INTELLIGENT SYSTEMS FOR FORECASTING AND DETECTING INSIDER THREAT

SoarTech
Modeling human reasoning.
Enhancing human performance.

OUR EXPERTISE AND PROVEN CAPABILITIES

	DECISION SUPPORT	BEHAVIOR MODELING	CYBER SIMULATION
	Multi-Future Probabilistic Forecasting	**Cognitive Red-Team Agents**	**Cyber Sandbox for Insider Threat Training**
AUTONOMY	Multiple agents search alternative paths through complex behavior models in parallel	Enables scalable, repeatable wargaming and testing of security and network infrastructure	Agent-based cyber ecology provides autonomous adversarial and legitimate users
ADAPTATION	Any-time forecast adjusts in real time to incoming data; runs 10^4x faster than real time	Learned behavior model exposes novel attack vectors	Dynamic Tailoring adapts adversaries and environment to maximize learning
HUMAN/SYSTEM INTERFACE	Yields probability distribution over alternative futures to support ACH and mitigate cognitive anchoring	Agents acting as virtual threats allow human experts to test variations in high level goals	Constructive sims are readily available for continuous training and evaluation

Relevant Research to be Leveraged:

Probabilistic Forecasting

Mechanism: Monte Carlo search of structured environment (cf. MCTS)

15 min predictions t = 140 sec
15 min tails t = 140 + 900 sec

Geospatial Results (DARPA RAID, DeepGreen; JIEDDO; RDECOM PROPS)

Demonstrated on HTN behavior models (e.g., cyber-attack models)

Dominates other technologies

Dominates human staff

- 10^4x faster than real time on conventional hardware; parallelizable for further gains
- Generates distribution over possible futures
- Any-time algorithm supports real-time data updates from cyber sensors

Dynamic Understanding of DNS Data

Problem: detect IPTs from DNS Type A records
Data pipeline exploits graph DB

21,250 IPs (internal)   1,638,439 Edges   782,575 URLs (external)

Insert All Type A Records → MySQL (RDB) → Transform to Graph Representation → OrientDB (Document GraphDB) → Queries Restricted by Results of Analysis Agents → Output

Suspect Data Files (Month 2)
Remove All DNS Servers
Remove All URLs
Store Localized Results on the Graph

Suspect Data Files (Month 2)
Benign Data Files (Month 1)
Various Analysis Agents (Beaconing Detector, Precursor Detector, Subgraph Enumerator etc.)

Repeated Connection
Single Connection

Resulting graph: IP degree (top, blue) and URL degree (bottom, yellow)

Innovative scoring function detects beaconing robustly

Bipartite graph
→ local processing
→ scalable architecture

CYber SecuriTy INstruction Environment

FileSystem Diagnostics
Existing C4ISR Terminal
SoarTech Test App

Alphaville Virtualized Instance Michigan Cyber Range (Merit)

Interface Middleware

Dynamic Tailoring GameState
Instance Mgr
Account Mgr
Logging Mgr
Logging DB
Account DB

SOAR ATTACKER
SOAR DEFENDER
SOAR USER
SCR2AM

Air-Force Virtualized Network Implementation (Phase II)

Instructor Interface

KAB LABORATORIES

Simulated Cognitive Cyber Red-team Attacker Model

Soar SC2RAM Agent
Soar SC2RAM Agent
Soar SC2RAM Agent

Symbolic Long-Term Memories

Procedural
Cue-response patterns
- Coded from cognitive analyses
- Learned by chunking

Semantic
Updatable attacker tactics
- Exploit DB
- Web-page templates
- Structure of target NW

Episodic
Virtual sensing from experience
- Detection of novel situations
- Action modeling

Perception → Symbolic Working Memory → Action

Red Team Leader
3. Analyst
2. Engineer
1. Trainee

High-Level NW Events
Network Under Test
Attack Commands
Attacker Toolbox
NW Security Automation

Low-Level NW Interactions
ihmc
Sol/Luna Framework: Parsing, Execution, Visualization

Bidirectional Behavior Models

rTÆMS behavioral representation
- captures goal structure, preconditions, resources, task interactions
- maps tasks to data sources

Soar Cognitive Processing
- Behavior model is *inside* a single *Soar* agent (semantic memory)
- Pattern matching, goal-directed reasoning, learning, hypothesis testing and confirmation

Polyagent Monte-Carlo Forecasting
- Multiple *tropistic agents* explore *inside* the behavior model
- Scalable, fast, probabilistic, any-time

Research Area of Interest:

Current approaches to detecting insider threat are *reactive* and *limited*:
- *reactive* because they focus on what threats have done in the past, rather than anticipating what they may do in the future.
- *Limited* because they focus on network cyber vulnerabilities without reasoning about threats' goals and objectives.
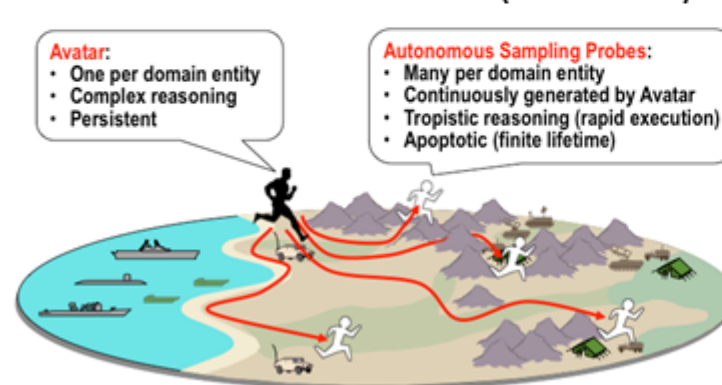
SoarTech's innovative capabilities can provide:
- Models and assessments of behavior for automatic detection of indicative and anomalous behaviors for the *Active Indicators track*.
- Simulation Based Human Systems Integration to model system and enterprise performance for the *Inference Enterprise Models (IEM) track*
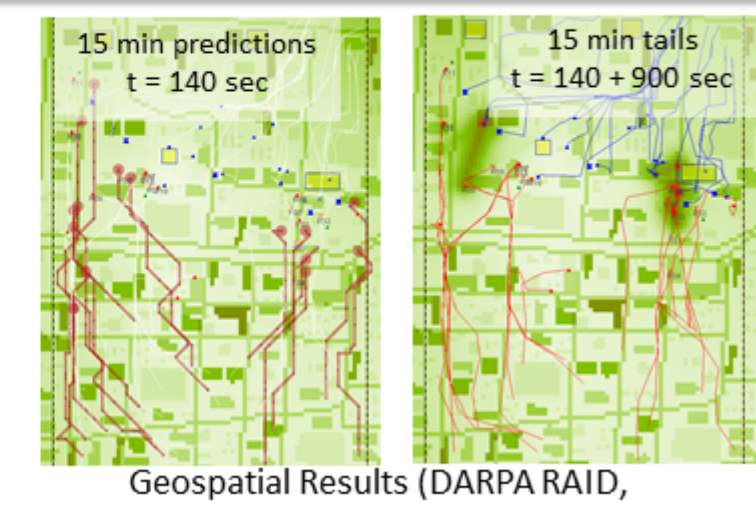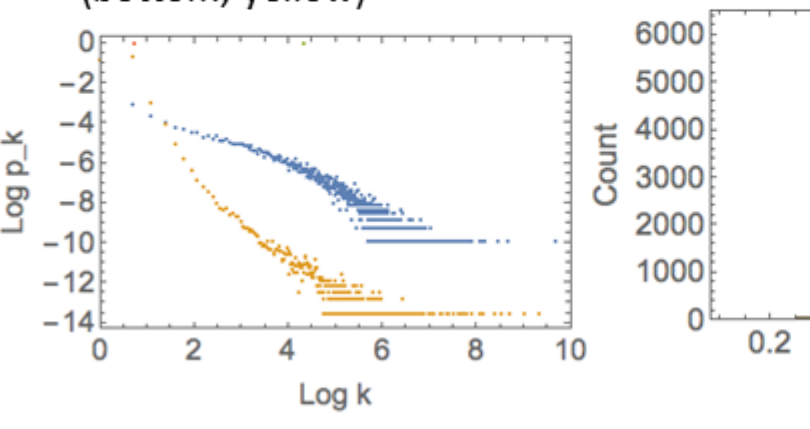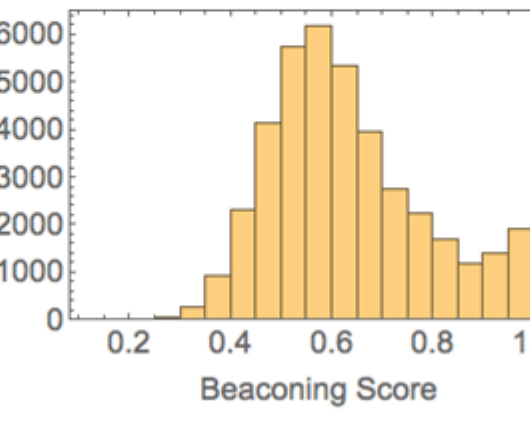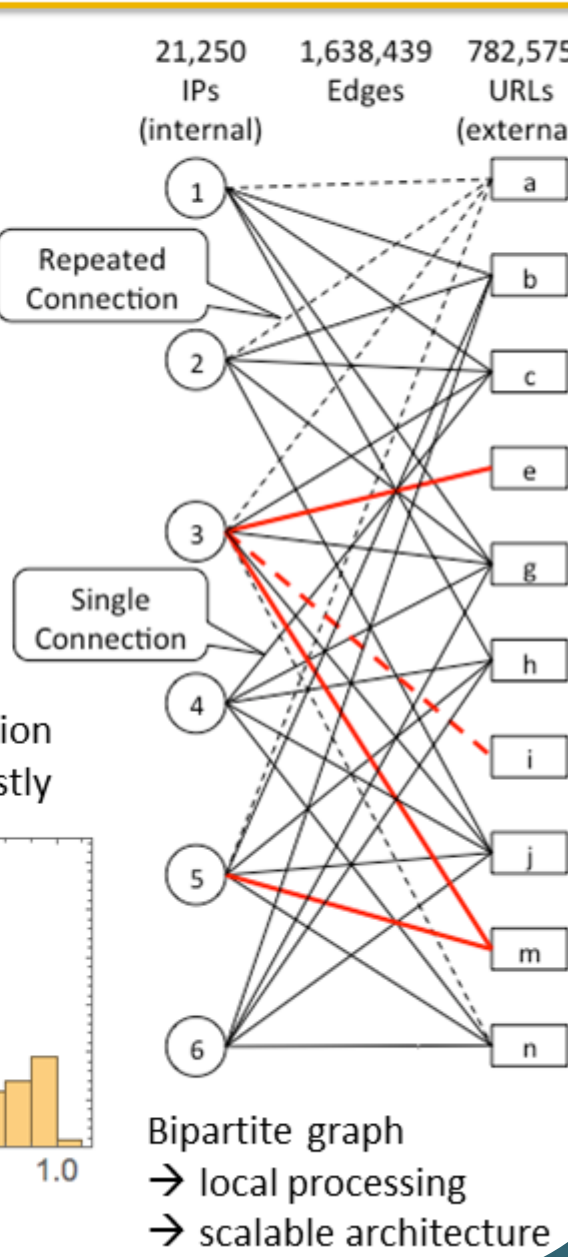
ENHANCING INSIDER THREAT DEFENSE THROUGH BEHAVIORAL MODELS AND SIMULATION BASED FORECASTING

SoarTech POCs

Dylan Schmorrow, Ph.D.
Chief Scientist
703.424.3138
dylan.schmorrow@soartech.com

Denise Nicholson, Ph.D., CMSP
Director of X
407.616.7651
denise.nicholson@soartech.com

Jose Nazario, Ph.D.
Senior Scientist
734.887.7644
jose.nazario@soartech.com