Agent Logic DoD Capabilities Briefing

Complex Event Processing
Across the Command, Across the Community

AGENT LOGIC
TO DETECT AND RESPOND

All-Source/Multi-Source Intelligence Event Detection, Correlation, Knowledge Management, Decision Support, Real-Time Alerting & Response

Randy Wood
VP Federal Sales
703 498 8915
randy.wood@agentlogic.com

AGENT LOGIC
TO DETECT AND RESPOND

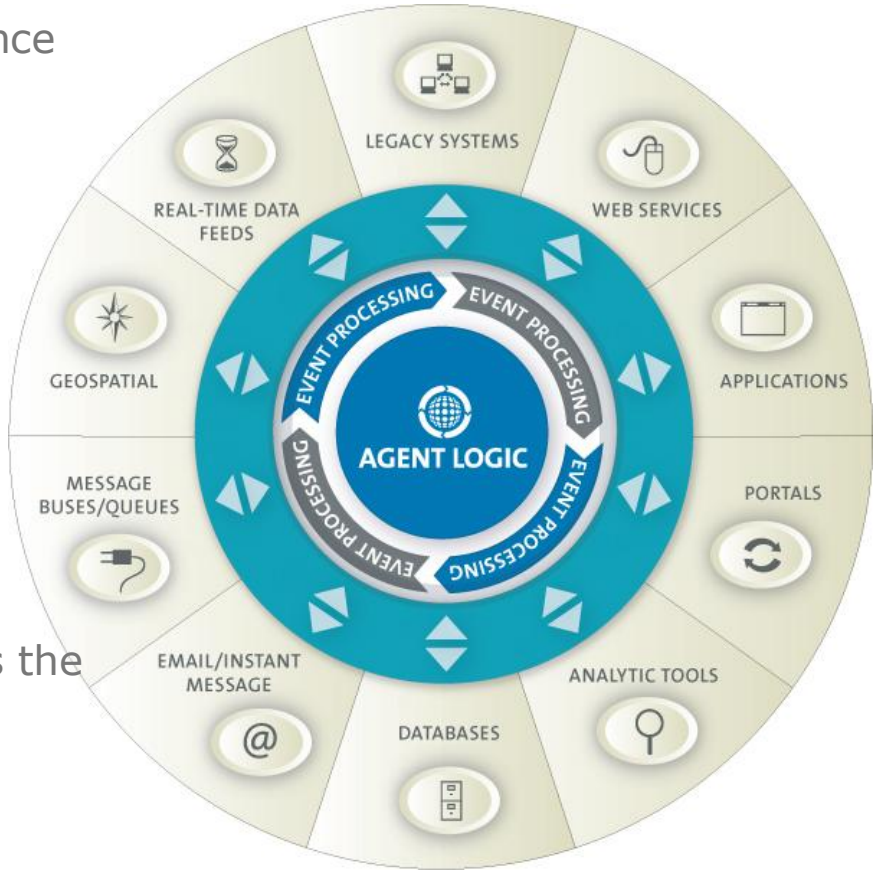
Overview

Company Background

- Real-time business intelligence software leader
- Purpose Built for National Security & Intelligence
- Privately-held & profitable (100% CAGR)
- Fourth-generation software architecture
- In-Q-Tel Partner – 2002
- Cleared TS/SCI Staff

Product Capabilities

- (ALL) Multi-source intelligence for the analyst
- Detection & response to events of interest
- User Defined Experience
- Operationally proven & in production
- Enable Real-time situational awareness across the enterprise



AGENT LOGIC
TO DETECT AND RESPOND

The DoD/IC Standard for Multi-Int Correlation & Alerting

Vision

Leaders, Commanders and The War Fighter Should Have **CONCURRENT** Access to **ALL** Sources of Information in Order to Visualize the Battlespace and Common Operational Picture

Mission

Provide Persistent, Timely, Usable and Relevant Analysis And Alerting/Response to Government/Military Leaders, Commanders & Analysts

Customer Experience

Connectedness – People, Information, Knowledge, Action

AGENT LOGIC
TO DETECT AND RESPOND

Agent Logic: Highlighted Customers

- NGA
  - Real-Time Detection, Correlation and GIS Alerting for Time Dominant Operations
- NSA
  - Real-Time alerting for time-critical decisions
- NCTC
  - Monitoring of data across multiple levels of classification, with routing and alerting to the high side (L2H)
- CIA
  - Multiple programs including message traffic monitoring, open source data collection, and intelligent alerting applications
- USCG
  - Maritime Domain Awareness (MDA) operational support
- INSCOM
  - Information Dominance Center
  - USFK
  - Geospatial alerting to analysts and watch officers based on tactical message traffic (TACELINT, IPIR, TACREP, etc.) JWICS accessible for USFK PACOM users.
- Fortune 100 Financial Institutions
  - Automated alerting and evidence collection based on “Phishing” attacks
  - Complex credit card fraud detection

AGENT LOGIC
TO DETECT AND RESPOND

The Problem We Solve…

The DoD/IC "sees" and processes only 10% of the SIGINT and 12% of IMINT on any given day

- 90% of what is collected is wasted…
- Accuracy & Completeness in establishing common operational picture are impeded by sheer volume of data from I&W, C4ISR & other data sources (All Source)
- Dependencies and relationships between EVENTS (operationally relevant changes in one or more data sources) are difficult to determine
- Extremely difficult to identify—in real-time—which events are related and signify emerging opportunities and threats?
- Missed opportunity or major crisis; the data was there, but no one connected the dots!

Persistent Surveillance Implies Persistent Analysis: Evolving From Situational Awareness to Situational Dominance

CEP for Humans: What People Want

- User-managed and defined operational intelligence, information enrichment, and real-time alerting
- Give analysts/decision makers the ability to exploit live event streams and data sources on the fly – without consuming valuable IT-staff resources
- Support 'communities of interest' by allowing teams to share rules – preserve knowledge
- Focus on creating intelligence from multi-source data while it's still 'fresh'
  - Temporal, geospatial, text, numeric analysis capabilities exposed to end user
  - Powerful correlations to discover meaningful (and subtle) relationships
- Self serve analytics and event enrichment (Context & Experience)
- Respond to "velocity of change" not just "velocity of events"
  - Dynamic rule creation against dynamic events…
- Multi-channel, actionable notifications and alerts
  - Enhance existing work environments instead of introducing new applications
  - **Objective**: automate or facilitate rapid response

AGENT LOGIC
TO DETECT AND RESPOND

Solution: Real-Time Business Intelligence

Traditional Business Intelligence	Real-Time Business Intelligence
Historical orientation	Present & future orientation
Lookback analysis for failure points	Pattern analysis of key trends & their impact
Queries and scheduled reports	Rules-based analytics and instant notifications
What happened? Who caused it?	What *is* happening now? What is likely to happen next? Who needs to know?
Transform data into information	Transform info overload into actionable intelligence

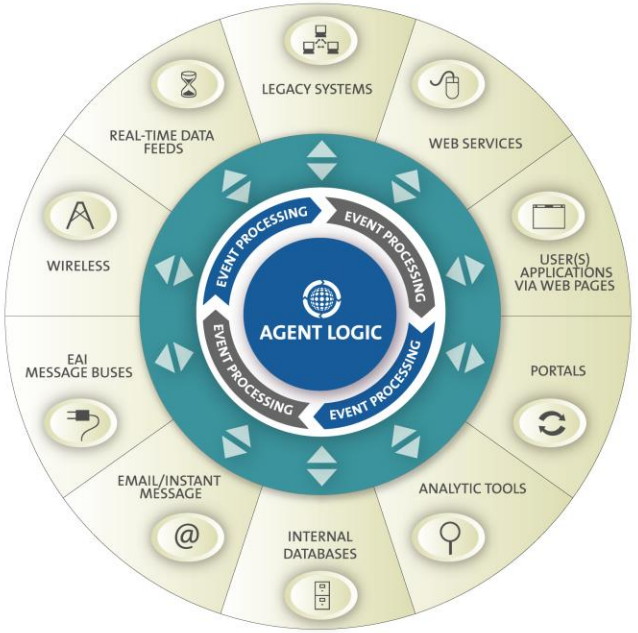
Agent Logic harnesses information overload for informed, proactive decision-making.

AGENT LOGIC
TO DETECT AND RESPOND

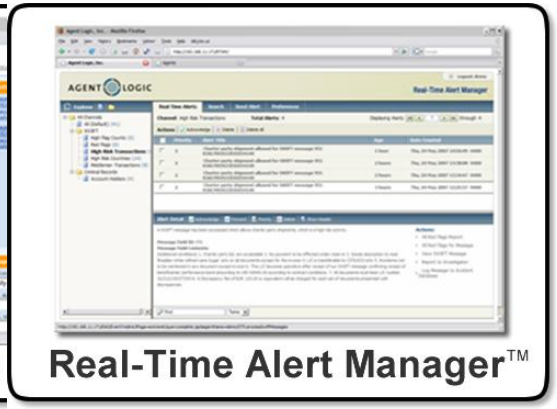
Agent Logic RulePoint™ - What we do

Transfer the power of CEP into the user's hands while minimizing the impact on IT resources

- "Listen to" (monitor) multiple sources (all source) simultaneously for data events…
  e.g., Transactions, Geospatial tracks, Non Events (Something should have happened), Database Updates, Tactical Message Traffic (TACREP, TACELINT, IPIR, etc.), Financial Transactions, Communications Tracking Activity, Closed Caption feeds, RSS Feeds, Web page changes and more.
- Present event properties directly to users for rule creation - single & complex correlations
  - –Time, Geography, Cross-source Correlation
- Based on user-defined rules, when events of interest are detected, initiate user-defined responses
- Information-rich Alerts
  - –Actionable, Filtered, and Contextual
  - –Directly to browser, IM, email, desktop apps Cell, pager, PDA, Voice system, other
- Business Process Initiation or Machine to Machine System Actions




GIS Applications


Real-Time Alert Manager™

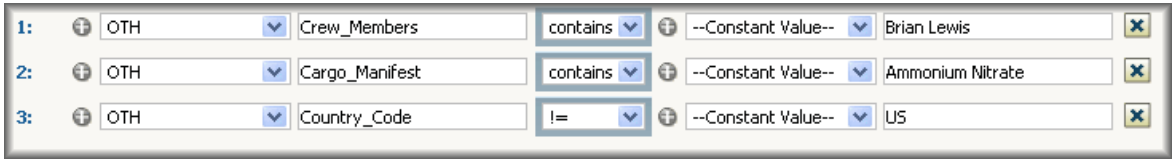
AGENT LOGIC
TO DETECT AND RESPOND

Agent Logic Rule Types - 3 Basic Modes:

- Templates

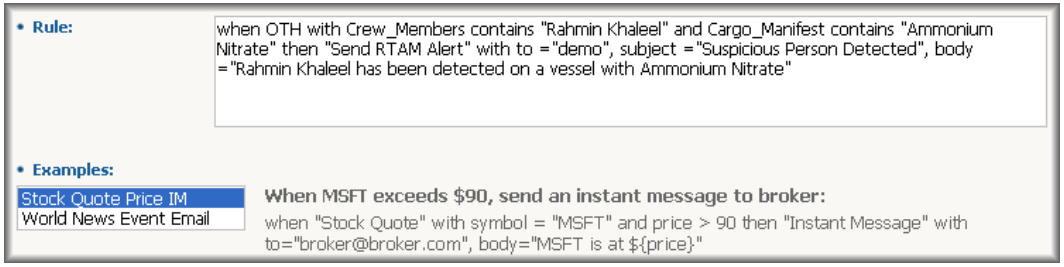
Parameterized Rules

- Wizard



More powerful customization and extensibility

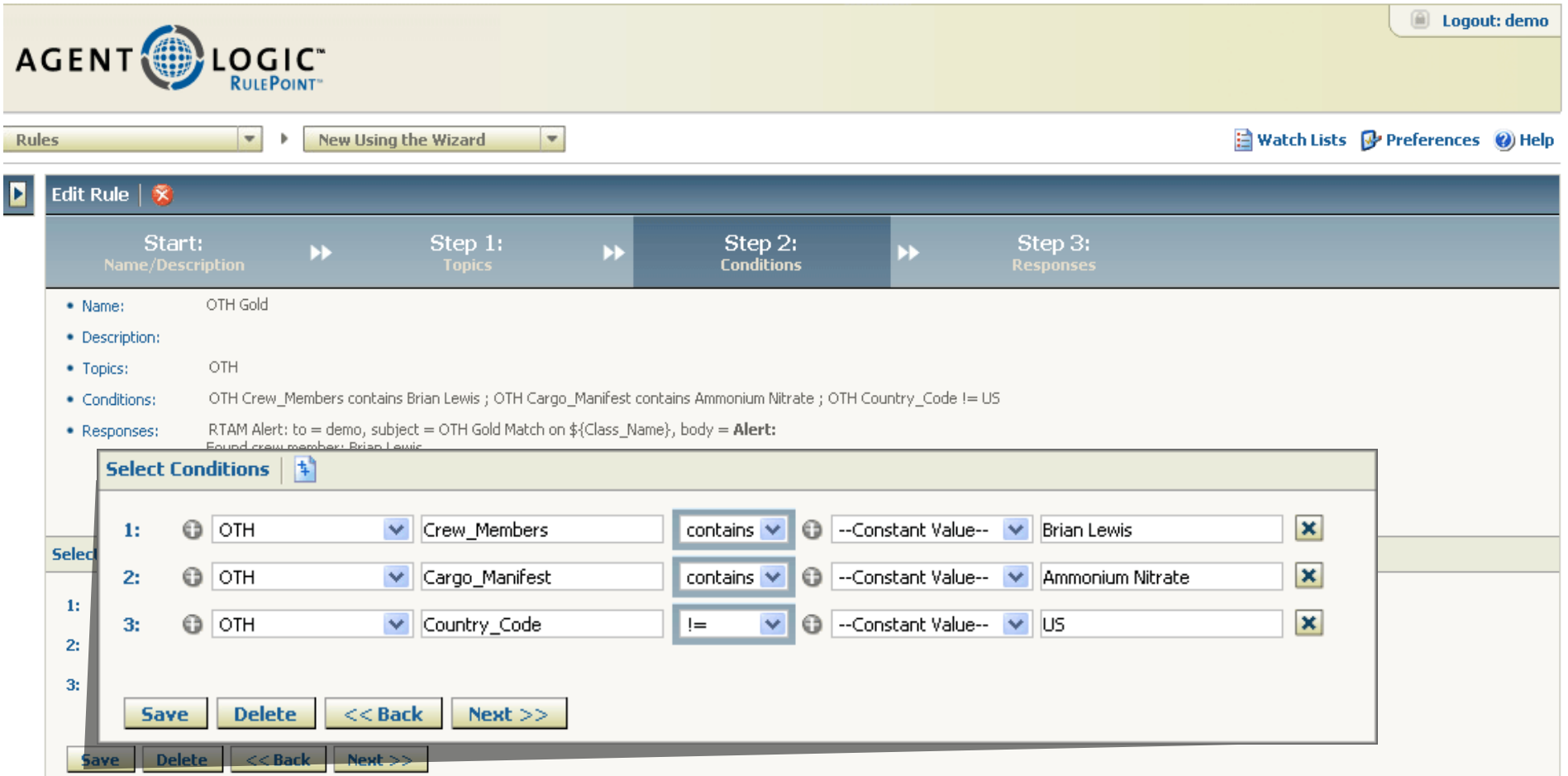
- Advanced Mode



Rapid rules deployment for Advanced Users

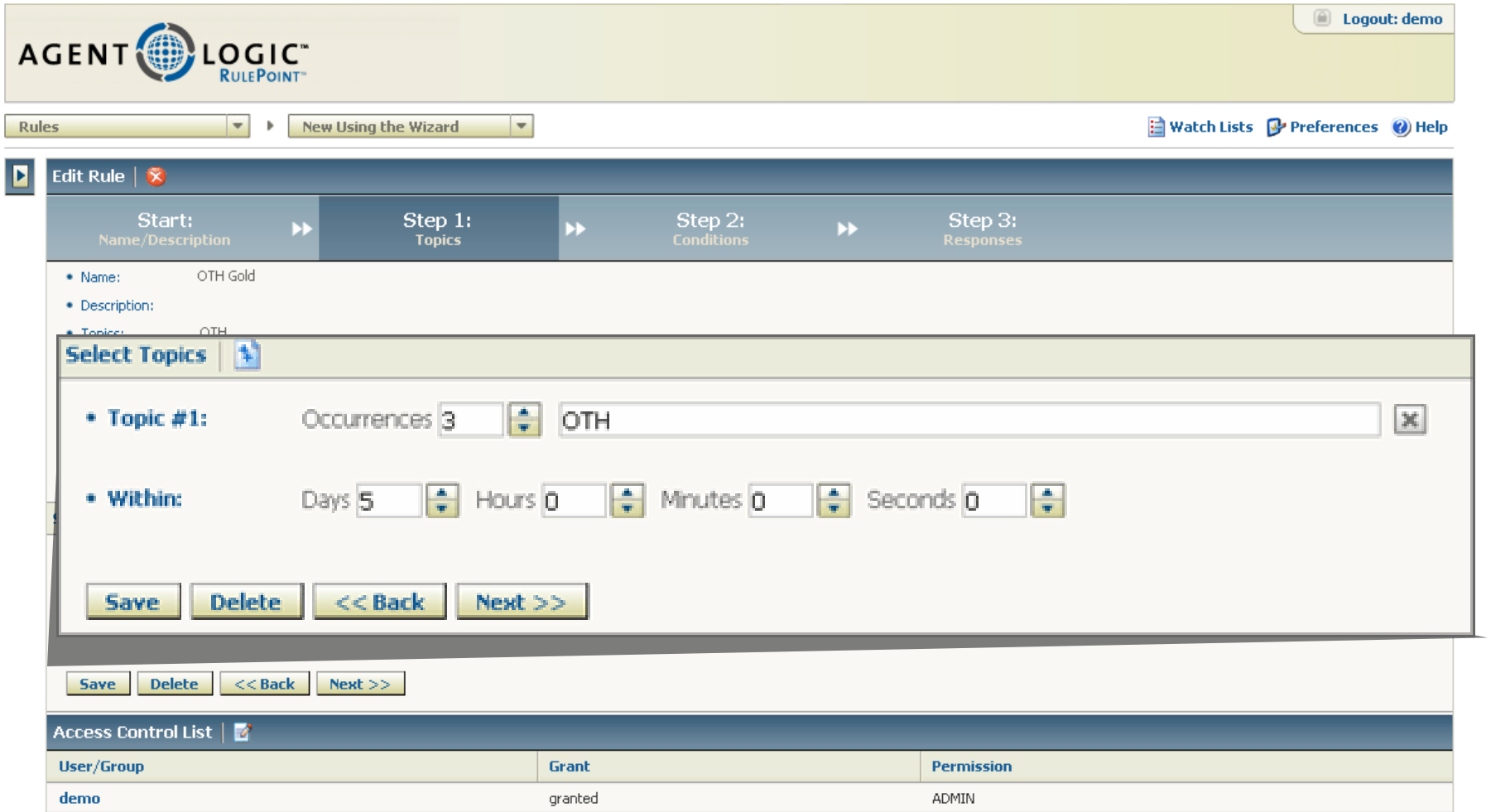
AGENT LOGIC
TO DETECT AND RESPOND

RulePoint ™ Subscriptions & Rule construction



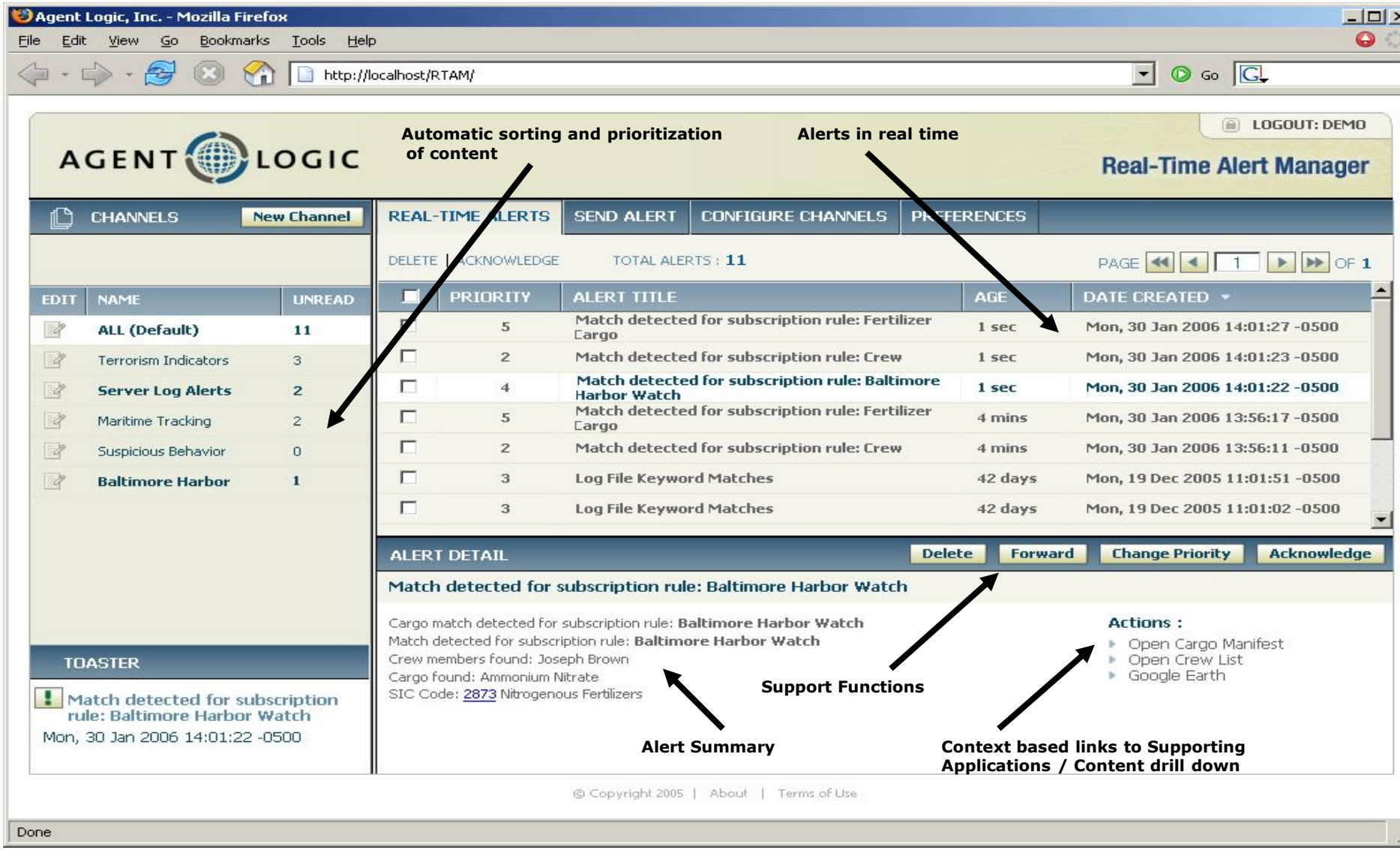
AGENT LOGIC
TO DETECT AND RESPOND

RulePoint ™ Subscriptions & Rule construction



AGENT LOGIC
TO DETECT AND RESPOND

Real Time Alerts – RTAM (AJAX based / no mobile code)

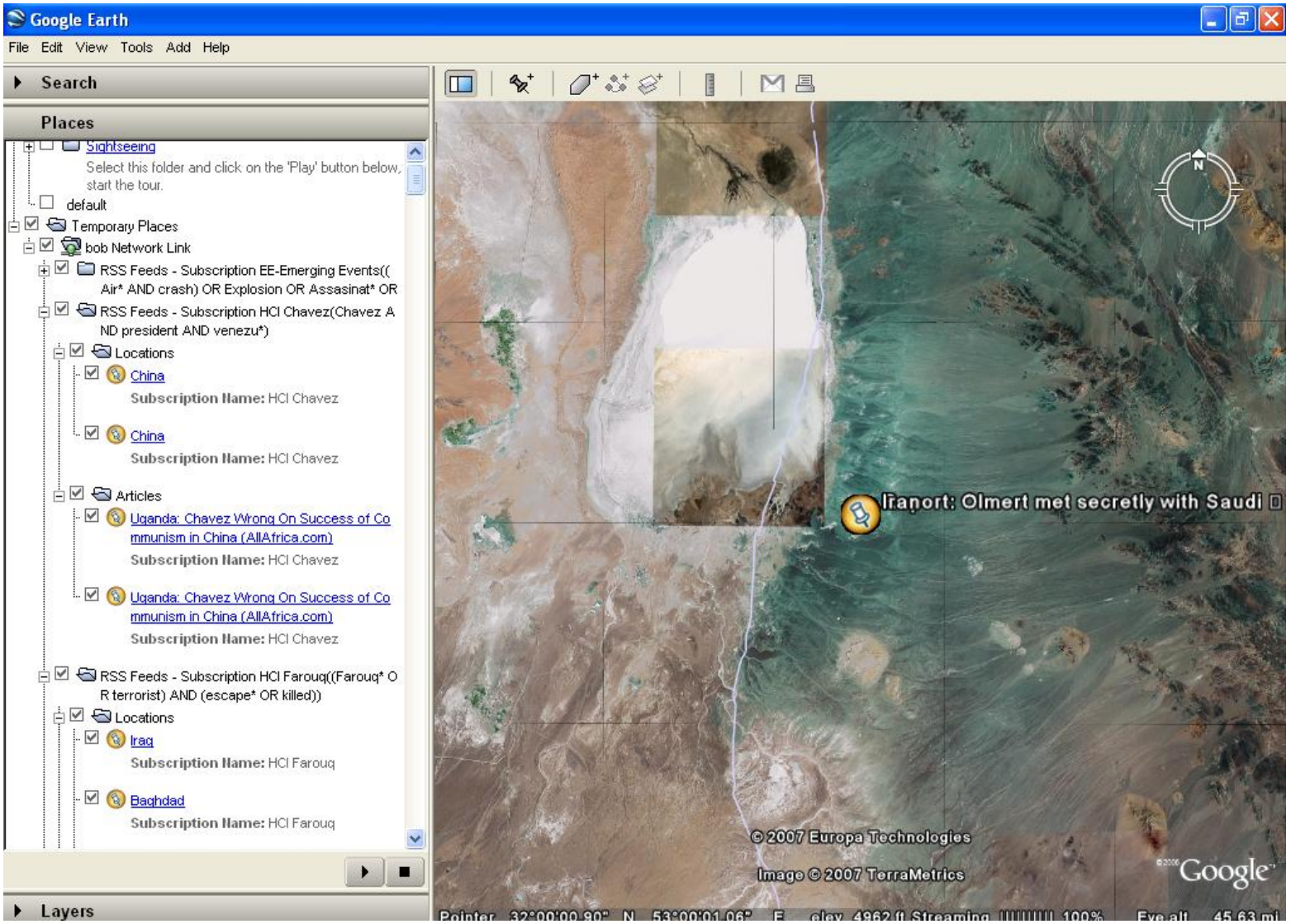


AGENT LOGIC
TO DETECT AND RESPOND

Real-Time Alerts: Watch Officer

AGENT LOGIC
TO DETECT AND RESPOND

Real-Time Alerts: Geospatial Integration

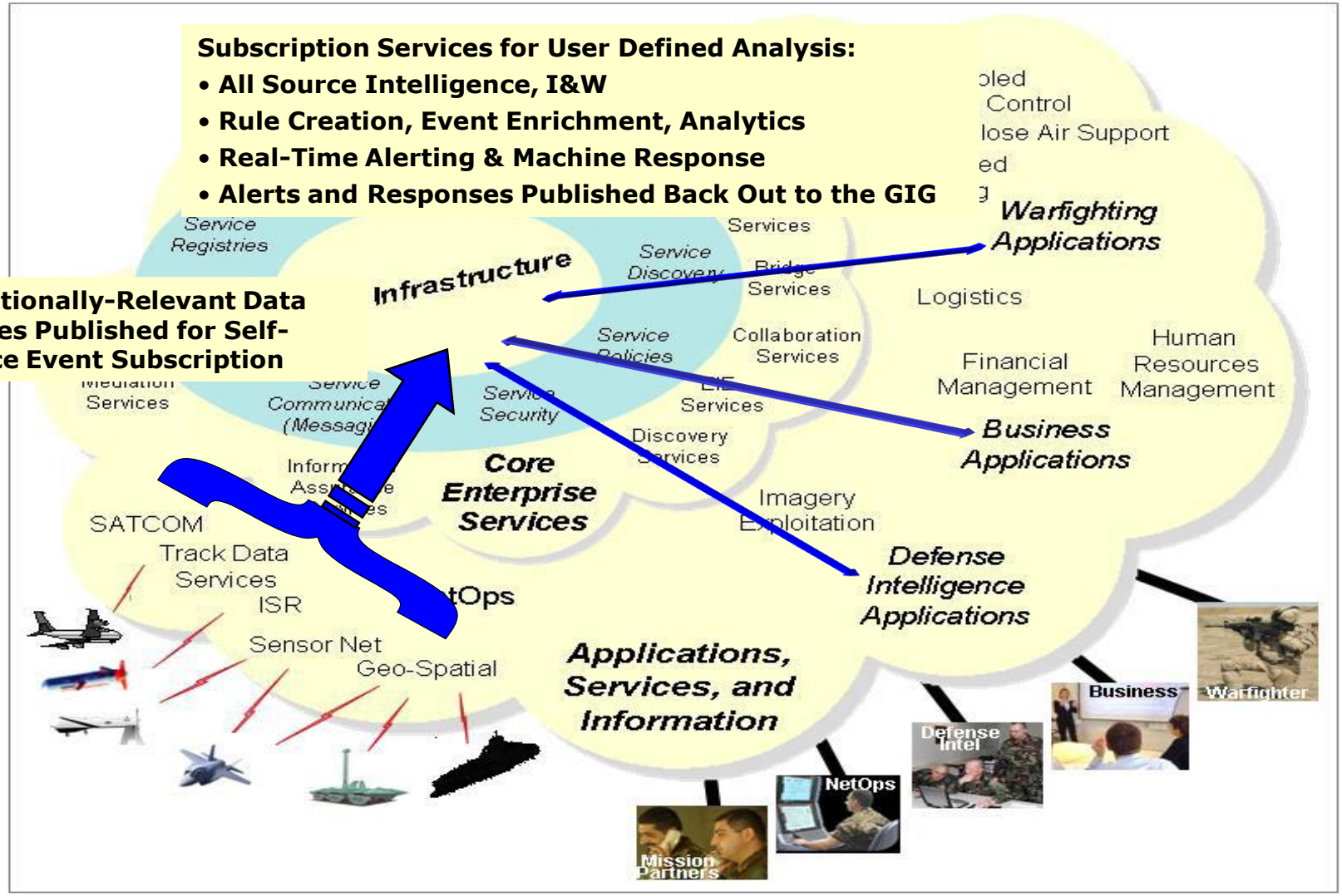


Event Processing & Alerting – SOA on the GIG

Subscription Services for User Defined Analysis:

- **All Source Intelligence, I&W**
- **Rule Creation, Event Enrichment, Analytics**
- **Real-Time Alerting & Machine Response**
- **Alerts and Responses Published Back Out to the GIG**

Operationally-Relevant Data Sources Published for Self-Service Event Subscription

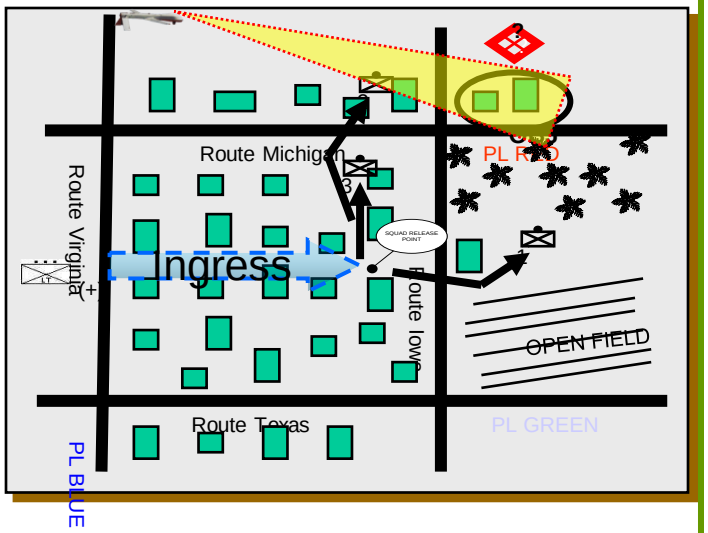


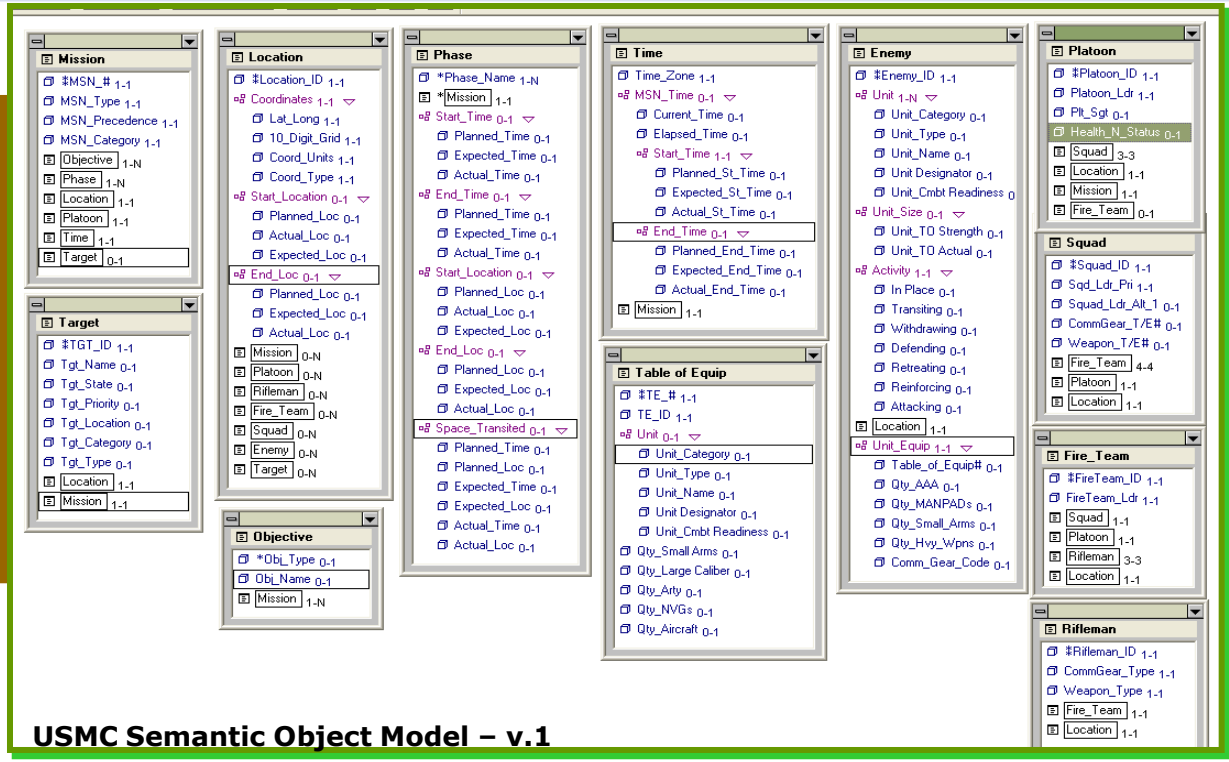
DoD GIG Architectural Vision For a Net-Centric, Service-Oriented DoD Enterprise; Version 1.0, June 07

AGENT LOGIC
TO DETECT AND RESPOND

Event Processing in the GIG – Valuable Information/Right Time (VIRT)

High Value Target Raid - USMC





USMC Semantic Object Model – v.1

Example Condition of Interest

1-1. Notify me if my target location is no longer valid.

1-1.a. The distance we are concerned with is a variable. For this instance, we say +/- 100m

In_1.0 //Target Location has changed//

1 Current target location not as planned

[Mission]:Msn_#, Msn_Type-HVT[Phase]:= Ingress, [Target]:Tgt_ID, [Location]: Location_ID, Coordinates ≠ Coordinates Planned

** "Event Processing in the GIG," Rick Hayes-Roth; Professor, Information Science; Naval Postgraduate School*

AGENT LOGIC
TO DETECT AND RESPOND

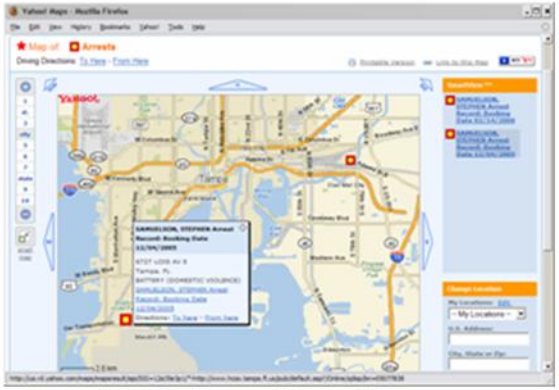
Situational Dominance – Power to the Warfighter

- Tailorable process for monitoring Conditions of Interest (COIs) and alerting operators.*
- Vocabularies that operators find natural and useful in characterizing their COIs.*
- An expression language that operators can write and read to define COIs that uses their own vocabulary simply.*
- Standard solutions for expressions involving temporal and spatial intersections. Make it easy to "mix in" space and time dimensions to virtually any ontology.*
- User Defined, SOA-Compliant – Supports Web Services for event ingestion, rule creation and alert/response publishing
- Simple, powerful UI to quickly handle velocity of event change, NOT just event velocity
- Self-Serve Analytics – Spatial, Temporal, Numerical, Entity Extraction, Event Enrichment

**** "Event Processing in the GIG," Rick Hayes-Roth; Professor, Information Science; Naval Postgraduate School***

AGENT LOGIC
TO DETECT AND RESPOND

Multi-Channel Information Delivery



GIS Applications

Ajax / Widgets

Real-Time Alert Manager™

Alert
Visualize
Publish

Portals & Dashboards

Personalized
RSS Feeds & Wikis

Instant Notifications

AGENT LOGIC
TO DETECT AND RESPOND

Cross-Domain Challenge

- The Problem
  - Multiple networks at different classification levels
    - Many account names, computers, procedures
  - Analysts must separately log in to check e-mail, web, news, databases, etc.
  - No automated, timely notification of new and changing information

- The Solution: Agent Logic L2H Product/AgentOWL™
  - Automatic high-side notifications based on low-side events (user-defined rules)
  - Automatic movement of data to High Side using existing data transfer infrastructure
    - User-defined filtering logic/high-level event detection rules on Low Side (as required)
    - User-defined alerting and complex event detection rules on High Side
    - Automated monitoring of items of interest on Low Side

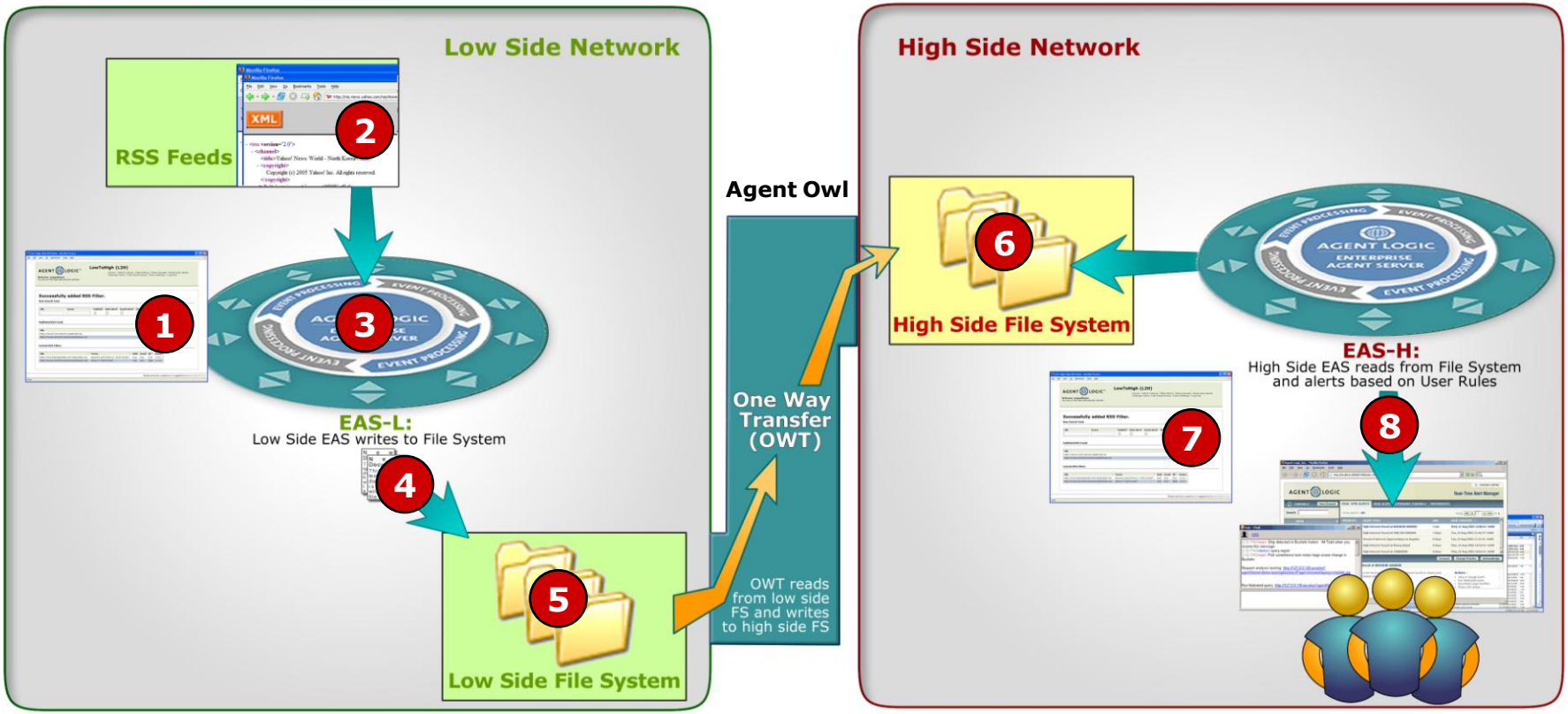
AGENT LOGIC
TO DETECT AND RESPOND

LowToHigh/AgentOwl™ Applications

- Open Source RSS Feed Monitoring and Alerting
  - Monitor, filter and forward relevant RSS news stories
  - Alert users via multiple channels to arrival of new stories
- Email Transfer and Alerting
  - Monitor email inboxes, filter and forward relevant messages
  - Alert users via multiple channels to arrival of new stories
- Copy and Paste
  - When a user finds interesting information on a low-side network, they can press CTRL-C to copy that information into an EAS "Copy and Paste Client" and forward it into a high-side environment
- Blog/Wiki Synchronization and Alerting
  - Monitor blogs and wikis, filter and forward relevant entries
  - Alert users via multiple channels to arrival of new entries
- Geospatial Synchronization and Alerting
  - Monitor low-side geospatially oriented data for relevant changes
  - Update high-side geospatial applications with new data

AGENT LOGIC
TO DETECT AND RESPOND

Example: LOW SIDE Open Source Feed - Data Flow



1. On the low side, an administrator or user sets up subscription rules, which determine the data that gets placed in the high-side One-Way Transfer Mechanism (OWT) queue. Administrator-defined rules apply to all users, but a user can create personal low-side rules as well.
2. Agent downloads user-specified feeds on a scheduled basis
3. Agent parses the contents of the feed and matches the contents against the user's rules
4. If the contents match the user's filter criteria, the document is placed in a directory that is accessed by the OWT on a scheduled basis
5. Agent Logic-L adds a header to the copied data that provides routing and delivery instructions to the high-side Agent Logic (Agent Logic-H)
6. Agent Logic-H monitors a directory for incoming files. When new files are detected, Agent Logic-H determine the owner of the message
7. The incoming files are filtered according to the user's high-side filter criteria to determine alerting channels
8. Alerts are sent to users via email, instant message, or Real Time Alert Manager™ based on the filter criteria

AGENT LOGIC
TO DETECT AND RESPOND

Examples…

- **Support to the WARFIGHTER**
  Operationally Relevant Event Changes Across the Battlespace: 1.) Counter IED - Blue Force Tracking data correlated with relevant SIGINT, ELINT & IMINT events "Alert me when X SIGINT events occur near a particular humvee more than X times. . 2.) OTH Target Tracking – OTH tracking data correlated against user-defined NAI polygon & watchlist – Geospatial alerting derived.
- **Cable Traffic Monitoring, Correlation, and Alerting**
  High-side alerting based on message traffic: "Alert me when a particular person or place shows up in message traffic more than X times within a particular period of time, and if so, send me a higher priority alert." (Automatic web-browser, E-Mail, IM)
- **Transactional Analysis (Time Based)**
  User-driven rule-based transactional analysis: "Let me know (Alert Me) when Party A engages in a transaction with Party B where country of transit = "South Africa" and Goods Type = "A1" and Party A has previously shipped other goods of specified types within a certain time period."
- **Open Source Data Monitoring**
  Open source data monitoring, correlation, and alerting with LowToHigh functionality: Analysts are able to receive alerts (e-mail, web, IM) on the high side when open source data matches high-side items of interest. Non-technical users are able to configure rules to determine on what and how they'd like to be alerted.
- **Enrichment: Automating the "checkables" process**
  Automatic enrichment of data: "When I receive an alert than includes mentions of specific people/entities, automatically check these other databases to see if those people also show up in those databases. If there are matches, also send me those records as part of the alert."
- **Link Analysis Situational Awareness**
  Alerting based on Link Analysis events (Provide alerts when Analyst Notebook charts on other user computers change): "Alert me when any analyst notebook chart belonging to users in my workgroup contains new linkages to people on my personal watch list, where there is cable traffic within the past 10 days associated with the new linkages."

AGENT LOGIC
TO DETECT AND RESPOND

Progressive Solutions for Complex Event Processing

1. User-Driven & Defined Experience
End USER drives rapid definition of sophisticated correlation rules. No IT involvement and no costly software development involved!

2. On-the-Fly Analytics
Quickly snap in 3rd party analytics and data sources for event detection and response – eliminates long development cycles for new functionality

3. Concurrent, Multi-Source Capable
Correlation of disparate data elements with spatial & temporal logic

4. Event Enrichment
Intelligent watch list monitoring/updating; Enhance event context & experience w/ rule-fired reach back to other complementary events

5. User-Controlled Rule Chaining
Enable rule layering – event sharing to augment currently-configured rules

6. Event Sensing & Ingestion
Dynamically update to rule topics when events occur with new properties

7. Shared Rule Creation (Responsibility to Share)
Rules created as templates – allows advanced users to share/preserve knowledge and essential practices for analysis and response

8. Data Normalization & Abstraction
Quick rule definition w/out end user needing to know how topics are defined; Eliminates lengthy and expensive software feature development

9. Robust, 3rd Party Application Integration
Out-of-the-box integration & connectors w/ DBMS, JMS, web, IM, email, GIS, IRC; Eliminates custom dev for data source integration

10. Real-Time Alerting
DHTML-Based, Actionable Responses, Content Rich, Multi Channel

AGENT LOGIC
TO DETECT AND RESPOND

Agent Logic Operational Environment

Inbound Source Connectors

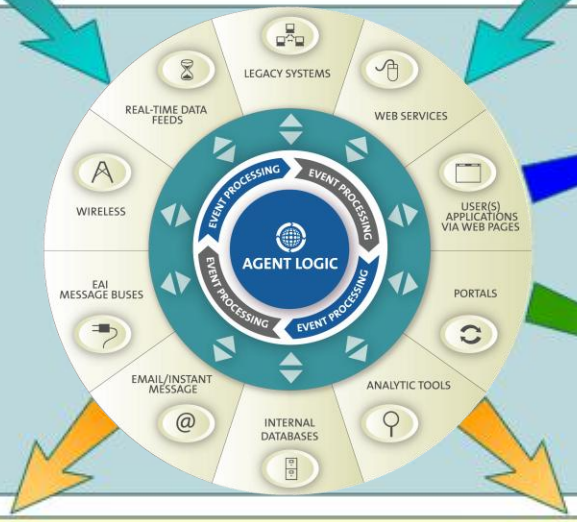
AOL Instant Messenger, Other IM Services, Attensity, Digital Harbor, Enterprise Java Beans, File Systems (read, write, execute, etc.), finger, FTP, FTP spidering, GCCS (select apps), Groove, HTTP/HTTPS, i2 Analyst Notebook, IMAP, Inktomi, Inxight FactFinder/ThingFinder Summarizer, Categorizer, IMAP, IWS, IRC, Jabber, Falcon View, Java-based APIs, JBuddy, JESS, JBoss MQ, JMS, Lotus Notes, Lucene, Lumetta, MetaCarta, Metamatrix, Microsoft Exchange, Microsoft Excel, Microsoft Word, Mohomine, MQ Series, NNTP, NORA, OpenMap, Oracle AQ, Oracle Spatial, PDF (ingest), POP3, RMI, serial ports, SMTP, SNMP, SOAP, Sockets (e.g. TCP/IP streams), Oracle, SQL Server, MySQL, PostgreSQL, Stratify, Telnet, Unix Mail, XML-RPC, Websphere MQ, database log files

Host Platforms

Windows
Solaris
Trusted Solaris
LINUX
SE LINUX

Authentication

Active Directory
NT Domain
LDAP
NIS
UNIX User
UNIX GROUP
SecureID
PKI/CAC Support
Anonymous
Standard Auth (Web)



MLS Environments

SUN (TSOL)
TCS (NTOP 1 & 2)
DTW (TSOL BASED)
SE LINUX
Owl

Enhanced Discovery

Inxight
Xylab
Lumetta
IP Fabrics
Other third party products

AOL Instant Messenger, Attensity, Digital Harbor, Enterprise Java Beans, File Systems (read, write, execute, etc.), finger, FTP, FTP spidering, GCCS (select apps), Groove, HTTP/HTTPS, i2 Analyst Notebook, IMAP, Inktomi, Inxight FactFinder/ThingFinder Summarizer, Categorizer, IMAP, IWS, IRC, Jabber, Falcon View, Java-based APIs, JBuddy, JESS, JBoss MQ, JMS, Lotus Notes, Lucene, Lumetta, MetaCarta, Metamatrix, Microsoft Exchange, Microsoft Excel, Microsoft Word, Mohomine, MQ Series, NNTP, NORA, OpenMap, Oracle AQ, Oracle Spatial, PDF (ingest), POP3, RMI, serial ports, SMTP, SNMP, SOAP, Sockets (e.g. TCP/IP streams), Oracle, SQL Server, MySQL, PostgreSQL, Stratify, Telnet, Unix Mail, XML-RPC, Websphere MQ, DTW (DODIIS select applications, Google / Keyhole Earthviewer, Aspect VRU T2S (via ASCII file submission API), Text to Speech Third Party products

Outbound Destination Connectors