U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

John Michalski

SNL Department 5621

Threat Characterization

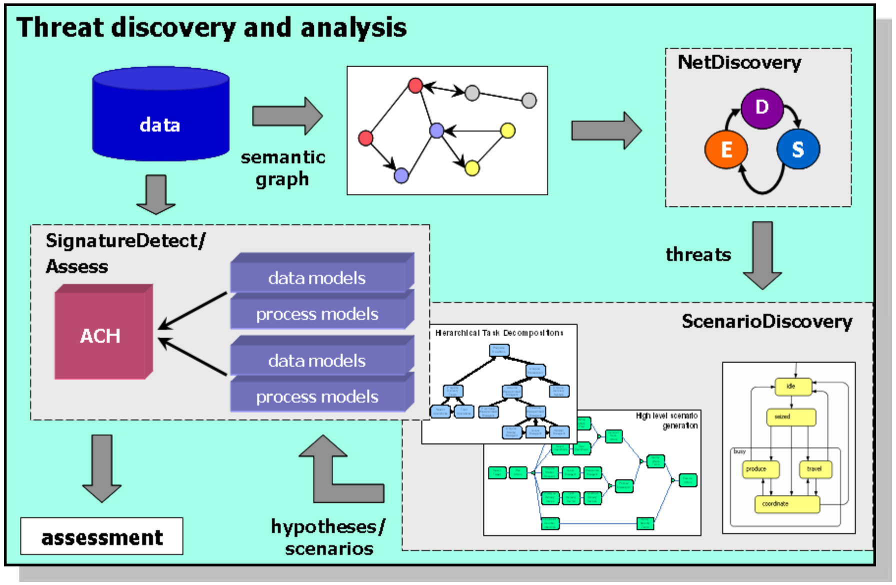
Summary Slide: Threat Characterization

Outcomes: Develop a network analysis toolset to allow an analyst to efficiently “crawl” large data sets to discover relevant threat information.

Road Map Challenges:“The ability to discover & understand emerging threats and vulnerabilities is a prerequisite to developing effective countermeasures”

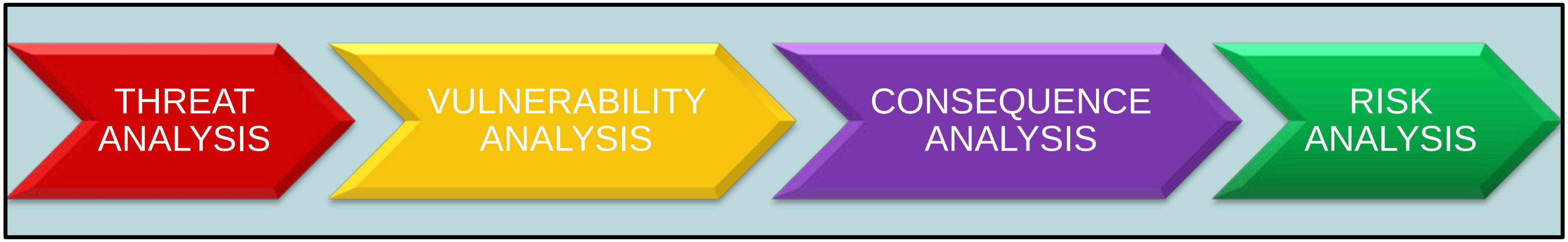
Major Successes:

- Implemented prototype front end crawler and semantic analysis engine (Sandia National Labs).
- Transition Development work to the Institute for Complex Additive System Analysis (ICASA) Center (NMTech)
- Quarterly threat reports being produced



- **Schedule:** Improvements to both the analyst process and GUI Interface, 4Q 2009; Transition maintenance and development to ICASA, 02/2010; Quarterly threat reports 3/30/10 to 12/30/10
- **Level of Effort:** $175k
- **Funds Remaining:** ~$50K
- **Performers:** SNL, NMTech
- **Partners:** OPUS Consulting

Integrated Risk Analysis Approach



THREAT ANALYSIS

VULNERABILITY ANALYSIS

CONSEQUENCE ANALYSIS

RISK ANALYSIS

What Threats are we Concerned about?

Evaluate effects of cyber vulnerabilities

What are the physical impacts?

Assess and quantify the Risk?

We Are Here

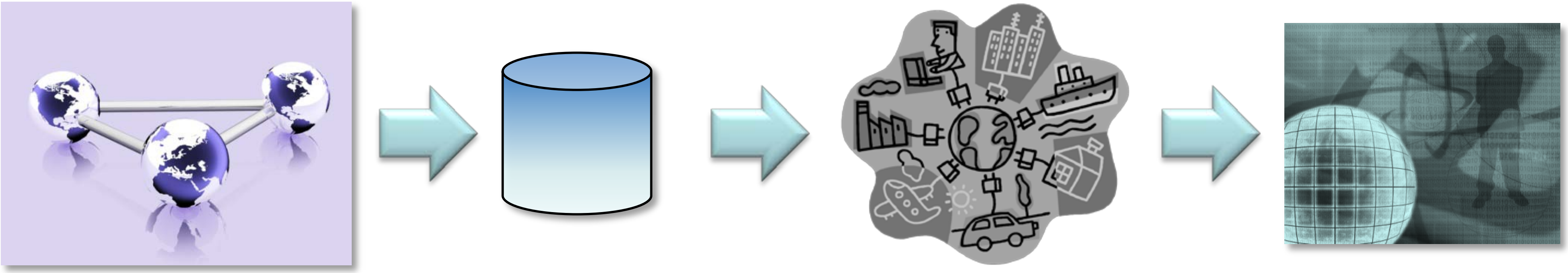
<u>Threat Analysis</u>: *What are the threats of interest?*

Mission: To reduce the risk of critical infrastructure disruptions due to cyber attacks on control systems

Approach and Execution

- **Leverage open and closed source data** to better quantify the level of threat in terms that are meaningful to the energy asset owners
  - Use Graph based analysis to discover relationships in data
- **Analyze and evaluate Data**, from plausible data associations
  - What kind of information can be found in the data sources about a specific vulnerability/topic?
  - What kind of “chatter” can be found on the internet.
- **Review viable scenarios**
  - Identify Scenarios that leverage viable attack paths that can be realized by the level of capability of the threat.
  - Identify and describe attack vectors
- **Provide mitigation** strategies

Approach and Execution



Focused Crawling
Inline Translation
Metadata
Harvesting

Sandia formulates topic search and key words

Data Wrapping
Data Warehousing
Data Indexing
Blog/Forum
Handling

Intermediate processing: The binding of information is stored and indexed for page/blog recovery

Link/Content Analysis
Discovery Oriented
Analysis
Time-series/Event
Detection
Fusion / OSINT / Multi-Source
SME integration

Information Processing: Review Word relationships identify patterns of interest. Sandia & ICASA Analyst

Findings
Reports

Sandia analyst and SME review: validate information on intelligence network. Capture salient points, produce report

Technical Accomplishments, Quality, and Productivity

- **Previous Project Accomplishments**
  - Developed and delivered a threat framework for sharing classified in an “open” forum
  - Developed and delivered a generic threat matrix to quantify threat capability in an unclassified environment
  - Developed a graph based algorithm for part of speech and concept community identification
  - Improved tool set: work out bugs in software to facilitate improvement in information processing
- **Current Accomplishments (2010)**
  - Transitioned tool development responsibility to ICASA (NMTech) for leveraging ongoing development and maintenance
  - Continued to improve tool set: graphical user interface
  - Produced 1Q threat report for DOE

Technical Accomplishments, Quality, and Productivity

- **Challenges to Success**
  - Developing a mechanism for the intelligence community to share actionable threat information
  - The data mining field is dynamic, new approaches are required
    - Create partnerships that leverages expertise

Technology Transfer, Collaborations, and Partnerships

- **Continue collaborations with SNL's threat analysts and the intelligence community**
  - Identify and understand *emerging* threats to the electric and O&G infrastructures
- **Continue partnership with the ICASA Center**
  - Maintain technical expertise in the dynamic field of data discovery
- **Continue to work with public/private stakeholders**
  - Develop a mechanism for sharing threat information

Next Steps

- **Approach For Next Year**
  - Continue tool feature-set enrichment
    - Streamlined interface to crawl engine
    - Better integration between database / analytic tools
    - Periodic retrieval / computational analysis
  - Add Trends analysis reporting capability

Questions?