PROGRESS SOFTWARE

Enabling Information Dominance

Complex Event Processing in Network Centric Operations

John Trigg
Principal Product Manager – Apama
Progress Software

Agenda

- Introduction
  - Complex Event Processing
  - The Relationship between CEP and SOA
  - Using CEP and SOA to Drive Information Advantage
- Use Cases & Benefits
  - Digital Battlespace
  - Homeland Security
  - Intelligence Monitoring
- Conclusions

The Challenge

Identify Opportunity

- How can we monitor all relevant activity to ensure visibility, control, and automation?
- How can we analyze operating conditions to understand risk?
- How can we act on threats and opportunities while we can still do something about them?

Reduce Decision Making Timeframe

- How can we automate action and manage by exception?

Increase Operational Efficiency

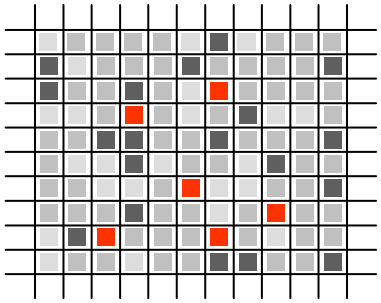
- How can we discover and predict new opportunities and threats that we have yet to anticipate?
- As we automate, how can we ensure we comply with regulations and effectively govern our operations?

Align Operations and IT

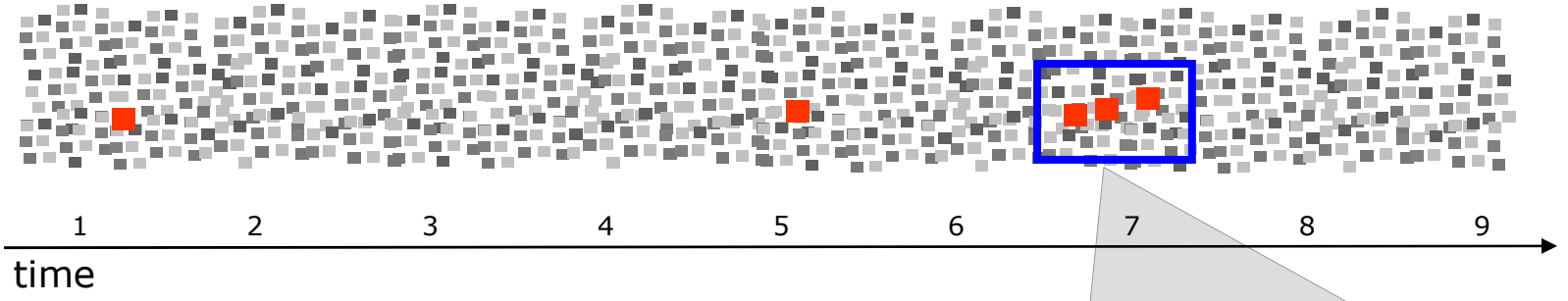
CEP Requirement Today

- From NCOIC website
  - The missing link in today's disaster recovery efforts is a working network. And the key to emergency response is accurate information that enables first-responders to know what happened, who's responded, and what is still required.

Complex Event Processing
A New Computing Physics



Static Data Processing: "How many signal intercepts between targets have we had in the last 24 hours?"



Complex Event Processing: "When 3 signal intercepts occur within 2 minutes of one another from the same source to 5 suspect destinations, dispatch unit to source IN REAL TIME."

OK, but what is an “Event”?

Events are data elements – collections of attribute-value pairs - that capture the state (or changes to state) of real-world or computer-based objects. Events consist of data and temporal attributes that represent the “what”, “when”, and “where” of an object - the state of an object or the interaction of objects at a particular time.

Real World Examples

- Stock market trades and quotes
- RFID signals
- Satellite telemetry data
- Card swipes at a turnstile
- ATM transactions
- Network activities/faults
- Troop movement on battlefield
- Activity on a website
- Electronic funds transfers
- SCADA alerts

SIGINT Scenario

If the **Target Acquisition Radar** is detected
FOLLOWED BY

Communications intercepts indicate the presence of a missile battery

AND

The **location** does not match a previously known missile battery

ALL WITHIN
ANY **15 SECOND** WINDOW

Action

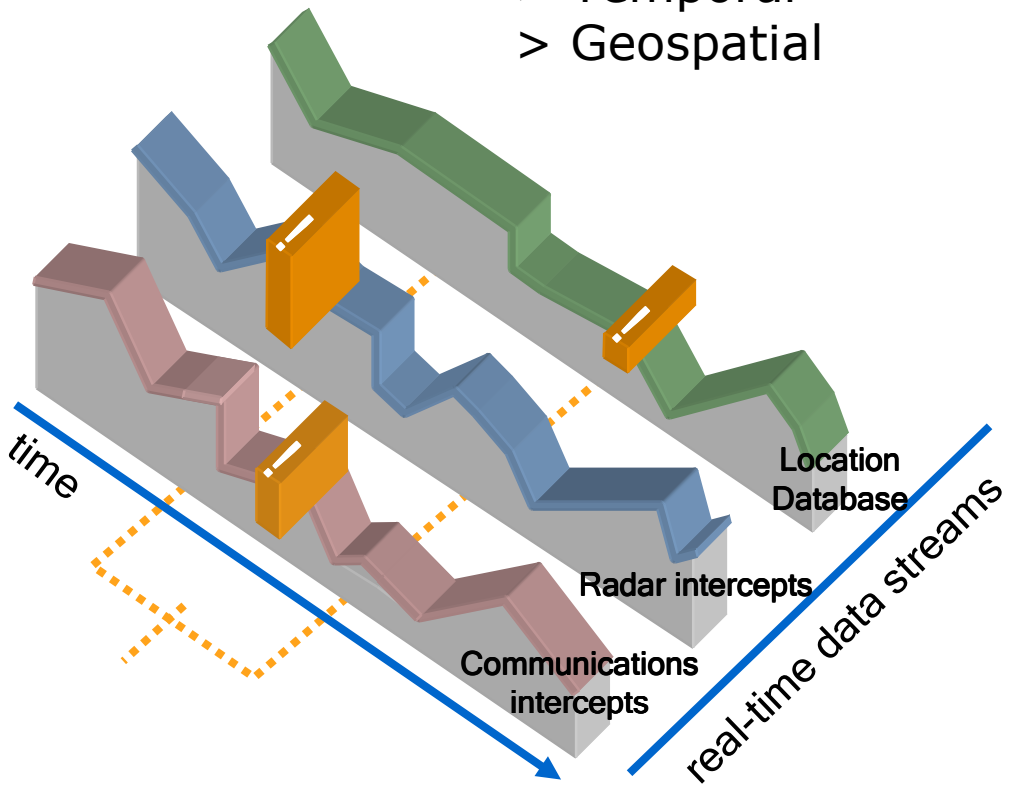
THEN

Establish an MEZ

Order EO/IR/SAR surveillance of the area

Multi-Dimensional
Any-To-Any
Correlation

Correlate
> Logical
> Temporal
> Geospatial



Relationship between SOA and EDA

Monitoring Service Oriented Events

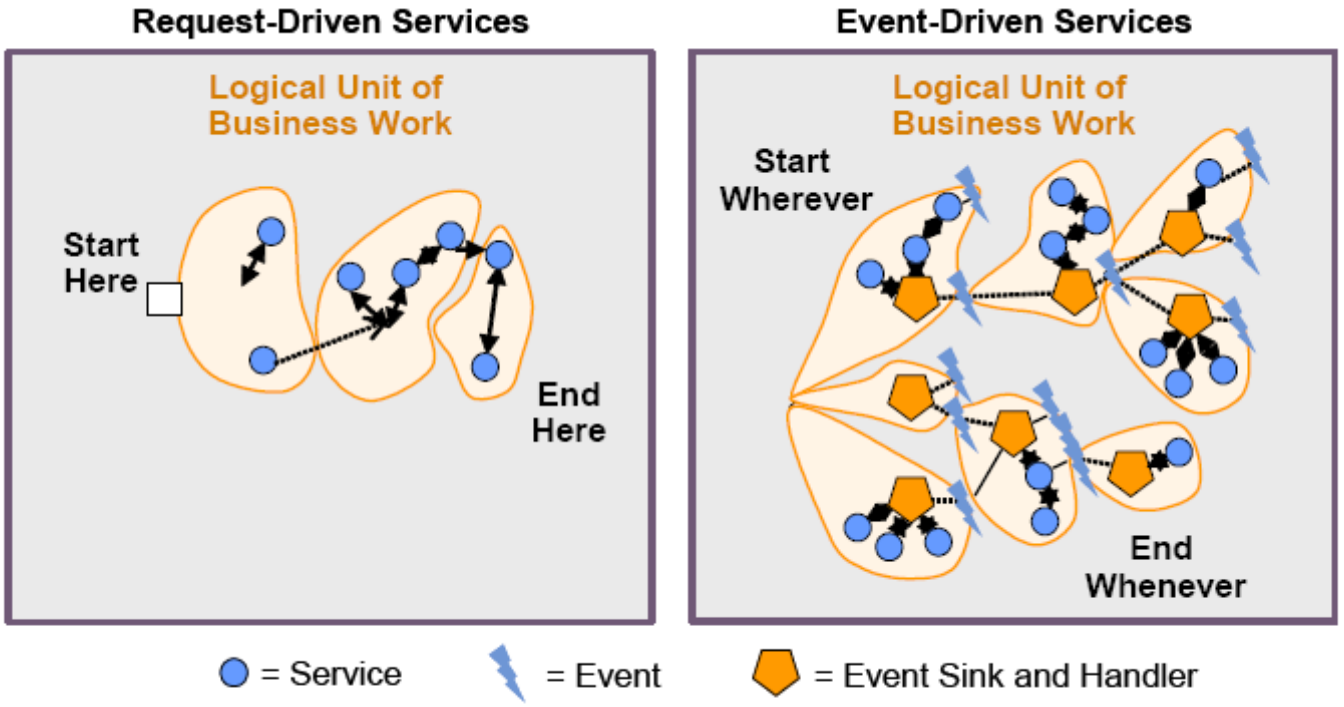
- Growing market view:
  - Harmony between SOA and EDA: “Advanced SOA”

> Over the last few months, we have seen **increasing interest in the SOA-EDA connection**, both from enterprises and the vendor community. …..Thought leaders at leading SOA and integration vendors are coalescing visions and product strategies for SOA, integration, and event processing. This is all great to see.
>
> Seybold, February 2006

> Forrester has long advocated **you should treat event handling capabilities as part of a full-featured SOA** — along with numerous other capabilities, such as policy-based processing, multichannel coordination, filtered message delivery, real-time business management, and more.
>
> Forrester, 2004

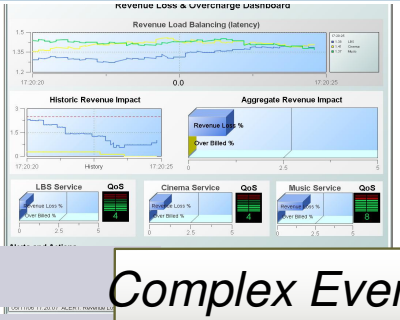
- CEP operates in conjunction with SOA
  - SOA’s generate events
  - CEP can monitor, analyze – and act

Evolution of SOA – Event Driven



Source: Gartner (August 2007)

CEP - Inbound Event Monitoring



Radar: new target acquired		***…5 minutes?***
Communications	***…2 minutes***	***…potential threat?***
Civilian Air Defense	***…10 minutes***	***…airline reports?***

Complex Event Processing

Telemetry/ Field Sensors

Messaging Infrastructure

Intelligence Events

Alerts

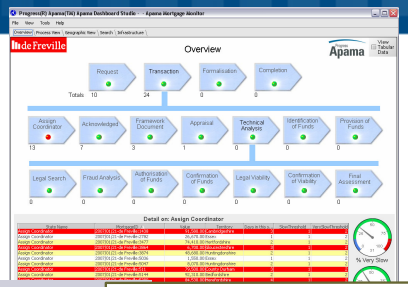
Monitoring in Real Time with CEP

Intelligence Application

Data

Reference Data

CEP - Application Event Monitoring



Intelligence	***…5 minutes***	***…reported sightings***
Logistics	***…60 minutes***	***… suspect cargo arrival***
Traffic	***…10 minutes***	***…local police patrol on scene***

Complex Event Processing

Messaging Infrastructure

Alerts

Intelligence

Logistics

Traffic

Monitoring Existing Applications in Real Time with CEP

PROGRESS SOFTWARE

Defense Use Cases & Benefits

Digital Battlespace & Network-Centric Warfare

Problem & Opportunity

Location(x,y,z)

Fuel remaining

Ammunition remaining

Damage indication

Location(x,y,z)

Ammunition remaining

Vital signs

- Digital events now available from battlespace due to
  - GPS (x,y,z)
  - Other sensors (fuel, remaining ordinance, enemy siting etc.)
  - Wireless technologies
- Data Explosion (millions of objects, thousands of updates per second) just creates a bigger problem
- How to capitalize on this data to provide higher quality intelligence in the field before it's too late?

Problem & Opportunity

Location(x,y,z)

Fuel remaining

Ammunition remaining

Damage indication

Location(x,y,z)

Ammunition remaining

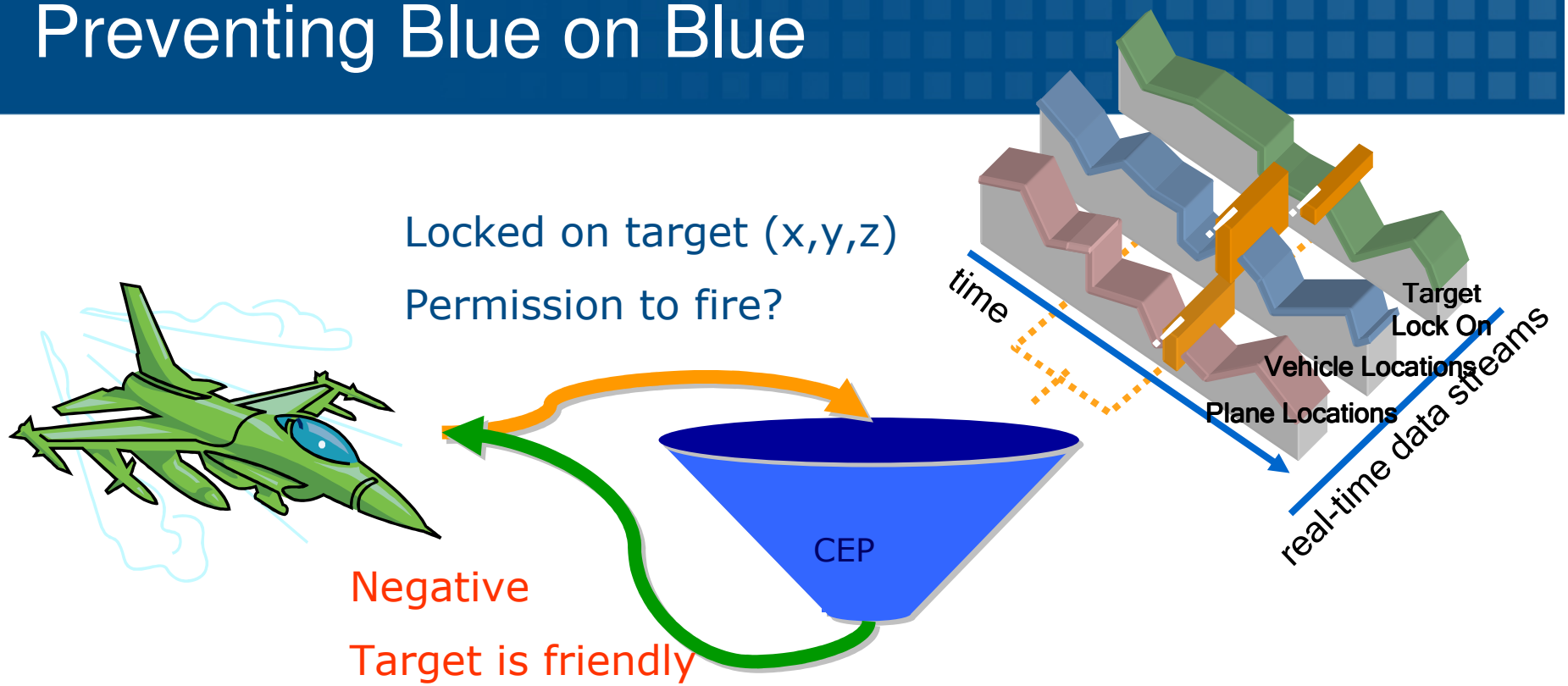
Vital signs

CEP

Sense & Respond

CEP enables immediate informed response

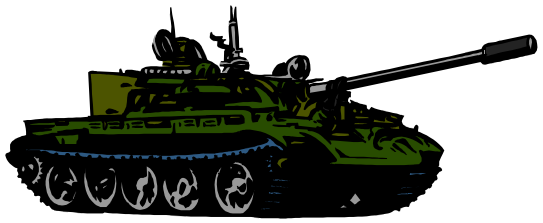
Preventing Blue on Blue

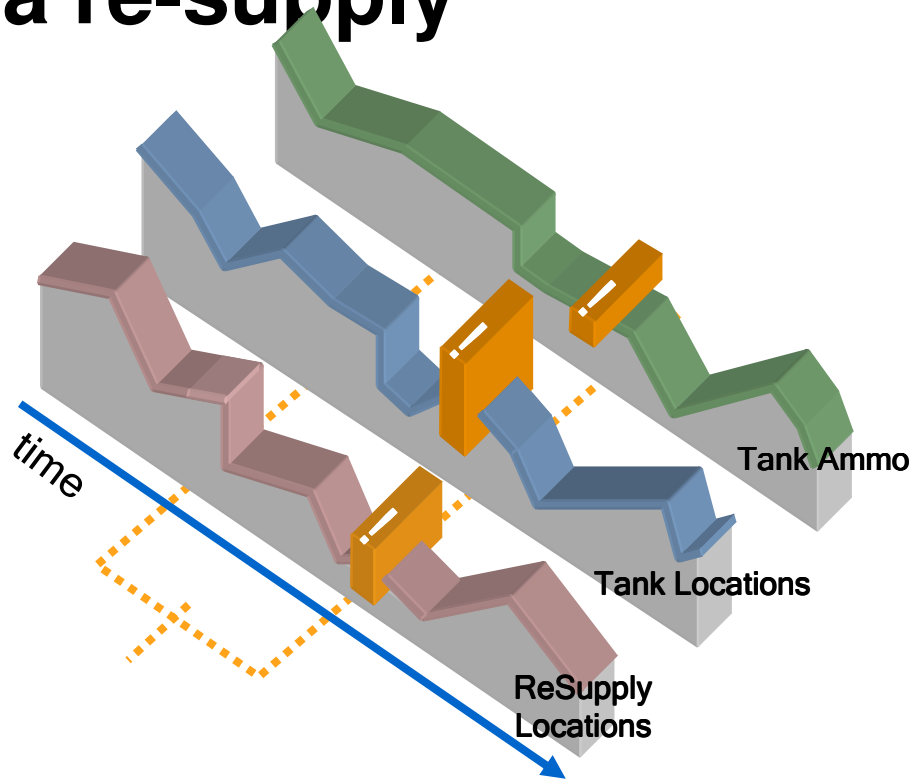


CEP can track the locations of thousands of vehicles and instantly identify location intersections, e.g. locking a missile on a friendly vehicle

Anticipatory Logistics

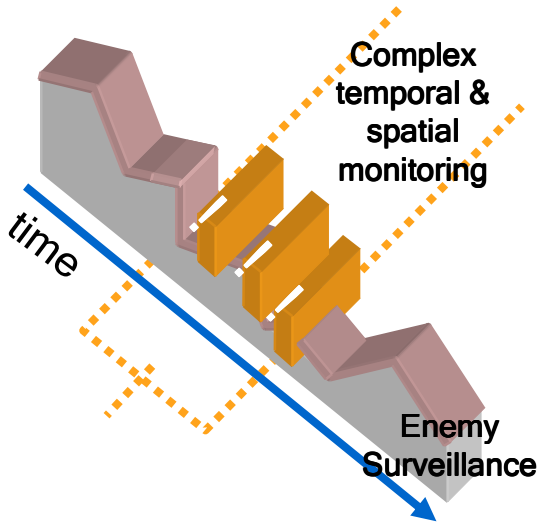
- **Warn any tank commander if his ammunition falls below 30% and he is over 1 hour from a re-supply**





Spotting an Enemy Refuelling Point

- **Tell me if more than three enemy tanks become stationary for more than 5 minutes within the same 100 meter square, within a 5 hour period (if so order a bombing mis**



PROGRESS SOFTWARE

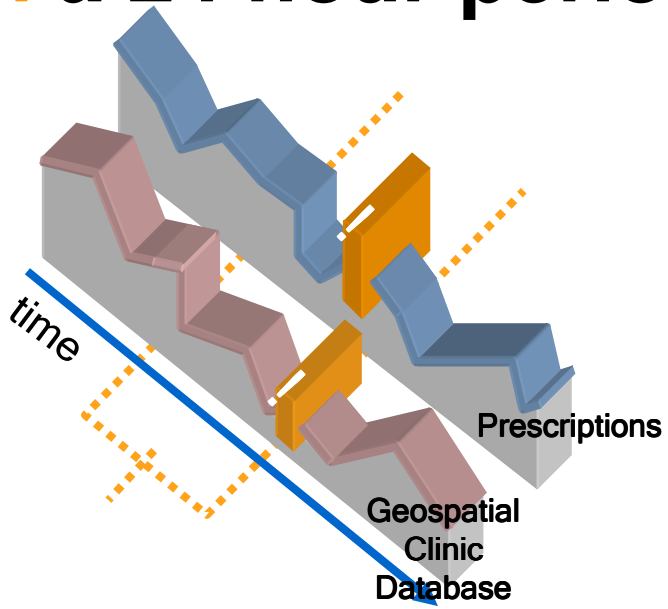
Homeland Security & Intelligence Monitoring

Homeland Security & Intelligence Analysis

- Opportunity
  - CEP can spot patterns in intelligence data in real-time
  - Increase accuracy of intelligence reporting
  - More positive, less negative reporting

Anti-Terrorism

- **Tell me if any 3 separate clinics in the same city prescribe any drug that may be used to treat symptoms of bio-terrorism within a 24 hour period**



Criminal Tracking

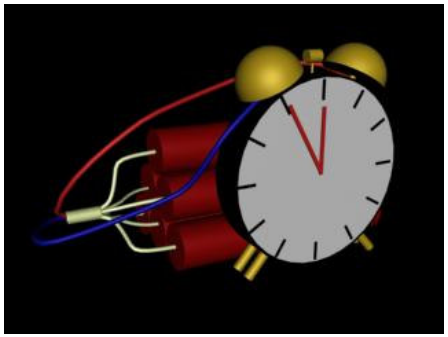
- Tell me if any tagged paroled prisoner goes into an area that violates parole, including:
  - Bars frequented by known criminals
  - Within 100 feet of someone with a restraining order against him

Criminal/Terrorist Monitor

- If there are more than 5 calls to a suspect number, lasting less than 30 seconds, within 1 hour then alert an Operative and monitor activity on the numbers the calls came from

Criminal/Terrorist Monitor

- If the same user (IP address) accesses websites about bomb-making and truck rental and fertilizer supply within 1 day then alert an Operative



PROGRESS SOFTWARE

Conclusions

The Value of CEP & SOA in Network Operations

- Unify monitoring across infrastructure
  - Use a SOA approach to normalize event sources
  - Monitoring as another service on the bus
- Predictive Real-Time Intelligence
  - Absorb & act on field intelligence in real-time
  - Process millions of potential patterns in parallel
- Real-Time Security
  - Detect and stop security breeches as they happen
  - Capture and replay actual state to discover emerging patterns

- Gain dominance in your field from the information you have available to you AS IT HAPPENS

Questions?

PROGRESS SOFTWARE

Enabling Information Dominance

Complex Event Processing in Network Centric Operations

John Trigg
Principal Product Manager – Apama
Progress Software