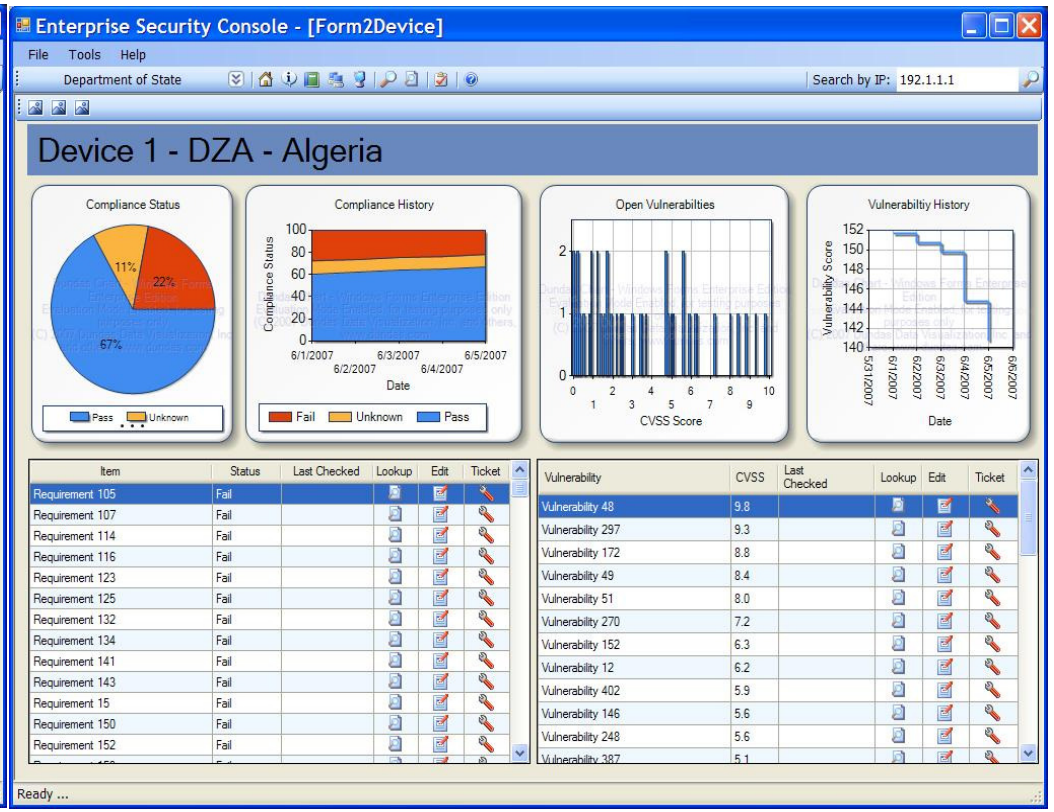


PG

Transition To Better Situational Awareness

Get Good Risk Info to the Right Managers to Enable Remediation and Tracking





PG

On the horizon

- Normalizing Inventory And Linking To Business Value
  - Facilitates Compliance Reporting
  - Enables Continuous Monitoring Of Authorized Systems
  - Helps Prioritize Incident Response
- Reconciling OVAL With 800-53 Based Assessments
  - After a SCAP-based scan is done, how much of my review is complete?

PG

Contacts

John Streufert, Chief Information Security Officer, Department of State - **streufertj@state.gov**

Marian Cody, Chief Information Security Officer, Environmental Protection Agency - **cody.marian@epa.gov**

Mary Sue Holland, Director, Office of Computer Security, Bureau of Diplomatic Security, DoS - **hollandms@state.gov**

Dr. George Moore, Chief Computer Scientist, Office of Information Assurance, Bureau of Information Resource Management, DoS – **mooregc@state.gov**

Calvin Reimer, Chief, Evaluation and Verification Division, Office of Computer Security, DoS – **reimercr@state.gov**

Paul Green, President & CEO, G2 – **paul.green@g2-inc.com**