SecureFusion

Lessons Learned in SCAP Enterprise Deployments

October 2009

GIDEON TECHNOLOGIES

Know your assets. Know your risk.

Presentation Roadmap

- SCAP Evolution
- SCAP Readiness
- Enterprise Deployment Case Study
- Enterprise Deployment Lessons Learned
- Recommendations for SCAP Deployment

Copyright © 2009 Gideon Technologies, Inc.

SCAP Evolution

- **SCAP Then –** Focused more on unifying vulnerability management data primarily via OVAL(l), CVE(e), CVSS(m).

- **SCAP Tomorrow** - expansion in compliance, remediation, and network monitoring. With greater participation (NIST, MITRE, NSA, DHS), additional specifications will involve.

- **Simple Definition –** NIST sponsored, community enriched list of specifications that aim to establish standardized expression & reporting for languages, enumerations, and metrics.

- **Importance** – interoperability of information sources is key in government enterprises. SCAP is provides a common protocol for improved data interfaces and data management.

Copyright © 2009 Gideon Technologies, Inc.

SCAP Readiness

- Focus on ***solutions*** that
  - Begin to establish the framework for processes that sustain interoperability of information across groups (C&A, Security Ops, Compliance, etc)
    - Refine workflow for *integrating, automating, and orchestrating* information security activities across an enterprise infrastructure
  - Support new NIST Standards (***SCAP validated tools***) that provide authoritative requirements traceability to the NIST SP 800-53 and other appropriate specifications
  - Offer original and up to date content for current and emerging specifications
- Focus internally on ***process*** and ***synergies***
  - **Define KPIs** (Key Performance Indicators) for operational and reporting activities for enterprise IT Risk Management from the operator to the CISO
  - **Identify** relationships amongst data values across disparate security, compliance, and risk groups.

Copyright © 2009 Gideon Technologies, Inc.

SCAP Enterprise Case Study

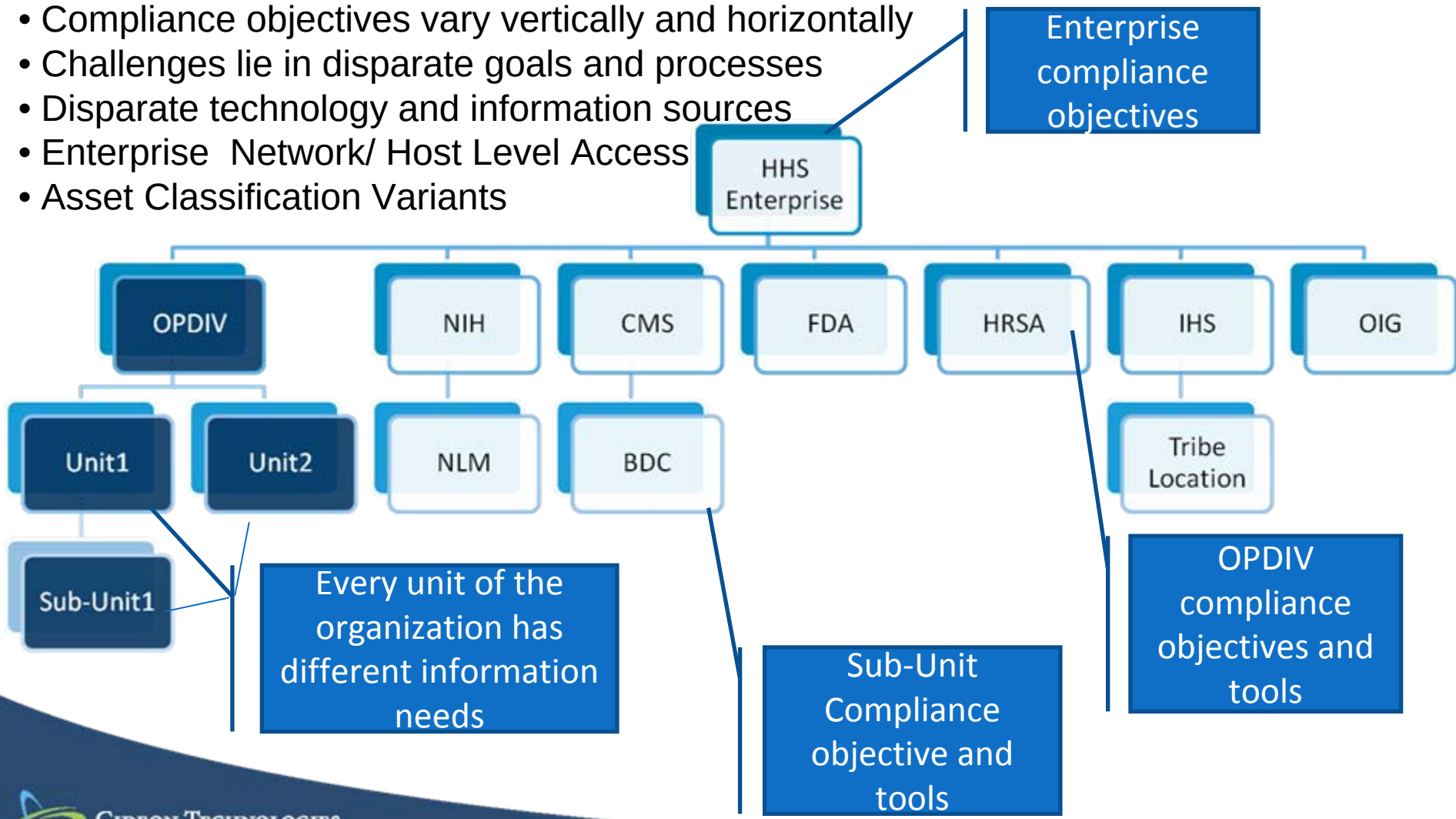
GIDEON TECHNOLOGIES
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

SCAP Enterprise Deployment - DHHS

Complicated and Large SCAP Deployment

- Compliance objectives vary vertically and horizontally
- Challenges lie in disparate goals and processes
- Disparate technology and information sources
- Enterprise Network/ Host Level Access
- Asset Classification Variants

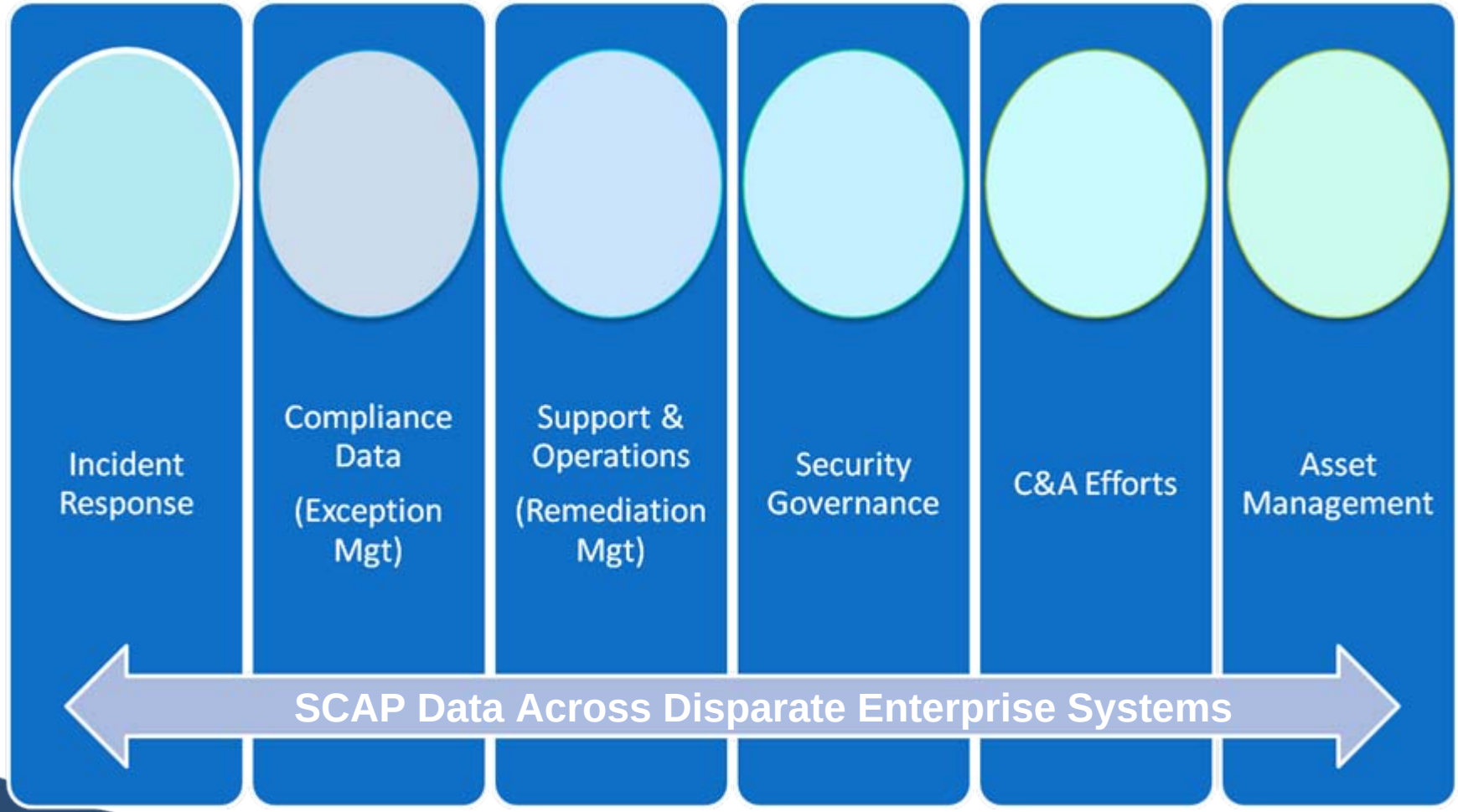


Gideon Technologies
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

SCAP Enterprise Deployment - DHHS

SCAP Across Disparate Enterprise Systems Enables A More Holistic View



Uniformity in Data Facilitates Cohesive Review

Gideon Technologies
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

SCAP Enterprise Deployment – DHHS

- Platform solution incorporates SCAP across embedded tool sets
  - i.e : Vuln to Config Data, Policy Gaps to Config Gaps, Asset Information to Compliance Metrics
- SCAP facilitates data aggregation
- Future for further integration is built-in
  - Coupled with SOA, APIs are easy to instantiate APIs
- Integration Possibilities
  - Web Application Security
  - Incident Response
  - Software Auditing and License Management
  - Network Operations
  - Logging
  - Risk Management
- SCAP Logistics on Integration Possibilities
  - Establish common **Language, Enumeration,** and **Metrics**
  - Originating and validating content is pivotal
  - Content is king

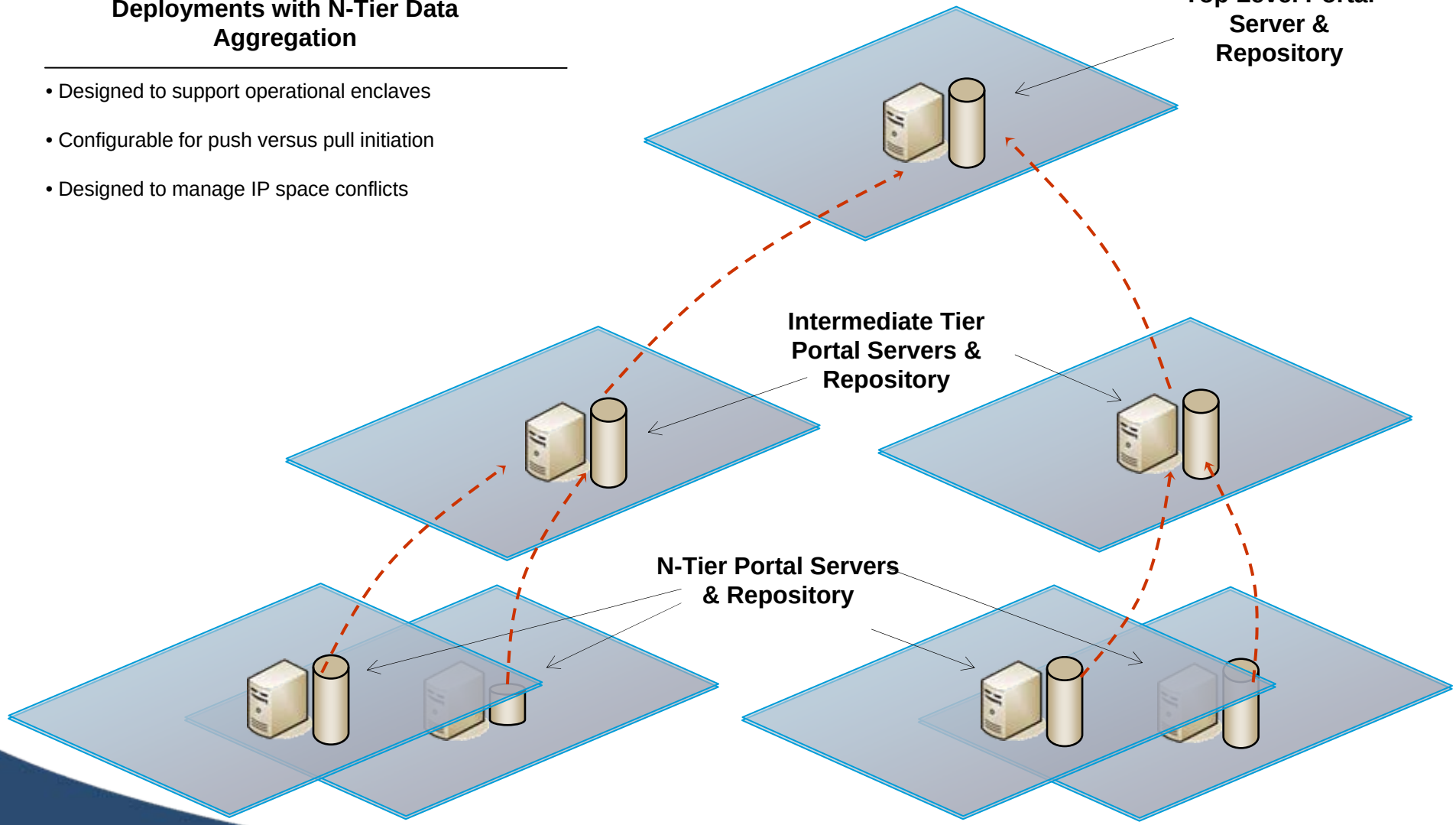
GIDEON TECHNOLOGIES
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

Aggregation Example via SCAP Solution

Deployments with N-Tier Data Aggregation

- Designed to support operational enclaves
- Configurable for push versus pull initiation
- Designed to manage IP space conflicts



Copyright © 2009 Gideon Technologies, Inc.

SCAP Enterprise Deployment – Lessons Learned

Content Challenges

- Updates
- Accuracy of content
- Exception Management

Multiple Organizational Layers

- Introduces challenges on accommodating multiple layers of objectives
  - Conflicting goals and objectives
  - Goals 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

Copyright © 2009 Gideon Technologies, Inc.

Recommendations for SCAP Enterprise Deployments

GIDEON TECHNOLOGIES
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

Enterprise SCAP Deployment Recommendations

#1: Understand your process

- Know process limitations, boundaries
- Can an enterprise approach work with this enterprise's process

#2: Understand your Assets

- What information do you need related to your assets?
- How often do you need to see this information?
- How do you classify your assets

#3: Move Away From Point Solutions

- One information source cannot tell the whole story
- Cross-referencing information is essential

#4: Metrics-based Reporting

- Successful deployment should culminate in meaningful metrics
- Common metrics across the enterprise

#5: Operational Independence

- Dependencies for information gathering
  - Information access challenges, business impact considerations

GIDEON TECHNOLOGIES
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

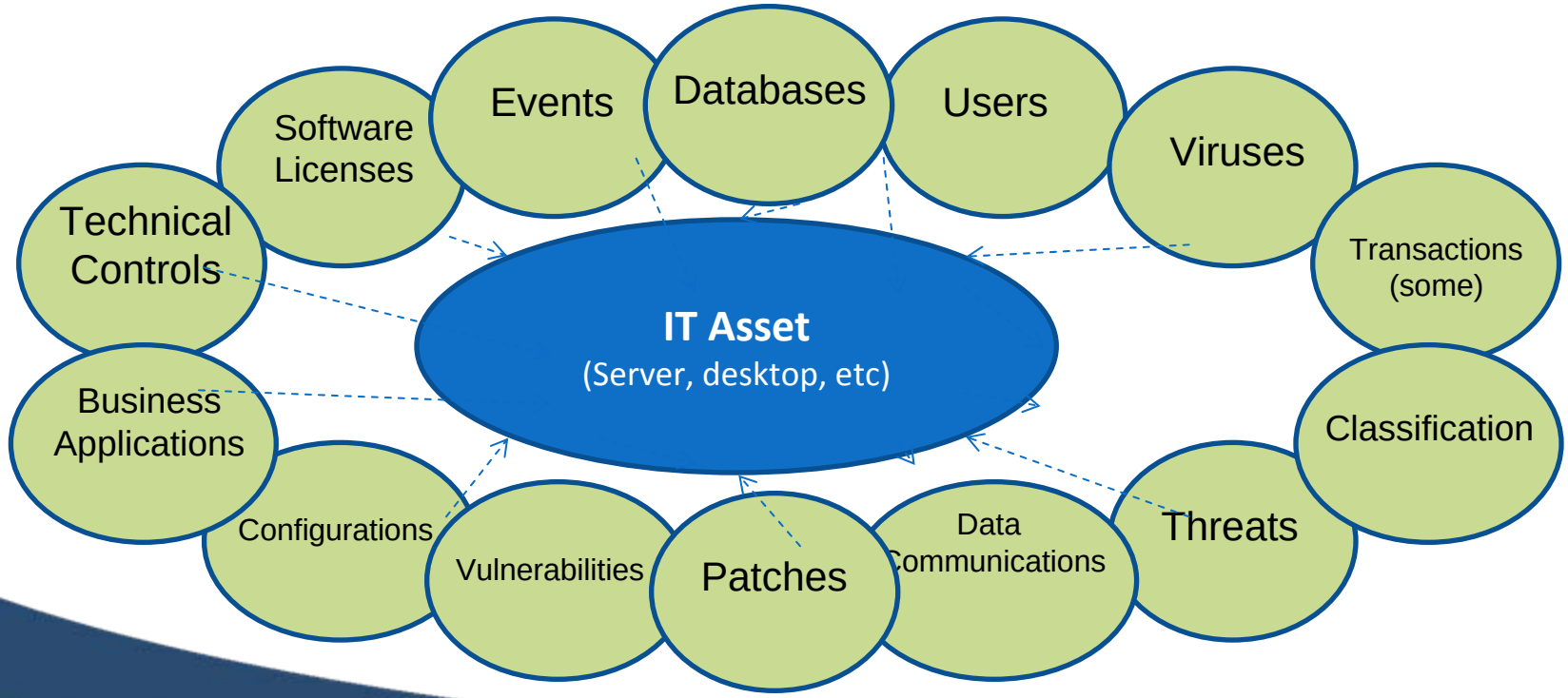
#1: Understand your process

- Obtain executive support
  - Key in successful implementations
  - Everyone needs to understand a clearly defined vision for enterprise SCAP solution
- Identify processes that make sense for enterprise data sharing via SCAP
- Determine if groups are willing to play nicely
  - Establish commonalities in benchmarks, metrics, etc
  - Learn to meet halfway in order to get the most of an enterprise SCAP solution
- What content makes sense?
  - 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

Copyright © 2009 Gideon Technologies, Inc.

#2: Understand your Assets

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



GIDEON TECHNOLOGIES
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

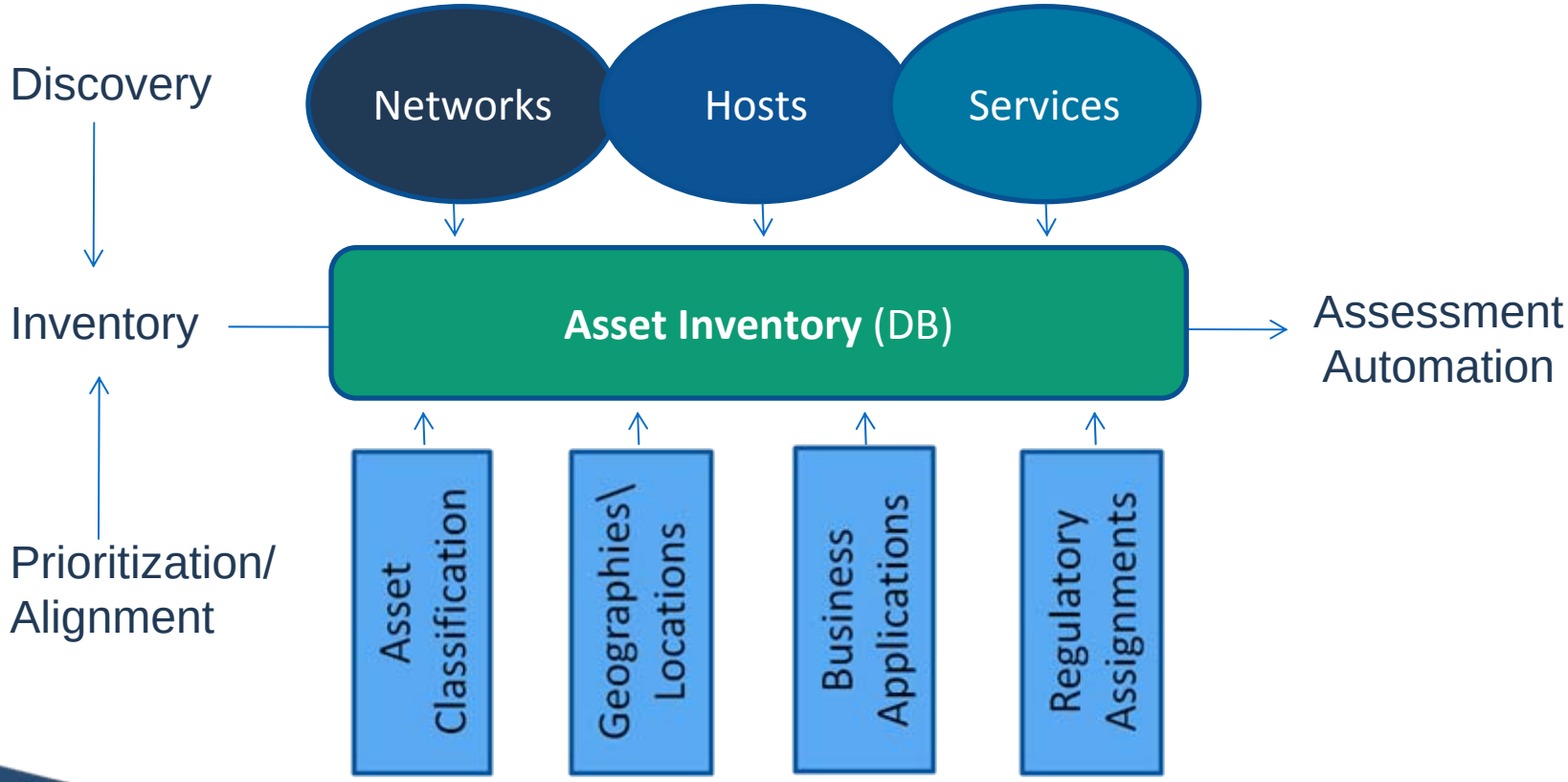
#2: Understand your Assets

- A tough lesson learned:
  - 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 key business applications?
    - What are the most critical assets?
    - How have our assets changed?
    - Where do we store data?

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

Copyright © 2009 Gideon Technologies, Inc.

Discovery: The Foundation of Effective CA



GIDEON TECHNOLOGIES
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

#3: Move Away From Point Solutions

- Never scales well for enterprise efforts
  - Too many assets for an effective point solution
- Greater difficulties to integrate
  - Time consuming
  - Data format interoperability
  - Custom APIs
- No common methodology
  - Differences in administering point solution by administrator/ user
- Point solution substitutes
  - Native platform controls could provide for validation to enterprise solutions
- Point solution is no substitute for enterprise solutions

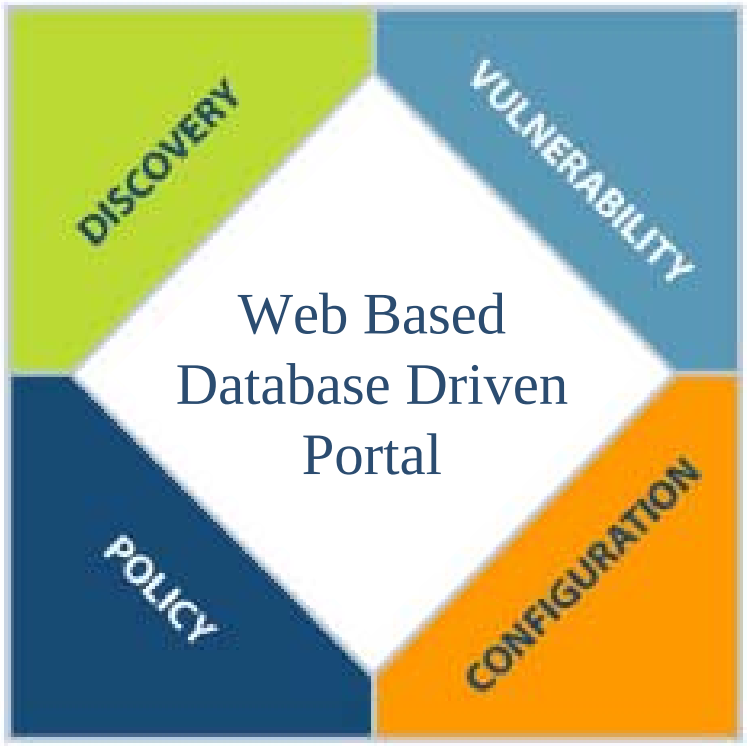
Copyright © 2009 Gideon Technologies, Inc.

#3: Move Away from Point Solutions

- An enterprise solution can provide broad assessment capabilities without cost and complexity

•Asset Inventory
•Procurement/Fulfillment
•Rogue Tech. Identification
•Prohibited Services
•M&A Due Diligence
•Network Change Mgmt
•Asset Classification

•Company Standards
•Industry (PCI)
•Customer (SAS70)
•Regulatory (SOX/HIPPA)
•Vendor (MS, RedHat)
•Audit (ISO/NIST)



•Vulnerability Assessments
•Patch Validation
•Firewall Rules Testing
•Web Application Security
•Database Security

•User Access/Provisioning
•Password Controls
•Software Compliance
•Sensitive User Rights
•System Files/Permissions
•Anti-Virus Compliance
•System Configuration
•Change Mgmt Validation

GIDEON TECHNOLOGIES
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.

#4: Metrics-Based Reporting

- Socialize metrics
  - 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 by business unit and business application
  - Comparative/competitive analysis
    - Vulnerabilities by Application (ERP | OE | Payroll | E-Commerce)
    - SOX Controls by Business Unit (HQ | SE | NE | NW | Central)
- Metrics facilitate trend reporting
  - 65% compliance might be good news!
    - Internal baselines need to be determined

Copyright © 2009 Gideon Technologies, Inc.

BP #5: Operational Independence & Intelligence

Content considerations

- Develop internally or subscribe to content from content providers

Operational Considerations for Solutions

- Easy deployment (i.e. agentless)
- Bandwidth throttling
- Control of date/time/frequency

Operate independent of Operations

- Processes should validate, not depend on…
- Information should provide actionable items for remediation

Copyright © 2009 Gideon Technologies, Inc.

About Gideon Technologies

- Founded by PWC security and compliance experts
- Serving Public Sector and Critical Infrastructure Markets
- Offices in Atlanta, GA and Washington DC

- The Company provides compliance and risk measurement solutions
  - Scalable - Easy to deploy and integrate - Standards based

- The leading vendor of SCAP tools for Risk Management & Compliance
  - OVAL Board Members – we help guide the standards
  - Co-chair of ISAlliance.org VOIP SCAP Working Group
  - Most NIST Validations of any Vendor – 2 years in a row!
  - Largest Enterprise SCAP implementation in the industry – 200,000+ Assets at US DHHS

Copyright © 2009 Gideon Technologies, Inc.

Contact Information

Tony UcedaVelez
Director
(678) 317-4307
tonyuv@gideontechnologies.com

Scott Armstrong
VP Marketing & Alliances
703-564-2425
sarmstrong@gideontechnologies.com

GIDEON TECHNOLOGIES
Know your assets. Know your risk.

Copyright © 2009 Gideon Technologies, Inc.