

Decision Support for Computer Network Defense

Richard Pietravalle

781-271-7994 • rpietravalle@mitre.org

Air Force MOIE

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

MITRE
Technology
Program

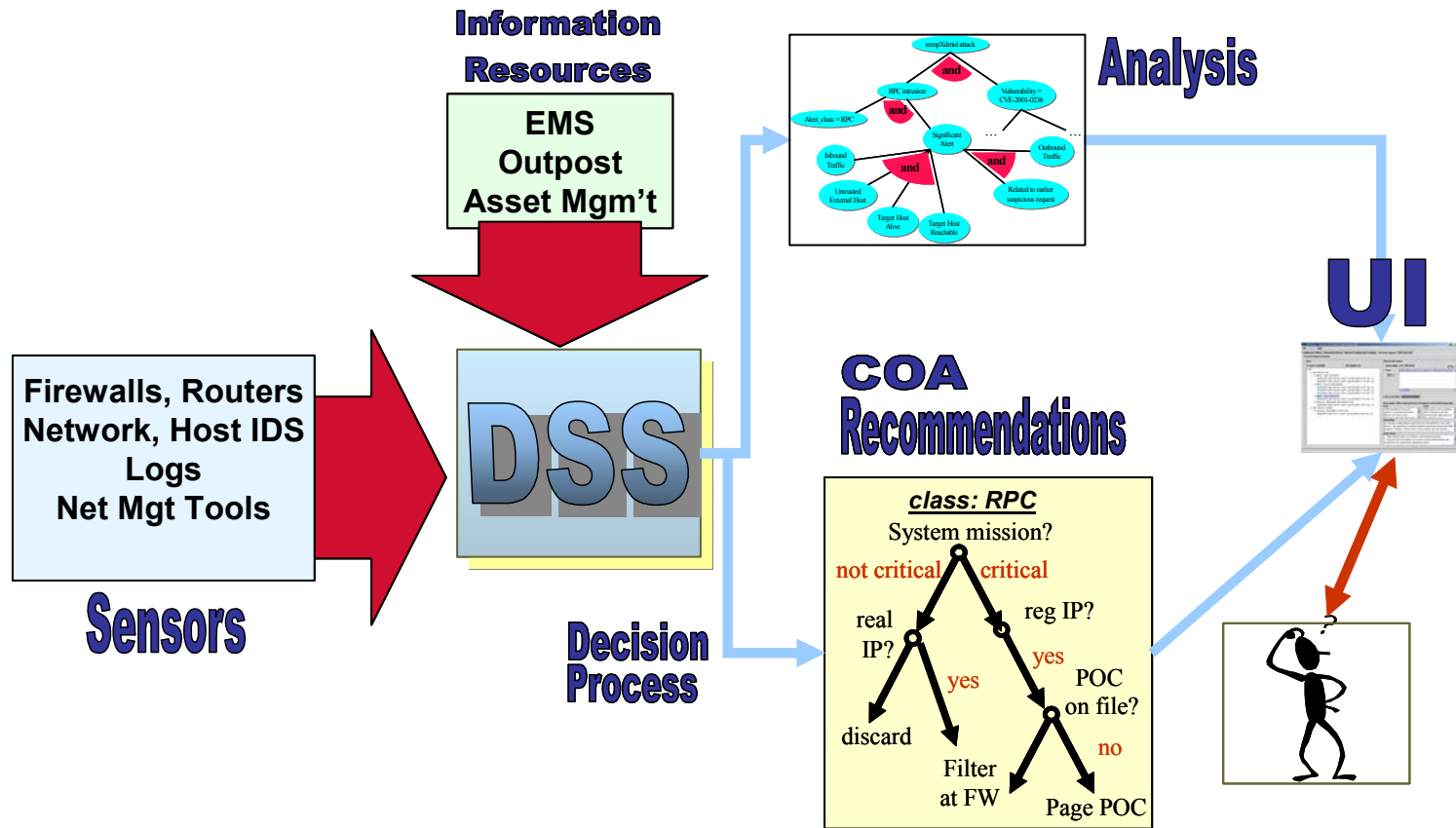
Problem

- **Computer network defense (CND) needs automated assistance:**
 - **Overwhelming quantity of data**
 - **Numerous complex and disjoint tools**
- **Decision formulation time and total action response time are too long.**



Need new decision support approaches to improve the total CND effort

Background



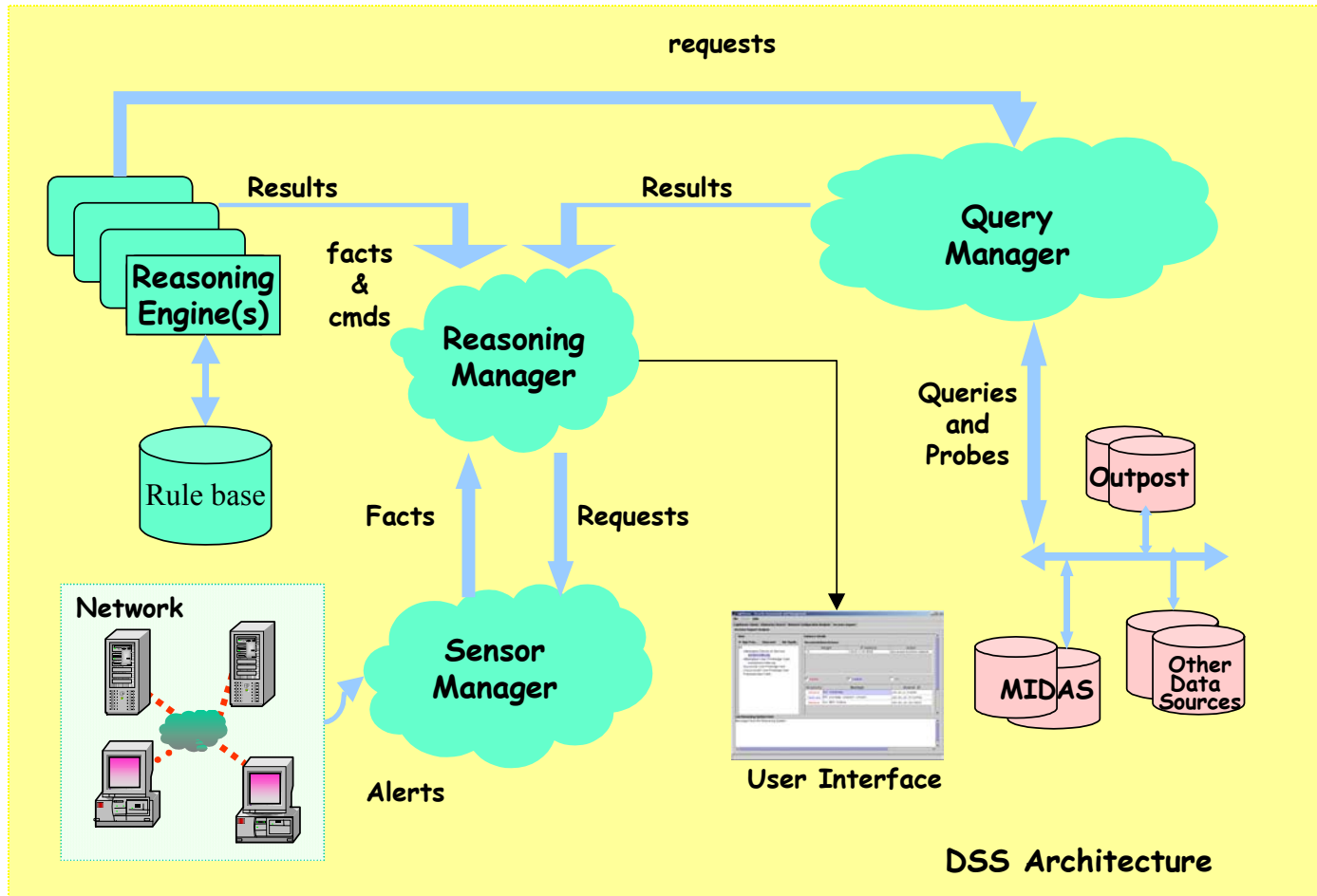
Objective

- **Research, design, and develop a decision support system to provide course of action recommendations for CND in the face of a dynamically changing computer and network environment**

Activities

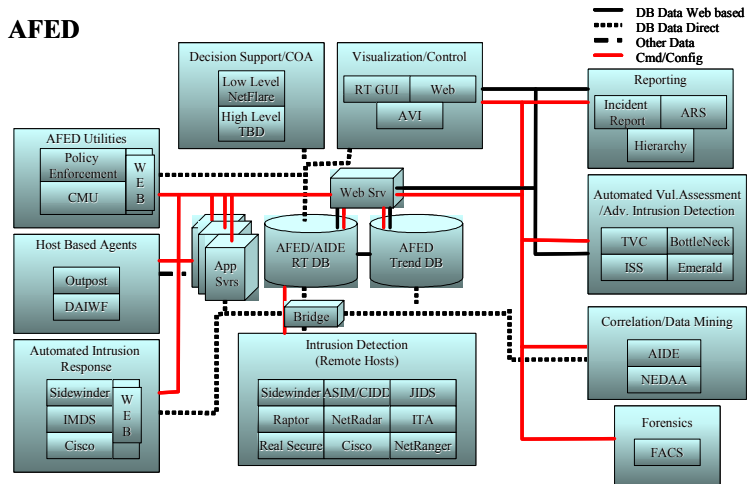
- **Extend FY02 research by investigating selected, specific environments**
 - **Qualify and select one or more environments**
 - **Investigate the CND environment in those selections**
 - **Develop an enhanced prototype; observe results from test locations to gain additional research insights**

Highlight

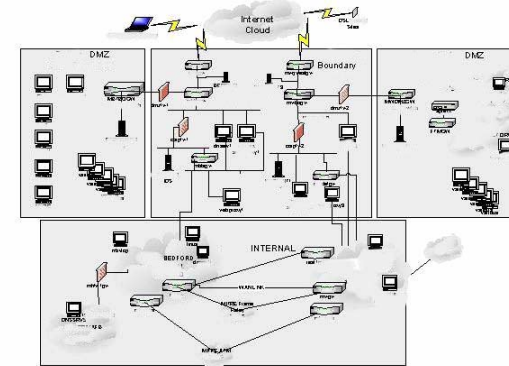


Highlight

AFED



MITRE



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 of automating course of action determination; impact follow-on community research and product development
- **Relevant knowledge capture and dissemination**
 - Dialogue/share with existing network defense research efforts (e.g., AFRL, AFIWC, etc.)

Future Plans

