

# Cogynt – Continuous Intelligence Explained

“

*"Intelligence is the ability to adapt to change"* \_Stephen Hawking.

## Introduction

The objective of the Cogynt Continuous Intelligence (CI) platform is to reduce the uncertainty of decision making in time sensitive, highly complex sociotechnical<sup>1</sup> environments, 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.”<sup>2</sup>*

The challenge and opportunity for current intelligence analyst 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, and 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.

---

<sup>1</sup> A social technical environment consists of entities made of people and systems who exhibit observable behavior.

<sup>2</sup> Intelligence analysis: a target-centric approach/Robert M. Clark, 5<sup>th</sup> edition, 2016

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

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

## Cogynt: A Continuous Intelligence Platform: Technical Solution Overview

Continuous Intelligence (CI) is a term derived from a Gartner report (W. Roy Schulte)<sup>45</sup> addressing a commercial challenge - analyzing big data in motion (on a continuous basis) and gleaning actionable insights from that data. 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)<sup>678</sup> 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:

- **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;
- **Real-Time Analytics** -Cogynt continuously processes streaming data, applying HCEP [ a form of Artificial Intelligence (AI)] 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

---

<sup>3</sup> <https://complexevents.com/2019/02/28/is-complex-event-processing-part-of-artificial-intelligence/>

<sup>4</sup> Gartner Paper: Innovation Insight for Continuous Intelligence; W. Roy Schulte, Thomas Oestreich, Melissa Davis, Pieter den Hamer: 7 August 2020

<sup>5</sup> Gartner Briefing: Five Best Practices for Real-Time Analytics and Continuous Intelligence; W. Roy Schulte

<sup>6</sup> Hierarchical Complex Event Processing (HCEP) is Cogility's branded definition of Cogility's patented CEP technology.

<sup>7</sup> *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. HCEP is generally intended for high-speed, real-time event processing in business or governmental situations where critical decisions must be made quickly at a human management level based upon large flows of low-level event data."*

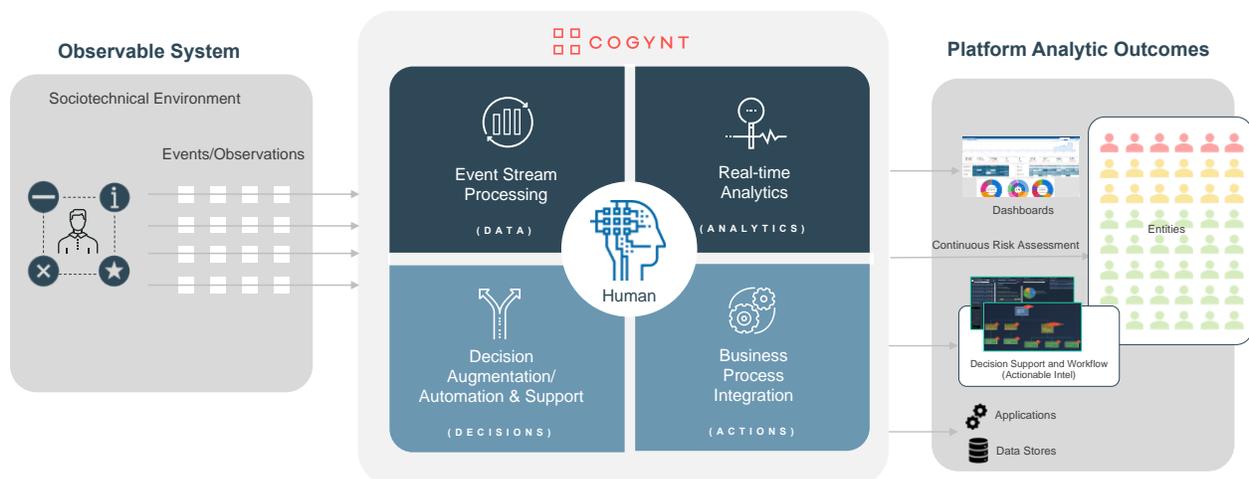
<sup>8</sup> <https://complexevents.com/2019/02/28/is-complex-event-processing-part-of-artificial-intelligence/>

calculate the statistical likelihood of future events. These statistical computations support risk analysis and opportunity predictions;

- **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;
- **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;
- **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.

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 .

The outputs from the Cogynt CI platform include an enterprise 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.



*Figure 1 Cogynt CI Platform End to End Solution*

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 non disruptive to an existing enterprise ecosystem, it provides the ability to ingest and stream events to external applications or databases that serves the enterprises' 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 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 there is a 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 effectively and most efficiently focus on the highest and most consequential risks/opportunities.

## 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"<sup>9</sup> techniques for understanding the intelligence problem: The Structure Analysis Techniques (SAT)<sup>1011</sup> 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

---

<sup>9</sup> [https://en.wikipedia.org/wiki/Systems\\_thinking](https://en.wikipedia.org/wiki/Systems_thinking)

<sup>10</sup> Structured analytic techniques for intelligence analysis/ by Richard J. Heuer, Jr., and Randolph H. Pherson

<sup>11</sup> Trade Craft Primer, United States Government, 2009

“model” that determines how the analysis will process the data and generate actionable intelligence.

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) and leverage the insight: this helps in “projection of future status” and thus facilitates effective decision making, which is the goal of any intelligence process. Figure 2, developed by Mica Endsley (United States Air Force)<sup>12</sup> 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.

The goal of the Coglynt 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.

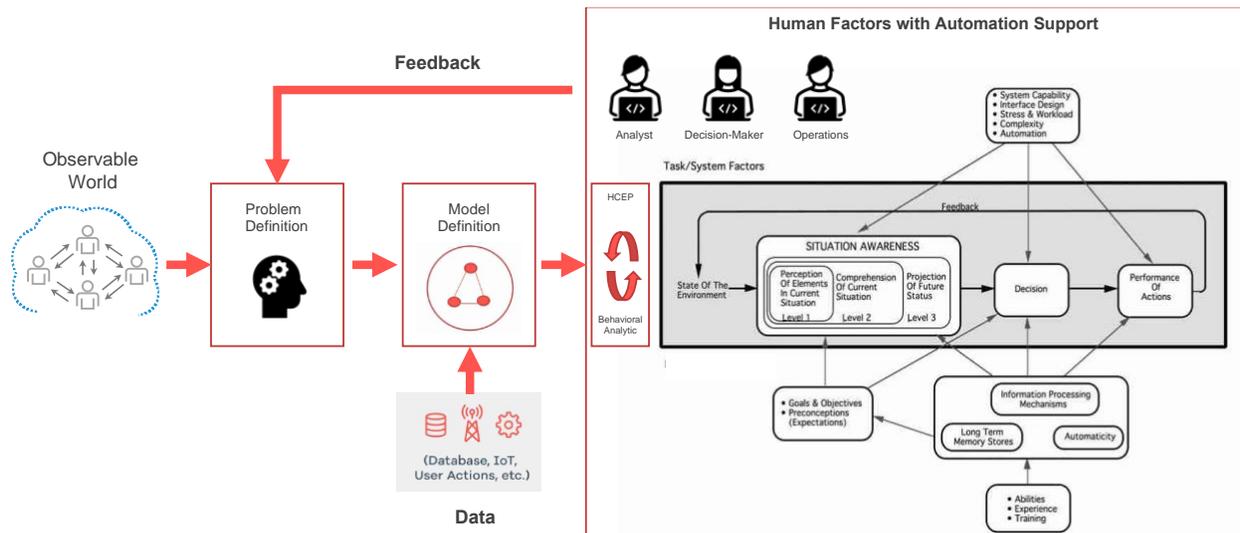


Figure 2 Model of Situation Awareness in dynamic decision making (Endsley, 1995)

The Coglynt 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

<sup>12</sup> Situation Awareness Misconceptions and Misunderstandings, Mica R. Endsley, United States Air Force. *Journal of Cognitive Engineering and Decision Making* 2015, Volume 9, Number 1, March 2015, pp 4-32

computation costs<sup>13</sup>, for example, must be weighed against the overall benefit of mitigating potential risk, or timely siezing opportunity.

## Cogynt Continuous Intelligence: Decision Risk and Latency

The Endsley model clearly identifies that a decision must be made based on predicted future events. Decision making is a complex process that needs to be architected<sup>14</sup>. To support decision making processes and apply prudent automation, Gartner<sup>15</sup> 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 Counter-Insider Threat Program, which involves the complex task of predicting 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 automation 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. Latency in the analytic decision process reduces the value of information to the point of being useless. 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 environment--hours, days, or even weeks may be acceptable decision latencies for solution approaches in the category of decision support.

---

<sup>13</sup> Cloud costs should always be a consideration in any analytic process. Amazon and Google provide cost calculators that you can use to understand the cost prior to setting up the infrastructure and deploy analytic jobs.

<sup>14</sup> Gartner Paper: *How to Manage the Risks of Decision Automation*; 20 January 2020, Pieter den Hamer, W. Roy Schulte

<sup>15</sup> Gartner Briefing: *The Future of Data and Analytics: Reengineering the Decision*, 2025; Briefing: Frank Buytendijk, Pieter den Hamer, Gareth Hercschel, Jorgen Heizenberg, Mike Rollings, Erick Brethenoux

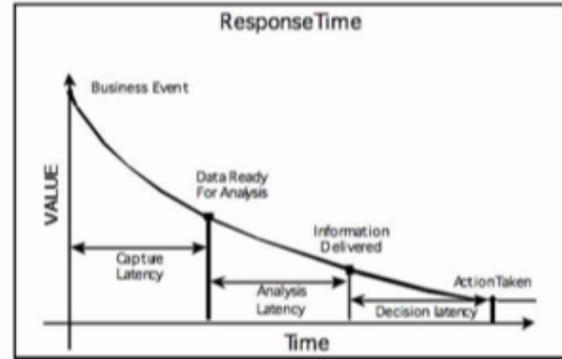


Figure 3 Decision Complexity and Risk<sup>16,17</sup>

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

## Coglynt Continuous Intelligence: Phased Approach to Proactive Risk Mitigation

In summary, Coglynt 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)<sup>18</sup> is applied to filter or triage the entire entity population for behavioral patterns, and to apply risk assessment on a continuous basis. For

<sup>16</sup> Gartner Paper: *How to Manage the Risks of Decision Automation*: 17 August 2022, Pieter den Hamer, W. Roy Schulte

<sup>17</sup> <https://www.brcommunity.com/articles.php?id=b373>

<sup>18</sup> “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,

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.

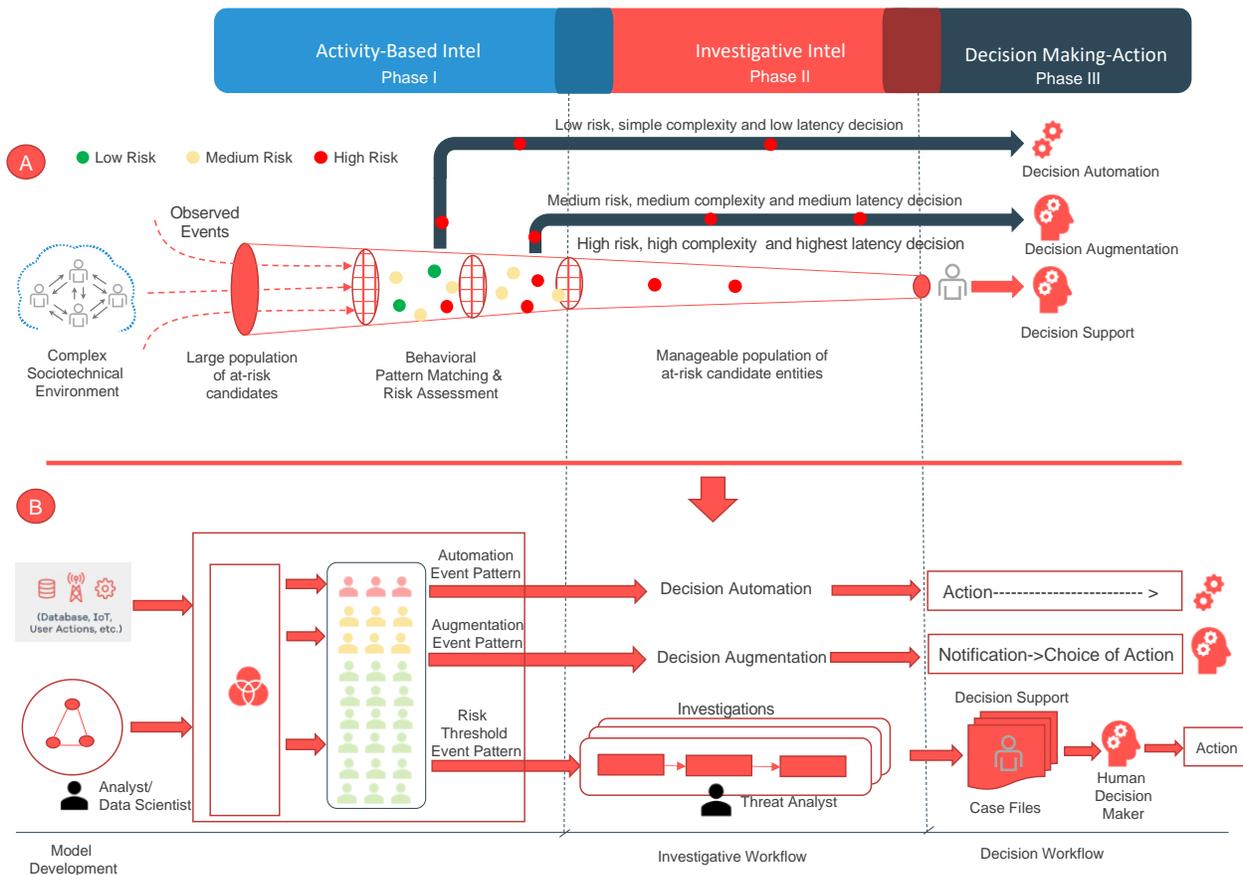


Figure 4 Coglynt - Continuous Intelligence Risk Management and Decision Management Approach

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

Phase II: Investigative intelligence<sup>19</sup> 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. This is where ABI helps solve the 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 tagged for more detailed review, or intercession. The analyst applies his or her workflows that culminate in a case file for further assessment, decision making, and follow-on 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.

## 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 acknowledge and address the challenge that today's data volume, complexiy and speed exceed the capability of legacy solutions. CI provides the means to address and get ahead of this challenge, 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.

---

<sup>19</sup> 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.