



Analytic Technology Industry Roundtable Threat Assessment Use Case

7 November 2017

*The following material and related
discussions are Confidential to the Analytic
Technology Industry Roundtable.*



Agenda

- Alignment of Use Cases to Classes of Analytics
- Use Case – Threat Assessment
- Threat Assessment Working Group
- System Architecture
- Data Visualization and Results
- Demonstration
- Next Steps



Alignment of Use Cases to Classes of Analytics

USE CASE\Analytics		Text (Unstructured) Analytics	Structured Descriptive Analytics	Predictive Analytics	Geospatial Analysis	Link/Network Analysis	Imagery Analysis	Voice Analysis	Biometrics	Streaming Analytics
Cyber (defensive and “other”)		O	C	O	M1	C	O	O	O	C
Insider-Threat / Counter-Intel		M2	C	O	M1	C	O	O	M1	M1
Command and Control (or C4ISR)		M2	C	M1	M1	C	O	O	O	C
Law Enforcement		C	C	M1	M1	C	M1	O	C	O
Counter-terrorism		C	C	M1	M1	C	M1	O	M2	M2
Counter-proliferation		C	C	M1	M1	C	M1	O	O	M2
Counter-narcotics		C	C	M1	M1	C	O	O	O	M2
Financial crimes and money laundering		O	C	M1	M1	C	O	O	O	M1
Disaster Relief		M1	C	O	C	O	O	O	O	M2
Search and Rescue		O	C	O	C	O	M1	O	O	M2
Disease Control		M1	C	M1	C	C	O	O	O	M2









Use Case – Threat Assessment

Threat assessments: Lower the risk of targeted violence by proactively identifying, assessing and mitigating threats.

- Implementation Objectives:
 - Illustrate the integration of multi-modal analytical disciplines
 - Use the cumulative power of multi-vendor integration
 - Data Fusion and Enrichment – Augment Data with Geo-Reference Data, Additional Events of Interest
 - Provide data to the Analysis Exchange
 - Retrieve data from the Analysis Exchange for analysis
- Limitations
 - Use Case developed using publicly available data set
 - Primarily Static Source data - Not a dynamically updated data set
- Future
 - Establish enhancements, data acquisition, acceptance criteria regarding use case from customers like those present



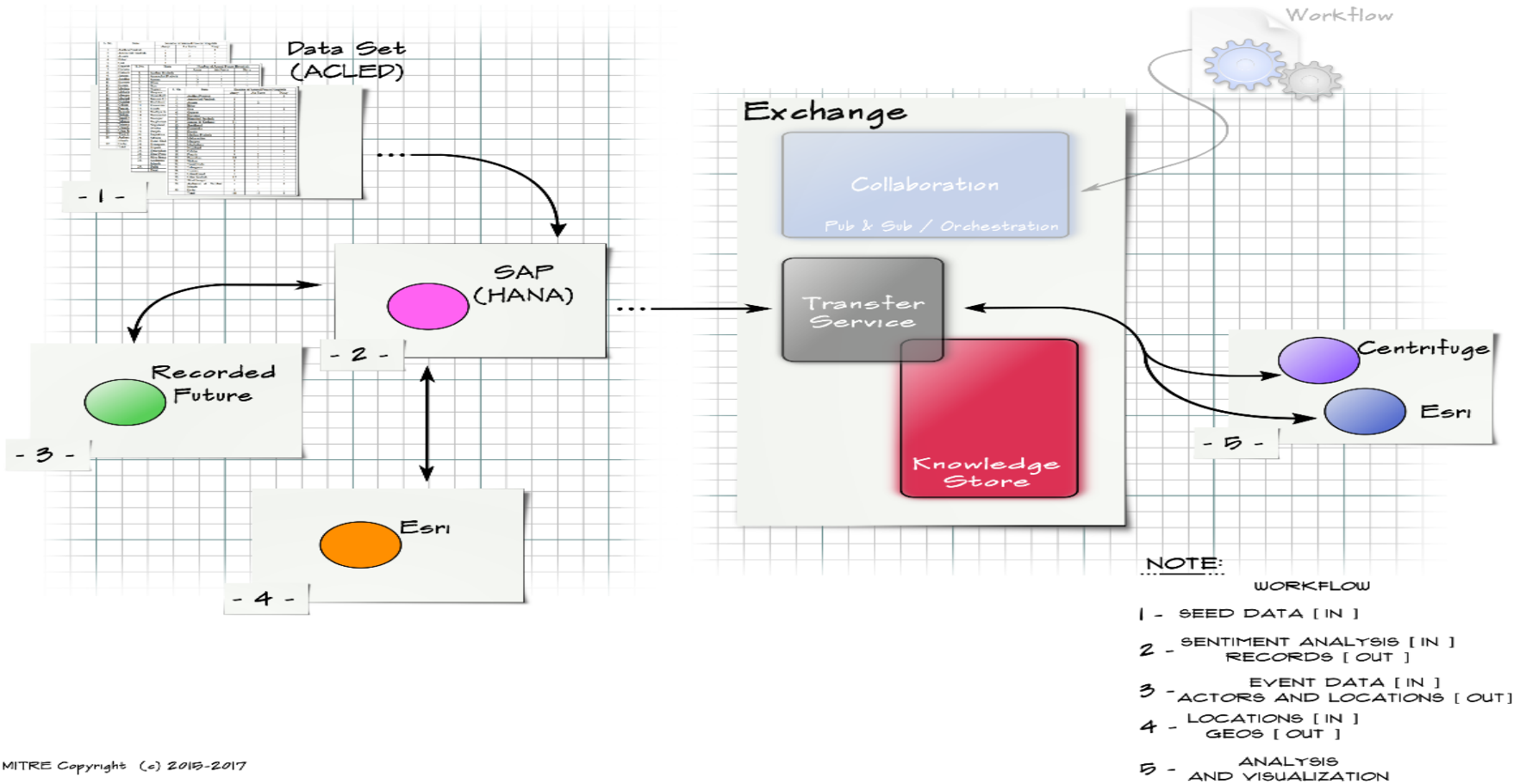
Threat Assessment Working Group

Company	Technology	Capability
	<ul style="list-style-type: none">• SAP HANA; In-Memory Data Management	<ul style="list-style-type: none">• Data Ingest/Storage• Text Analysis• Search Web Services
	<ul style="list-style-type: none">• ArcGIS Platform	<ul style="list-style-type: none">• Maps and Imagery• Geo-processing Analytics• Visualization
	<ul style="list-style-type: none">• Centrifuge Analytics	<ul style="list-style-type: none">• Visual Data Analysis• BI Charts, Link Analysis, Geospatial (with ESRI)• Temporal Analysis
	<ul style="list-style-type: none">• OSINT Mining	<ul style="list-style-type: none">• Open and Closed Source Collection, Analysis



System Architecture

USE CASE 2: THREAT ASSESSMENT



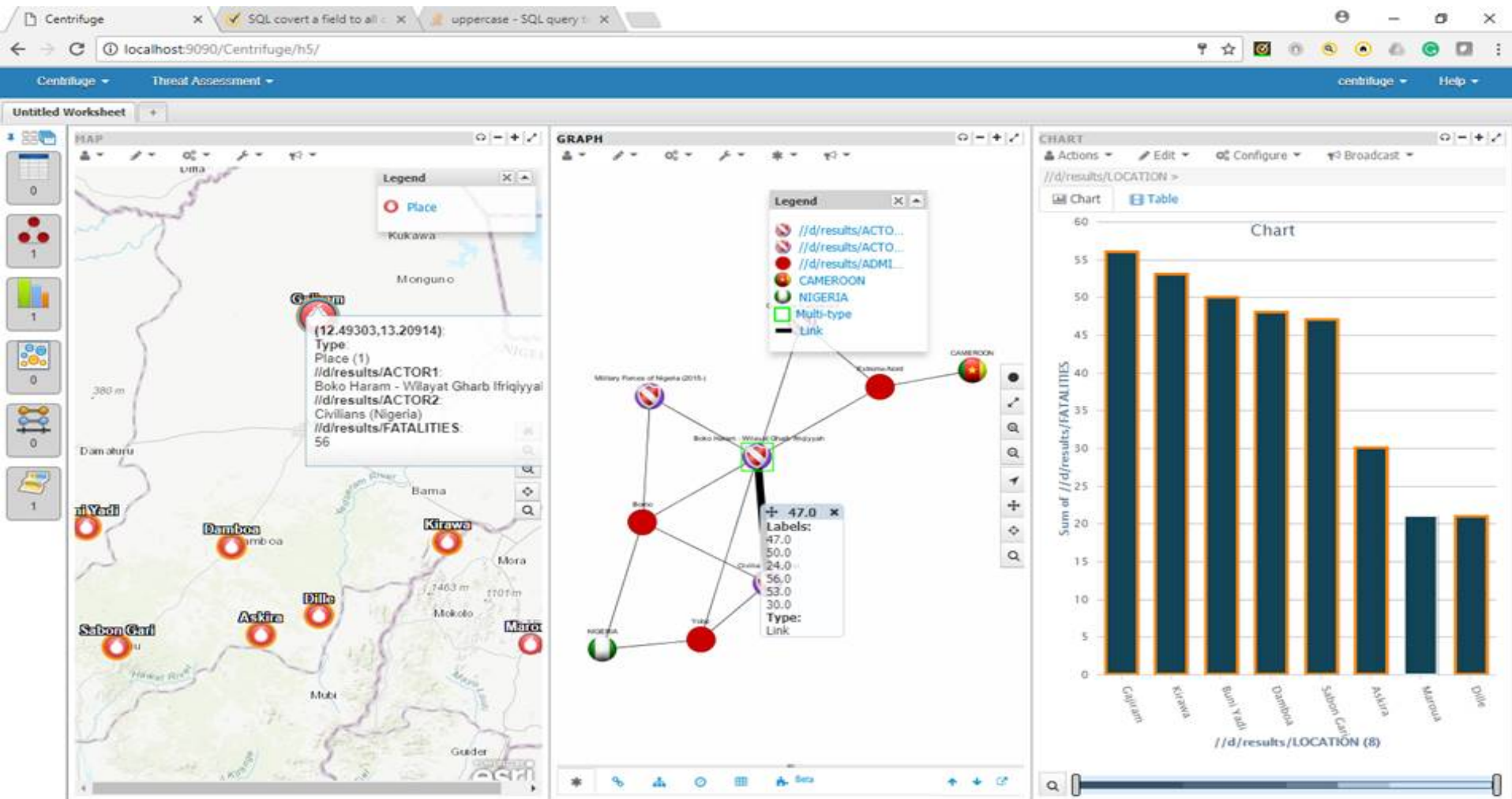
MITRE Copyright (c) 2013-2017



Analytic Technology
Industry Roundtable



Data Visualization and Results









Next Steps: Incorporating more analytic

- **Predictive** or anticipatory analysis is the application of data science and statistical algorithms to determine the probability of these future outcomes
 - Does the known Boko Haram behaviors of the past help determine the likelihood of an event, or series of events, occurring in the future
- **Streaming** analytics can be viewed as the means to provide real-time situational awareness and, as necessary initiate action, without active human intervention.
- **Imagery** analysis describes the extraction of useful information from any sort of sensor-related data contained in bidimensional graphic format.
 - Examples of data include photographs, remotely-sensed multi-spectral imagery from satellites and aircraft, ultrasound, magnetic resonance imaging (MRI), infra-red photography, seismographs, et al.



Threat Assessment Team Technical Leads

Company	Technical Leads
	Brian P. Adams brian.adams@sapns2.com
	Brian Biesecker BBiesecker@esri.com
	Lorne Hanson lhanson@centrifugesystems.com
	CW Walker cw@recordedfuture.com