Implementing An Integrated Network Defense Construct

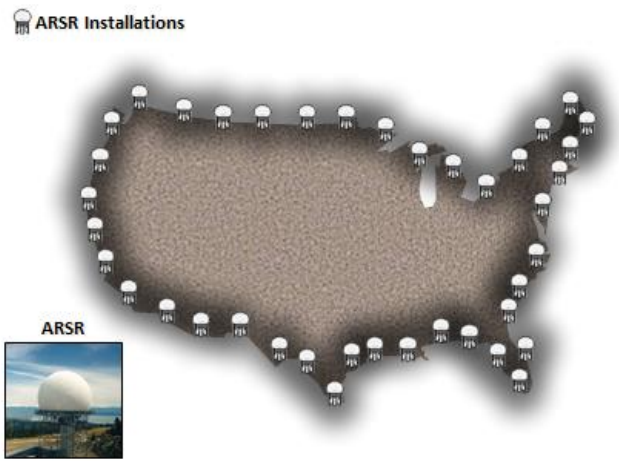
Maj Ronald "Rusty" Clark
Maj Jonathan Butts, PhD
Robert F. Mills, PhD

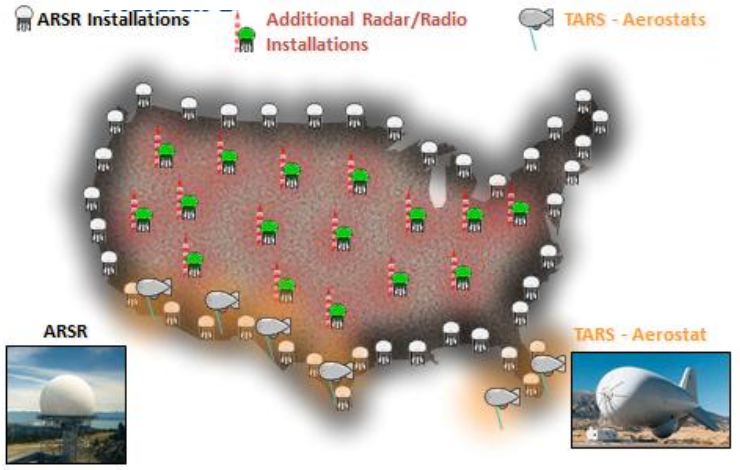
Overview

- Motivation
- Purpose and Scope
- Network Defense Background
  - Areas of Improvement
- Integrated Air Defense System
- Integrated Network Defense Construct
- Recommendations
- Summary

Motivation

- September 11, 2001
  - Cold War-era air defense model
  - Lack of ability to track internal traffic
- Perimeter-based model of defense was inadequate
- Modern enterprise network defense models share many similarities





Purpose and Scope

- Purpose
  - The construct of network defense is inadequate to protect sensitive information in enterprise infrastructures
  - This research seeks to apply lessons learned from the United States air defense structure to the networking defense paradigm

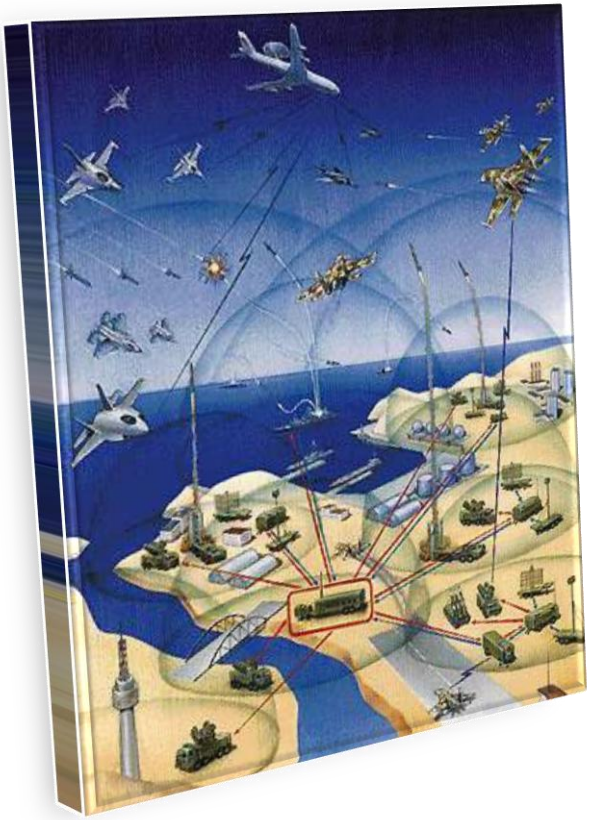
- Scope
  - Examines the IADS construct in the abstract
  - By analogy, explore fundamental principles in the system to improve identification, control and eradication of threats on enterprise networks

Background

- Network Defense
  - Security mindset
  - Layered Defense
- The Cyber Defense Dilemma
- Areas for Improvement
  - Signature-based Methodology
  - Data Inundation
  - Network Visibility
  - Shared Operational Picture
  - Agile Command Structure

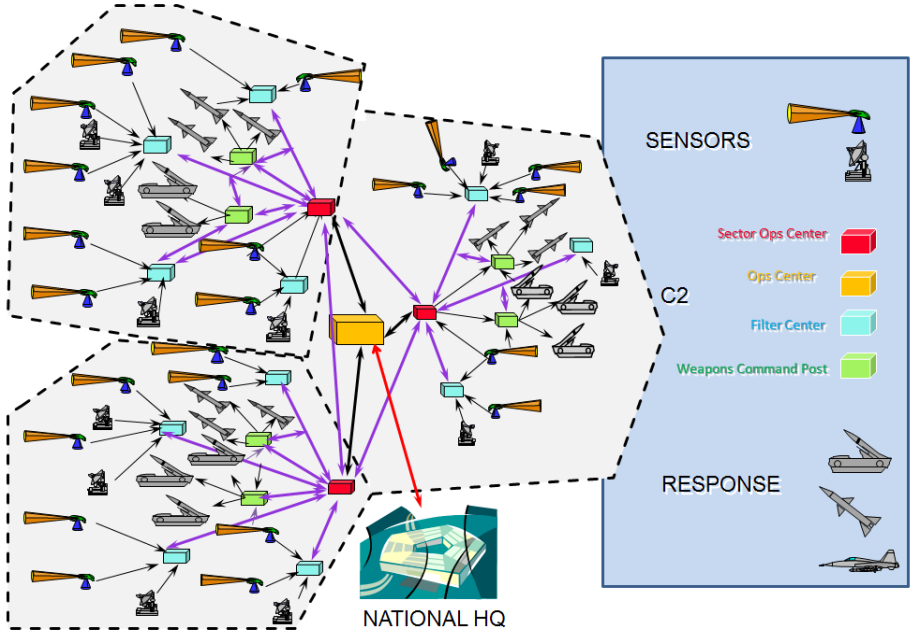
Integrated Air Defense

- Evolution of IADS
- Structure
  - Command and Control
  - Threat Identification
  - Battle Management
  - Engagement



Command and Control

- Architecture enables tasking, collaboration and response actions across areas of responsibility
- Requires a mature C2 approach
  - Self-synchronizing collaboration model
  - High degree of shared awareness
- Agility necessary to react to dynamic situations, while coordinating actions with numerous entities

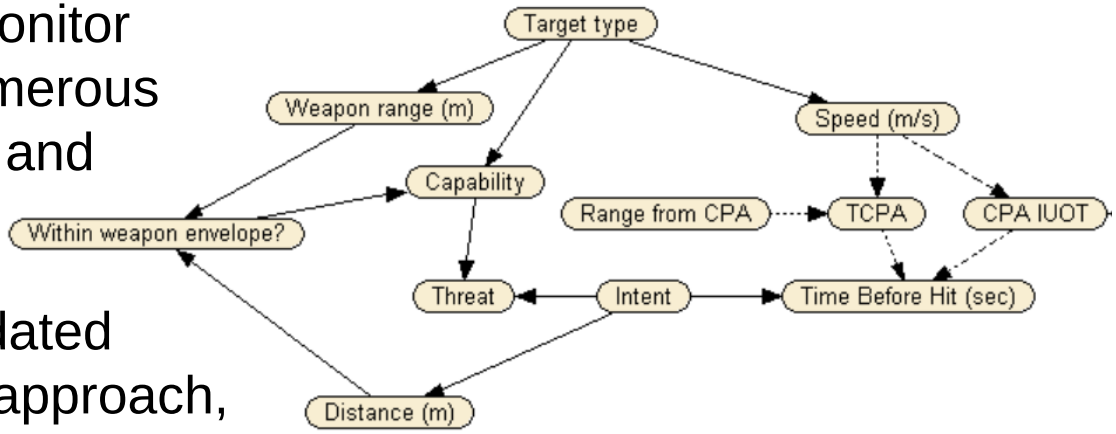


Threat Identification

- Begins once a target (track) is detected in the search area
- Tracks are evaluated via IFF transponders
- Wide variety of sources using differing reporting protocols
  - Flight Plans
  - Radar, Acoustic, Optronic Sensors
  - Visual observation
- Information fed into/aggregated at filtering centers and sent to SOCs, and the collective system
  - Swarm model of communication used ensures all entities are up-to-date
- Tracks identified as hostile are labeled threats

Battle Management

- Controllers continuously monitor threats, conferring with numerous sources to ascertain origin and assess intentions



- Collection systems are updated using a Bayesian network approach, making it possible to handle imperfect observations

- Common interface provides
  - "Drill-down" ability on a target
  - Automated intent-assessment logic
  - Special symbology helps comprehension

- Information fed immediately to decision makers

Engagement

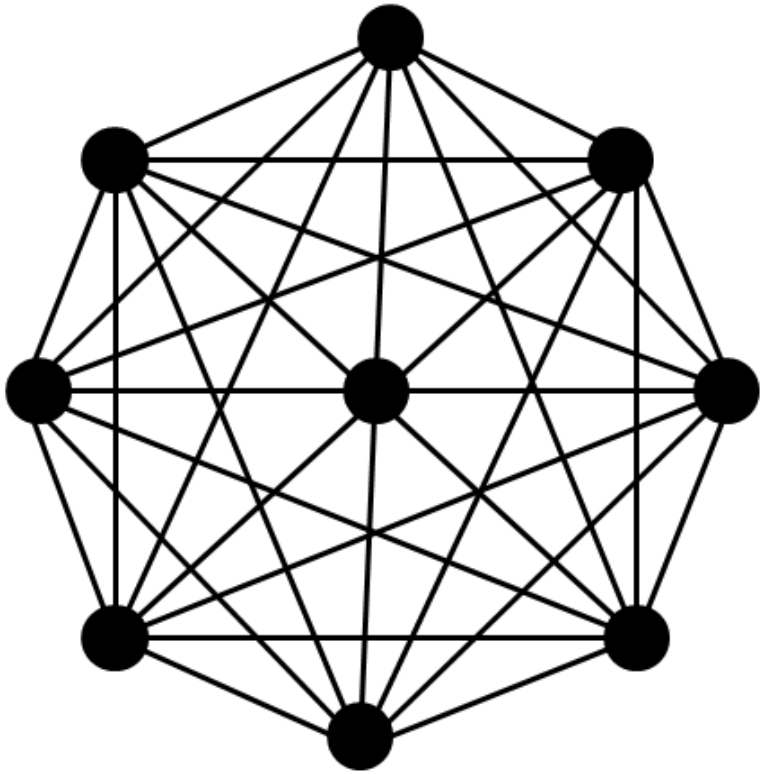
- Controllers restrict, redirect, or destroy the threat
- Respond with a range of capabilities
  - Radio
  - Combat Air Patrol
  - Air defense artillery
  - Air and Missile Defenses

Integrated Network Defense

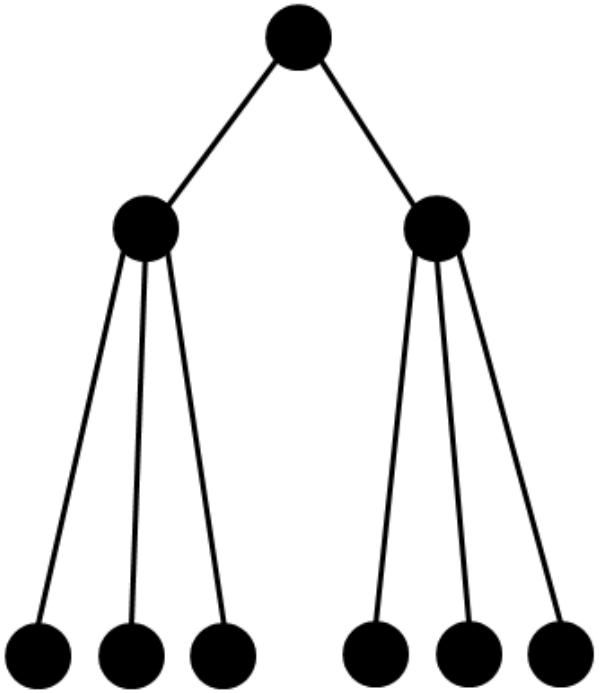
- Command and Control
- Threat Identification
- Battle Management
- Engagement

INDS Command and Control

IADS Meshed C2 Architecture

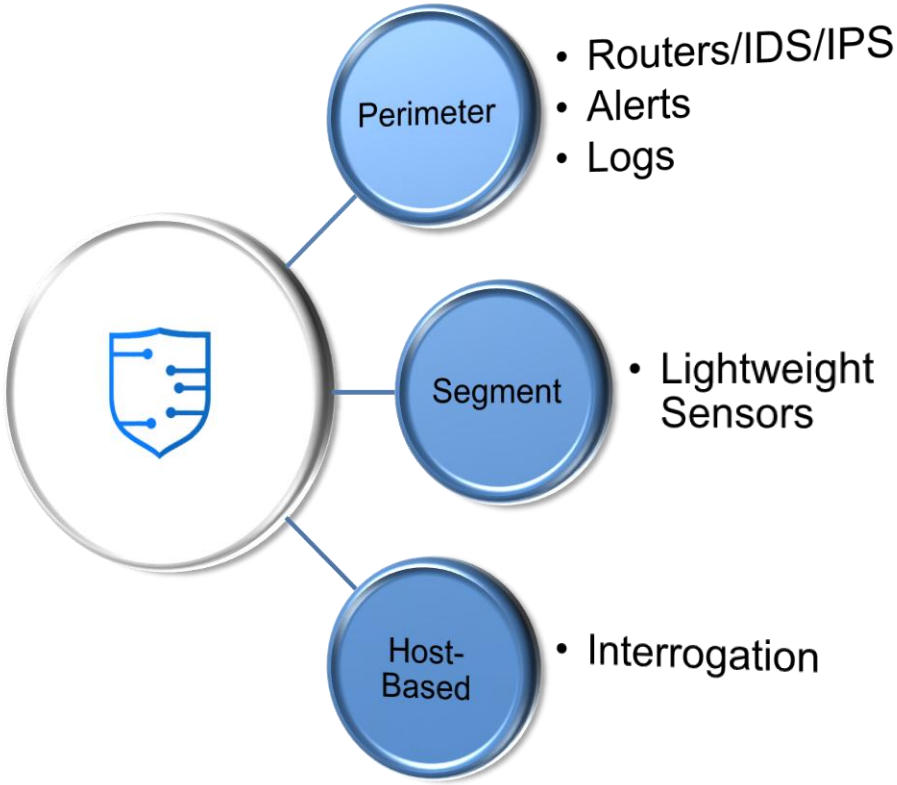


IT Hierarchical C2 Architecture

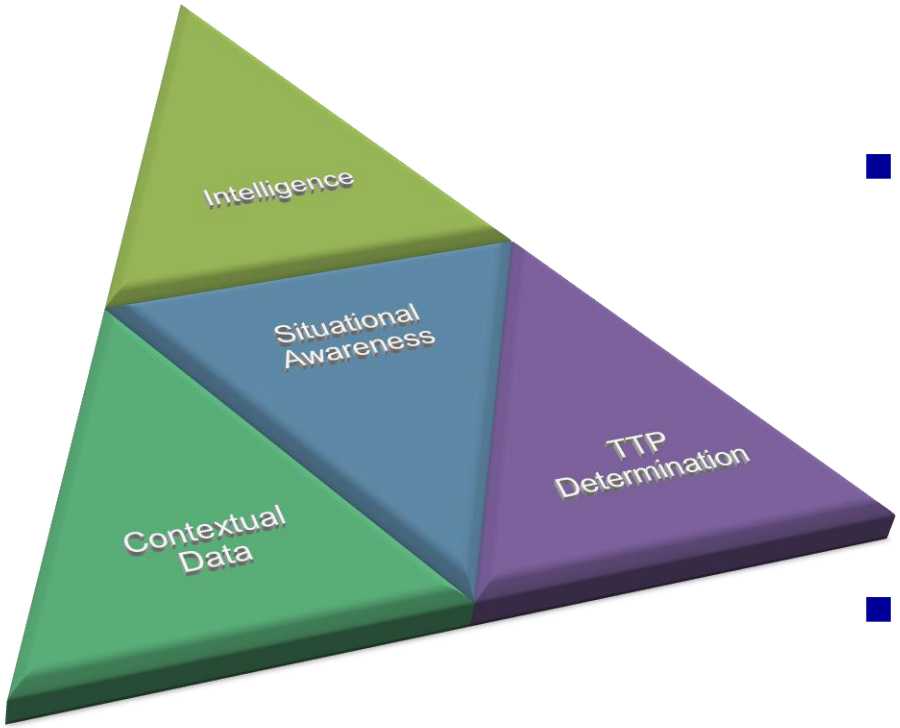


Threat Identification

- Typical network traffic sensing devices examine traffic at gateways
  - Fail to observe interactions at the physical layer of communications
- To counter this problem
  - Network needs to be instrumented to identify and track the adversary
  - Focus must turn to movements throughout the network

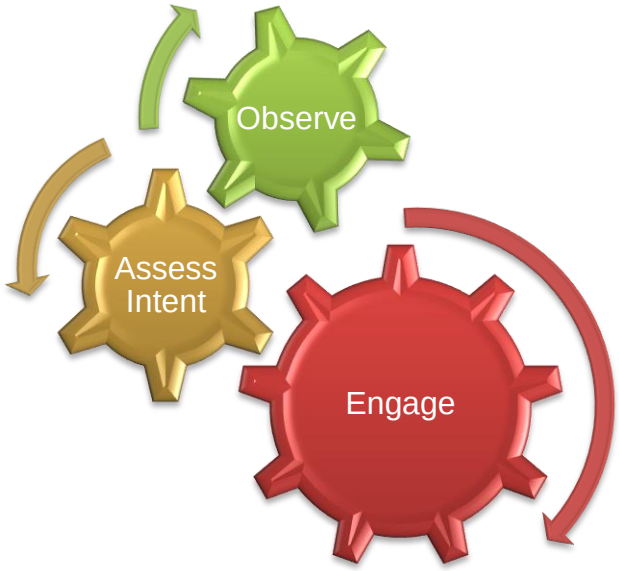


Battle Management



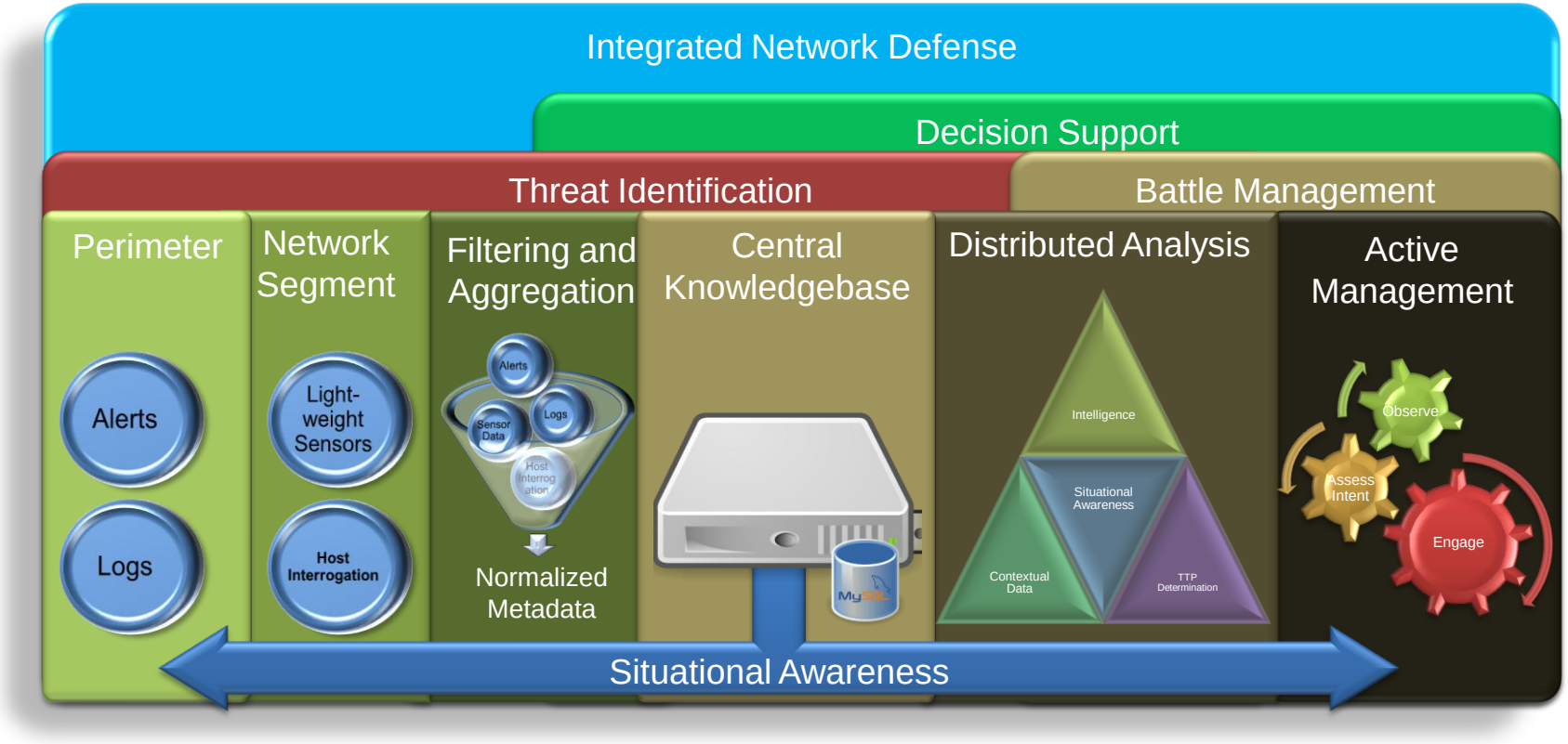
- Distributed analysis and decision support to accurately quantify threats
  - Shares analytical resource burden
  - Aids in threat ID
- Each level in defensive construct is distinct in focus and information need, but information necessary for each level is derivable using common data
  - Situational awareness framework institutes collective workforce against a common foe
- Gain an understanding of adversary
  - Exploitation vector
  - Methods of persistence
  - Intentions

Engagement



- Response actions
  - Actions beyond the gateway are highly controversial; ethical and legal concerns
  - Within boundaries of corporate network are within the authority of defenders
- Delegated Authority
  - Eliminate
  - Redirect
  - Continue to monitor

Integration



Recommendations

- Incorporating an INDS can be accomplished by enacting three changes to the current network defense architecture
  - Personnel
    - Allocated at Each Geographic Location
    - Trained to perform distributed network threat identification and analysis
  - Develop a collaborative environment
    - Meshed operational structure
    - Means to collaborate
  - Network enclaves instrumented to adequately ID threat activity
    - Sensors
    - Visualization capabilities

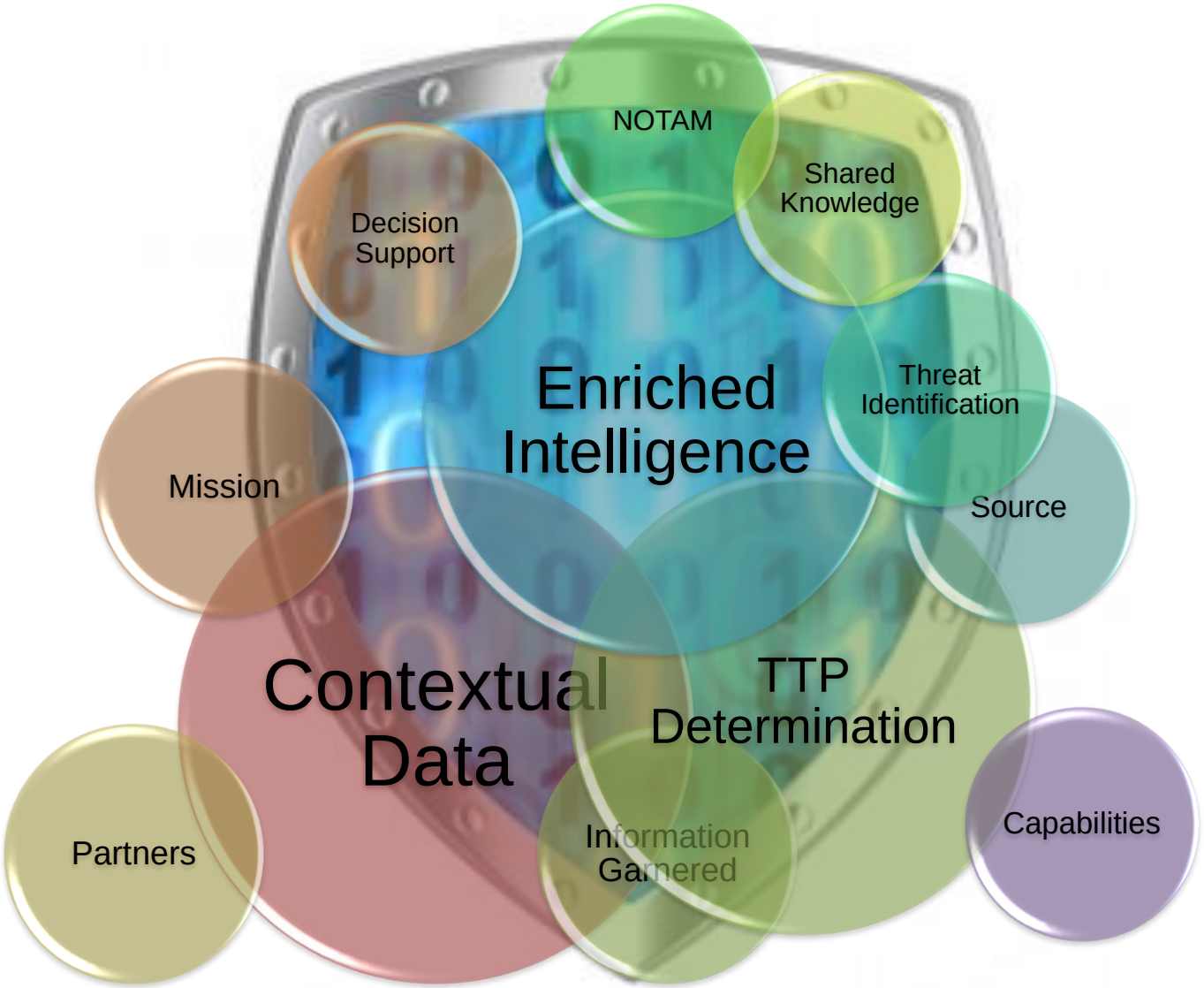
Areas of Improvement

AOI	Improvement	Result
Signature-based Methodology	Sensors	Improved visibility enables threat ID with lateral movement
Data Inundation	Distributed Analysis	Identify threats to the end mission
Network Visibility	Sensors	Track threats as they maneuver through the network
Shared Operational Picture	Knowledgebase	Tailored views based on need
Agile Command Structure	Meshed Org Structure	Accelerated tasking and response

Summary

- Despite advances in perimeter defense, enterprise networks are still vulnerable to infiltration by persistent adversaries
  - Inadequate threat picture; No means to facilitate defensive actions
  - Network configurations lack ability to provide visibility down to host level
  - Defenders and mission owners do not share operational information
- Applying abstracted IADS principles provides
  - Agile, distributed command structure and analytical workforce
  - Empowers mission owners to take active roles in defense
  - Lessens adversarial advantage with correlation of indicators & shared knowledge

Questions


NOTAM
Shared Knowledge
Decision Support
Threat Identification
Enriched Intelligence
Mission
Source
Contextual Data
TTP Determination
Partners
Information Garnered
Capabilities