

# Decision Support for Computer Network Defense

**Richard Pietravalle**  
781-271-7994 • [rpietravalle@mitre.org](mailto:rpietravalle@mitre.org)

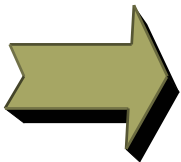
Air Force MOIE

The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow and orange to the left of the text.

**MITRE**  
**Technology**  
**Program**

# Problem

- **Computer network defense needs improvement:**
  - **Overwhelming quantity of data**
  - **Numerous complex and disjoint tools**
  - **Operators typically not technical experts**
- **...So response time is too long and tends to an “all or nothing” approach**



*Need fast, automated assistance in evaluations and recommendations*

# Background

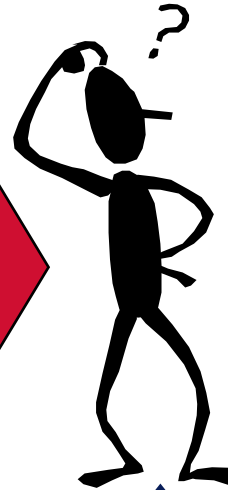
## Sensors

Firewalls  
Routers  
Network IDS  
Host IDS  
System Logs  
Application Logs  
Net Mgt Tools  
User Feedback

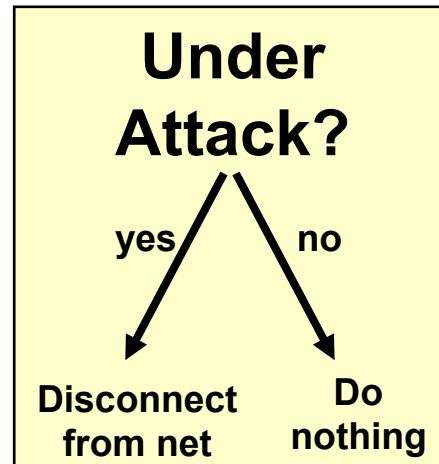
## Repository

DB History  
Outpost  
Tivoli  
etc.

## Decision Process



## Current Algorithm



- Correlate data and identify fundamental "observables"
- Link specific COA recommendations to particular states defined by observables

**MOIE Focus**

# Objective

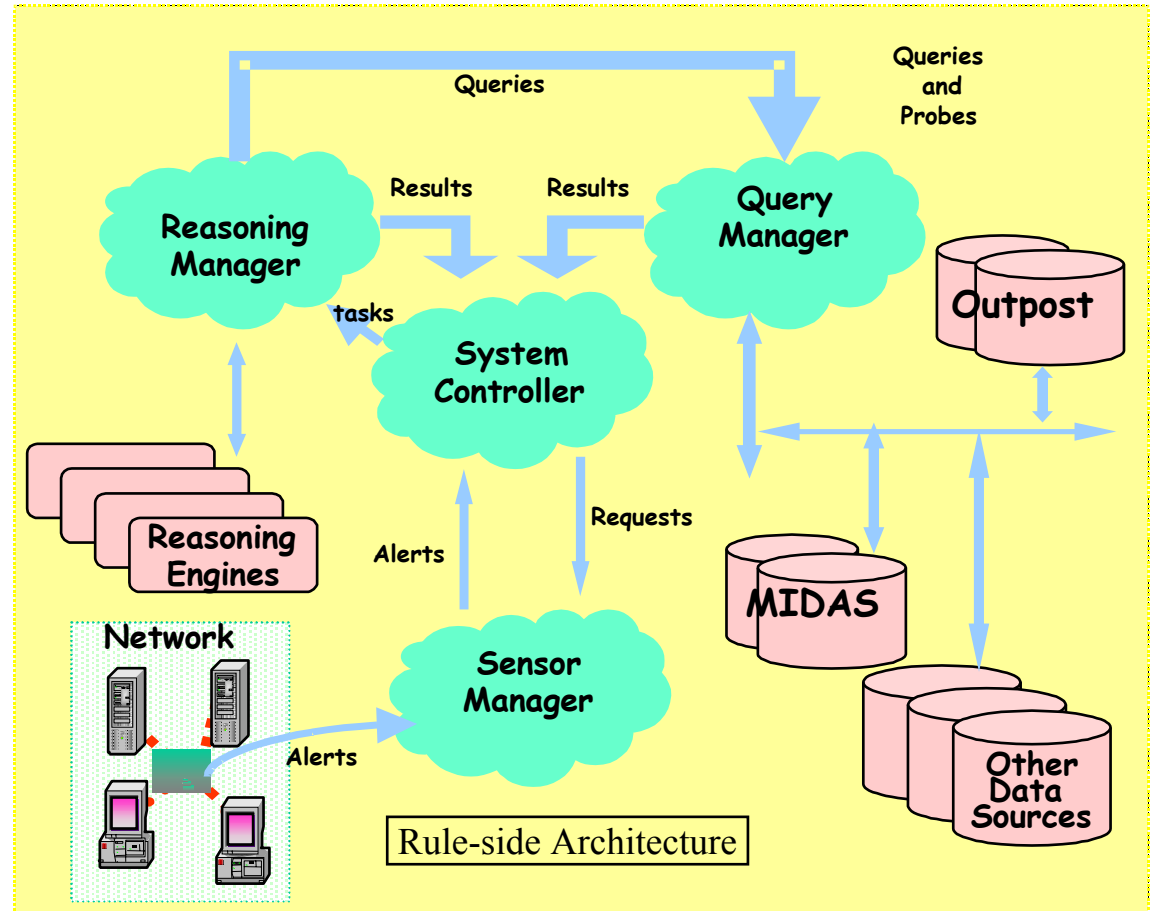
- **Research and design a system that...**
  - **Analyzes network state**
  - **Adapts to dynamic conditions**
  - **Produces timely course of action recommendations**
- **Develop proof of concept prototype**

# Activities

- **Leverage MITRE operational experience to identify critical states that would benefit from automated COA recommendations**
- **Develop rule-based system within existing management infrastructure to identify the “observables” of critical states**
- **Research and develop mapping between observables and COA recommendations**

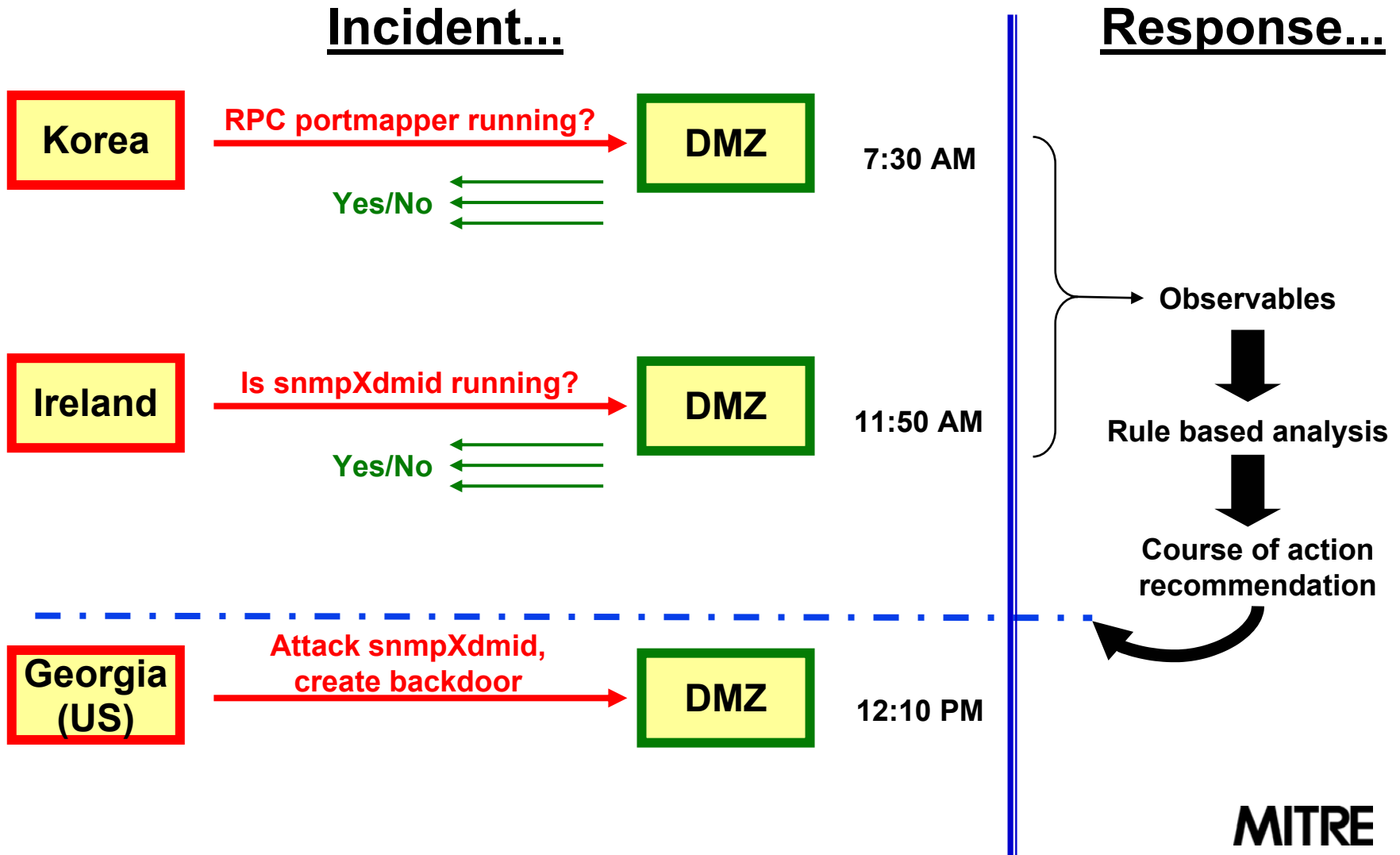
# Highlight

- Selected scenarios
- Developed architecture
  - Modeled scenario
    - rules, sensor events
    - formal descriptions
- Picked rule-based tools
- Started software implementation
- Began developing additional scenarios



(MIDAS= MITRE Intrusion Detection Analysis Suite)

# Highlight: Initial Scenario



# Impacts

- **Customer operational mission**
  - Long-term improvement in ability to defend critical computer and network assets with typical staff
- **Academic / R&D**
  - Publish papers on feasibility to automate course of action determination; impact follow-on community research and product development
- **Relevant knowledge capture and dissemination**
  - Dialog/share with existing network defense research efforts (e.g., AFRL, AFIWC, etc.)

# Future Plans

