DATASHEET

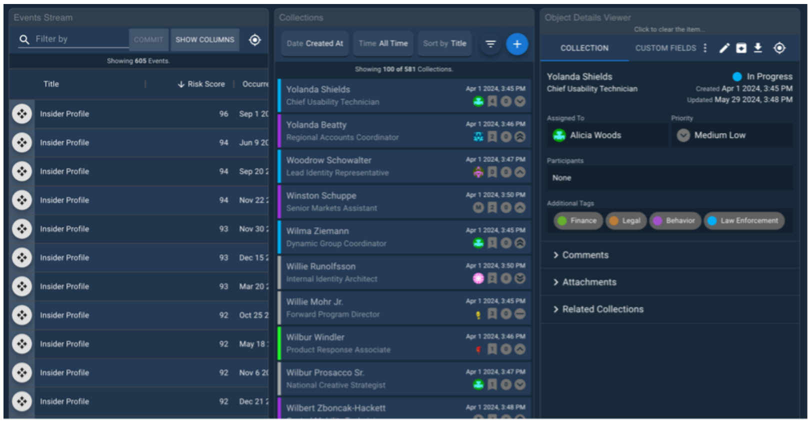
COGILITY

Cogility™ Counter-Insider Threat

Proactive, Whole-Person Insider Risk Management

Summary

The most impactful threats to your organization are due to insider risk. Unfortunately, most counter-insider threat (C-InT) 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 C-InT detection, prediction, and mitigation solution.



Showing 605 Events.

Title	↓ Risk Score	Occurre
Insider Profile	96	Sep 1 20
Insider Profile	94	Jun 9 20
Insider Profile	94	Sep 20 2
Insider Profile	94	Nov 22 2
Insider Profile	93	Nov 30 2
Insider Profile	93	Dec 15 2
Insider Profile	93	Mar 20 2
Insider Profile	92	Oct 25 2
Insider Profile	92	May 18 2
Insider Profile	92	Nov 6 20
Insider Profile	92	Dec 21 2

Showing 100 of 581 Collections.

Yolanda Shields Chief Usability Technician	Apr 1 2024, 3:45 PM	4 0
Yolanda Beatty Regional Accounts Coordinator	Apr 1 2024, 3:46 PM	2 0
Woodrow Schowalter Lead Identity Representative	Apr 1 2024, 3:47 PM	0 0
Winston Schuppe Senior Markets Assistant	Apr 1 2024, 3:50 PM	M 2 0
Wilma Ziemann Dynamic Group Coordinator	Apr 1 2024, 3:45 PM	1 0
Willie Runolfsson Internal Identity Architect	Apr 1 2024, 3:50 PM	2 0
Willie Mohr Jr. Forward Program Director	Apr 1 2024, 3:45 PM	3 0
Wilbur Windler Product Response Associate	Apr 1 2024, 3:46 PM	1 0
Wilbur Prosacco Sr. National Creative Strategist	Apr 1 2024, 3:47 PM	1 0
Wilbert Zboncak-Hackett	Apr 1 2024, 3:48 PM	

Yolanda Shields
Chief Usability Technician
● In Progress
Created Apr 1 2024, 3:45 PM
Updated May 29 2024, 3:48 PM

Assigned To: Alicia Woods
Priority: Medium Low
Participants: None
Additional Tags: Finance, Legal, Behavior, Law Enforcement

> Comments
> Attachments
> Related Collections

Cogynt C-InT 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 C-InT 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 C-InT model, and bespoke dashboards / reports
- Preempt high-consequence incidents while helping personnel in need of support

Solution

Cogility's C-InT 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 unified real-time platform (URP), 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 C-InT programs to help organizations more efficiently respond to and prevent insider threat incidents.

Modernize Your Counter-Insider Threat Program

Cogility's whole person approach to Counter-Insider Threat management offers organizations a more efficient and effective means to manage, prevent, and mitigate insider risk. Powered by Cogynt URP for continuous intelligence, Cogility C-InT 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 C-InT 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.

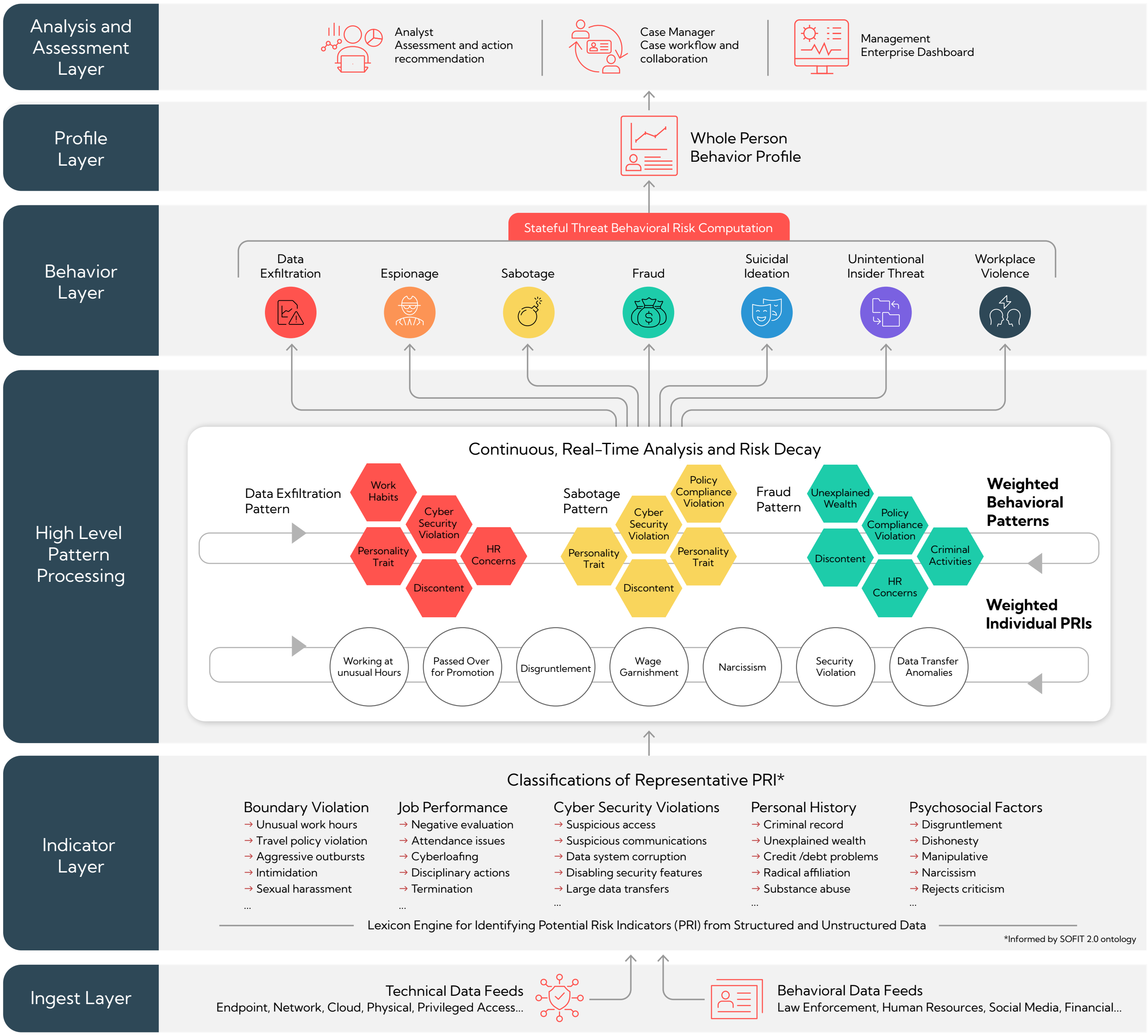
Cogynt captures and analyzes both technical and psychosocial data in real-time to identify, distill, and score complex patterns of high-risk behaviors, maintaining state and taking into account risk decay. This enables your team to see the warning signs before insider threats become high consequence 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 C-InT 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, pre-defined analytics, no-code authoring, dynamic scoring, and rich case management to expedite results.

The Industry's Most Advanced Whole Person C-InT Solution



Analysis and Assessment Layer

Analyst
Assessment and action recommendation

Case Manager
Case workflow and collaboration

Management
Enterprise Dashboard

Profile Layer

Whole Person Behavior Profile

Behavior Layer

Stateful Threat Behavioral Risk Computation

Data Exfiltration | Espionage | Sabotage | Fraud | Suicidal Ideation | Unintentional Insider Threat | Workplace Violence

High Level Pattern Processing

Continuous, Real-Time Analysis and Risk Decay

Data Exfiltration Pattern: Work Habits, Cyber Security Violation, Personality Trait, HR Concerns, Discontent

Sabotage Pattern: Policy Compliance Violation, Cyber Security Violation, Personality Trait, Personality Trait, Discontent

Fraud Pattern: Unexplained Wealth, Policy Compliance Violation, Discontent, Criminal Activities, HR Concerns

Weighted Behavioral Patterns

Weighted Individual PRIs

Working at unusual Hours | Passed Over for Promotion | Disgruntlement | Wage Garnishment | Narcissism | Security Violation | Data Transfer Anomalies

Indicator Layer

Classifications of Representative PRI*

Boundary Violation
→ Unusual work hours
→ Travel policy violation
→ Aggressive outbursts
→ Intimidation
→ Sexual harassment
...

Job Performance
→ Negative evaluation
→ Attendance issues
→ Cyberloafing
→ Disciplinary actions
→ Termination
...

Cyber Security Violations
→ Suspicious access
→ Suspicious communications
→ Data system corruption
→ Disabling security features
→ Large data transfers
...

Personal History
→ Criminal record
→ Unexplained wealth
→ Credit /debt problems
→ Radical affiliation
→ Substance abuse
...

Psychosocial Factors
→ Disgruntlement
→ Dishonesty
→ Manipulative
→ Narcissism
→ Rejects criticism
...

Lexicon Engine for Identifying Potential Risk Indicators (PRI) from Structured and Unstructured Data

*Informed by SOFIT 2.0 ontology

Ingest Layer

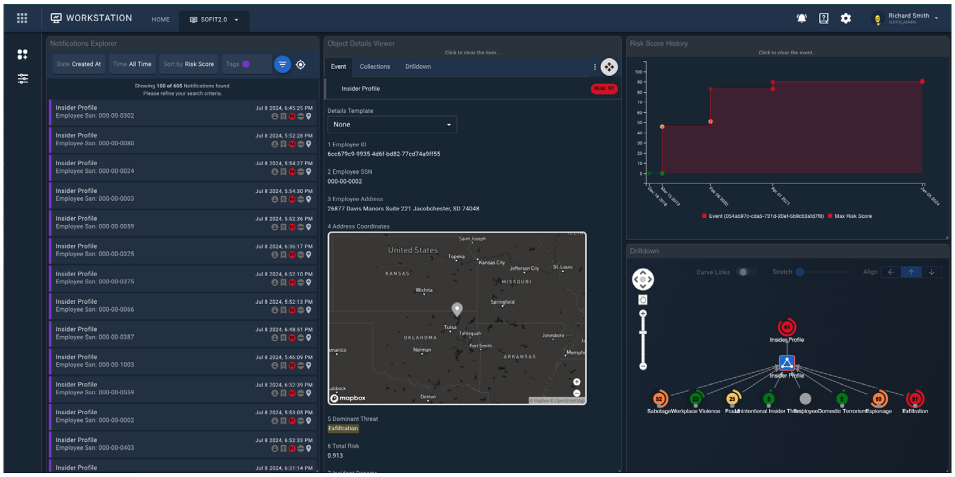
Technical Data Feeds
Endpoint, Network, Cloud, Physical, Privileged Access...

Behavioral Data Feeds
Law Enforcement, Human Resources, Social Media, Financial...

Inner Workings

Cogility's Counter-Insider Threat solution, powered by our Cogynt URP for continuous 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.

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.



Showing 100 of 605 Notifications found.
Please refine your search criteria.

Insider Profile
Employee Ssn: 000-00-0302 Jul 8 2024, 6:45:25 PM 96

Insider Profile
Employee Ssn: 000-00-0080 Jul 8 2024, 5:52:28 PM 94

Insider Profile
Employee Ssn: 000-00-0024 Jul 8 2024, 5:54:27 PM 94

Insider Profile
Employee Ssn: 000-00-0003 Jul 8 2024, 5:54:30 PM 94

Insider Profile
Employee Ssn: 000-00-0059 Jul 8 2024, 5:52:36 PM 93

Insider Profile
Employee Ssn: 000-00-0325 Jul 8 2024, 6:36:17 PM 93

Insider Profile
Employee Ssn: 000-00-0375 Jul 8 2024, 6:32:10 PM 93

Insider Profile
Employee Ssn: 000-00-0066 Jul 8 2024, 5:52:13 PM 92

Insider Profile
Employee Ssn: 000-00-0387 Jul 8 2024, 6:48:51 PM 92

Insider Profile
Employee Ssn: 000-00-1003 Jul 8 2024, 5:46:09 PM 92

Insider Profile
Employee Ssn: 000-00-0559 Jul 8 2024, 6:32:39 PM 92

Insider Profile
Employee Ssn: 000-00-0002 Jul 8 2024, 5:53:05 PM 91

Insider Profile
Employee Ssn: 000-00-0403 Jul 8 2024, 6:52:33 PM 91

Insider Profile Jul 8 2024, 6:31:14 PM

Insider Profile Risk: 91

Details Template: None

1 Employee ID
6cc679c9-9935-4d6f-bd82-77cd74a9ff55

2 Employee SSN
000-00-0002

3 Employee Address
26877 Davis Manors Suite 221 Jacobchester, SD 74048

4 Address Coordinates

5 Dominant Threat
Exfiltration

6 Total Risk
0.913

Cogility C-InT 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 BI 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 C-InT solution, powered by our Cogynt URP for continuous 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 **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

08/24