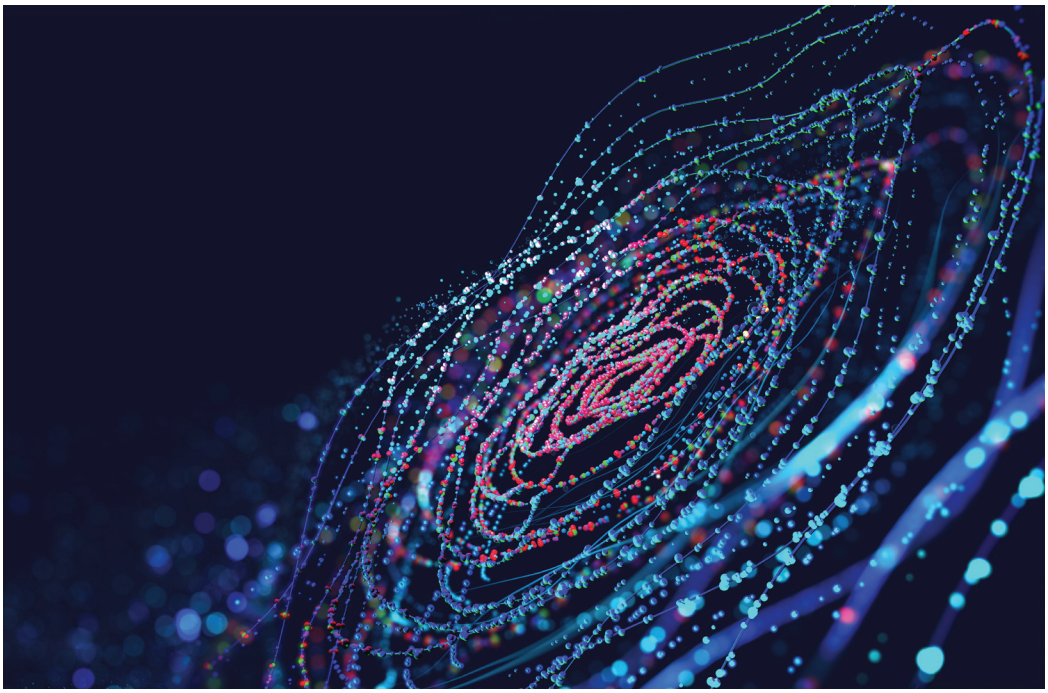


Cogynt – Continuous Intelligence Explained

COGILITY

"Describing a past event is not intelligence analysis; it is reciting history. True Intelligence is always predictive."

ROBERT M. CLARK

Introduction

The objective of the Cogynt Continuous Intelligence (CI) platform is to reduce the uncertainty of decision-making in time sensitive, highly complex sociotechnical environments,[1] at scale. In general terms, Cogynt is an intelligence platform intended to serve intelligence practitioners in the commercial and government sectors. The word "intelligence" itself has broad reference and means different things to different people; for the purposes of this paper, we quote Robert M. Clark:

> Intelligence in general can be thought of as a complex process of understanding meaning in available information. A typical goal of intelligence is to establish facts and then to develop precise, reliable, and valid inferences (hypotheses, estimations, conclusions, or predictions) for use in strategic decision-making or operational planning.[2]

The challenge and opportunity for current intelligence analysis practitioners is the glut of information that emanates from sociotechnical environments, including cyber activity, social media, IoT devices, and many other sources of human and system generated digital data. This massive, aggregated data can be used to develop insights that identify risk or opportunity for an enterprise, thus enable informed, timely, proactive decision-making.

The intelligence analysis community today struggles with inadequate tools and limited analytic solutions that fail to support a timely comprehensive analysis of the problem domain. Specifically, current solutions limit the analyst's situation awareness and ability to analyze alternative hypotheses and the risks associated with decision/action options. The enterprise is left with the difficult choice of accepting risk or missing potential opportunities. As we have learned from customers, the rate of increase of data volume is faster than their ability to triage and analyze the data; consequently, the analytic challenges are increasing with time. Customers are starting to realize that they need to rethink their processes and invest in more effective tools and analytics to get ahead of this challenge.

Cogility's mission is to improve the quality and efficiency of critical analytic processes. We offer Cogynt, a Continuous Intelligence platform that greatly automates low-level, highly time-consuming analysis by defining (behavioral) patterns that replicate human assessment (a form of AI[3]).

This paper describes the Cogynt CI platform from four perspectives: 1) technical capabilities; 2) organizational effectiveness and efficiencies; 3) decision complexity and risk, and 4) a phased approach to proactive risk mitigation (or timely exploitation of opportunity).

1 A socialtechnical environment consists of entities made of people and systems who exhibit observable behavior.
2 Robert Clark, *Intelligence Analysis; A Target-Centric Approach Fifth Edition*, 1st ed. (CQ Press, 2016).
3 David Luckham and David Luckham, "Is Complex Event Processing Part of Artificial Intelligence?," Real Time Intelligence & Complex Event Processing, March 2, 2019, https://complexevents.com/2019/02/28/is-complex-event-processing-part-of-artificial-intelligence/.

Cogynt: A Continuous Intelligence Platform: Technical Solution Overview

According to Gartner, "Continuous intelligence is a design pattern in which real-time analytics are integrated into business operations, processing current and historical data to prescribe actions in response to business moments and other events."[4]

Cogility has developed Cogynt, a streaming real-time analytic platform that very effectively resolves the challenge. Cogynt's patented, real-time analytic (Hierarchical Complex Event Processing or HCEP)[5,6,7] drives its analytic core. With its multiple additional platform capabilities, it aligns nicely with the Gartner CI framework, hence, the adoption of the CI term to describe the Cogynt platform.

Based on the Gartner CI framework—extended by Cogility to include the human—Cogynt consists of 5 basic elements:

1. **Event Stream Processing** – Cogynt ingests data from multiple concurrent data sources, processes the data in motion (real-time), and stores analytic results, making the results available to downstream data consumers.
2. **Real-Time Analytics** – Cogynt continuously processes streaming data, applying HCEP to filter and match events to hierarchical patterns. This process maintains the statefulness of the matched patterns while applying computations to the data; it contemporaneously applies Bayesian computations to calculate the statistical likelihood of future events. These statistical computations support risk analysis and opportunity predictions.
3. **Decision Automation / Augmentation and Support** – Cogynt ensures that decision-making is timely informed by the intelligence process. Decision-making is a complex process driven by operational requirements, policies, and risk. Because decision solutions are typically architected, Cogynt can implement/automate or augment decision-making processes. For the most consequential decisions, Cogynt supports investigative intelligence methods (e.g., link analysis) and collaborative case management capabilities to validate any system-generated risk.
4. **Business Process Integration** – Cogynt allows for other systems and applications to be integrated; thus, Cogynt can be a consumer of, or producer to, other systems or applications.
5. **Human** – the human directs the purpose of the CI platform by defining the patterns that the system looks for, defining the decision processes employed, and interpreting the results.

4 "Definition of Continuous Intelligence - Gartner Information Technology Glossary," Gartner, n.d., https://www.gartner.com/en/information-technology/glossary/continuous-intelligence.

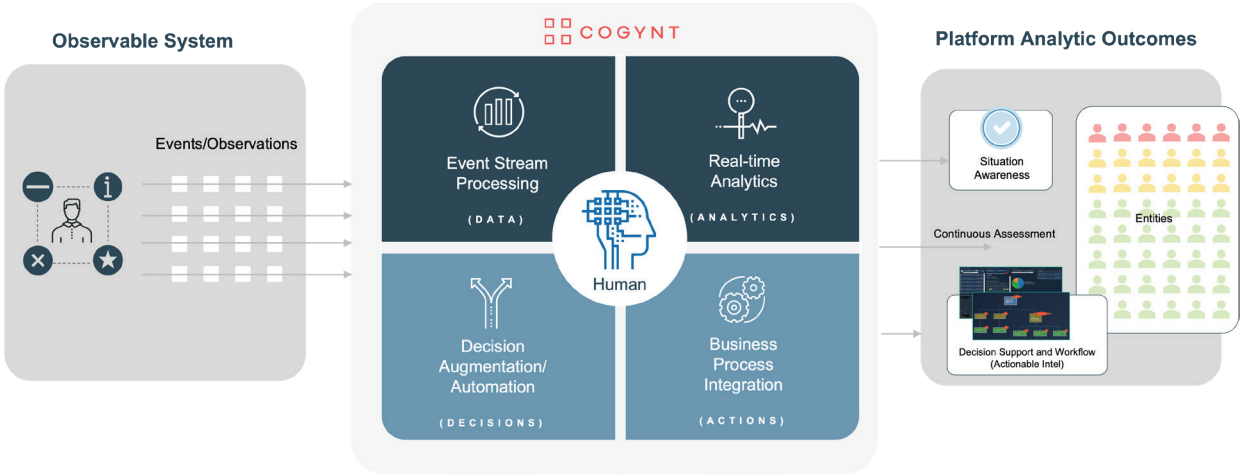
5 Hierarchical Complex Event Processing (HCEP) is Cogility's branded definition of Cogility's patented CEP technology.

6 Complex Event Processing (CEP) is a meta-framework of techniques (e.g., event filtering, event pattern matching, causal and timing analysis, hierarchical abstraction of events, construction of complex events, specification of event hierarchies) for processing flows of events in real time and abstracting humanly understandable and actionable information from those event flows. https://complexevents.com/2019/02/28/is-complex-event-processing-part-of-artificial-intelligence/

7 https://complexevents.com/2019/02/28/is-complex-event-processing-part-of-artificial-intelligence/

The realization of the Cogynt CI platform is illustrated in Figure 1. The platform ingests data from a sociotechnical environment (observable behavior), processes "events" in real time, and maintains a stateful understanding of the world. As new information is ingested into the platform, it updates that understanding. This is critically distinct from non-streaming systems, which require queries to update the understanding. As the scale increases, a query-based approach starts to break down due to latency and steeply increasing query costs.

Figure 1. Cogynt CI Platform End to End Solution



The outputs from the Cogynt CI platform include an enterprise Business Intelligence (BI) dashboard for visualizing trends and viewing aggregated analysis, and an analyst workstation enabling detailed forensic analysis. The analyst can granularly research (audit) a system generated notification and validate (or invalidate) that notification.

The Analyst Workstation supports team collaboration and case file management for typically high decision risk situations, such as insider threat, or other high consequence decision-making.

Cogynt is also nondisruptive to an existing enterprise ecosystem. It provides the ability to ingest and stream events to external applications or databases that serve the enterprise's data and analytic needs.

Finally, Cogynt is an elastically scalable platform ideally suited to be in the Cloud. Cogynt currently is deployed and running at scale in Amazon Web Services (AWS) and Google Cloud Platform (GCP). The Cogynt CI platform is employed and operating on several extremely large-scale applications in cyber threat intelligence, and the Counter-Insider Threat Professional Program for the federal government.

In summary, Cogynt is a highly scalable CI platform that can analyze extremely large threat surfaces (e.g., cyber infrastructure threat analysis, threat IP addresses, insider threats). It performs continuous assessment on the entire problem domain to provide predictive intelligence. In this context, predictive intelligence refers to the real-time assessment of behavior and the statistical likelihood that a future event might occur. This unique insight enables the analysts (and consequently the entire enterprise) to be proactive rather than reactive.

The balance of this paper explains how the Cogynt CI platform applies predictive intelligence in shrinking the proverbial haystack. This capability enables precious human analyst resources to focus on the highest and most consequential risks/opportunities effectively and most efficiently.

Continuous Intelligence: Organization Effectiveness and Efficiency

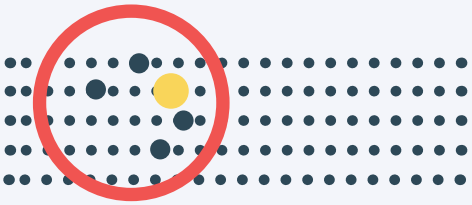
An effective intelligence process starts with the clearest possible understanding of the problem or the issue under scrutiny. A wide array of techniques is available for achieving this clarity—(beyond the scope of this paper) but it is worth mentioning because developing intelligence on the wrong problem is a common and wasteful investment of time and resources.

There are several "systems thinking"[8] techniques for understanding the intelligence problem. The Structure Analysis Techniques (SAT)[9] is one such method—specifically developed for intelligence practitioners. SAT applies rigorous techniques for problem understanding and definition and the development of directly pertinent intelligence. Using SAT or other approaches serves as an essential starting point to define the target of the analysis. Once this definition is represented in Cogynt's zero-code authoring environment, the analyst uses Cogynt to create a model that determines how the analysis will process the data and generate actionable intelligence.

This continuous process is easily adaptable to changing environments, priorities, and conditions.

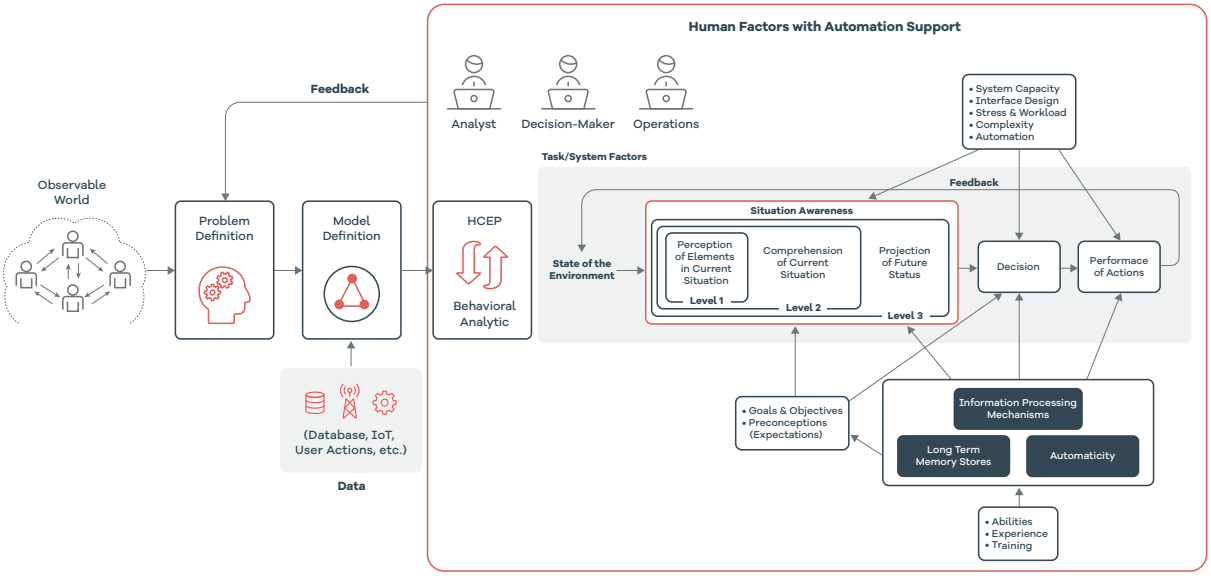
Once the model is established, deployed, and running, CI then becomes a human-centered process that enables the analyst to acquire effective Situation Awareness (SA)[10] and leverage the insight: this helps to "project future status" and thus facilitates effective decision-making, which is the goal of any intelligence process. Figure 2, developed by Mica Endsley describes a closed loop process that is a reasonable approximation of what an intelligence team (analyst, decision makers, and operations) must do to develop actionable intelligence, inform decision makers, and identify the best action(s) from multiple potential alternatives. This continuous process is easily adaptable to changing environments, priorities, and conditions.

8 https://en.wikipedia.org/wiki/Systems_thinking
9 https://www.intelligence101.com/structured-analytical-techniques/
10 https://en.wikipedia.org/wiki/Situation_awareness



The goal of the Cogynt CI platform is to enable this process for the intelligence analyst who develops the SA for decision makers—and to accomplish this task as efficiently and effectively as possible. Note, as indicated in Figure 2, that external influences (such as “stress of workload and insufficient information processing mechanisms and interface design”) may impact this process and possibly hinder SA development.

Figure 2. Model of Situation Awareness in Dynamic Decision Making (Endsley, 1995)



The Cogynt CI platform positively addresses these “external” challenges by reducing analyst workload and stress, through HCEP automation of analysis and an intuitive user interface. The design allows analysts to work at “think speed,” to quickly analyze system generated intelligence and validate that intelligence. Information processing is also fully addressed with the use of the cloud with almost infinite computing resources available to handle the largest workloads. Of course, very large analytic problems might drive operational cost. Storage and computation costs, for example, must be weighed against the overall benefit of mitigating potential risk, or timely seizing opportunity.

Cogynt Continuous Intelligence: Decision Risk and Latency

To support decision-making processes and apply prudent automation, Gartner[11] has identified three classes of decision-making based on decision complexity and risk, shown in Figure 3. Decisions considered low-risk and simple are most readily supported by automation, while those with medium decision complexity and risk are more appropriately supported by decision augmentation, which provides structured options to the decision makers. For complex or chaotic decision environments, decision-making is considered high-risk and decision support is best applied.

In the case of the Counter-Insider Threat Program, which involves the complex task of predict-ing human behavior, it is, in every instance, critical to make the correct assignment of risk and accurately calculate a person's insider threat risk. Based on the Gartner framework, a decision support strategy is best applied. This requires that Cogynt's extensive automa-tion be supplemented by human in the loop processes, aided by Cogynt's continuous risk assessment.

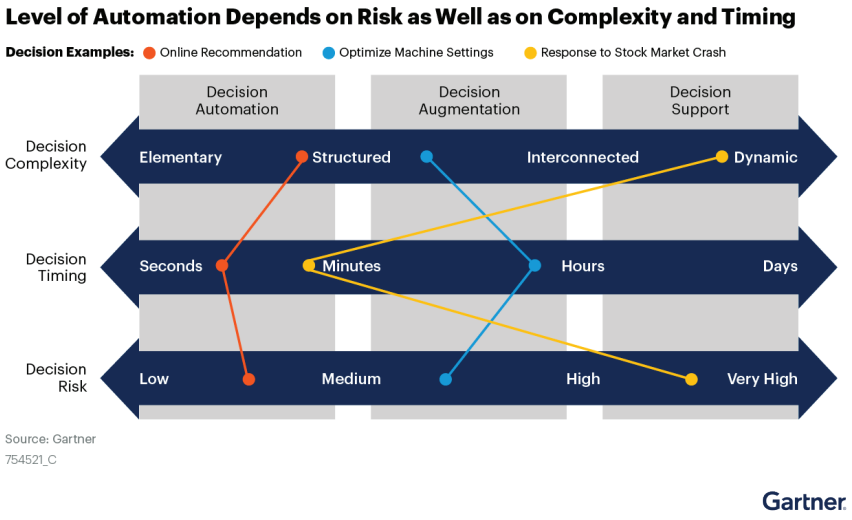
Decision timing is also a factor to consider in decision-making: the value of the information depends, in large measure, on how quickly an optimal decision must be made. The response time from receiving an event to establishing SA and projecting the future (per the Endsley model) should be as short as possible, allowing the decision maker the maximum amount of time to make timely and informed decisions.

In the case of cyber security, fast decision times (seconds) afforded by automated decision-making can prevent a breach—adding a human in the loop process could obviate the benefit.

However, when intensive human investigative efforts are needed to support decisions that carry high risk—within highly dynamic and chaotic environments—hours, days, or even weeks may be acceptable decision latencies for solution approaches in the category of decision support.

The Cogynt CI platform contemporaneously supports all three types of decision processes shown in Figure 3. As a result, Cogynt CI can simultaneously address many different decision scenarios, enabling organizations to be proactive in response to highly dynamic environments.

Figure 3. Decision Complexity, Risk, and Latency



11 https://www.gartner.com/document/4017721

Cogynt Continuous Intelligence: Phased Approach to Proactive Risk Mitigation

In summary, Cogynt CI is a behavioral analytic platform that analyzes big data and provides highly scalable, real-time actionable intelligence and decision support. Continuous intelligence is a pipeline process consisting of three phases of analysis to inform and determine appropriate action. These three phases consist of: Activity-Based Intelligence, Investigative Intelligence and Decision-making-Action. Each of these three activities apply different processes that work in conjunction with one another to: a) achieve the desired intelligence outcome / action outcome, b) be predictive, c) to reduce uncertainty, and, d) to mitigate risk (or leverage opportunities).

Phase I: Activity Based-Intelligence (ABI)[12] is applied to filter or triage the entire entity population for behavioral patterns, and to apply risk assessment on a continuous basis. For certain patterns within the population, if a threshold is met, and depending on the predetermined decision risk criteria, a risk notification can result in a decision that—at user discretion—may be automated, augmented, or enriched through investigative intelligence. The benefit of this approach is that the entire entity population can be continuously monitored, and the associated risks can best be handled based on operational requirements, thus allowing for optimal risk management. Figure 4A illustrates this process, which can be visualized as a funnel. At the mouth of the funnel there is the complex sociotechnical environment and entity population, where all the observed events are ingested and processed. The entity behavior is assessed, demonstrating how automation and risk-based behavioral assessments can be effectively derived and managed at significant scale. This process, moreover, organizes the risk based on "decision risk criteria"—each risk is appropriately handled by the decision or investigative intelligence process.

> Continuous intelligence is a pipeline process consisting of three phases of analysis to inform and determine appropriate action.

12 *"Activity-based intelligence (ABI) is an analysis methodology that rapidly integrates data from multiple sources to discover relevant patterns, determine and identify change, and characterize those patterns to drive collection and create decision advantage. ABI practitioners have advanced the concept of large-scale data filtering of events, entities, and transactions to develop understanding through spatial and temporal correlation across multiple data sets."* Patrick Biltgen, Ph.D.; Todd S. Bacastow, Ph.D.; Thom Kaye; and Jeffrey M. Young, 2017, United States Geo Intelligence Foundation

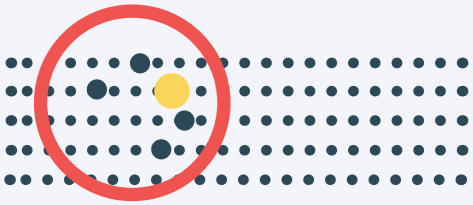
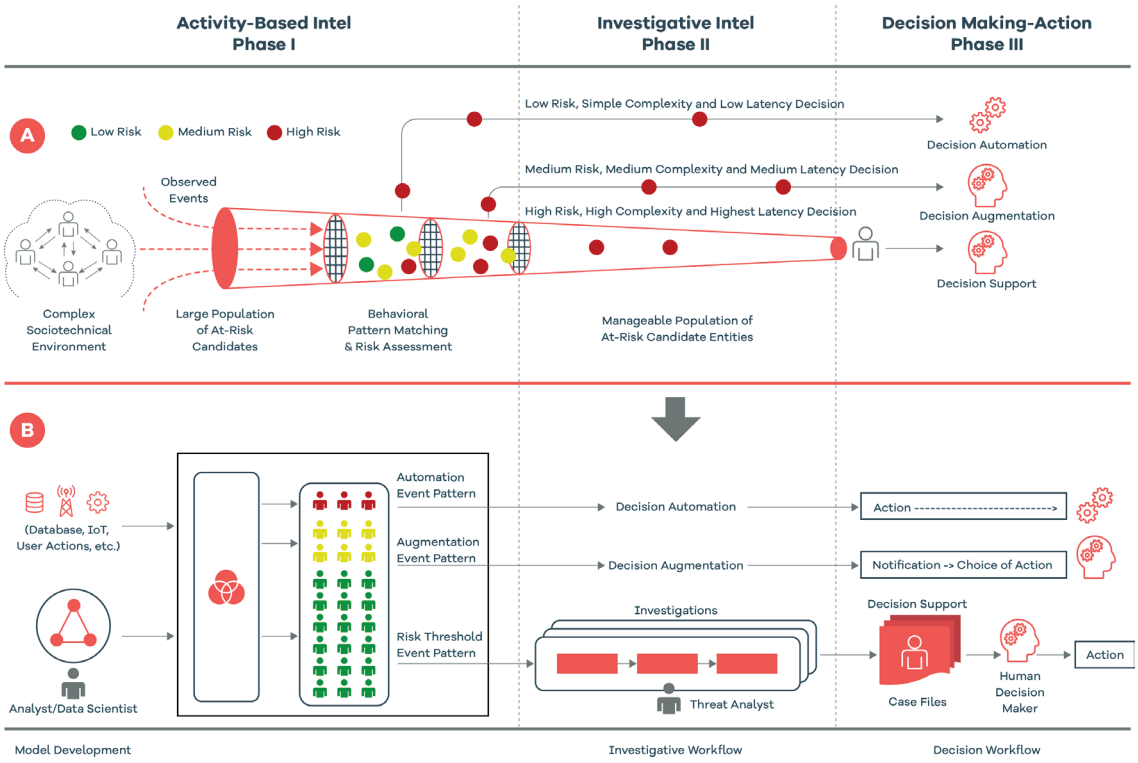


Figure 4. Cogynt–Continuous Intelligence Risk Management and Decision Management Approach



Phase II: Investigative intelligence[13] is best applied to situations that require the most detailed possible knowledge about an entity and its pattern of life. Because investigative intelligence is very thorough, time consuming, and human intensive, it is best applied to high-risk (i.e., highly consequential) decisions. One of the traditional limitations of investigative intelligence is that the analyst must start with an already identified target. ABI helps solve this problem. ABI serves as the target generator for investigative analysis. Figure 4B illustrates this process. The entity population is stratified based on risk, and investigative intelligence is applied to those entities exhibiting the risks that the policy has designated for some level of more detailed review, or intercession. The analyst applies their workflows that culminate in a case file for further assessment, decision-making, and follow-up action.

Phase III: Decision-making action is the application of highly informed risk management processes. Depending on the risk and pertinent operational requirements, some decisions are best made within milliseconds, while others can be made within hours or even days, as illustrated on the right of Figure 3. The decision framework is based on decision risk—the decision architect needs to define how best to strike the balance between decision risk and automation to proactively mitigate risk.

Cogynt provides the means by which a thoughtful decision framework can be implemented. The process consists of decision automation, augmentation, and support. Figure 4 illustrates the CI process—how decision-making is informed and enabled, and the preemptive or otherwise responsive actions that can be implemented.

13 Investigative intelligence is used to develop patterns of life for individual entity or group that commonly applies techniques such as link analysis, timeline analysis to fully assess the risk.

Conclusion

Today's intelligence analysts and decision-makers, and by extension the enterprise, confront intelligence challenges of enormous scale and complexity, involving problem domains addressing both risk and opportunity. To be competitive, the enterprise needs to adapt to the increasing, dynamic challenges of the sociotechnical environment when the data and complexity exceed the capability of legacy solutions.

CI provides the means to address and get ahead of these challenges, and to thereby position the enterprise to proactively manage both risk and opportunity.

The Cogynt CI platform is a mature CI solution that can be quickly instantiated and will deliver value to most any enterprise for the types of challenges described in this paper.