COGILITY

Cogynt – Continuous Intelligence

Decision Advantage leads to Competitive Advantage

Introduction

The demands of Counter-Insider Threat (C-InT) assessment to fully address the insider threat analysis problem exceeds currently fielded solutions and overwhelm the cognitive limitations of C-InT professionals. In contrast to current practice that is largely reactive, a continuous intelligence platform with an advanced behavioral analytic is needed to achieve a comprehensive, proactive C-InT program that can handle the data analytic demands and decision support for C-InT professionals who cannot afford to get it wrong. Analysis of behavioral as well as technical data in a predictive analytics environment will deliver a whole person C-InT program that helps to predict potential insider threat risks so that risk mitigation efforts can be applied to help deter or avoid insider threat incidents.

In today's connected world, enterprises are swimming in an ocean of events and data. These signals — generated within the enterprise and connected to external parties and systems — must be monitored and assessed for risk or opportunity to the enterprise. Real-time situation awareness (SA) and predictive intelligence are needed to make rapid, informed decisions and respond to changing dynamics in the marketplace. The consequence of overlooked scenarios or delayed response can be catastrophic for the enterprise. Cyber threats, insider threats, IoT operations, operational safety and other risks can quickly manifest into cyber breach, reputation damage, increased insurance premiums, lost market share — all affecting the organization and the bottom line.

Enterprises have realized that they can't just hire people to get ahead of the problem: They need smart solutions and processes that better utilize their current staff to get left of harm or to capitalize on opportunities. This decision advantage leads to competitive advantage.

With the emergence of event stream processing and real-time analytics technologies, Continuous Intelligence (CI) solutions offer an effective response to these challenges. A CI solution must have the right balance between automation and human-in-the-loop (HIL) in providing real-time SA, real-time analytics, and decision support. These enablers help the staff focus on the right challenges (risks or opportunities) and ensure that the best intelligence is made available to the decision makers.

Cogility has developed Cogynt, an integrated CI platform that amalgamates multiple data sources and performs behavioral analytics to deliver real-time SA, predictive analytics and decision support at cloud scale. Cogynt enables an enterprise to have rapid, high confidence intelligence allowing decision makers to make informed decisions in the most complex time sensitive situations.

Definition of Continuous Intelligence (CI)

Continuous intelligence is an advanced analytics paradigm that leverages data stream processing and real-time analysis to provide instantaneous insights and actionable recommendations. It integrates data from multiple sources and offers ongoing analysis to aid timely decision-making across various scenarios. The primary characteristic of CI is its ability to process and analyze data continuously as it is generated, rather than in batch mode or at scheduled intervals.

Cogynt – A CI Platform

Cogility's Cogynt integrated CI platform comprises five essential elements of continuous Intelligence, with the human as a central element ensuring the results are valid and the context is clear when presented to decision makers, or when acting on automation results.

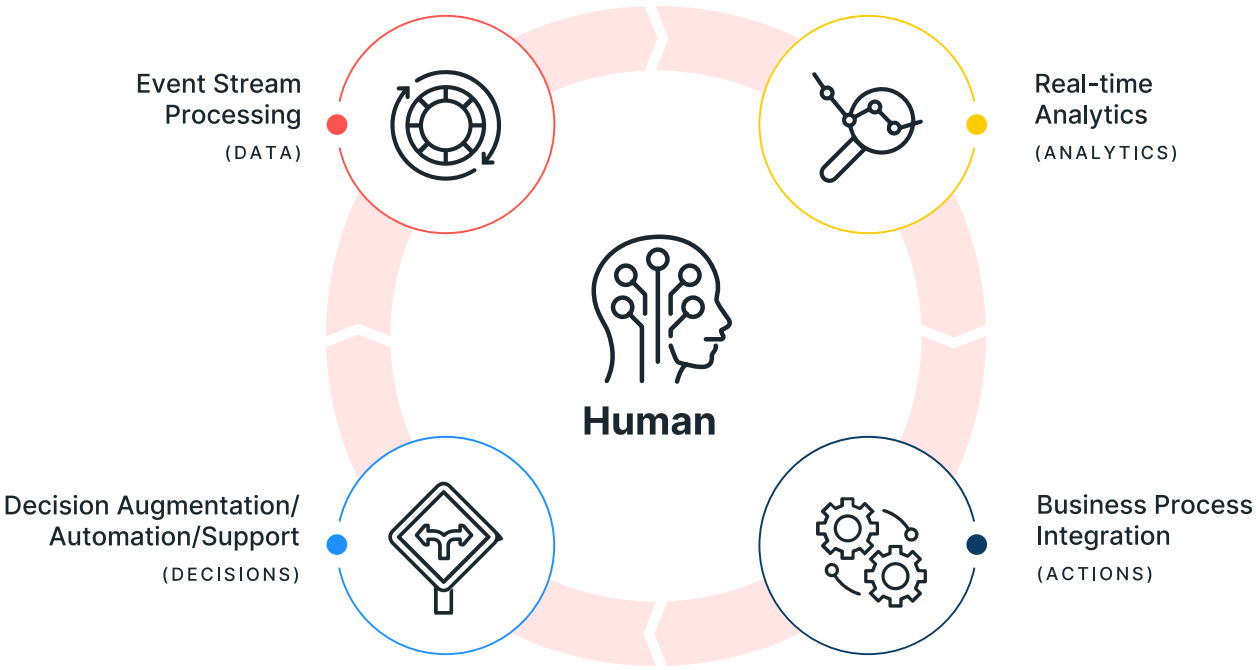

Figure 1. Cogynt CI Platform

The 5 essential CI elements are:

- **Event Stream Processing** are software systems that perform real-time or near-real-time calculations on event data “in motion”.
- **Real-time Analytics** based on Hierarchical Complex Event Processing (HCEP) detects patterns to generate higher level, more relevant summary data (complex events), while performing continuous risk assessment leading to informed insights and actionable intelligence.
- **Decision Augmentation/Automation/Support** provides effective situational awareness, automated notifications, event validation and workflow support.
- **Business Process Integration** allows for other systems and applications to be easily integrated.
- **Accounting for Human factors** to ensure the users (analysts and decision makers) are effective and efficient in performing their tasks which is achieved through a combination of automation and intuitive easy to use analysis tools that eliminates low-level and less productive tasking allowing the analyst to spend more time on what is important.

Cogynt CI Platform is a Force Multiplier

The Cogynt CI platform can be characterized as a force multiplier allowing organizations to easily scale and agilely respond to changes providing valuable contextualized intelligence without having to add additional personnel. The impact of Cogynt can be expressed in terms of:

- **Efficiency** — greatly improves the utilization of staff by focusing on the real problems (highest risks or opportunities), greater throughput, and faster decision making.
- **Capability** — continuous and stateful understanding of all entity risk (opportunity) with system generated notification that is auditable. This greatly increases confidence in the risk (opportunity) assessment.
- **Impact Amplification** — by empowering the analysts and decision makers to develop real-time, contextualized and auditable intelligence. This positions the enterprise to be more competitive, resulting in improved bottom-line performance.

Continuous Intelligence Explained

The goal of intelligence is to be predictive, enabling decision makers to anticipate impactful events and make informed, proactive (rather than reactive) decisions.

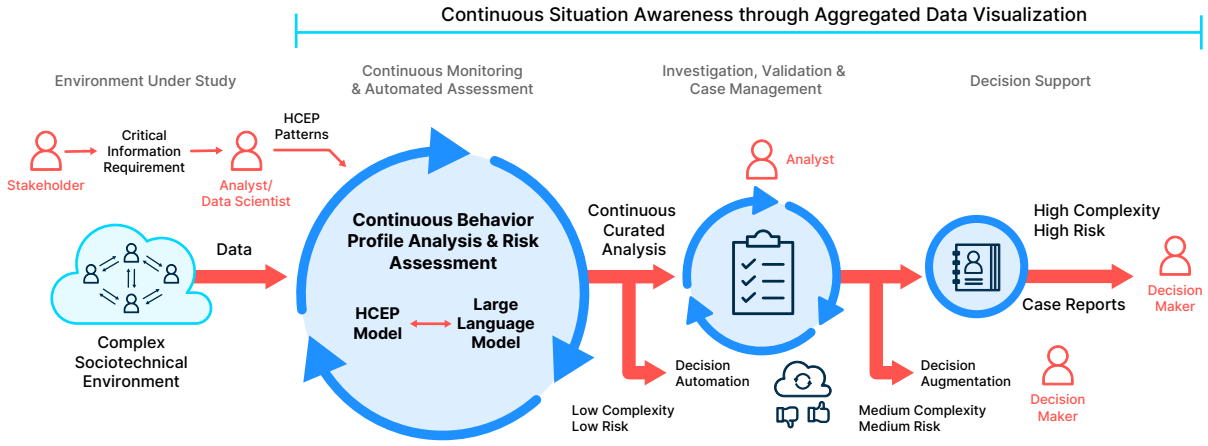

Figure 2. Cogynt CI Process

Good intelligence can be classified in terms of relevancy, actionability, confidence (e.g. risk) and timeliness. A seamless CI process includes the collection, analysis and decision-making approaches that best suit the organization's mission. As illustrated in Figure 2, Cogynt has embraced these concepts in building an integrated CI solution.

The Cogynt CI process provides powerful stream processing (data in motion) capability enabled by highly scalable Apache Kafka and Flink, which are market leading and proven stream processing technologies. These tools are augmented with Cogility's patented HCEP real-time analytic. HCEP, which is the analytic core that allows internet scale processing power, is further enhanced with Cogynt's easy to use no-code authoring environment enabling agility (to quickly define and deploy analytic changes) which is essential in reducing the typical software code-test-code-test cycles. As a result, the HCEP analytic produces highly curated analysis continuously to support flexible analysis and decision processes, from decision automation to case management to decision support.

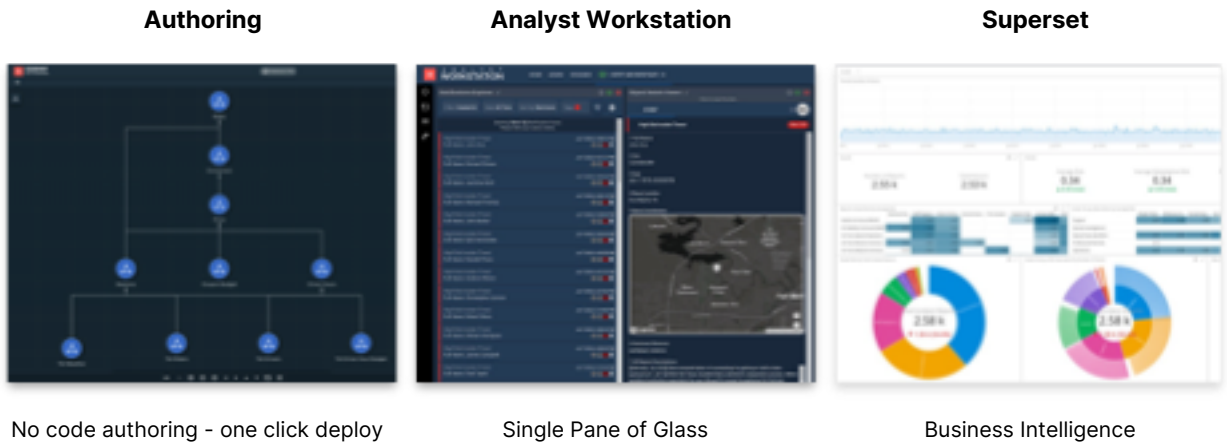

Figure 3. Cogynt CI Platform User Interface Examples

Figure 3 shows the Authoring, Analyst Workstation and Apache Superset BI Dashboard user interfaces. The curated analysis is made available through an intuitive UI, called Analyst Workstation, where the analysts have the flexibility to seamlessly evaluate and investigate any of the curated events to support a given intelligence investigation. Advanced SA is made available with both the Analyst Workstation for specific events and SuperSet for aggregated analysis. If a subject of intelligence is deemed necessary, Cogynt has an advanced case management capability that allows any workflow process to be defined allowing for team collaboration to ensure the curated analysis is fully vetted. In many cases this ensures specialists' contributions are considered at the proper times.

Cogynt CI Real-Time Analytic – HCEP

Cogynt is distinguished from all other streaming or CI platforms because of HCEP. A form of expert-based AI, HCEP is based on five basic principles:

- **Computational Hierarchy** — which is in the form of a Directed Acyclic Graph (DAG). This allows for increasing levels of abstraction which is essential in transforming data into insight.
- **Stateful CEP** — is stateful in that the HCEP DAG maintains its history of matched or partially matched patterns. This is critical for auditability, validity assessments and responding in real time to complex situations with historical components.
- **Continuous Risk Assessment** — for fully or partially matched patterns, statistical events are generated based on Bayesian or other preferred risk model approaches. This continuously reevaluates risk for all new data upon arrival.

- **Manual Actions** — this allows for an analyst to refute pattern matches, based on a potential false positive or other reason, and Cogynt will automatically recompute the risk score and all other implications of the change.
- **Event Pattern Constraint Language (EPCL)** — is a no code domain specific language that allows analysts and data scientists to easily create and deploy behavioral models applying HCEP principles.

HCEP empowers the analyst to discover difficult to detect signatures or profiles that many rule-based and ML solutions will miss. HCEP is expert driven, with the power of hierarchical stateful event pattern matching. ML can be limited due to the lack of training data and it is ill-equipped to identify new signatures that are not represented in training data. Rule-based systems often reach a level of complexity where it is too difficult to manage, and they are not stateful. The advantages of Cogility's HCEP capability have been demonstrated with AI Bot swarm detections that social media companies have not been able to detect. For more information, please see the YouTube video recently posted https://www.youtube.com/watch?v=afuY8hXVop8

Use Cases Across Industries

Cogility sees a range of cross industry applications for CI where comprehensive and real-time SA and actionable intelligence are critical:

- Public safety and security,
- Cyber security
- Healthcare
- Manufacturing
- Energy
- Financial
- Etc.

Challenges and Considerations

Many of the streaming analytic technologies are available for free from Apache Foundation such as Apache Kafka, Flink and Pinot, but unless you or your company have tremendous technical depth to package these technologies, it will be a very difficult undertaking. Cogility offers Cogynt as a complete CI solution that can be deployed within a few hours, and you can start building your application almost immediately with some authoring training and with Cogility's expert consulting support.

Conclusion

Continuous intelligence is a new class of analytic platforms enabled through event stream processing, real-time analytics, decision automation, augmentation and support, and business process integration. CI offers the ability to reduce operational risk, enhance decision making in the most complex operational environments where timely and informed decision making is essential to your competitiveness.

COGILITY

Visit **www.cogility.com/counter-insider-threat** to obtain more information and request an expert demo.

Cogility
15495 Sand Canyon Ave. #150
Irvine, CA. 92618

sales@cogility.com
+1 949.398.0015

01/25