Cogynt – A Comprehensive Solution for Counter-Insider Threat Analytics

COGILITY

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, behavioral analytic platform 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 help achieve a proactive 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.

Cogynt Capabilities

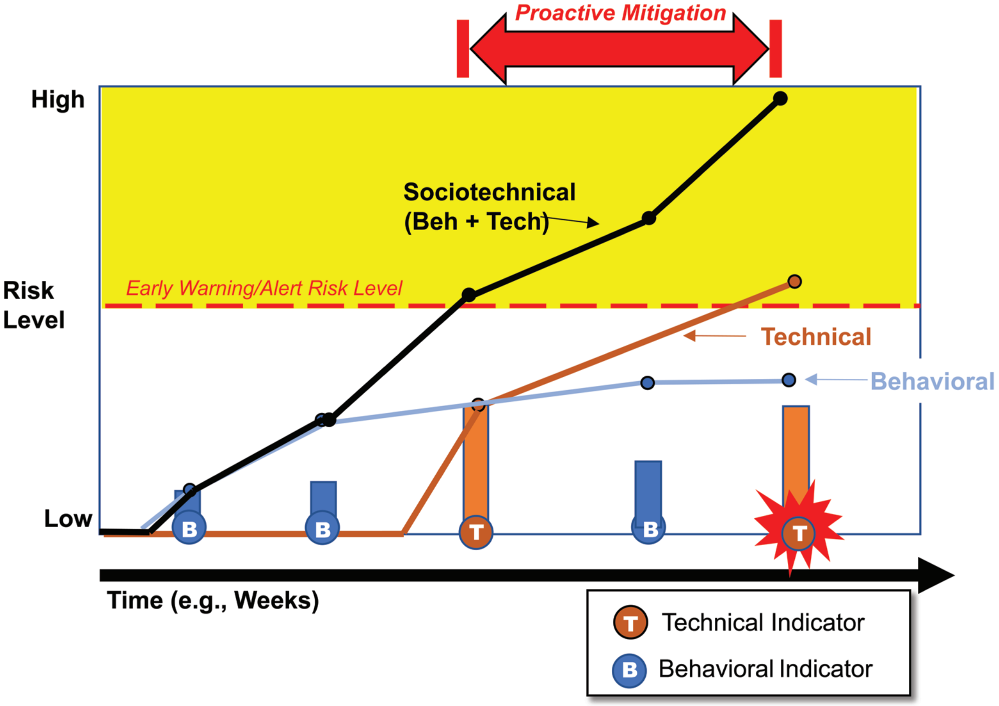
1. Human in the Loop
2. Multiple Simultaneous Data Source Ingestion
3. Semantic Analysis to process structured or unstructured data at scale
4. Complete Behavioral Modeling Environment with a self-documenting model that may be reviewed and validated by third-party experts
5. Real-Time Behavioral Analytic to hierarchically process event patterns to yield actionable intelligence
6. Real-Time Continuous Risk Assessment to assess behavioral patterns
7. Visualizations to present and allow manipulation of complex data and relationships in various contexts (geospatial, link charts, hierarchy charts, graphs and histograms, lists, etc.)
8. Case File Management to support workflow
9. Audit support to ensure compliance with organizational policies
10. Enterprise Dashboard Views to support Business Intelligence to convey risks, hot spots, and trends
11. Open Architecture that can be easily integrated with other applications and data stores
12. Scalable to the needs of the enterprise and big data to be processed
13. Platform is Easy to Install and Manage

Background

Insider threats are actions by trusted individuals with access to organizational assets that may harm the organization or its assets—these acts include insider data theft/exfiltration, sabotage, espionage, fraud, maladaptive behavior, workplace violence, and unintentional insider threats.[1] With potentially catastrophic consequences, these incidents often are perpetrated by individuals with personal predispositions (psychological factors such as depression or personality traits such as narcissism or anti-social personality disorder) that lead them to react or act-out in response to work- or life-stressors.[2]

Figure 1 is a notional plot of insider threat risk that distinguishes between contributions of technical indicators (online behavior) versus psychosocial/behavioral indicators, demonstrating how the combination of both data sources in a comprehensive C-InT approach can provide early warning, and greater opportunity for proactive mitigation that gets "left of boom."[3]

Figure 1. Sociotechnical (behavioral) data enables proactive mitigation to get "left of boom."



[1] Cappelli, DN, Moore, AP, & Trzeciak RF. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud).* Addison-Wesley.

[2] Shaw, ED & Sellers, L. (2015). Application of the Critical-Path Method to Evaluate Insider Risks, *Studies in Intelligence 59(2)* (Extracts, June 2015)

[3] Greitzer, FL, Purl, J, Leong, YM, and Becker DE. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. *IEEE Symposium on Security and Privacy Workshops*, 197-206.

Compared with typical reactive programs that limit analysis to technical data, programs that incorporate behavioral data monitoring and analytics (deriving from Human Resources, Security, Performance Reviews, Financial, Criminal, etc.) can gain insight about personal predispositions, precipitating events (stressors), or concerning behaviors that reveal higher-risk individuals who show behavioral signs weeks or months prior to the incident.[4,5,6]

The Federal Insider Threat Program was established in 2012 by Presidential Executive Order (EO) 13587.[7] Following this, the Federal agencies derived their own policies and instructions that define authorities, responsibilities, and relevant constructs—including threat behaviors of concern and definitions of contributing factors or indicators associated with these threats. All entities benefit from such standardization, but each organization may apply its own criteria or priorities, informed by its mission and culture, to implement its C-InTP.

For the DoD, a knowledge base of more than 140 Potential Risk Indicators (PRIs) has been defined by the Defense Counterintelligence and Security Agency (DCSA). This hierarchy of PRIs compares with other knowledge bases that have been developed, such as the *Sociotechnical and Organizational Factors for Insider Threat (SOFIT)* ontology[8] that was developed under a contract with the Intelligence Advanced Research Projects Activity (IARPA). The DAF C-InTP has continued to advance this PRI knowledge base by incorporating concepts described in the SOFIT ontology as well as other frameworks for understanding insider threats—particularly the Critical Pathway to Insider Risk (CPIR) model developed to better understand the role of contributing factors.[9] These resources represent valuable guidance to understand and define insider threat behaviors and the basis for these behaviors.

[4] Shaw ED, Fischer L. Ten tales of betrayal: an analysis of attacks on corporate infrastructure by information technology insiders, Vol. 1. Monterey, CA: Defense Personnel Security Research and Education Center. 2005

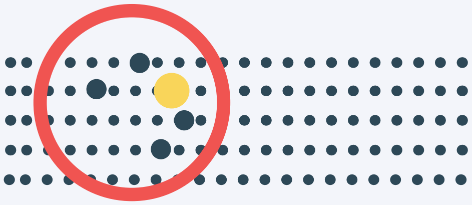
[5] Greitzer, FL, Purl, J, Leong, YM, and Becker DE. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. *IEEE Symposium on Security and Privacy Workshops*, 197-206.

[6] Greitzer, FL. (2019). Insider Threats: It's the *HUMAN*, Stupid! *Proceedings of the Northwest Cybersecurity Symposium*, April 8-10, 2019. Article No. 4, pp. 1-8. ACM ISBN 978-1-4503-6614-4/19/04

[7] https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

[8] Greitzer, Purl, Leong, Becker (2018)

[9] Shaw and Sellers (2015)

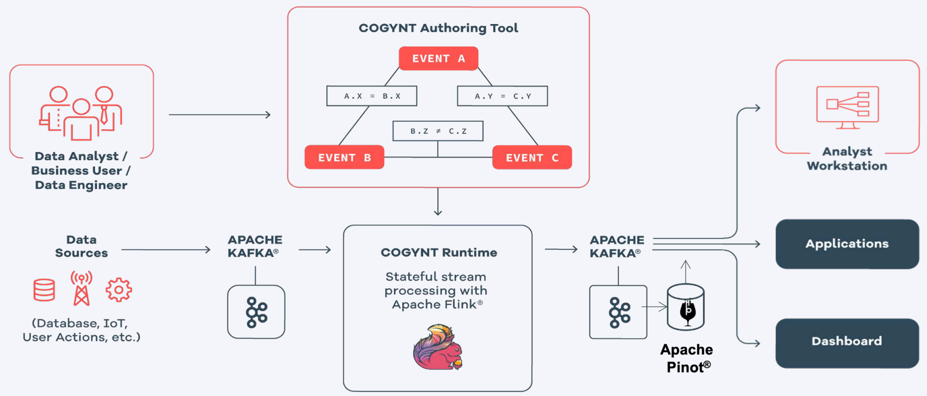


Cogynt Continuous Intelligence Behavioral Analytic Platform

Cogility has developed an advanced, big data, and highly scalable behavioral analytic platform called "**Cogynt**" that can continuously monitor the behavior of many thousands or millions of entities and continuously assess risk over extended periods of time. The ability to conduct this level of analysis, assuming the data and sufficiently detailed behavioral patterns are defined, allows for organizations and enterprises to conduct insider threat assessments of their employees and alerts C-InT analysts about concerning behavioral trends/potential risks so mitigating actions can be taken prior to a serious incident.

A readily configurable and adaptable continuous intelligence platform, **Cogynt** offers all the essential capabilities needed to augment and support a highly mature and effective C-InTP that meets or exceeds best practices.[10] A logical depiction of the **Cogynt** platform solution architecture is shown in Figure 2.

Figure 2. Cogynt Behavioral Analytic Platform



The **Cogynt** platform components and their role within the architecture are:

- **Data Sources:** Streaming or batched 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.
- **Cogynt Event Stream Processing and Storage:** The analytic results are streamed from Apache Flink to Apache Kafka and Apache Pinot for Storage. Results are displayed in the Analyst Workstation and Superset Dashboard.
- **Cogynt Analyst Workstation:** a dynamic and interactive user interface enabling the analyst to view analytic results and to review and validate system generated intelligence.
- **Applications:** As an open system, **Cogynt** can be shared with any event driven system or application.
- **Dashboard Interface:** provides the **Cogynt** Superset dashboard and enables access to any other preferred dashboards through the **Cogynt** open system architecture.

[10] Henderson, J., & Cavalancia, N. (2019). *2019 Insider Threat Program Maturity Model Report*. https://cdn2.hubspot.net/hubfs/5260286/PDFs/Whitepapers/insider-threat-maturity-report-2019.pdf

Cogynt Behavioral Analytics and HCEP

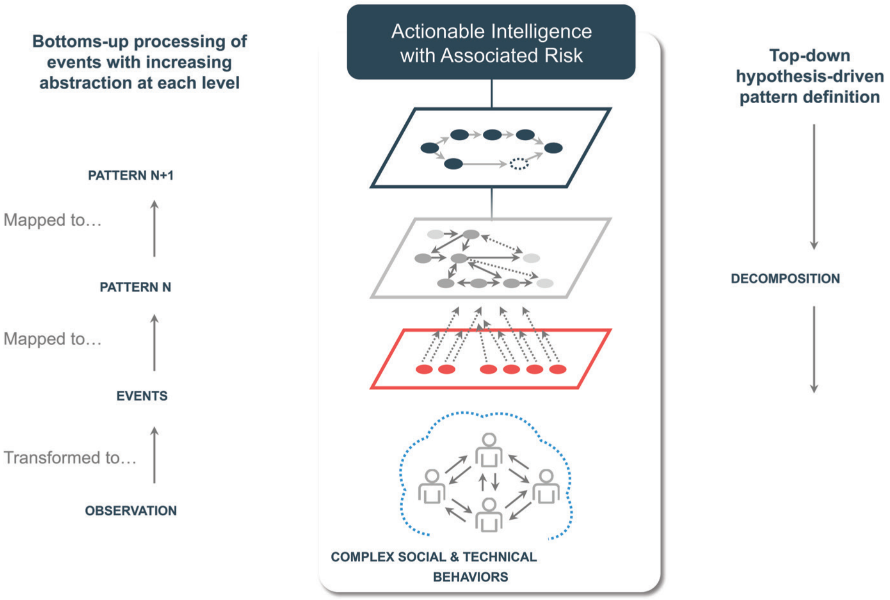

Bottoms-up processing of events with increasing abstraction at each level
Actionable Intelligence with Associated Risk
Top-down hypothesis-driven pattern definition
PATTERN N+1
Mapped to…
PATTERN N
DECOMPOSITION
Mapped to…
EVENTS
Transformed to…
OBSERVATION
COMPLEX SOCIAL & TECHNICAL BEHAVIORS

Figure 3. Hierarchical Complex Event Processing (HCEP)

The heart of **Cogynt** contains a patented behavioral analytic called *Hierarchical Complex Event Processing (HCEP)*. The principles of HCEP are rooted in system theory[11] and CEP.[12] For insider threat, **Cogynt** can model a whole person insider threat profile by defining all the relevant behavioral types that make up an insider threat profile. 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. In addition, HCEP allows for partial event pattern matches, which represents an indicator (or a collection of indicators) representing a behavior, but not a complete pattern of a definitive target threat behavior. **Cogynt** maintains the state of the event patterns over time, which allows analysts to look for trends and changes in behavior.

The general HCEP concept is represented in Figure 3. The top-level event pattern represents the whole person profile, and the lower-level patterns represent *indicators* (which are basically the "building blocks" of behavior patterns). The lowest level represents interpreted data, or *observations*, which are building blocks of indicators. Data or events are processed from the bottom up to infer observations from the real world consisting of people exhibiting sociotechnical behaviors. These observed events are matched to event patterns that may eventually culminate in an insider threat incident. The ability to continuously assess a person's behavioral profile state and changes in the profile are key to predicting insider threats.

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

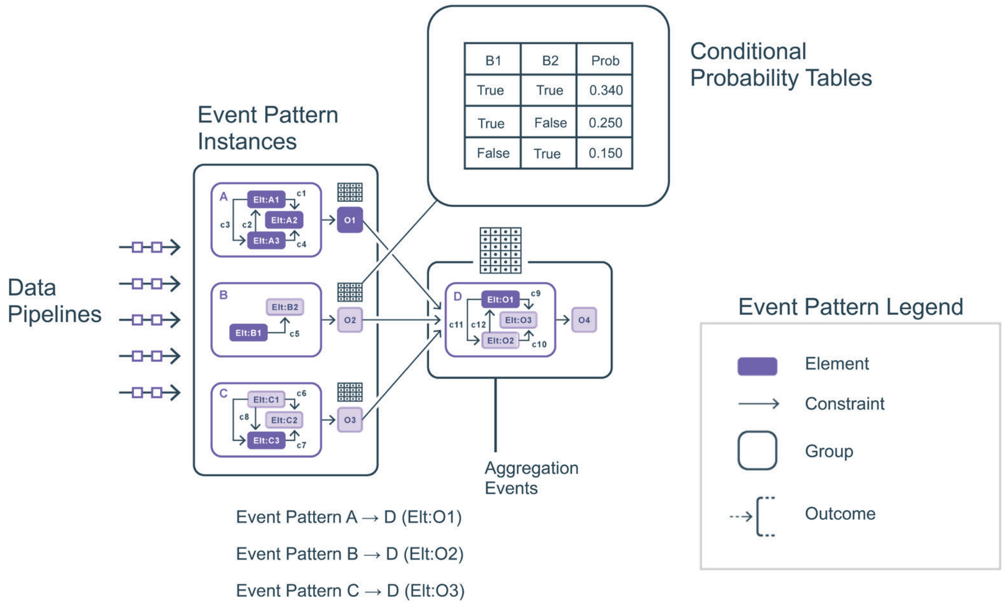
[12] https://en.wikipedia.org/wiki/Complex_event_processing

Another critical facet of HCEP is continuous risk assessment of a person's insider threat profile. **Cogynt** applies a Bayesian Belief Network[13] (BBN) computation method for computing risk based on the hierarchical structure of the event pattern model. This risk assessment allows analysts to weigh the value of one indicator over another based on the risk assessment. Applying BBN allows analysts to not only assess developing behavioral patterns but weigh the importance of one behavior over another as to the risk it poses to the organization.

Figure 4 represents an example set of event patterns (A, B, C, and D) where event patterns A, B, and C output complex events to event pattern D. The diagram shows data entering at the left as inputs to the event patterns. The diagram shows each of the event patterns where A is fully matched—generating an event O1 as output—and where event patterns B and C contain partial matches. The analyst defines the statistical importance of each element as it relates to risk. Applying BBN computations, **Cogynt** processes both matched and unmatched statistical event patterns up the hierarchy.

For example, event pattern A is the only pattern providing a factual output. Event patterns B and C provide statistical outputs (O2 and O3) that are inputs to event pattern D. The output O4 from event pattern D consists of one factual and two statistical elements that inform the O4 statistical result. This general approach is how behavioral risk is propagated through the behavioral hierarchies, allowing the analyst to have complete visibility of the state of any given behavior and statistical risk assessment.

Figure 4. Cogynt Notional Event Pattern



B1	B2	Prob
True	True	0.340
True	False	0.250
False	True	0.150

Event Pattern A → D (Elt:O1)

Event Pattern B → D (Elt:O2)

Event Pattern C → D (Elt:O3)

[13] https://en.wikipedia.org/wiki/Bayesian_network

Figure 5. Notional C-InT Behavior and Risk Assessment in processing composite behaviors

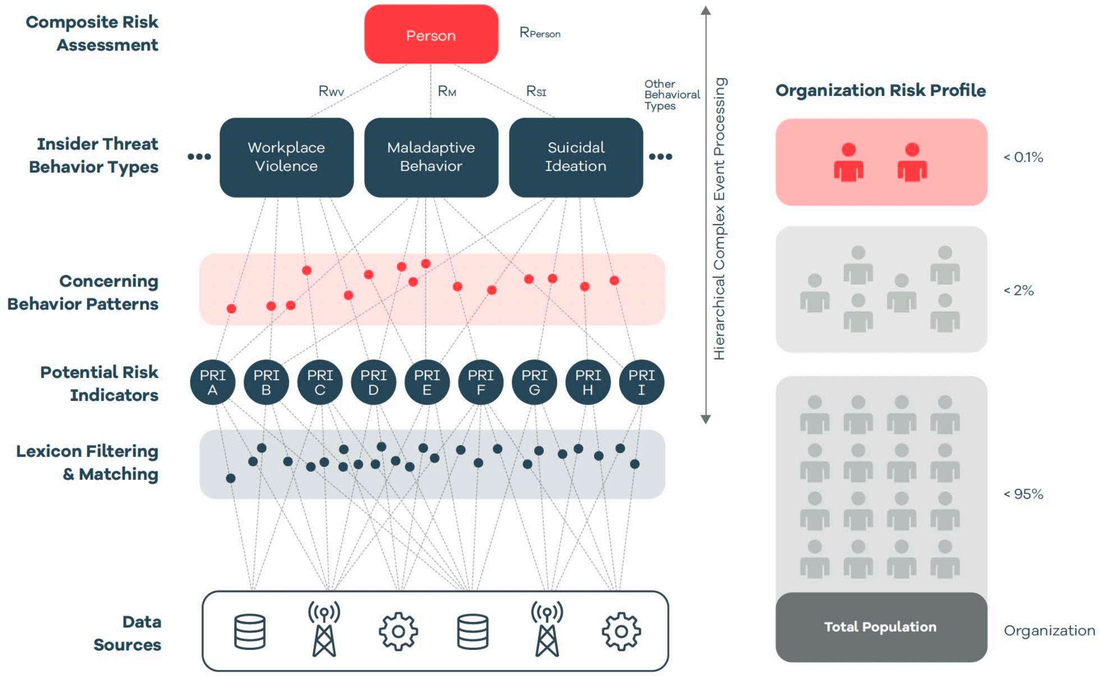


Figure 5 is a notional **Cogynt** HCEP process as applied to insider threat. The figure depicts the matching process and continuous risk assessment where multiple threat-behavior types contribute to an individual's behavioral risk assessment, which is assessed on a continuous basis. The mapping proceeds from PRIs to threat behavior types, with varying strengths of association between PRIs and behavior type. This means that the relationships between PRIs and behaviors are dynamic—research suggests that there are complex, dynamic relationships among PRIs that produce different risk assessments when combined into various patterns.[14]

The powerful hierarchical complex event processing capabilities of **Cogynt** provide a unique approach to assessing insider threat risk in this complex environment. Furthermore, the modeling capabilities in **Cogynt** allow it to capture other dynamic qualities of PRIs, such as decreases in risk over time.

Data or events are ingested and filtered using lexicons that define a PRI that is associated with a behavior (e.g., Workplace Violence) with an estimated risk weighting reflecting the extent to which the PRI is indicative of the behavior. The accumulation of risk is computed for every person/entity within the organization, and over time, these accumulated risk scores may be compared across the organization to identify individuals who are of greatest concern.

This concept of risk decay, which is currently under study in the insider threat research community, suggests that different types of PRIs may be subject to different decay parameters (e.g., those that relate to personality traits may be expected to be stable over time, while others that relate to more transient events such as network activity, may be subjected to more rapid decay in associated risk).[15]

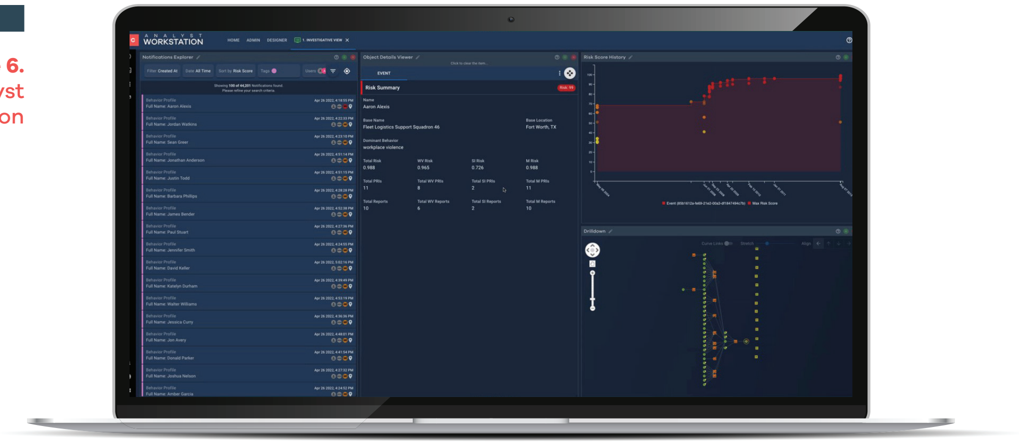
[14] Greitzer & Purl (2022)
[15] Greitzer & Purl (2022)

Cogynt Analyst Support

HCEP is the workhorse that processes vast amounts of data and matches it with event patterns over time, notifying the analyst when a predefined behavioral threshold has been reached. The **Cogynt** Analyst Workstation (Workstation)—shown in Figure 6—allows the analyst to review this output, determine its accuracy, and instigate a workflow with other analysts or subject-matter experts—such as a psychologist or law enforcement professionals—to review the event and reach an informed decision.

The Workstation provides a suite of flexibly configurable, interoperable tools or widgets that supports an intuitive and seamless analyst workflow to assess behavioral thresholds and build a case file. The analyst can upload files to support case management and export case file data to support external reporting needs. The Workstation provides an assortment of visualizations such as link charts, maps, event drill down charts (event tree), and line charts for risk history that may be combined based on the user's preference.

Figure 6. Cogynt Analyst Workstation



Showing 100 of 44,201 Notifications found.
Please refine your search criteria.

Behavior Profile
Full Name: Aaron Alexis
Apr 26 2022, 4:18:55 PM

Behavior Profile
Full Name: Jordan Watkins
Apr 26 2022, 4:22:33 PM

Behavior Profile
Full Name: Sean Greer
Apr 26 2022, 4:23:10 PM

Behavior Profile
Full Name: Jonathan Anderson
Apr 26 2022, 4:51:14 PM

Behavior Profile
Full Name: Justin Todd
Apr 26 2022, 4:51:15 PM

Behavior Profile
Full Name: Barbara Phillips
Apr 26 2022, 4:28:28 PM

Behavior Profile
Full Name: James Bender
Apr 26 2022, 4:52:38 PM

Behavior Profile
Full Name: Paul Stuart
Apr 26 2022, 4:27:36 PM

Behavior Profile
Full Name: Jennifer Smith
Apr 26 2022, 4:24:55 PM

Behavior Profile
Full Name: David Keller
Apr 26 2022, 5:02:16 PM

Behavior Profile
Full Name: Katelyn Durham
Apr 26 2022, 4:39:49 PM

Behavior Profile
Full Name: Walter Williams
Apr 26 2022, 4:53:19 PM

Behavior Profile
Full Name: Jessica Curry
Apr 26 2022, 4:36:36 PM

Behavior Profile
Full Name: Jon Avery
Apr 26 2022, 4:48:01 PM

Behavior Profile
Full Name: Donald Parker
Apr 26 2022, 4:41:54 PM

Behavior Profile
Full Name: Joshua Nelson
Apr 26 2022, 4:27:32 PM

Behavior Profile
Full Name: Amber Garcia
Apr 26 2022, 4:24:52 PM

Risk Summary
Risk: 99

Name
Aaron Alexis

Base Name
Fleet Logistics Support Squadron 46

Base Location
Fort Worth, TX

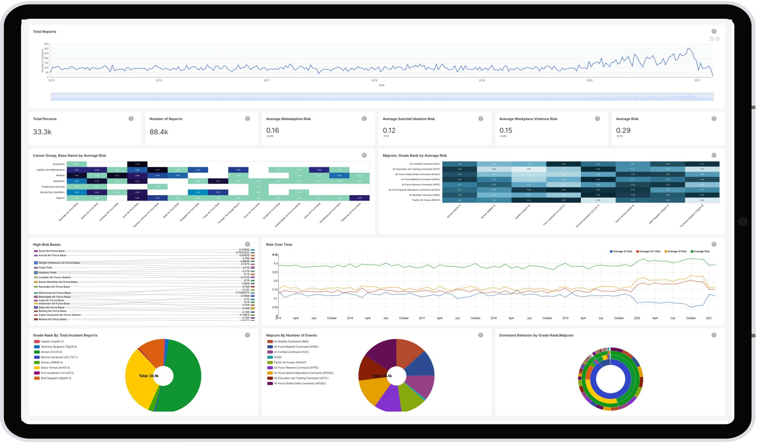
Dominant Behavior
workplace violence

Total Risk	WV Risk	SI Risk	M Risk
0.988	0.965	0.726	0.988

Total PRIs	Total WV PRIs	Total SI PRIs	Total M PRIs
11	8	2	11

Total Reports	Total WV Reports	Total SI Reports	Total M Reports
10	6	2	10

Figure 7. Superset BI Dashboard



Total Reports
Total Persons
33.3k
Number of Reports
88.4k
Average Maladaptive Risk
0.16
Average Suicidal Ideation Risk
0.12
Average Workplace Violence Risk
0.15
Average Risk
0.29
Career Group, Base Name by Average Risk
Majcom, Grade Rank by Average Risk
High Risk Bases
Risk Over Time
Grade Rank By Total Incident Reports
Majcom By Number of Events
Dominant Behavior by Grade Rank/Majcom

The Superset dashboard (Figure 7) is another view—particularly of interest to stakeholders who need to see the big picture of data in the aggregate, or enterprise view. The Superset dashboard provides the added benefit of allowing users to interact with the data—i.e., the user can inspect an area such as a spike in risk or number of incidents and examine the source of incidents, such as based on the organization or geography.

Conclusion

Insider Threat is a low probability, high consequence risk that organizations face daily. Over the past 10 years, this threat has gained the full attention it deserves to develop better tools for mitigating insider threat risk. An effective C-InT program requires policies, instructions, and procedures on how to manage insider threat risk—an advanced continuous intelligence behavioral analytic platform is needed to do this effectively.

The **Cogynt** platform is uniquely qualified to meet the immense analytic and information-processing challenges faced by insider threat analysts across government and industry.