INSIDER RISK

Information Sheet

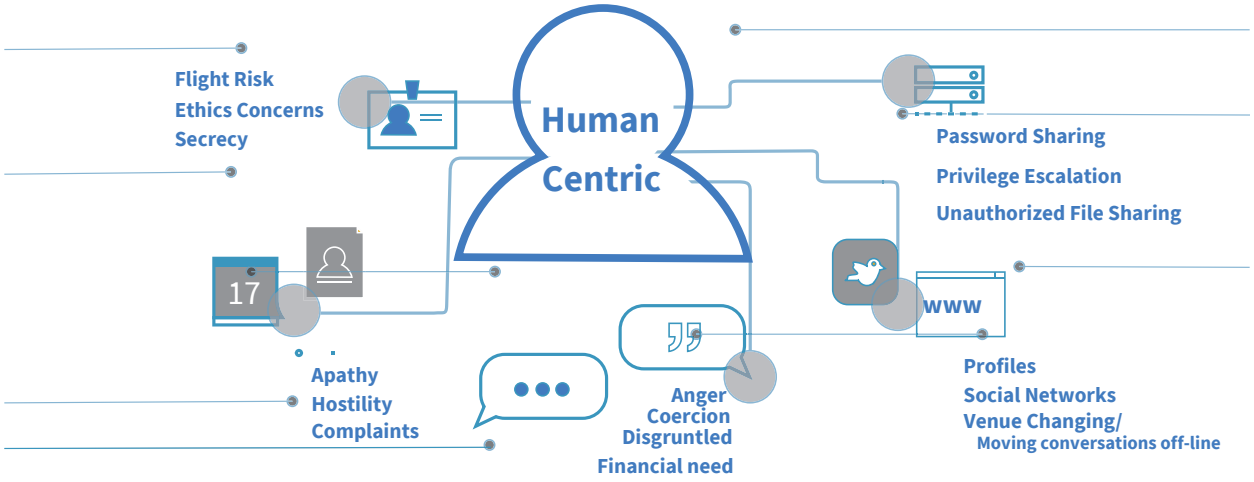
DIGITAL REASONING CAPTURES THE HIDDEN INSIGHTS THAT UNMASK INSIDER THREATS

Malicious insiders are few in number, but their actions are among the most damaging. The cost of attacks and data leakage attributed to insiders has reached an estimated $300 billion annually, with an average loss per victim of around $15 million. The difficulty is identifying precisely who poses a threat within trusted groups that have been granted privileged access.

Traditional data monitoring techniques have proven to be inadequate. Rules-based alerts and anomaly detection models that work off of machine generated data may flag potential concerns, but cannot adapt to context nor be relied upon to reveal identity. The result is excessive false positives, minimal insight into a user's intent, and alerts that arrive too late to prevent data theft or physical attacks.

Digital Reasoning's Cognition platform outperforms conventional solutions at finding insider threats because our algorithms model the individual insider's mindset and intents based on understanding the contents of their communications. This enables construction of psychological profiles that pinpoint which insiders are most likely to pose a threat and, more importantly, serve as a key signal indicating when they are likely to strike.

- Detect risks *before* they become security incidents
- Reduce false positives by up to 95%
- Increase escalations by up to 5x
- Will process 10 billion conversations in 2020
- Proven in the most arduous of regulatory environments



Enterprise	Government	Health Care
Uses communications to discern intent, improve accuracy, and reduce false alerts		
100% coverage of employees organically surfaces threats and avoids flawed risk-based sampling		
• Protect proprietary business information, competitive data, and sensitive records • Prevent leaks of M&A, customer and employee data • Protect employees from coercion or blackmail	• Safeguard data that could compromise security • Identify workplace rage and potential violence • Protect critical infrastructure • Identify high-risk individuals and prevent physical attacks	• Ensure contractors adhere to agency policies and procedures • Protect valuable patient data from being sold or mishandled • Ensure HIPAA and Data Protection Act compliance • Uncover employees who are compromising hospital records and business data

Digital Reasoning | Finding Truth
(615) 567-8853 | info@digitalreasoning.com | digitalreasoning.com | 701 Cool Springs Blvd, Fifth Floor, Franklin, TN 37067

INSIDER RISK Information Sheet

Digital Reasoning

HOW DIGITAL REASONING PROACTIVELY FINDS THREATS

We take a fundamentally different approach detecting insider risks before they become security incidents. Legacy techniques are limited to reactively analyzing machine generated data and user actions to identify breaches that have already occurred. In stark contrast, our algorithms model an insider's intent by understanding the content of their communications so that malicious users can be stopped before they commit an offence.

FOCUS ON THE HUMAN, NOT THE INHUMAN

Imagine that you had to get to know your best friend only by observing where they traveled, what they purchased and the websites they visited. While it would be informative, your picture would be incomplete.

Unfortunately, this is precisely how most insider threat detection tools operate. By monitoring written and spoken communications and patterns, Digital Reasoning is able to overcome this fundamental limitation and identify your employee's intent, locate vulnerable personalities, and alert the organization to suspicious actions and behaviors.

A PROVEN PEDIGREE

Used by 15 out of the top 20 global banks, our patented approach to deriving insights from human communications will process 10 billion conversations in 2020. Our machine learning models have been proven in the most arduous of regulatory environments and are trusted to proactively locate risks from insider trading to conspiracy and harassment. By combining multiple weak signals into profiles of risky behavior, we inform organizations of human risks before they become international fiascoes.

Most insider threat detections programs look for signals in data: unusual network access, excessive printing, downloads of sensitive records. The problem is that analysis of structured data and keyword searches are too imprecise and often lead to false positives. They can also fail to spot malicious acts too subtle to generate an alert. A sophisticated criminal might assiduously avoid known triggers, while someone who poses a physical threat may leave no clues in structured data.

Unlike the inflexible rules-based methodologies of conventional solutions, Cognition uses natural language processing and machine learning to bring a human-like acuity to automated searches. It accumulates and authenticates insights by semantically analyzing the data that best captures hidden intent – human communications.

Adopting an intent based approach to insider threat detection amplifies the scale and effectiveness of existing programs without additional hiring and its associated expense.

SCENARIOS

SCENARIO 1:

PREVENTION OF IP THEFT BY DEPARTING EMPLOYEE TEAM

A sector analyst in a leading global hedge fund, disgruntled with his pay, began interviewing at a competing firm. By analyzing his communications, Cognition alerted the HR and InfoSec teams that the employee was a potential flight risk. Using our Connect investigation app a broader scheme was discovered to not only move the whole team to the new firm, but also to bring elements of the team's quantitative models.. Using this information, the firm was able to engage the team members in salary discussions and issue targeted policy reminders that resulted in the team staying with the firm, keeping the firm IP safe.

SCENARIO 2:

SOCIAL ENGINEERING

External criminals mounted a sophisticated social engineering attack, impersonating an external IT services auditor to build a pretext intended to manipulate security staff into letting them into the building. Even though the communications were not reported directly to the Information Security team, Cognition recognized the concern one of the phishing victims expressed in a message to her colleague. A quick investigation revealed that the identity was faked and the attack was thwarted.

Digital Reasoning | Finding Truth
(615) 567-8853 | info@digitalreasoning.com | digitalreasoning.com | 701 Cool Springs Blvd, Fifth Floor, Franklin, TN 37067