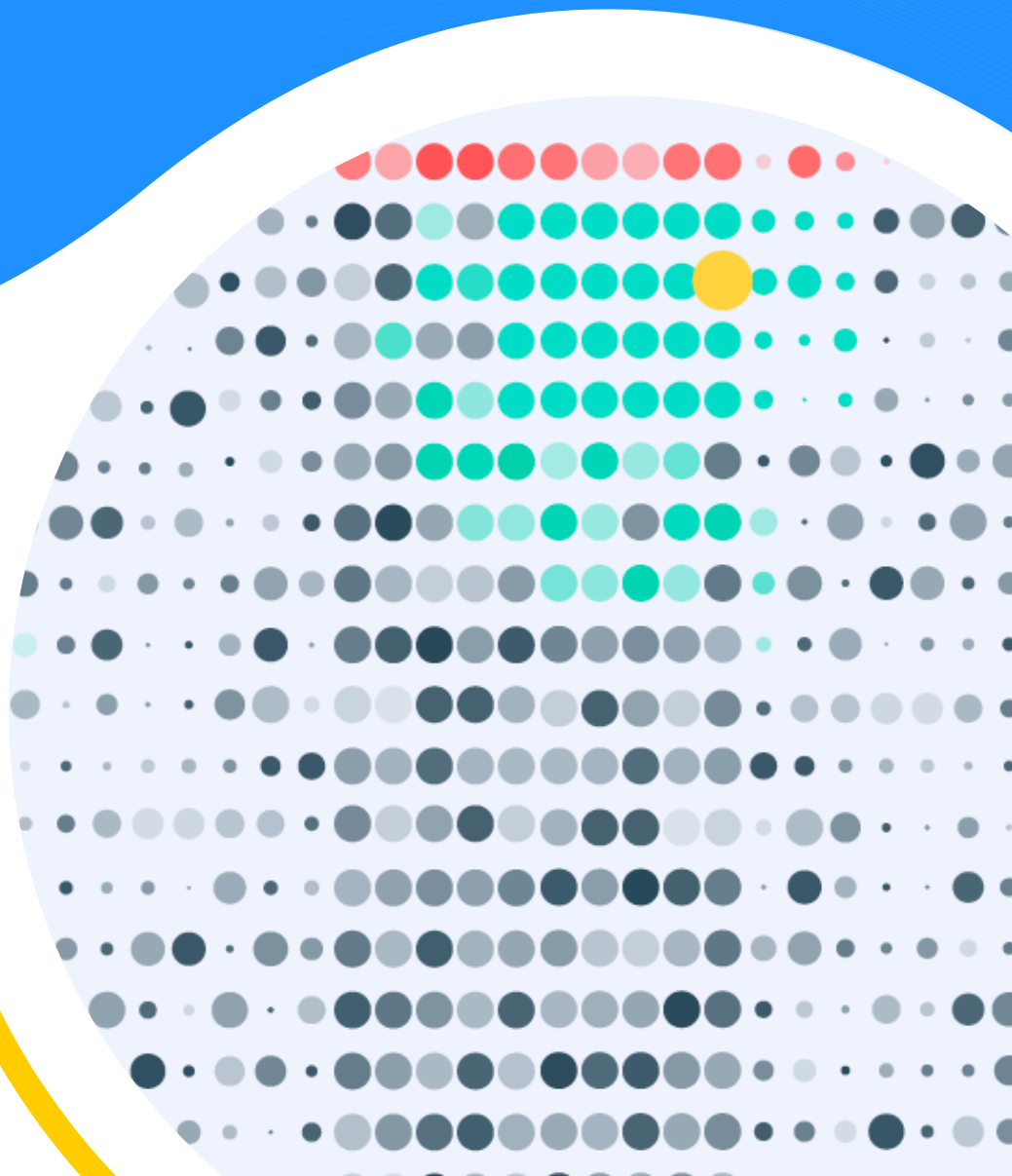


Cogynt – a Unified Real-Time Platform for **Continuous Intelligence**

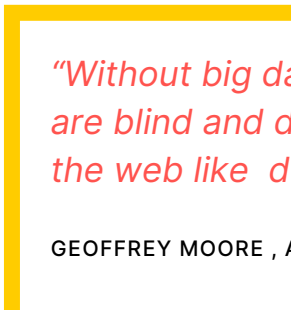


Introduction

Intelligence analysts and decision makers, and by extension the enterprise, are largely behind the curve when it comes to implementing effective predictive intelligence solutions. This is due to the ever-expanding flow of data and the limitations of current IT and analytic systems. Analysts are simply overwhelmed, resulting in unquantifiable risk exposure and lost opportunity for the enterprise.

At Cogility, we regularly hear from executives and operational managers that the intelligence solutions and staffing in place can, at best, adequately track only Level 1 and Level 2 risks (i.e., the highest level risks). Their concern is Level 3 and Level 4 risks: these cannot be adequately tracked with existing resources, could at any moment evolve into higher risk, and will evade detection because their current intelligence solutions and staffing don't have the level of automation or bandwidth to identify and monitor them. This challenge is common to both government and industry: it forces a conscious decision to monitor less than the entire risk surface.¹

Cogility has spent more than 10 years researching and developing technology to address this critical issue. The result of this effort, Cogynt, is a unified real-time platform (URP) which we believe provides the most comprehensive, versatile, and integrated continuous intelligence solution in the market, capable of taking on the most complex real-time decision-making challenges — efficiently and cost-effectively.



“Without big data analytics, companies are blind and deaf, wandering out onto the web like deer on a freeway.”

GEOFFREY MOORE , AUTHOR , AND CONSULTANT

1 Risk Surface is normally referred to in the context of cyber. In this paper, a risk surface considers all types of risk that include both technical and socio related risks.

What is Cogynt?

Cogynt is a URP that delivers continuous intelligence (CI) for analysts, data scientists, and decision makers. The platform integrates event streaming, advanced analytics, no-code modeling, and intelligence augmentation. Applying an expert AI approach, Cogynt enables analysts and data scientists to directly design models, examine results with full traceability, and optimize outcomes.

Cogynt accomplishes this by ingesting all available data and matching this data (events) — in real time — to targeted patterns of behavior. Targeted behaviors are those impacting risk levels or identifying the emergence of opportunity. These behavioral patterns, as discussed below, are in almost all instances well known by the enterprise's subject matter experts (SMEs), and can be easily incremented or modified as new information and insights dictate. Further, Cogynt continuously assesses risk (or opportunity) for each entity or developing scenario of interest to the enterprise.

During the continuous, real-time processing of data (events), if an analyst-defined threshold behavioral pattern is met, Cogynt publishes a new detection event. This instantly informs Cogynt Analyst Workstation (the investigative and visualization tool), or can be communicated to other applications in the enterprise.

Each event notification provides a wealth of information, including a quantified risk assessment with full provenance of all the underlying event history. This allows the analyst to quickly validate and understand the context of a given notification. In intelligence work, developing context is an essential, challenging, and time consuming task. Since Cogynt delivers this context on a continuous basis, precious analyst time and effort are saved. This results in timely notice, improved decision-making, and greatly expanded knowledge of the entire risk surface.

The Cogynt platform is a proven, scalable platform that is currently being applied in two broad market areas — counter-insider threat intelligence and cyber threat intelligence. In both, the demand for extensive, timely, and actionable intelligence is crucial. However, its capabilities to solve complex intelligence challenges in other industries knows no bounds.

What makes the Cogynt platform so powerful? Its integrated architecture, event streaming and behavioral analytic technology, no-code authoring, investigative and visualization functionality, and case management workflow.

At its core, Cogynt is a URP that delivers continuous intelligence (CI) for analysts, data scientists, and decision makers.

Cogynt Architecture

The Cogynt CI platform is a modern URP augmented with Cogility's patented real-time analytic, no-code authoring environment, and extensive integration capabilities. This system was built for big data problems that can be elastically scaled within cloud environments. Today, Cogynt supports VCP deployment in an organization's private cloud within cloud service environments: Amazon Web Services (AWS) and Google Cloud Platform (GCP). Figure 1 is a logical depiction of the Cogynt URP, summarized in the bulleted paragraphs below:

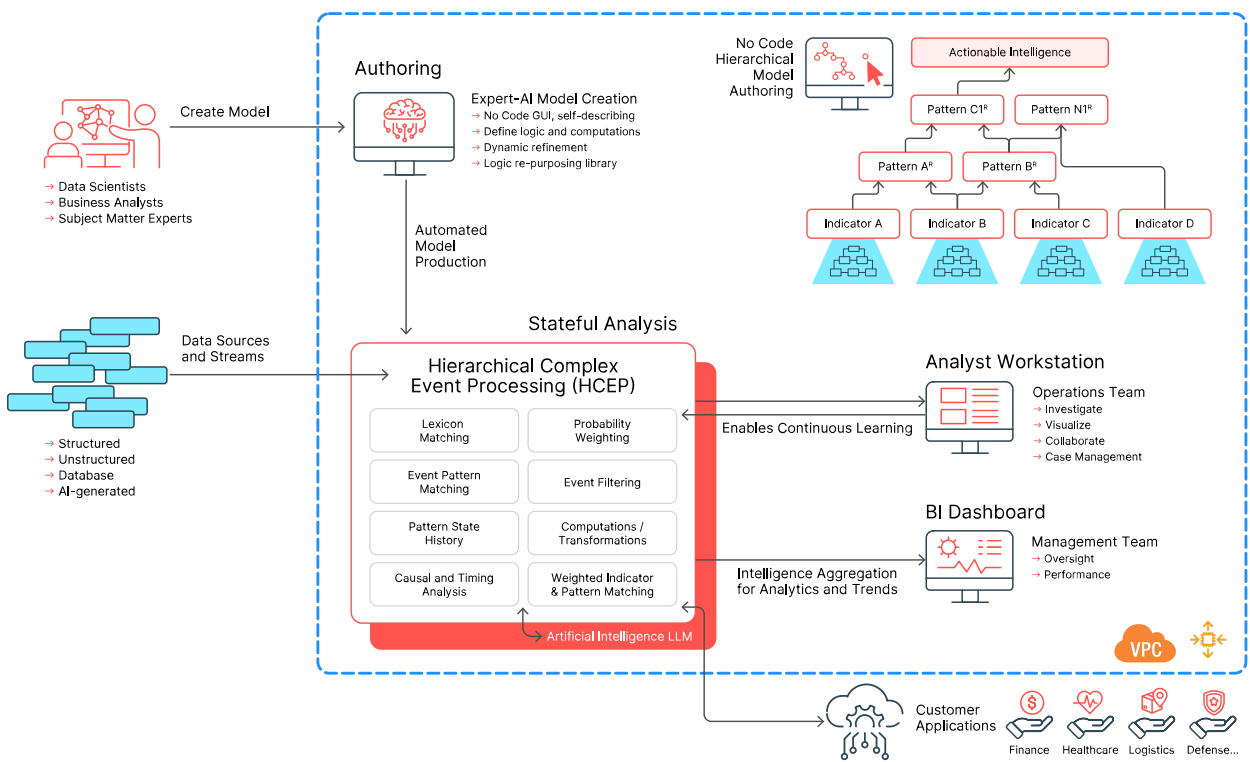


Figure 1. Cogynt Unified Real-Time Platform

The Cogynt platform components and their role within the architecture include:

- **Data Sources:** Streaming or batched data, including structured, unstructured, database and AI-generated data, are ingested via Apache Kafka connectors.
- **Cogynt Authoring Tool:** Used by the analyst to define/ manipulate lexicon, event patterns, computation logic, and risk models that comprise the Expert AI modeling created within a no-code GUI. Developed models are automatically produced for use in the HCEP engine.
- **Cogynt HCEP Analytic Engine:** Models are automatically configured within HCEP to produce analytic results that are streamed from Apache Flink to Apache Kafka and Apache Pinot for analytics and visualization. Results are displayed in the Workstation and Superset tools.
- **Analyst Workstation:** A dynamic and interactive user interface enabling the analyst to view insights, examine with widget apps, and trace predictive findings. Workstation enables the analyst to assess and add notation, as well as invoke extensive case management workflow features.
- **Artificial Intelligence LLM:** Forthcoming AI LLM will further enhance analyst experiences.
- **Business Intelligence (BI) Dashboard:** Provides overall performance and program oversight within a BI dashboard and enables access to any other preferred dashboards through Cogynt's open system architecture.
- **Applications:** As an open system, Cogynt insights can be shared with any event driven system or application.

Cogynt Analytic

The heart of the Cogynt URP is the Hierarchical Complex Event Processing (HCEP) engine, which is a real-time behavioral analytic. The principles of HCEP are rooted in system theory² and CEP.³ Figure 2 is a logical depiction of the end-to-end analytic process, as shown in the HCEP conceptual solution. The diagram illustrates how event patterns are defined from the top-down, starting with a hypothesis. The top-level event pattern is then decomposed into lower-level patterns until the user reaches the raw event level, or observation. Once the model has been established and events are flowing into the HCEP analytic engine, events are matched from the bottom up. Within HCEP, the organic component of a behavior is an event pattern, and an event pattern follows the principles of CEP, where an event pattern, if fully matched, creates a new complex event that can trigger a higher-level event pattern. This process continues until it satisfies the full behavioral profile — hence the reference to Hierarchical in HCEP. While this process is ongoing, Cogynt is continuously assessing risk, applying a Bayesian Belief Network⁴ or other weighted statistical methods, and calculating a statistical likelihood of future events occurring. The event generated from this analysis is known as “actionable intelligence” — contextualized intelligence that a human or system can act upon. Cogynt maintains the state of the event patterns over time, which allows analysts to look for trends and changes in event patterns and risks. This allows analysts to advise decision makers of maturing risk profiles and can allow for implementation of early mitigation strategies. Alternatively, Cogynt can continuously assess opportunities to allow analysts to advise decision makers of maturing opportunity profiles and can allow for implementation of early acquisition strategies for competitive advantage.

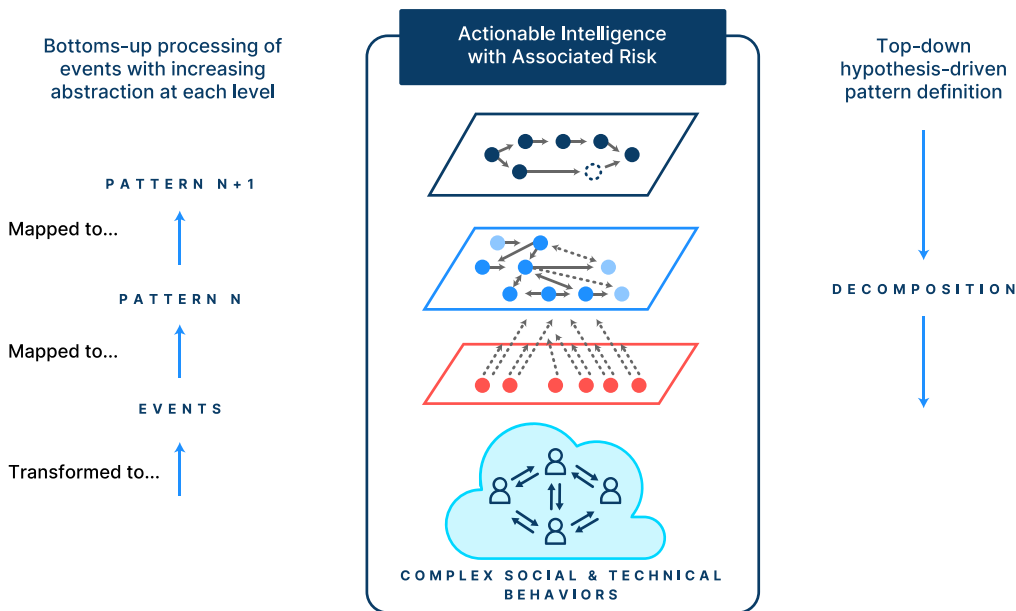


Figure 2. Logical depiction of Hierarchical Complex Event Processing

2 https://en.wikipedia.org/wiki/Systems_theory#:~:text=Systems%20theory%20is%20the%20interdisciplinary,and%20expressed%20through%20its%20functioning.

3 https://en.wikipedia.org/wiki/Complex_event_processing

4 Bayesian Belief Network: https://en.wikipedia.org/wiki/Bayesian_network

Applying an Expert AI approach, Cogynt is most strongly suited where AI/ML falls short — its ability to detect and track complex patterns of behavior that evolve over long periods of time, such as human behavior, or certain sophisticated cyber-attack scenarios, such as persistent threats.

The types of big data problems HCEP is well suited to solve are typically difficult to treat with current AI/ML analytics solutions. AI/ML have proven to be very effective in detecting certain types of patterns, such as speech translation, speech recognition, facial recognition, and many others. Applying an Expert AI approach, Cogynt is most strongly suited where AI/ML falls short — specifically, the ability to detect critical but infrequent events, and to track complex patterns of behavior that evolve over long periods of time. This includes areas such as human behavior, or certain sophisticated cyber-attack scenarios such as persistent threats. The approach provides full event traceability and negates potential AI hallucination and bias effects. In addition, Cogility’s forthcoming use of AI LLM within the Cogynt URP further enhances the assessment of unstructured data, no-code authoring, and its Analyst Workstation experiences.

As stated earlier, event pattern models are created using the no-code Cogynt Authoring tool, depicted in Figure 3, which describes the analytic process workflow.

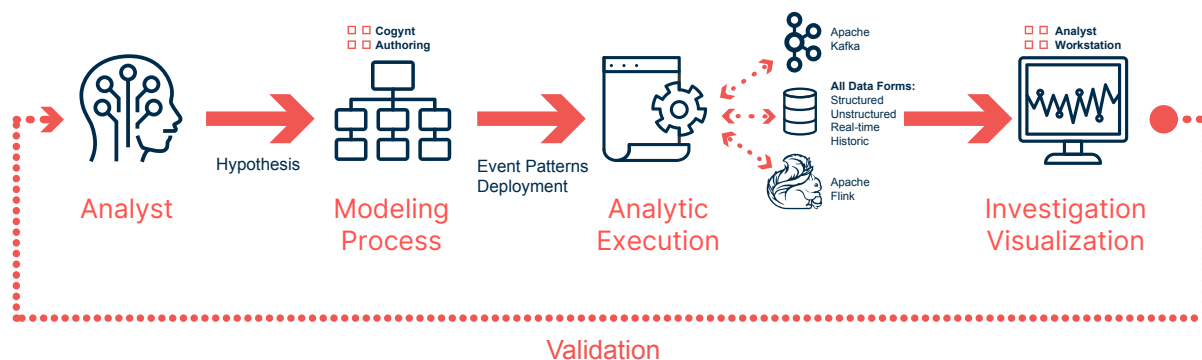


Figure 3. Cogynt End to End Analytic Process and Workflow

Figure 3 describes the basic Cogynt analytic process and workflow. Starting with the authored model (using The Cogynt Authoring Tool), the analyst can publish the model to the HCEP engine operating on Apache Flink. The analyst does not need to know further details about the coding process. The HCEP event pattern model deployment converts the model into a Directed Acyclic Graph (DAG), which defines the processing data flow within Apache Flink. At execution, the data sources are piped into Apache Flink, via Apache Kafka, and the analytic results are then stored back into Apache Kafka (not shown) and displayed within the Cogynt Analyst Workstation for viewing and analysis.

The Cogynt Authoring Tool, which is seamlessly integrated with Apache Kafka and Flink, greatly simplifies the challenge of creating, refining, and repurposing event patterns against streaming data. Its elegant modeling notation and semantics are easy to learn, enabling a novice analyst or data scientist to be productive in a matter of days. To accelerate an enterprise's learning, Cogility also offers training where team members develop the knowledge and skills to develop powerful event patterns and apply HCEP to solving what are typically very challenging analytic problems. The Cogynt Authoring tool provides a no-code modeling environment. This expands the analyst user base, who traditionally have limited coding skills, thus avoiding the need to involve software engineers to implement the analytic design through long software development lifecycles.

Typically, analysts must possess detailed technical knowledge of data sources and associated schemas and collaborate with data scientists to ingest them. The Cogynt Authoring tool eases this burden with its built-in Kafka Topic schema discovery — eliminating manual schema creation and mapping to source data. Cogynt Authoring tool and analytic process also handles changes elegantly. For example, a data scientist and analyst expressed more effective and efficient operations when comparing Cogynt to Apache NiFi:

“In NiFi, adding new data sources that alter the data model and require changes to the patterns is certainly possible, however, there are limitations in the complexity of the analysis, and performing regressions on already processed data is not simple in NiFi. With Cogynt, once a desired event pattern is produced, it is also very easy to integrate a new data element, no reindexing/recycle of the ETL, no schemas to update, no code required.”

Cogynt Visualization Tools

Cogynt Analyst Workstation

One of the key objectives of Cogynt is to make analysts more effective and efficient in delivering intelligence products to their stakeholders. To achieve this, Cogility has developed the Analyst Workstation (shown in Figure 4) which provides a rich suite of investigative analysis tools and visualizations, increasing analyst productivity, context, insight, timeliness, and overall efficiency.

The Analyst Workstation is a modern web-based tool that is highly configurable to the analyst's preferences. It delivers a great user experience in terms of flexibility and interoperability between the tools (widgets⁵) and the ability to seamlessly perform multiple analytic functions. Cogynt Analyst Workstation allows the “drag and drop” of information objects between UI widgets — eliminating the need to jump between tools and applications. This powerful interaction allows the analyst to work at “think speed” within their workflow, providing a direct boost in analyst productivity.

For example, a notification containing critical information about an event that poses a risk can be dropped on a map widget, identifying location.

The analyst may also wish to use Cogynt's auto-generated link chart, enabling the analyst to see any connections to other pertinent events or entities. Of critical importance is the drill down on the notification event, allowing the analyst to review and validate the source events that generated the notification event. Furthermore, the Analyst Workstation facilitates a flexible workflow approach and sharing of analysis with other analysts, using “Collections” as a means of collecting data relevant to intelligence task and tagging that analysis for others to review. All user actions are also auditable, ensuring compliance with enterprise policies and regulations.

Analyst Workstation allows the “drag and drop” of information between widgets — eliminating the need to jump between tools and applications.

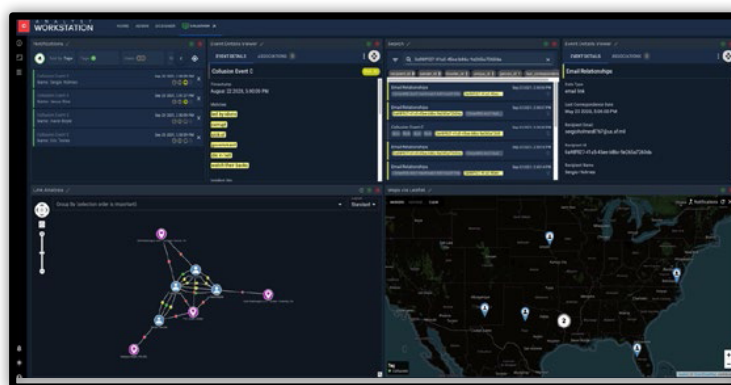


Figure 4. Cogynt Analyst Workstation User Interface

5 Widget: A widget is a single purpose software tool among many types of single purpose tools within Cogynt Analyst Workstation. Example widgets include a search widget, notifications widget, map widget, and link analysis widget.

Cogynt Superset — BI Dashboard

The Cogynt Superset Tool provides BI dashboard functionality (Figure 5) and is the perfect complement to the Cogynt Analyst Workstation. It provides aggregate analysis and context for the domain understudy, while the Cogynt Analyst Workstation provides the means to perform detailed, forensic analysis of the data.

The Superset Tool provides four essential BI functions that all enterprises need, which include:

- **Situational Awareness** – A comprehensive view of metrics and status.
- **Trend Analysis** – A determination of if and how the metric is changing over time.
- **Change Point Detection** – A significant change in a trend means that there is an underlying change in behavior of the metric being monitored, which could warrant further investigation.
- **Forecasting** – Given the trend history, this allows the analyst to forecast future trends.

The Superset Tool, like the Analyst Workstation, allows data to be visualized in real-time and can handle any scale of data. This allows analysts to explore the data easily and to create new views of various types within minutes. Figure 4 shows examples of the types of views provided by the Superset BI Dashboard, including event timelines, aggregate change analysis, heatmaps, pie charts, and many others that you would normally find in other popular BI solutions.

The Superset Tool, like the Analyst Workstation, allows data to be visualized in real-time. It can handle any scale of data, allowing analysts to explore the data easily and to create new views of various types within minutes.

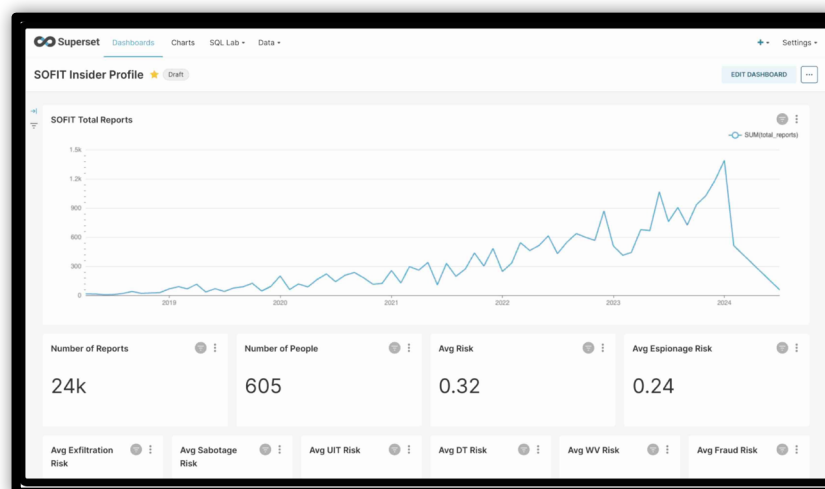


Figure 5. Cogynt Superset BI Dashboard

Cogynt Big Picture Wall Monitor Dashboard

To augment the Cogynt URP, Cogility can support a big picture wall monitor dashboard to enhance operational management. This enables command and control visualization to provide shared situational awareness, support decision making, and to enhance collaboration. This big picture dashboard capability can support various formats — on multiple monitors, as shown in the following photo (Figure 6), on a single monitor, or in a desktop configuration.



Figure 6. Cogynt Big Picture Wall Monitor Dashboard

Cogynt Deployment and Packaging

Additional features of the Cogynt URP are its automated deployment, integrated packaging, and operational resiliency. Cogility has fully automated the deployment of the Cogynt platform in AWS and GCP, supplemented with management tools to monitor the health of the platform. Figure 7 is a depiction of the Cogynt platform and enabling software components, including Apache Flink, Apache Kafka, Apache Druid, etc. Cogynt can be effectively managed, because the entire platform and associated software components are containerized images, orchestrated using Kubernetes. By leveraging Kubernetes, Cogynt can be centrally managed, elastically scale in the cloud, self-heal to ensure reliability and resilience, and is self-contained — it does not need to make external API calls to run. Finally, the packaging of this solution and enabling use of Kubernetes is a significant engineering achievement that allows the customer to focus on their mission without having to look under the hood.

By leveraging Kubernetes, Cogynt can be centrally managed, elastically scale in the cloud, self-heal to ensure reliability and resilience, and is self-contained meaning it does not need to make external API calls to run.

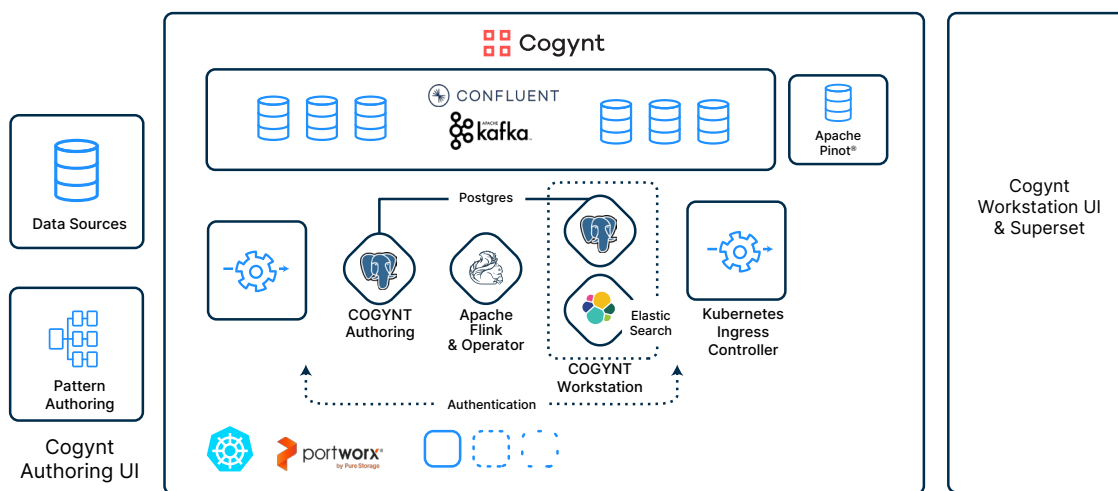


Figure 7. Cogynt CI Platform Deployment Solution

Conclusion

Cogility Cogynt is a unified real-time platform that provides comprehensive, versatile, and integrated continuous intelligence. It allows enterprises to achieve decision advantage by delivering contextualized, predictive insights regardless of data volume and diversity, and pattern complexity.

With Cogynt, analysts, data scientists, and subject matter experts can quickly connect to various data sources and more easily model complex event patterns within Cogynt's no-code Authoring tool — expanding the scope of what can be monitored and enabling the means for continuous model improvement. The Cogynt platform also publishes resulting events to external systems and provides contextual notifications to analysts within the Analyst Workstation — enabling them to deliver timely, high quality intelligence products to decision makers. The Superset Tool provides BI dashboard capabilities that facilitate performance insight and operational management.

Cogynt makes this possible with its flexible data ingestion, event streaming, behavioral analytic engine (HCEP), powerful visualizations, integrated packaging, and streamlined deployment. This is available to organizations as a cloud-scalable solution that has faster time-to-value, greater repurposeability, and lower total cost of ownership compared to a piecemeal, “build your own” event-driven analytics architecture. Leveraging Cogynt, organizations can more efficiently and effectively build CI applications that can address a wide range of government and commercial use cases such as supply chain intelligence, logistics optimization, fraud detection, customer intelligence, and operational intelligence.

If you'd like to learn more about Cogynt URP for continuous intelligence, please visit www.cogility.com or contact Cogility sales at sales@cogility.com.

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