Defense Information Systems Agency

A Combat Support Agency

Gaps in Automated Situational Awareness

Mr Joe Wolfkiel

DISA PEO MA IA5

November 1, 2011

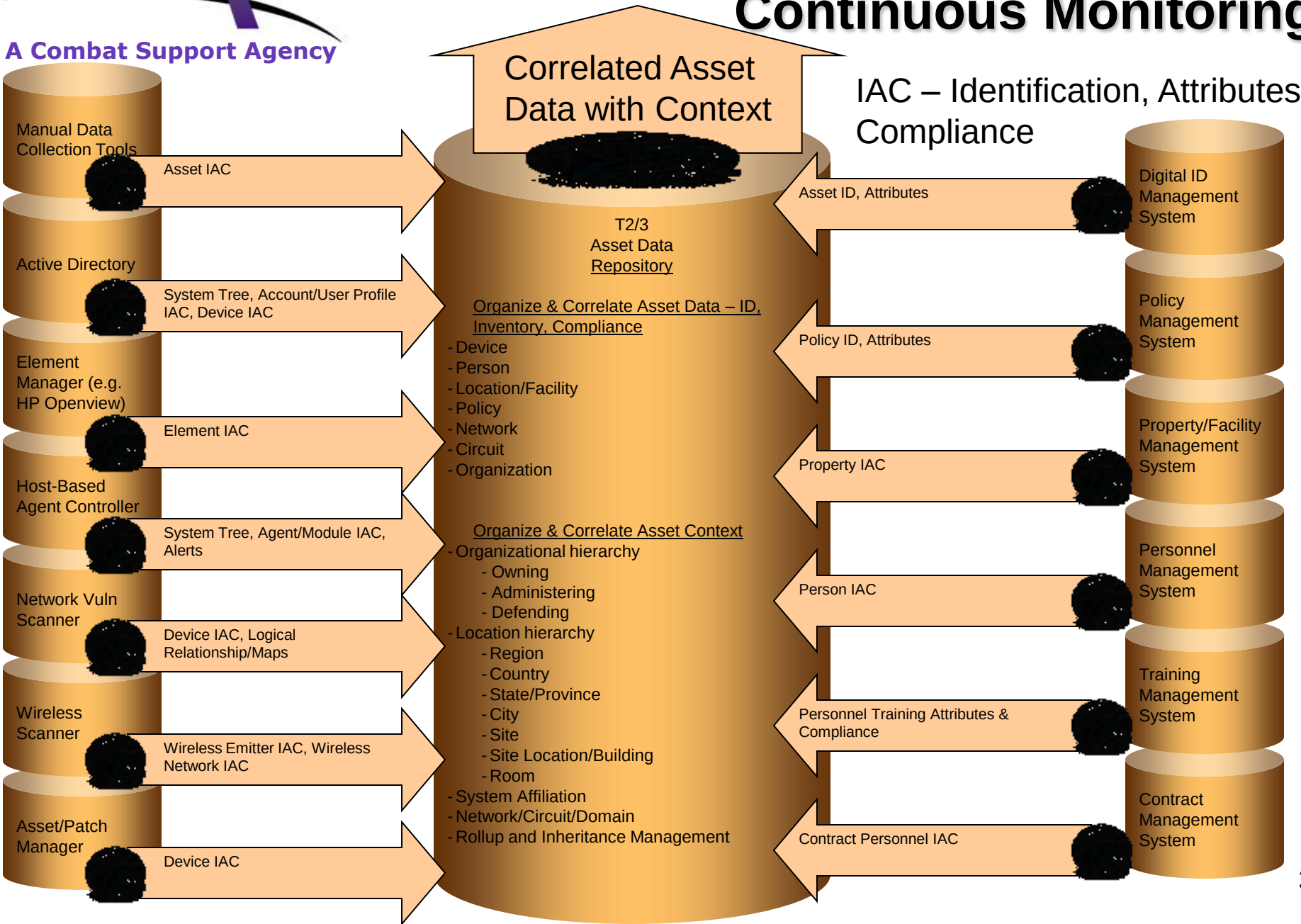
DISA
A Combat Support Agency

Overview

- Technical Gaps
- Conceptual Gaps
- Policy Gaps

Technical Gap: Sensor Inputs for Continuous Monitoring

A Combat Support Agency



DISA
A Combat Support Agency

Technical Gap: Data Analytics and Functionality

Bottom Tier Data Manipulation Capabilities

T2/3
Asset Data
Repository

Organize & Correlate Asset Data – ID, Inventory, Compliance
- Device
- Person
- Location/Facility
- Policy
- Network
- Circuit
- Organization

Organize & Correlate Asset Context
- Organizational hierarchy
  - Owning
  - Administering
  - Defending
- Location hierarchy
  - Region
  - Country
  - State/Province
  - City
  - Site
  - Site Location/Building
  - Room
- System Affiliation
- Network/Circuit/Domain
- Rollup and Inheritance Management

Functions

Sensor Fusion
- Correlate device IDs across sensors
- Aggregate asset attributes from multiple sensors
- Deconflict disparate findings from multiple sensors

Context Fusion
- Locate assets within appropriate operational context
- Provide aggregation based on location, organization, network, system accreditation boundary, etc.
- Manage inheritance of controls/findings across asset types

Compliance Calculation
- Run compliance definitions against inventory and status findings to compute compliance
- “Roll up” lower level compliance findings to higher-level compliance or controls
- Calculate reduction in risk for non-compliance due to compensating controls

External Reporting
- Report (in ARF/ASR) assets, asset inventory, and compliance to multiple endpoints in configurable format

DISA
A Combat Support Agency

Technical Gap: Data Analytics and Functionality

More Bottom Tier Data Manipulation Capabilities

T2/3
Asset Data
Repository

Organize & Correlate Asset Data – ID, Inventory, Compliance
- Device
- Person
- Location/Facility
- Policy
- Network
- Circuit
- Organization

Organize & Correlate Asset Context
- Organizational hierarchy
  - Owning
  - Administering
  - Defending
- Location hierarchy
  - Region
  - Country
  - State/Province
  - City
  - Site
  - Site Location/Building
  - Room
- System Affiliation
- Network/Circuit/Domain
- Rollup and Inheritance Management

Functions

Visualization
-Show asset summary data
  -Total assets with common inventory
  -Total assets comply/non-comply with control
- Show reporting status per:
  - Reporting Endpoint
  - Organization
  - Location
  - System
  - Asset

DISA

A Combat Support Agency

Technical Gap:N-Tier Rollup and Drill-Down

Correlated Asset Data with Context for FISMA & DHS

Enterprise CMRS/DPMS Capability

- Summarize Lower Tier Data and Operational Context
- Assess and assign values and severities to data
- Visualize data at enterprise level broken down by organization, location, and system
- Maintain historic summary data to enable trending
- Provide decision support to enable C2
- Evaluate and present data reporting compliance
- Support automated workflows for issue resolution
- Execute time-based analytics to identify emerging problems

- Create metrics and score information to assist in digital policy creation
- Ingest or create updated severity scores based on updated threat data
- Automate workflow for policy creation, C2 and compliance tracking, and dynamically created processes
- Bring in previously unknown data feeds to allow for correlation and enhanced scoring with emerging threats and measures
- Create taskings for data collection, reporting, detail, and format
- Create, maintain, and disseminate enterprise lists of “official” organization, location, and system names

Summary and Detailed Dynamic Data Provisioning

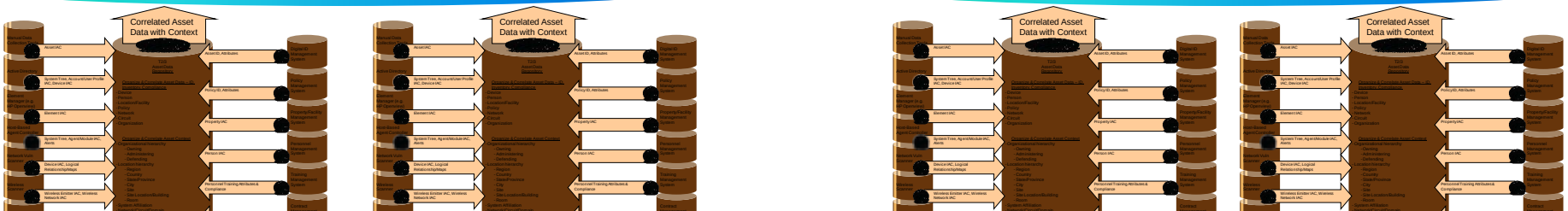
Summary and Detailed Dynamic Data Provisioning

Component Enterprise Asset Data Repository

- Aggregate Lower Tier Data and Operational Context
- Assess and assign values and severities to data
- Visualize data at enterprise level broken down by organization, location, and system
- Provide on-demand summary data to higher-tier enterprise queries
- Maintain data in optimized query and storage formats
- Provide decision support to enable C2
- Evaluate and present data reporting compliance
- Support automated workflows for issue resolution
- Execute time-based analytics to identify emerging problems

Component Enterprise Asset Data Repository

- Aggregate Lower Tier Data and Operational Context
- Assess and assign values and severities to data
- Visualize data at enterprise level broken down by organization, location, and system
- Provide on-demand summary data to higher-tier enterprise queries
- Maintain data in optimized query and storage formats
- Provide decision support to enable C2
- Evaluate and present data reporting compliance
- Support automated workflows for issue resolution
- Execute time-based analytics to identify emerging problems



DISA
A Combat Support Agency

Technical Gaps

- Contextual data tag definitions
- Ontologies for common informational constructs
  - System, Network, Person, Circuit, Location, Organization, Policy, etc.
  - Not just ontologies, but XML or equivalent representations
- Unified directory management and asset tagging capabilities

DISA
A Combat Support Agency

Conceptual Gaps

- **Full scope risk quantification and scoring**
  - **Concept of assigning "severities" to all aspects of assets, events, and other common risk indicators**
  - **Concepts for distributing severity scores**
  - **Occupational training and description of personnel who would assign and maintain severity scores – across federal & civilian space**
- **Requirement for "actionable" data**
  - **Defining the range of activities required to secure and defend networks – i.e. security facilities, training users, applying patches, etc.**
  - **Directly linking those "actions" to risk scored findings and severities**

DISA
A Combat Support Agency

Conceptual Gaps

- **Psychological concepts**
  - **How to incentivize and reliably drive desired behaviors**
  - **What did we really learn from previous pilots?**
- **What needs to be measured?**
  - **Can we define the "real" questions we're trying to answer?**
  - **i.e. what questions get answered by supplying a CONOP and a network diagram?**
  - **Can we obtain answers to the questions versus information required to derive the answers?**

DISA
A Combat Support Agency

Policy Gaps

- Compliance versus effective risk management
- Integrating business processes
  - Red/Blue team
  - C&A
  - CERT
  - Vulnerability Management
  - Deconflicting other policy – HIPPA, SOX, etc.

DISA

A Combat Support Agency

QUESTIONS?