Three Use Cases

The Analysis Exchange (AE) was designed to help government and industry achieve common goals and efficiencies. Government analysts can be assured that any of the ever-growing number of vendors participating in the AE can share information across multiple platforms. And participating vendors know they can continue to build upon their competitive advantages through proprietary features, while being responsive to their customers by sharing information with other vendors' systems. Due to the "plug n' play" nature of the Analysis Exchange Model 1.0, vendors are better able to compete for acquisitions more efficiently using fewer resources. This allows industry to build better, more cost-effective solutions and provides the government with access to more responsive, cost-saving tools to achieve their missions.

The benefits of the Analysis Exchange include:

- Using a more interoperable, consistent, and repeatable model allow vendors to compete for acquisitions more efficiently, saving time and money.
- Products and systems can become more effective at meeting government needs and requirements with less investment of resources.
- The AE can break down the data silos that multiple analytic tools typically create.
- Member companies can adopt consistent standards more quickly, saving them and the government time and money.
- The AE can develop a set of common standards and protocols for the analysis and analytics community.
- The AE can create enriched products for government use based on the results of different companies' products.

Three Use Cases

While the AE can be designed to support a virtually unlimited array of analytic combinations, the Roundtable is initially focusing on three key use cases that they believe will be particularly relevant to government analysts. In each use case, the AE has developed an ontology that will help analysts mine their existing rich sources of data. From this data, the AE will help analysts gain a more complete picture—and possibly reveal anomalies and discrepancies—that will help them identify bad actors at work.

Use Case – Fraud, Waste, and Abuse

Many thousands of government employees, contractors, and citizens receive reimbursements for travel from federal agencies each year. While the majority of people record their travel expenses honestly, it is an area that is ripe for fraud, waste, and abuse. With the AE, analysts can ask their IT departments to pool the information from different analytic systems into a common ontology. For instance, the AE provides a consistent structure for information from different sources relevant to a travel voucher, which data scientists/analysts can use to identify outliers/anomalies that require further investigation. Did an employee request reimbursement for mileage from an address where they do not reside or have never have resided? The AE empowers analysts to use all the tools at their disposal to gain a clear picture and identify potential risks.

Use Case – Threat Assessment

Threat assessments are a proven approach to lower the risk of targeted violence by proactively identifying, assessing and mitigating threats, yet the resource intensive methods utilized can make the process prohibitive in both time and money. Analytic capabilities are needed that reduce the costs of doing complex data exploration and increase the effectiveness in identifying trends and patterns of targeted violent events over time and space. For instance, even after complex geopolitical events unfold, it may be difficult to gather and visualize a complete picture of the full context. Did a terrorist group have other simultaneous activity? Is there a larger pattern that recurs throughout typical attacks that can be discovered? The AE allows analysts to collect information from various data and analytic sources that provide enrichment and depict them all together.

Use Case – Cyber Forensics

Cyber security experts are challenged to stay ahead of threats posed by hackers who continuously outwit common security systems and the individuals responsible for security. Cyber attacks are numerous, sudden, and require a speedy reaction time. Relevant data for forensically analyzing an attack may have to be drawn from different sources. When an attack occurs, an analyst principally wants to know who perpetrated the attack and the extent of the damage, which requires information from multiple sources. Given the brisk nature of cyber attacks, an analyst also wants to proactively monitor a network for threats and be able to stop them. This also requires multiple analytic sources to build a graph of interrelationships of the cyber environment and the potential bad actors. The AE can assist in pooling information from a variety of disparate sources to gather data for both reactive and proactive cyber analyses.

Interested in Learning More About the Roundtable?

The Analytic Technology Industry Roundtable meets monthly at The MITRE Corporation in McLean, VA. As a private, not-for-profit corporation that operates federally funded research and development centers, MITRE provides the Roundtable with a neutral environment, guidance, and structure. For more information or to learn about government engagement opportunities with the Roundtable, contact Director and Chair Dr. Angela O'Hanlon, email: amcintee@mitre.org. Or visit the Analytic Technology Industry Roundtable at: http://www2.mitre.org/public/analytic-technology/exchange.html.