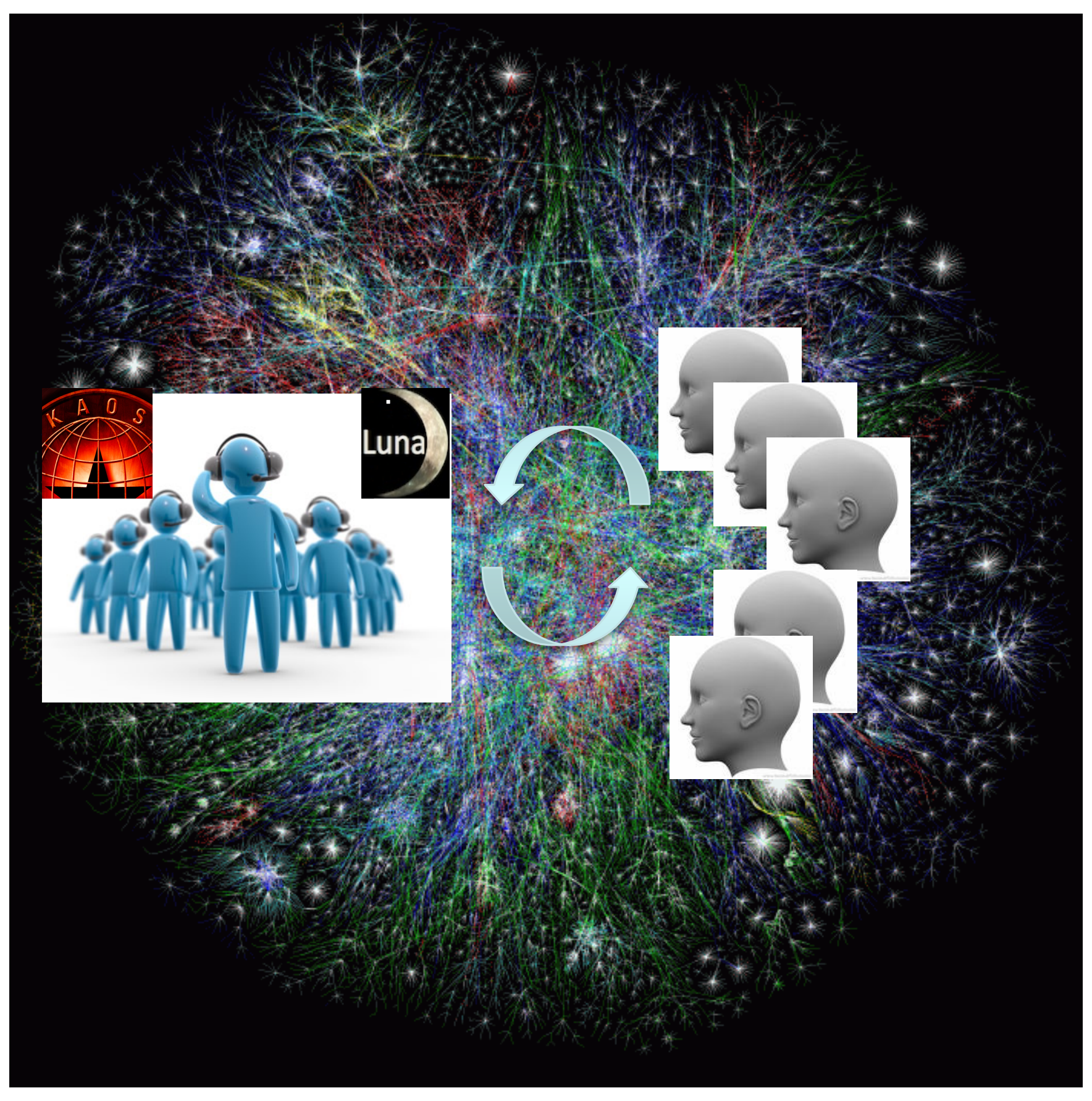
J. M. Bradshaw, M. Carvalho, L. Bunch,
T. Eskridge, P. Feltovich, R. Hoffman,
M. Johnson, J. Lott and D. Kidwell

Human-Agent Teamwork for Cyber Sensemaking in Network Operations

Objective: A cyber sensemaking framework for network operations that embodies the principles of human-agent teamwork.

Human-Automation Teamwork with Agents, Policies, and Visualization

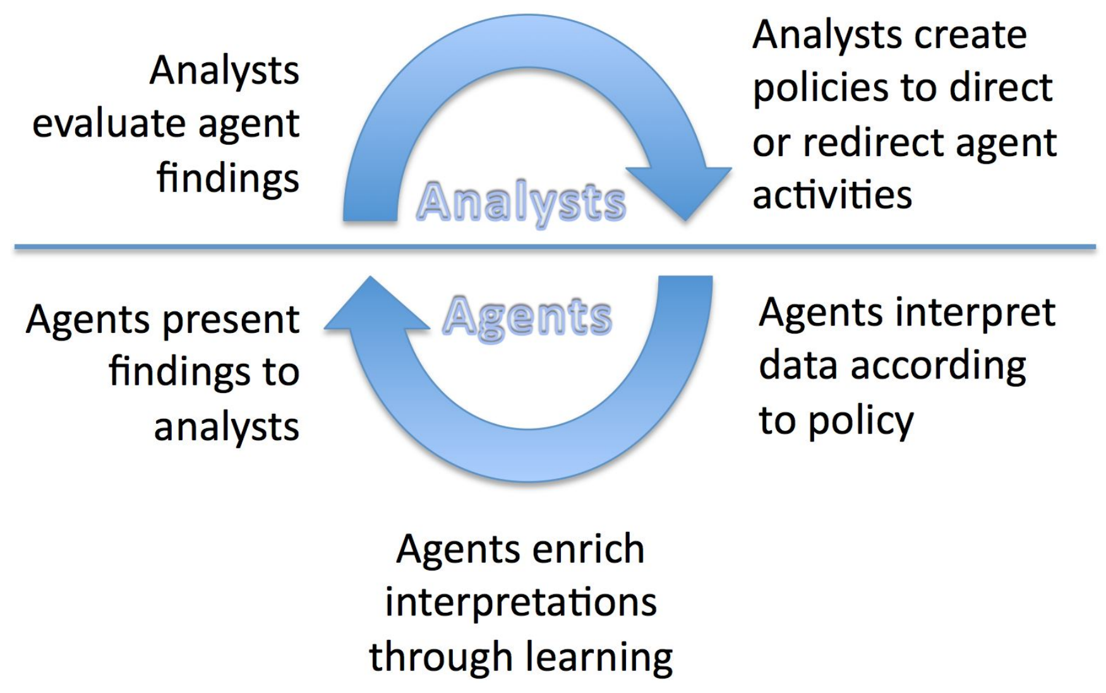


KAoS Policy Services and the VIA Cross-Layer Substrate: Ability to coordinate human-agent teamwork through dynamic, declarative, context-sensitive OWL policies.

Luna Agent Framework: Through integration with KAoS, the *Luna Agent Framework* supports teamwork properties. Optional state-based mobility allows dynamic optimization of computing resources.

OZ-Style Visualization: Leverages knowledge about human perception, cognition, and collaboration for proven human-performance enhancements.

Coactive Emergence

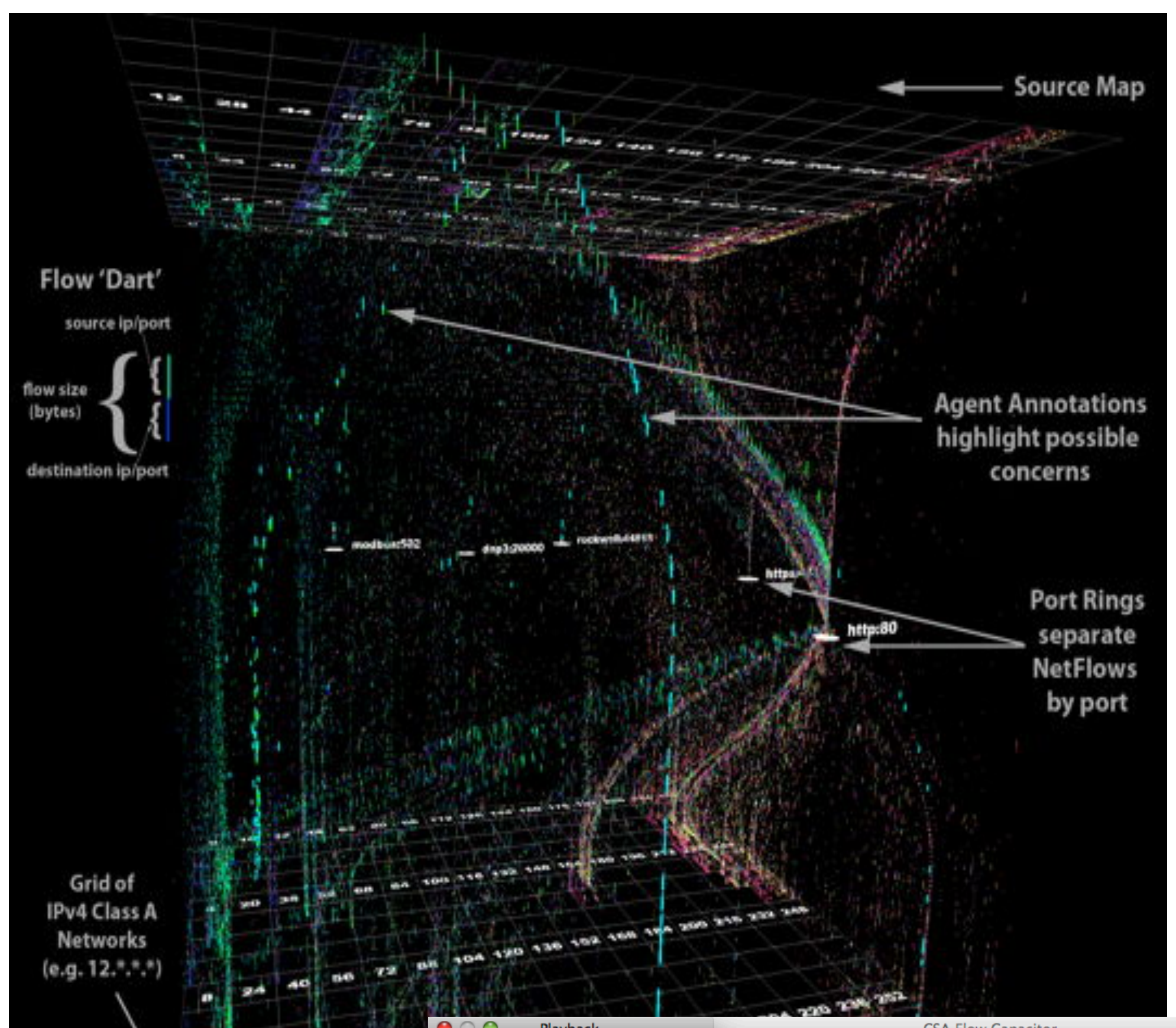

Analysts evaluate agent findings
Analysts
Analysts create policies to direct or redirect agent activities
Agents present findings to analysts
Agents
Agents interpret data according to policy
Agents enrich interpretations through learning

- Coactive emergence describes the process whereby useful interpretations of data are created through the interplay of interdependent sensemaking activities by analysts and agents
- First-order emergence of interpretive patterns arises from problem-space constraints currently expressed within policies and tool configurations
- Second-order emergence arises from dynamic changes to the problem-space constraints by agents and analysts

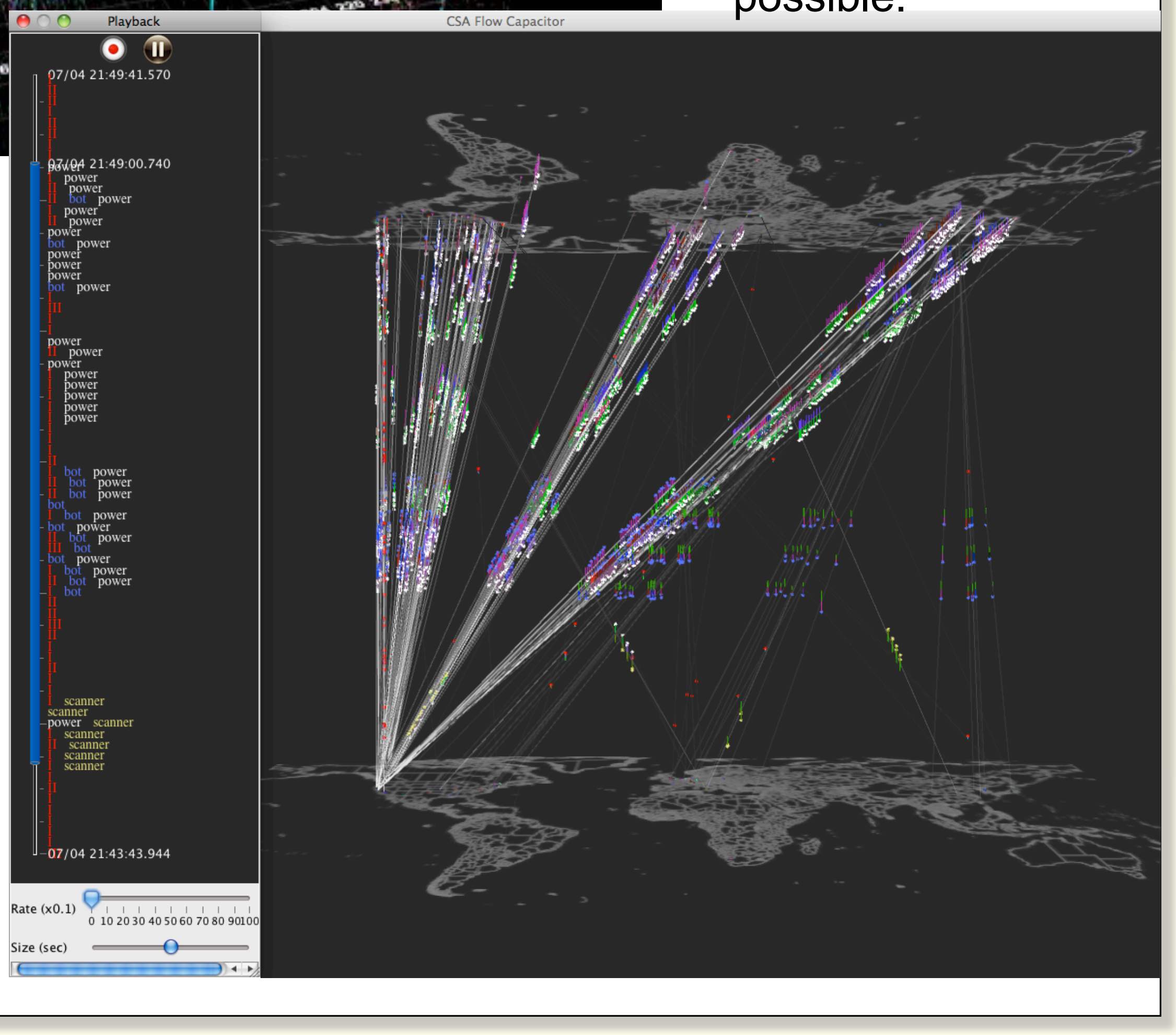
Organic Resilience

- Resilience is achieved through (1) on demand creation of self-organizing capabilities for problem mitigation and recovery; (2) engaging the adaptive capabilities of humans.
- Organic resilience builds on a biological analogue (inter-cell signaling and differentiation) to enable agent self-organization.
- Collective obligation policies represent duties of a group of agents without specifying in advance who must do what.
- Properties enabling organic resilience include:
  - self-organization and adaptation at all levels, and including both analysts and agents.
  - plasticity and redundancy of agents and operations.
  - feedback cycles for agents and analysts that allow the ongoing evaluation and correction of operations.

The Flow Capacitor

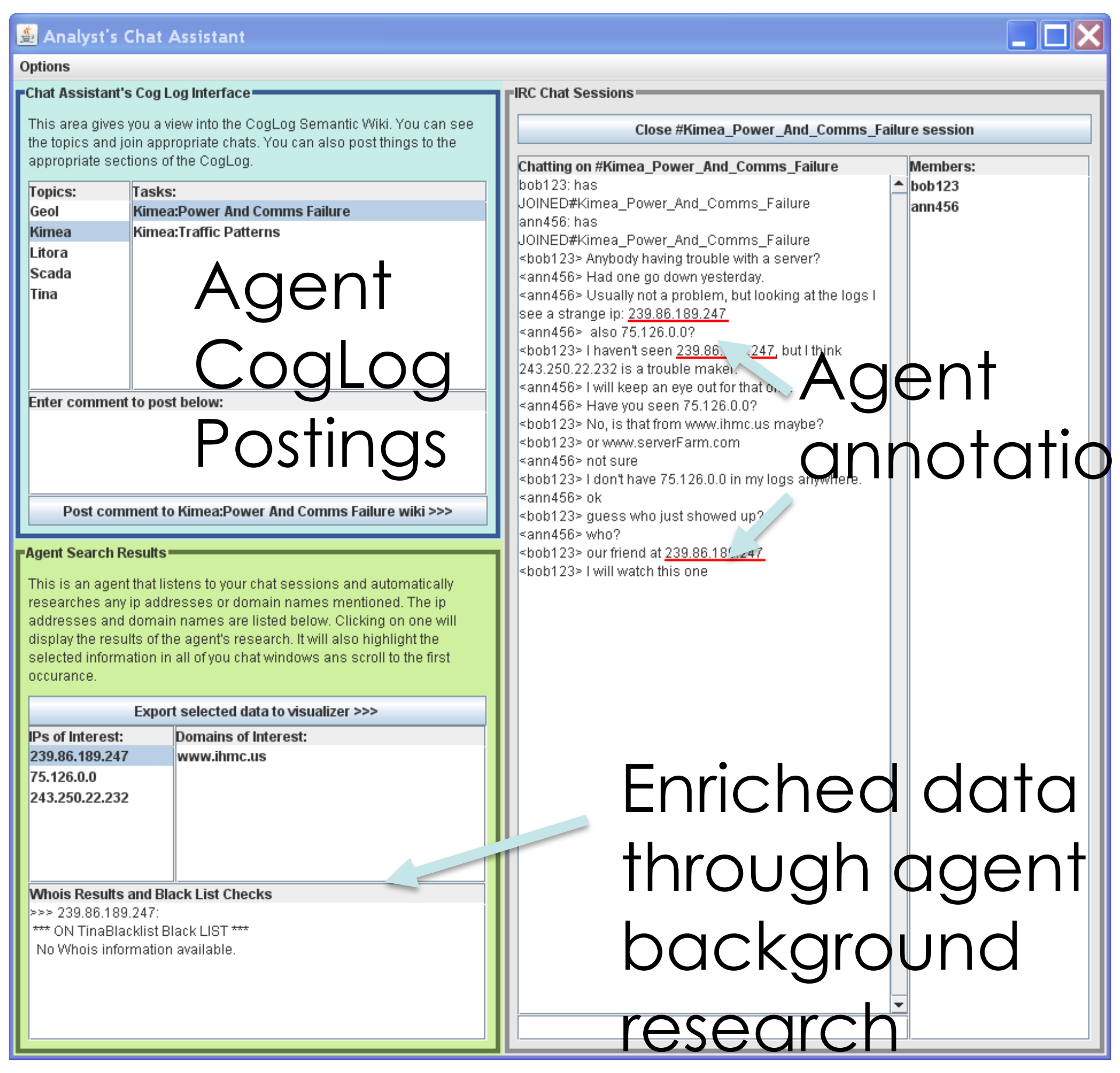

Source Map
Flow 'Dart'
source ip/port
flow size (bytes)
destination ip/port
Agent Annotations highlight possible concerns
Port Rings separate NetFlows by port
http:80
Grid of IPv4 Class A Networks (e.g. 12.*.*.*)
12
28
44
60

- NetFlow “darts” travel downward through IPv4 space.
- Agents tag and visually highlight flows of interest
- “Rings” constrain downward path of flows with specified properties.
- Multiple stacked planes allow exploration of complex questions
- An infinite variety of types of planes is possible.



- Attack stories can be read chronologically from bottom (oldest events) to top (newer events).
- Here we see:
  - Scanning
  - Response
  - Bot C2
  - DDOS attacks

The CogLog and the Live Advisory



Chat Assistant's Cog Log Interface

This area gives you a view into the CogLog Semantic Wiki. You can see the topics and join appropriate chats. You can also post things to the appropriate sections of the CogLog.

Topics:	Tasks:
Geol	Kimea:Power And Comms Failure
Kimea	Kimea:Traffic Patterns
Litora	
Scada	
Tina	

Enter comment to post below:

Post comment to Kimea:Power And Comms Failure wiki >>>

Agent Search Results

This is an agent that listens to your chat sessions and automatically researches any ip addresses or domain names mentioned. The ip addresses and domain names are listed below. Clicking on one will display the results of the agent's research. It will also highlight the selected information in all of you chat windows ans scroll to the first occurance.

Export selected data to visualizer >>>

IPs of Interest:	Domains of Interest:
239.86.189.247	www.ihmc.us
75.126.0.0	
243.250.22.232	

Whois Results and Black List Checks

```
>>> 239.86.189.247:
*** ON TinaBlacklist Black LIST ***
 No Whois information available.
```

IRC Chat Sessions

Close #Kimea_Power_And_Comms_Failure session

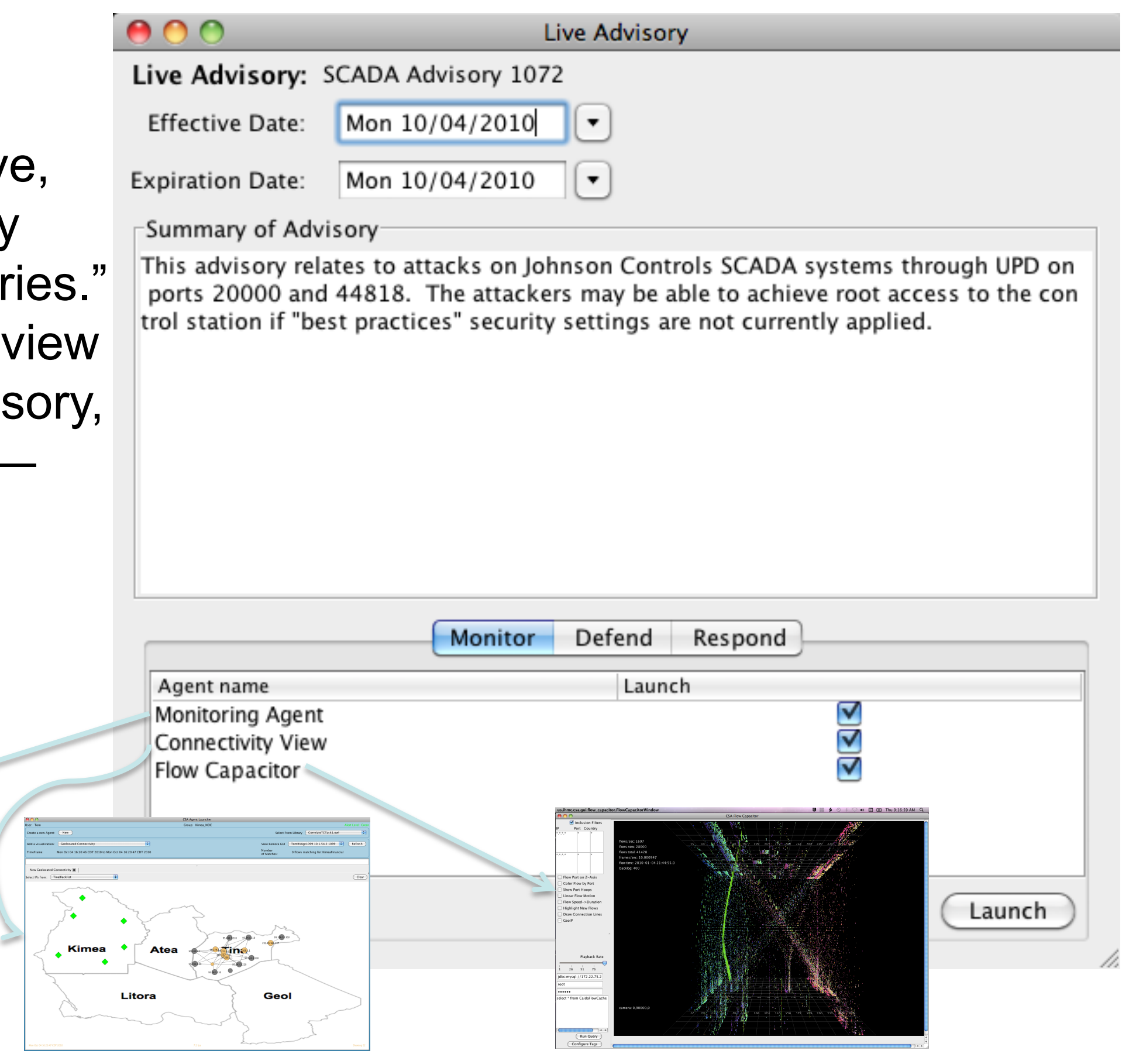
Chatting on #Kimea_Power_And_Comms_Failure

```
bob123: has
JOINED#Kimea_Power_And_Comms_Failure
ann456: has
JOINED#Kimea_Power_And_Comms_Failure
<bob123> Anybody having trouble with a server?
<ann456> Had one go down yesterday.
<ann456> Usually not a problem, but looking at the logs I
see a strange ip: 239.86.189.247
<ann456>  also 75.126.0.0?
<bob123> I haven't seen 239.86.189.247, but I think
243.250.22.232 is a trouble maker.
<ann456> I will keep an eye out for that one.
<ann456> Have you seen 75.126.0.0?
<bob123> No, is that from www.ihmc.us maybe?
<bob123> or www.serverFarm.com
<ann456> not sure
<bob123> I don't have 75.126.0.0 in my logs anywhere.
<ann456> ok
<bob123> guess who just showed up?
<ann456> who?
<bob123> our friend at 239.86.189.247
<bob123> I will watch this one
```

Members:
bob123
ann456

- The CogLog is a semantic Wiki-based tool prototype to aggregate agent and analyst findings.
- Agents can automatically “grab” pertinent data (e.g., IP addresses), enrich it through background research, and post it to the CogLog

- Agents can provide active, actionable information by generating “Live Advisories.”
- Remote colleagues can view the rationale for the advisory, replay the relevant data—and, potentially, launch protective actions.



Live Advisory: SCADA Advisory 1072

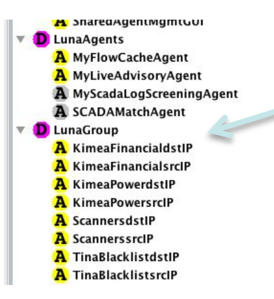
Effective Date: Mon 10/04/2010

Expiration Date: Mon 10/04/2010

Summary of Advisory

This advisory relates to attacks on Johnson Controls SCADA systems through UPD on ports 20000 and 44818. The attackers may be able to achieve root access to the con trol station if "best practices" security settings are not currently applied.

Agent name	Launch
Monitoring Agent	☑
Connectivity View	☑
Flow Capacitor	☑



FLORIDA INSTITUTE OF TECHNOLOGY 1958

ihmc FLORIDA INSTITUTE FOR HUMAN & MACHINE COGNITION