



Lessens Learned Using SCAP Tools

Scott Armstrong

Symantec Corporation

Agenda

- 1 Lessons learned - background
- 2 Lessons learned – preparation
- 3 Lessons learned – for a “typical” agency
- 4 Automation, Aggregation, and Blocking & Tackling
- 5 Closing recommendations

Lessons Learned – some background

- First there was CVE – just had 10 year anniversary!
 - CVE-1999-0001 submitted on **June 06, 1999**
 - Description: “ip_input.c in BSD-derived TCP/IP implementations allows remote attackers to cause a denial of service (crash or hang) via crafted packets. “
- Then an XML language was added (OVAL) for “checks”
 - Government sponsorship in ~ 2003
 - Vendors begin to engage and adopt in 2005 and 2006
 - oval:org.mitre.oval:def:1 submitted on **June 26, 2006**
 - Title: “Microsoft Windows XP SP1 (32-bit) is installed”
 - Note – this was an “**inventory check**”...
- CVSS started developing as sponsored by FIRST

Lessons Learned – some background

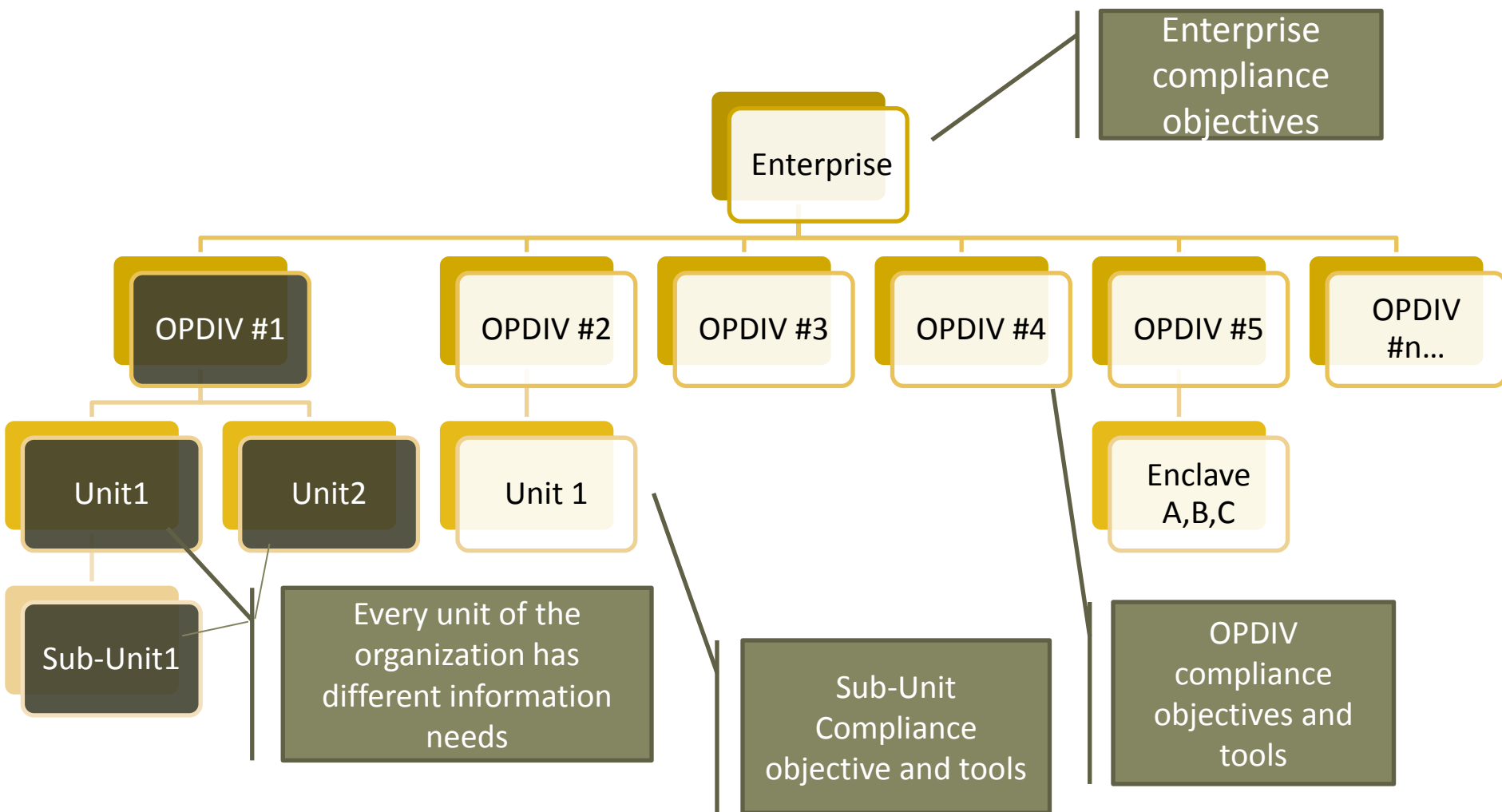
- Then an XML language was added (XCCDF) for “checklists”
 - Government sponsorship in ~2003/2004; publically released in 2005
 - Vendors begin to engage and adopt in 2005 and 2006
 - “SCAP” oriented products leveraging enumerations + XML languages began to be available in 2006 & 2007
- And then “S-CAP” and FDCC appeared
 - SCAP Validated Products first appear in February 2008
- Why does this history matter?
 - There’s more enumerations and potential emerging standards coming
 - Government and community processes have been maturing significantly
 - And it will continues to evolve and mature
 - More on that when it comes to lessons learned....

Lessons Learned – preparation...

- Get unbiased (and biased) Education
 - Management & cross functional groups – industry & gov't perspectives
- Understand the range of SCAP “applications” for automation
 - Vulnerability Management, Patch Management, Configuration Management
 - Asset Inventory & Management
 - Situation Awareness & Incident Response
 - Your vision of a new use case for your agency's or group's mission
 - OMB / FISMA / Other Compliance
 - The list is potentially endless and they **all** can have real ROI!
- Management sponsorship and buy-in
 - Consider having one or more SME's to support internal efforts

Lessons Learned

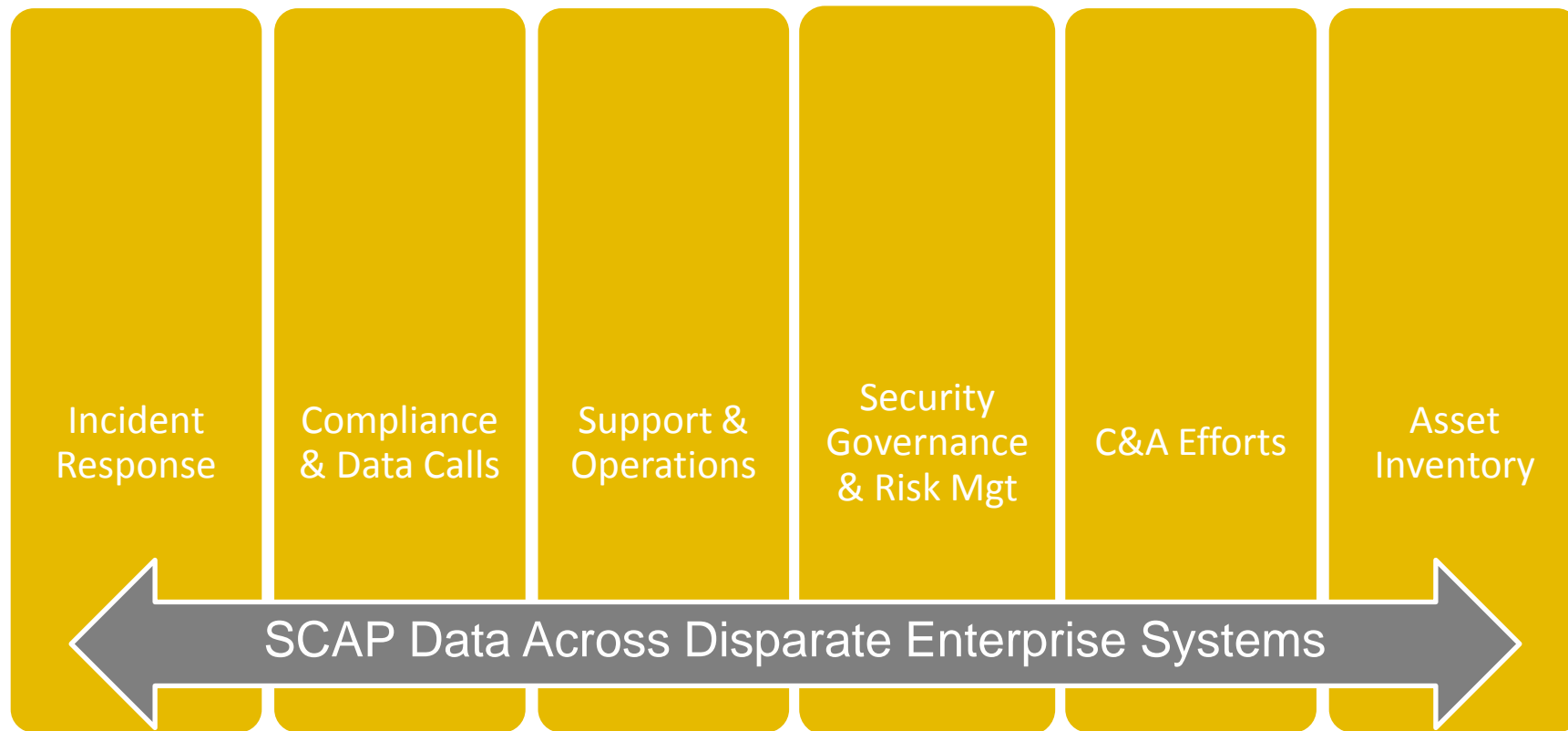
Profile of a typical “agency”



Profile of a “typical” agency – there is no “typical”

- Compliance objectives vary vertically and horizontally
- Many challenges due to disparate goals and processes
- Diverse technology and information sources
- No single enterprise network or host level access policies
- Asset classification variations across the board
- Enclaves are the **rule**, not the exception
- Data acquisition methodologies *need* to be flexible
- Expect exceptions to many rules (scientific workstations?)
- Many asset inventories, but authoritative answers still needed
- Different views of “enterprise” visibility depending hierarchy

Premise: SCAP Standards For Disparate Enterprise Systems Enables A More Holistic View



Uniformity in Data Improves Intelligent Collaboration

Standards enable automation and lead to tangible ROI

- But you still need to be an educated buyer
 - Whether point solutions or suites, ask for SCAP per your use cases
 - Classic SAIR Tier 1 SmartBuy style use cases; supports OMB & data calls
 - Network & Asset Discovery /Inventory – what is on your network - today?
 - Configuration data – how you compare to your baseline(s)?
 - Vulnerability Management - its Patch Tuesday – ready to scan pre & post patching?
 - Then add in your use cases
 - Specify must have and like to have SCAP requirements by use case
 - Specify what your content requirements and expectations are across the board
 - Don't forget your traditional requirements – no two products are the same!
 - What are your operational requirements?
 - What are your operational constraints?
 - What are your interoperability requirements?

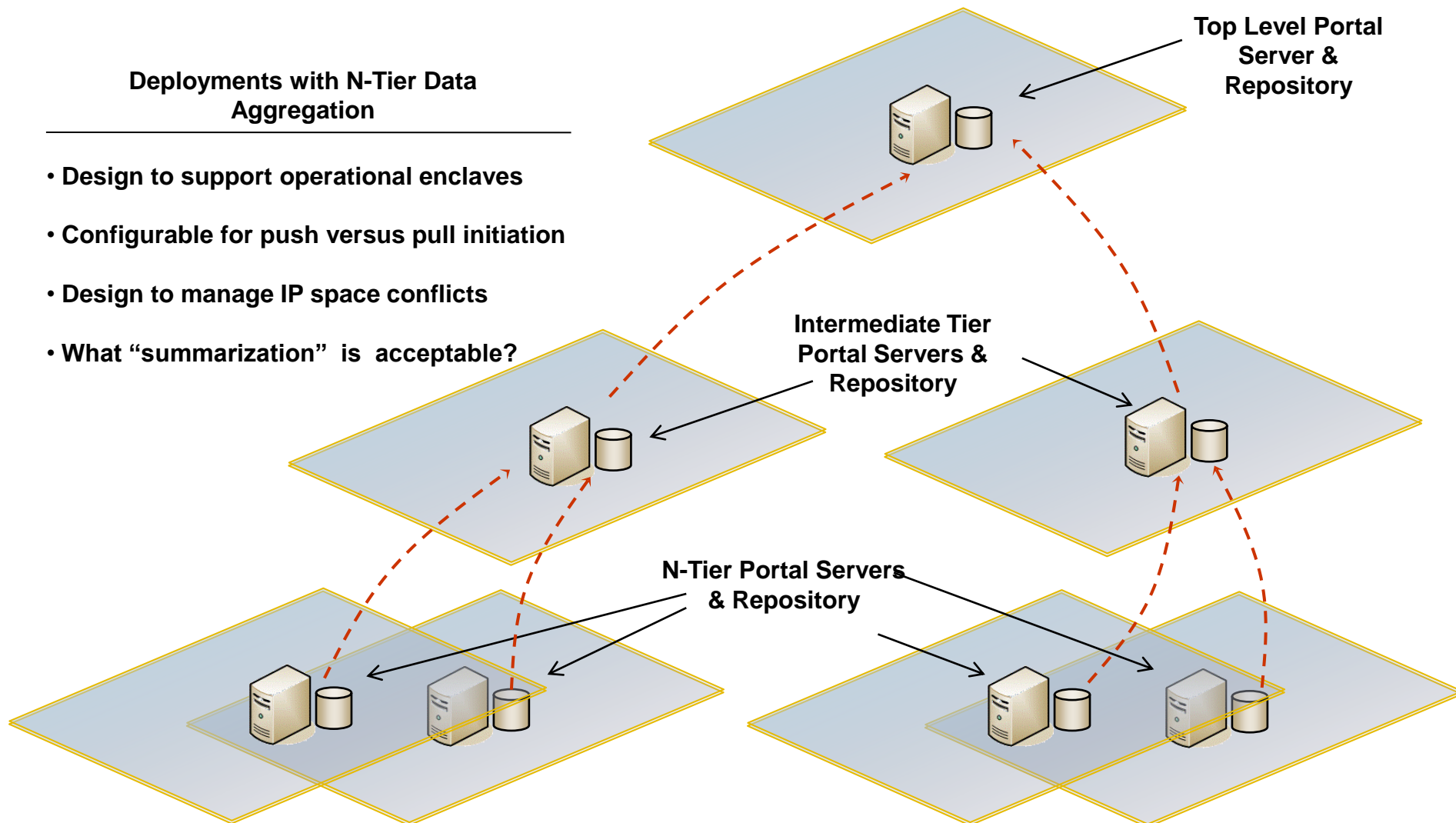
Standards enable automation and lead to tangible ROI

- Facilitates data aggregation
 - otherwise messy or vendor or GOTS specific – see next slide
- Other Integration Scenarios
 - Web Application Security
 - Incident Response, Risk Management
 - Software Auditing and License Management
 - Network Operations, Logging
 - Help Desk, CMDBs, Remediation, POAM systems
 - And the list continues....
- SCAP Logistics on Integration Scenarios
 - Establish common **Language, Enumeration, and Metrics**
 - Originating and validating content is pivotal
 - ***Content is king***

Aggregation – an example with generic applicability

Deployments with N-Tier Data Aggregation

- Design to support operational enclaves
- Configurable for push versus pull initiation
- Design to manage IP space conflicts
- What “summarization” is acceptable?



Basic Lessons Learned – Blocking & Tackling

- Content Management Plan – its not just about a “tool”
 - Updates - vendor versus gov’t expectations
 - Dev/Test/QA process for content
- Multiple Organizational Layers – it’s a reality
 - Introduces challenges on accommodating multiple layers of objectives
 - Conflicting goals and objectives - Goals often become equal to one another
 - Makes compliance relative
 - The snowball effect of policy exceptions
 - Conversely, excluding controls, signatures on checks
- IT Challenges
 - Local Permissions
 - For installing
 - Network Access
 - Jurisdiction over sub-nets or network zones
 - Outsourced network management introduces complexity

Recommendations

Top areas for “lessons learned” recommendations

- Recommendation 1: Understand your people, org, & processes
 - Know limitations, boundaries
 - Know approach will work with current processes and organizational boundaries
- Recommendation 2: Understand your asset requirements
 - Determine these requirements at the beginning of a project
 - What information do you need related to your assets?
 - How often do you need to see this information?
 - How do you classify your assets

Top areas for “lessons learned” recommendations

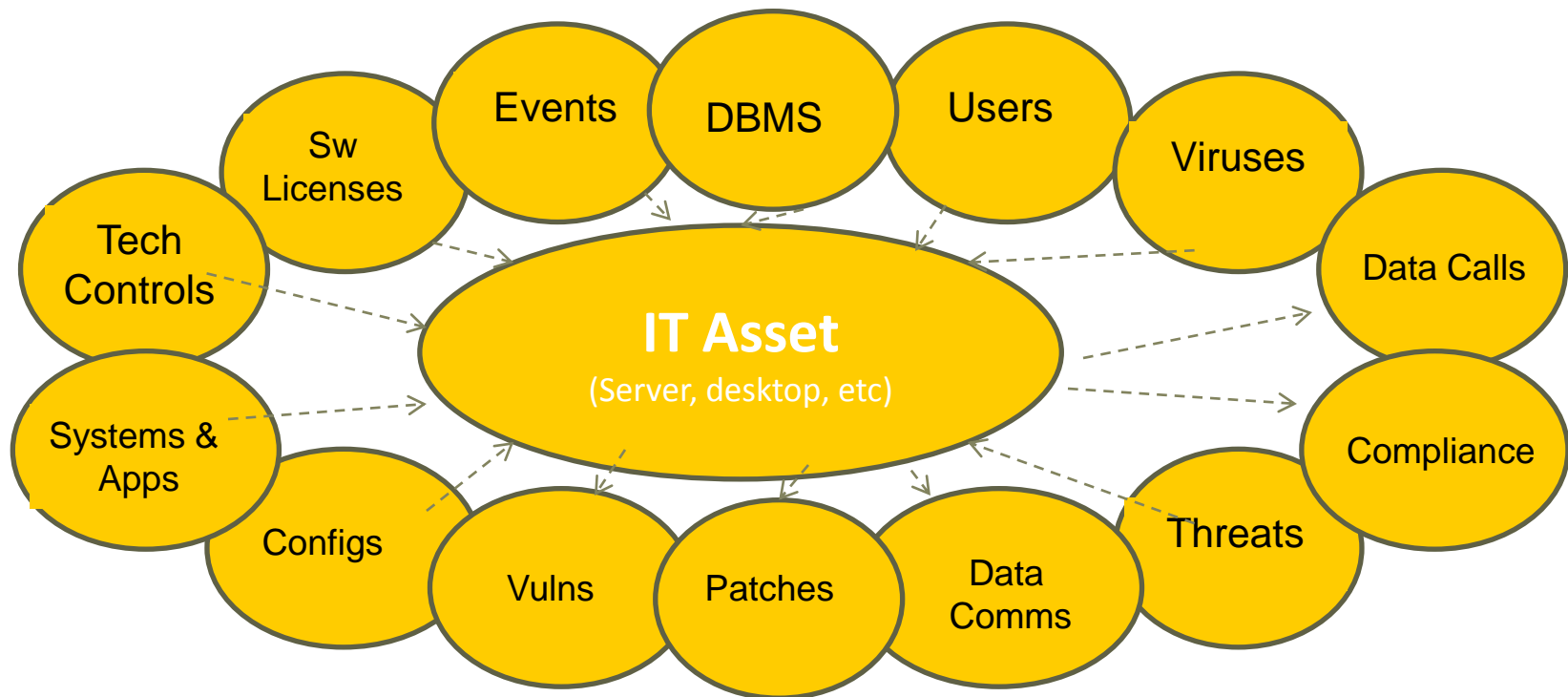
- Recommendation 3: Plan for and **require enumerations** across products/solutions
 - Require interoperability & SCAP Enumerations
 - Cross-referencing information is essential – Enumerations **are required**
- Recommendation 4: Metrics-based reporting key to success
 - Successful deployment should culminate in meaningful metrics – keep it standardized; keep it simple (CAG).
 - What gets measured & reported drives behavior
- Recommendation 5: Operational Independence
 - Dependencies for information gathering
 - Consider information access challenges, business impact considerations

Recommendation 1: Understand your people, org, & processes

- Obtain executive support
 - Key in successful implementations
 - Everyone needs to understand a clearly defined vision for an SCAP solution
- Identify processes that make sense for data sharing via SCAP
 - Determine if groups are willing to play nicely
 - Establish commonalities in benchmarks, metrics, etc
- Learn to meet halfway
- What content makes sense for your organization?
 - Identify content that needs to be there now vs. tomorrow
 - How are exceptions going to be handled? Suspended Controls vs. Exceptions
 - Process around content management
 - How does content get endorsed?
 - Outsourcing vs. internally developing content vs. gov't vs. vendor vs?

Recommendation 2: Understand your asset requirements

- The foundation of continuous monitoring is the **asset**
 - Most assessment criteria ties back to an asset
 - It is the hub with many spokes



Recommendation 2: Understand your asset requirements

- Asset inventory is a pre-requisite for success
- The degree to which you understand your assets is the degree to which your continuous assessment model will be successful
 - How many assets do we have?
 - Which assets support systems and key business applications?
 - What are the most critical assets?
 - How have our assets changed? Today? This week? This month?
 - Where do we store data?
 - Who should have access to this data for agency decision support needs?

“66% of all organizations admit to not having an accurate record of their IT assets” (Gartner)

Recommendation 3: Plan for and require enumerations across products/solutions

- Move away from solutions that do not include SCAP & interoperability for automation
 - Otherwise automation, and ROI, will be problematic
- Without a common framework, greater difficulties to integrate
 - Time consuming; pulls resources away from supporting your mission
 - Data format interoperability issues
 - Custom APIs versus reusable components
- No common methodology for metrics feasible without enumerations
 - Requires enumerations first to then compare common metrics
 - Differences in enumerations will magnify downstream reporting discrepancies

Recommendation 4: Metrics-based reporting key to success

- What gets measured gets done
- Socialize metrics – build consensus – think CAG
 - Metrics that never gain visibility are useless
 - Understand what metrics are used at macro and micro levels
- Metrics move the discussion to a strategic focus
- Adoption of metrics is key amongst senior leaders
- Report metrics for comparative/competitive analysis
 - Report by organization unit and system/LOB application
 - Comparative/competitive analysis
 - Vulnerabilities by System
 - FISMA Controls by Organization
- Metrics facilitate trend reporting
 - 65% compliance might be good news!
 - Internal baselines need to be determined

Recommendation 5: Operational Independence

- Content considerations
 - Develop internally and/or subscribe to content from content providers?
- Operational Considerations for Solutions
 - Easy deployment – appliance vs software versus VM's versus ?
 - Data acquisition requirements – for hosts & network devices by use case
 - Agent-less – Dissolving Agent – Persistent Agent – USB/Off-net Assessment Capabilities
 - Bandwidth throttling; SOA infrastructure; FIPS; RBAC; aggregation?
 - Control of date/time/frequency of use as associated with use cases
- Operate independent of operations, but support automation
 - Processes should validate, not depend on...
 - Information should provide actionable items for automation
 - Respect loose coupling of solutions

Lessons Learned – Final thoughts...

- Focus on solutions that
 - Support NIST Standards (SCAP validated tools) that provide authoritative requirements traceability to the NIST SP 800-53 and other specifications
- Focus internally on process and synergies
 - Ensure quick wins
 - Be realistic based on your organization
- Understand your interoperability expectations
 - Make sure it aligns with your vendors capabilities
- Understand your vendors capabilities and vision
 - Make sure it aligns with your interoperability expectations



Thank you!

Scott Armstrong, Symantec

E-mail: Scott_Armstrong@symantec.com

Phone: 571-314-6560

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.