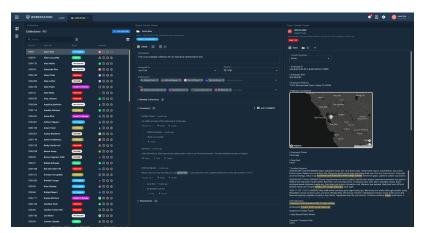
## COGILITY

# Cogility<sup>™</sup> Insider Risk Management

## Proactive, Whole Person Approach to Get Left of Harm

### **Summary**

The most impactful threats to your organization are due to insider risk. Unfortunately, most insider risk management (IRM) programs rely solely on detecting explicit security violations and anomalies. Information security staff need to detect and quickly react to security violations, suspicious user behavior, and malicious actions within distributed locations, devices, and infrastructure. However, disgruntled personnel with perceived grievances, or who have been compromised and coerced, may abused their access privileges by committing acts of data theft, fraud, and espionage. Worse yet, they may have varied, periodic, and often unmonitored psychosocial issues that culminate into disruptive, destructive, and damaging consequences to your operations, initiatives, and personnel. This includes incidents of sabotage and workplace violence. To get left of harm, you need to mature your insider risk management program with an end-to-end, whole person insider risk detection, prediction, and mitigation solution.



Cogynt™ IRM prioritized insider risk viewer, active case files, and case details

## Challenge

The demands of insider risk management programs can overwhelm the operational and assessment capabilities of insider threat analysts and case managers. Much time, investment, and resources are spent reacting to and gathering incident evidence, after the fact, from security information event management (SIEM), user behavior analysis (UBA), and other tools. This reactive approach fails to identify high-risk individuals early enough to mitigate or preempt their consequential actions. While policies and technical controls are threat deterrents, underlying behavioral and psychosocial risk indicators are largely unaccounted for — undermining the ability to achieve a more mature, proactive mitigation approach. Most insider risk programs are further hindered due to data and team isolation, threat analysis and collaboration delay, and cobbled toolsets that impact case management and workflow efficacy.

#### **Benefits**

- Move from reactive to proactive, whole person insider risk management
- Monitor for explicit and predictive determination of insider risk — continuously
- Modernize insider threat management coverage, assessment, and mitigation capabilities
- Accelerate IRM program expansion, maturity, and oversight
- Improve analyst case workload productivity with automated scoring, profiling, and collaboration
- Standardize insider risk codification, assessment, and threat response processes
- Leverage existing physical, endpoint, network, and cloud security investments and H.R., operational, and other psychosocial data sources
- Gain rapid time-to-value: non-disruptive deployment, extensible IRM model, and bespoke dashboards / reports
- Preempt high-consequence incidents while helping personnel in need of support
- Leverage Gen Al to quickly investigate and accurately summarize complex reporting

#### Solution

Cogility's IRM solution offers a comprehensive, whole person approach to managing insider risk. The system continuously monitors and correlates technical and behavioral / psychosocial potential risk indicators (PRIs) to detect, score, and alert on insider threats. The solution leverages Cogility's decision intelligence platform (DIP), Cogynt. Cogynt applies event streaming and advanced behavioral analytics technology to determine explicit and predictive insider threats with full traceability. When combined with its flexible data ingestion and case management automation, Cogility modernizes IRM programs to help organizations more efficiently respond to and prevent insider threat incidents.

## **Modernize Your Insider Risk Management Program**

Cogility's whole person approach to insider risk management offers organizations a more efficient and effective means to manage, prevent, and mitigate insider risk. Powered by Cogynt's DIP for continuous decision intelligence, Cogility IRM provides an integrated, scalable solution that can handle the challenging data processing and decision support demands associated with exceptional case assessment and threat response — modernizing your IRM program.

Our advanced stream data processing and patented behavioral analytics technology connects the dots across your existing security controls. It analyzes these technical PRIs to detect insider threats that require immediate response. However, your staff needs to go beyond the mere monitoring and reacting to observed security violations and anomalies.

Cogynt captures and analyzes both technical and psychosocial data in real-time to identify, distill, and score complex patterns of high-risk behaviors, maintaining state and taking into account risk decay. This enables your team to see the warning signs before insider threats become high consequence incidents. Cogynt's continuous monitoring, detection, risk scoring, and resulting potential insider risk profiles are fortified with integrated case management. Cogynt's case management features help streamline case assignment, priority, assessment, collaboration, evidence collection, and coordinated response processes.

To expedite deployment, Cogility IRM includes foundational insider risk models that can be tailored to meet your organization's mission requirements, policies, and priorities. The solution's stream data analysis can process your existing technical and behavioral data sources at scale and provides flexible data ingestion that is non-disruptive. This empowers your operations to move from a reactive to proactive stance — taking your insider threat management program to the next level.

## **Advantages**

- Predictive Intelligence
   Continuously monitor and assess the insider risk surface with stateful profiling, scoring, and alerting for effective threat insight, reaction, and prevention.
- Secure, Scalable, Non-disruptive
   Securely operates in your private
   cloud for scalable, real-time data
   processing and analysis from
   your existing controls and other
   sources.
- Whole Person Risk Management
   Comprehensive technical
   and psychosocial behavioral
   intelligence to support threat
   analysts and case assessors to
   make informed decisions.
- Foundational Threat Models
   Base set of insider risk models
   that can be readily tuned
   and expanded within a self documenting, no-code authoring
   environment.
- Integrated Case Management Dashboards, workflow tracking, and collaboration help streamline workloads from monitoring and assessment to case file evidence collection and threat response.
- Rapid Deployment
   Flexible data ingestion, predefined analytics, no-code authoring, dynamic scoring, and rich case management to expedite results.

Law Enforcement, Human Resources, Social Media, Financial...

#### Analysis and Analyst Assessment Case Manager Management Assessment Enterprise Dashboard recommendation and collaboration Layer Whole Person Profile Behavior Profile Laver Data Exfiltration Suicidal Unintentional Workplace Violence **Behavior** Fraud Layer Continuous, Real-Time Analysis and Risk Decay Weighted Data Exfiltration Sabotage Behavioral Pattern Pattern Pattern Patterns High Level Pattern Processing Weighted Individual PRIs Disgruntle - 120 Concerning Work Habits - 140 Policy Violations 910 Endpoint With Active 920 Authentication Authorization 520 Foreign Affiliat 930 Data Access Anomalies 540 Foreign Contacts 560 Foreign Travel Indicator 240 Major Security Violations 840 Interpersonal Issues Layer 850 Personal Stressors 950 Cyber Obfuscation 580 Foreign Assets 880 Personality/Character Traits 970 Command Usage 340 Nonjudicial Punishmen 980 Data Manipulation 360 Concerning Job Stat 640 Other Criminal Acts or Records 440 Credit and Debt Concerns SOFIT 2.0 Potential Risk Indicator (PRI) Framework Technical Data Feeds Behavioral Data Feeds

### The Industry's Most Advanced Whole Person IRM Solution

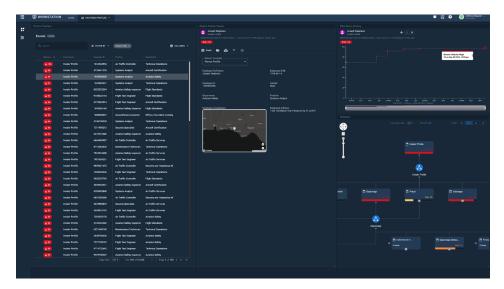
#### **Inner Workings**

Ingest Layer

Cogility's Insider Risk Management solution, powered by our Cogynt DIP for continuous decision intelligence, is uniquely designed and proven to meet the immense and dynamic information-processing, complex analytic, and workflow challenges faced by insider threat analysts across government and industry. Cogynt applies patented Hierarchical Complex Event Processing (HCEP) to ingest and analyze massive, diverse volumes of technical and behavioral data streams in real-time to monitor, score, and determine explicit and predicted insider risk.

Endpoint, Network, Cloud, Physical, Privileged Access...

As shown in the figure above, the top-level event pattern represents the whole person profile, and the lower-level patterns represent observations, which are building blocks of potential risk indicators (PRIs). Different combinations of PRIs reflect different behavioral insider threat patterns. Unstructured and structured data are processed from the bottom up and mapped to PRIs with estimated risk weights and decay characteristics. The HCEP process proceeds upwards from PRIs to threat behavior types, with varying strengths of association between PRIs and behavior patterns, and higher-level patterns that represent collections of PRIs. These PRI patterns, when observed together, provide stronger evidence (beyond the consideration of individual PRIs) that an insider threat incident, such as data exfiltration, workplace violence, or fraud, is in progress or imminent. The system allows for continuous monitoring of personnel, at scale — alerting insider risk analysts on individuals that exceed score thresholds.



Cogility IRM dashboard: case viewer, profiles, details, risk history, traceability

The analysis and assessment layer facilitates case management and program oversight. The Cogynt Workstation provides insider threat analysts and case managers a customizable, interactive dashboard suite of visualizations and profile information to assess behavioral thresholds and evidence to build a case file. Case management features support remote case submission, review, collaboration and status tracking. The integrated Superset Bl Dashboard tool provides additional visualization and reporting to provide executive and management views to gauge case performance and overall program trends.

#### **Get Left of Harm**

Over the past 10 years, the impact of insider threats have gained the full attention it deserves to mature processes and develop better tools to allow organizations to get left of harm.

A whole person approach with integrated case management is best suited to detect, prevent, and mitigate insider threats — efficiently, effectively, and at scale.

Cogility's IRM solution, powered by our Cogynt DIP for continuous decision intelligence, is uniquely designed and proven to meet and exceed best practices — increasing threat monitoring capacity, analyst and case manager productivity, and program efficacy across government and industry.

### **Capabilities**

- Insider threat analyst in the loop
- Multiple, simultaneous data source ingestion
- Semantic analysis to process structured or unstructured data at scale
- Complete, no-code behavioral modeling environment that is self-documenting
- Patented, real-time behavioral analytic to hierarchically process technical and psychosocial event patterns to yield actionable intelligence
- Dynamic scoring and profiling providing analysts with auditable evidence for informed assessment
- Visualizations to present and manipulate complex data and relationships in various contexts (geospatial, link charts, hierarchy charts, graphs and histograms, lists)
- Case management enabling file creation, risk assessment recommendations, custom annotation, review, and response coordination
- Audit support to ensure policy compliance
- Open architecture that can integrate with other applications and data stores

## COGILITY

Visit **cogility.com/insider-risk-management** 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