Lincoln Laboratory Cyber Situational Awareness Pilot

Tamara Yu – MIT Lincoln Laboratory

Concept

- An open Cyber situational awareness (SA) architecture enables rapid integration of sensor data and accelerates development of analytics
- Lincoln Lab is developing a novel Cyber SA system to evaluate data collection, analysis and visualization techniques and improve the lab's network security.

Command and Control

Lincoln Laboratory Network

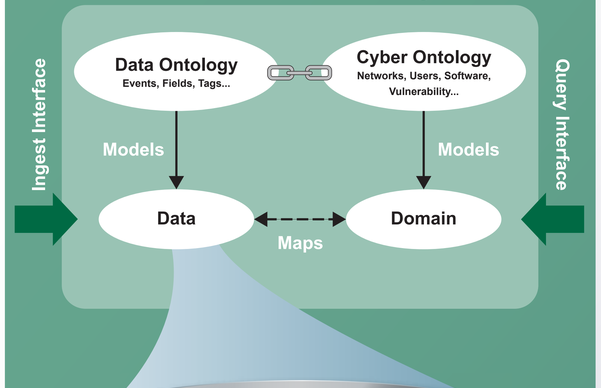
Data Feeds

- Server Logs (splunk>)
- Traffic Capture
- AV, HIPS & Vulnerability Scans (HBSS)
- Infrastructure Configurations
- Enterprise Management (SCCM)

Ingest and Enrich

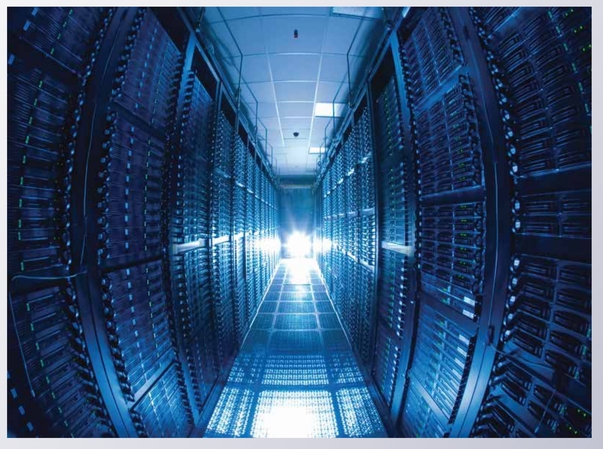
Ontology-based Ingest and Query Framework

Provide semantic abstractions for data access and reasoning



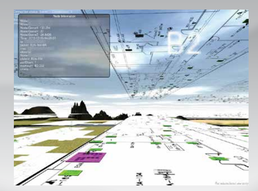
Store large amounts of dynamic heterogeneous data

Elastic Grid Computing

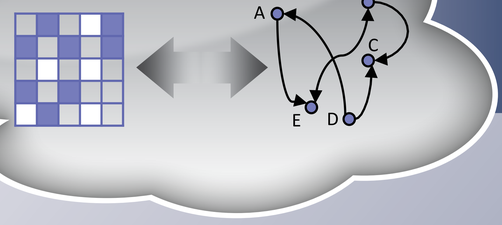


Run on a scalable computing platform based on LLGrid technology

Advanced User Interfaces

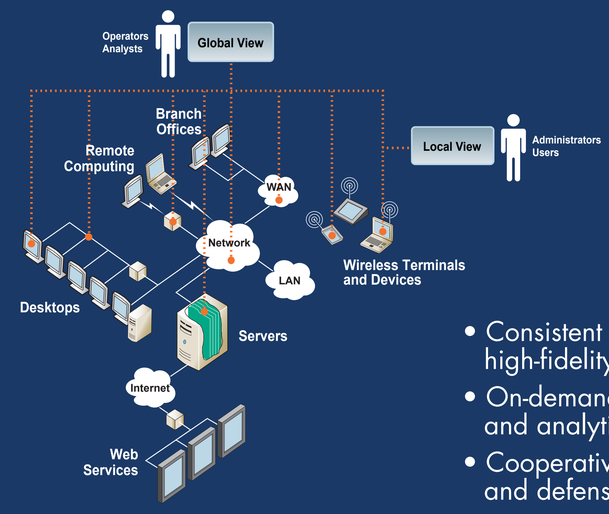


Advanced Analytics



Situational Awareness

Vision



- Consistent and high-fidelity views
- On-demand sensing and analytics
- Cooperative monitoring and defense

This work is sponsored by the Assistant Secretary of Defense under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Government.