Insider Threat Defense

2021 | FHITDWPv01

CANDA Solutions
THINGS DONE

10500 Little Patuxent Pkwy, S. 620
Columbia, MD 21044

855.55.CANDA (22632)
info@candasolutions.com

Inc. 5000 HONOREE

2018 GREATER WASHINGTON INNOVATION AWARDS™ FINALIST

WFMC Awards for Excellence in Case Management WINNER 2017

Gartner

SUMMARY

Many organizations today are struggling with Enterprise-wide Risk visibility including Insider Threat Defense (ITD). Our approach is to facilitate, centralize, improve and simplify ITD by connecting business units of any agency or corporation with an integrated and collaborative top-down and bottom-up approach.

Multiple human factors generate a high-risk profile, whether intentional or not. Thus, any ITD solution deem successful, must leverage the interdependencies of multiple Enterprise risks, internal and external factors, audits, prioritization, measurement, mitigation and reporting of the consolidated threats to the Enterprise with a goal of shortening detection to response time.

> *In 2018, 20% of cybersecurity incidents and 15% of data breaches originated from people **within the organization**.*
> *In the same year, the average annual cost of insider-related incidents to an organization was **$8.76** million.*
>
> "An Integrated Approach to Insider Threat Management"
> Gartner, Inc. | Feb 2020 | 3981556

INSIDER THREAT DEFENSE

Combining Continuous Vetting (CV), Counterintelligence (CI) and Insider Threat into a single analysis environment ensures that each of these critical functions are sharing information in the right context and only relevant alerts are raised. We are providing a holistic approach that breaks the mold of silos and pockets of excellence, to prepare integrated context for Cyber Security, Financial, Criminal, Foreign Influence, Identity Resolution, Behavioral Risks, Human Factor, Dark Web, Open Source and Social Media analysis. Our system provides notifications / escalations on the facilities, contracts and associated the workforce / companies under risk evaluation.

Our solution truly addresses *continuous, multi-factor situational risk awareness* across the entire Enterprise, along with all suspicious and reportable activities of selected individuals outside of the workplace in a way that is transparent and protects the privacy rights.

ITD module is based on the Enterprises' ability to setup a risk baseline based on variety of data sources across critical programs and personnel, facilities within FH ecosystem to access, manage, investigate and mitigate Risk continuously.

National Insider Threat Task Force

Detection of potentially malicious behavior involves authorized insider threat personnel gathering information from many sources and analyzing that information for clues or behavior of concern. A single indicator may say little; however, if taken together with other indicators, a pattern of concerning behavior may arise that can add up to someone who could pose a threat. It is important to consider relevant information from multiple sources to determine if an employee's behavior deserves closer scrutiny or the individual has no malicious intent but is in need of help.

This approach combines:

- Activities within the Enterprise (Insider Threat actions)
- Activities outside the Enterprise using push technology (true CV) based on configurable risk indicators
- A state-of-the-art case management system view of workforce personnel data

All in order to proactively identify and mitigate the threats before they fully mature.

ANALYTICS & TRUST (OR RISK) SCORE

Notion of "Deliver Uncompromised" war fighting capabilities must be part of the overall approach of USG and DIB for protecting critical information and/or technology being wittingly or unwittingly lost, stolen, denied or degraded. Big part of the risk assessment is ITD which should include set of technical and non-technical process countermeasures to monitor compliance with organization policies and deviations from expected role-based behaviors.

Countermeasures will inform and defend against workplace behaviors (deliberate or accidental) that may adversely affect business operations. Countermeasure recommendations and tradeoffs will have to be balanced against the potential to disrupt critical business processes and will evolve as the program matures or additional resources are available for implementation.

Organizational goals, policies, rules and legal framework are deconstructed to help define triggers that will alert the network activities in violation of those business rules and objectives. Triggers will be a hybrid of previously-developed proven triggers – tested in real-world engagements – and custom triggers that can focus on specific *high-risk personnel* and known tactics, techniques, and practices of illegal activities (e.g. inside traders, fraud, data theft, espionage).

Sensors collect data and alerted activity based on trigger definitions and scripts. All relevant data is aggregated from both audit and non-audit sources (e.g. Financial or Criminal reporting, Foreign Travel, Social Media, etc.) and once an alert occurs, our proprietary workflow and case management tool guides a repeatable response showing the custody, control, transfer, analysis and disposition of the alert. Our tool triages the alert via a Risk Score to establish priority of effort.

Alerts are analyzed against expected role behaviors and other disparate data sources (i.e. HR records, social media profiles, financial background, criminal, etc.) to determine disposition of the alert. Data sources can be configured based on the user role in the organization, position sensitivity, location, or other situational knowledge. The Fresh Haystack AI Decision Engine uses a variety of structured analytic models and methodologies (SMA, Relational Network Analysis, Symantec Analysis, Content Analysis) to recognize patterns, regressions, and clustering from a number of

disparate data sources (i.e., HR records, financial backgrounds, Social Media presence, current 'workload', known associates, legal records, non-work-related travel, etc.) to build contextual evidence around the observed anomaly. As a Convolutional Neural Network, this decision engine can process additional data/decisions quickly with scalable results as the adoption of the program deepens and requirements or policy change.

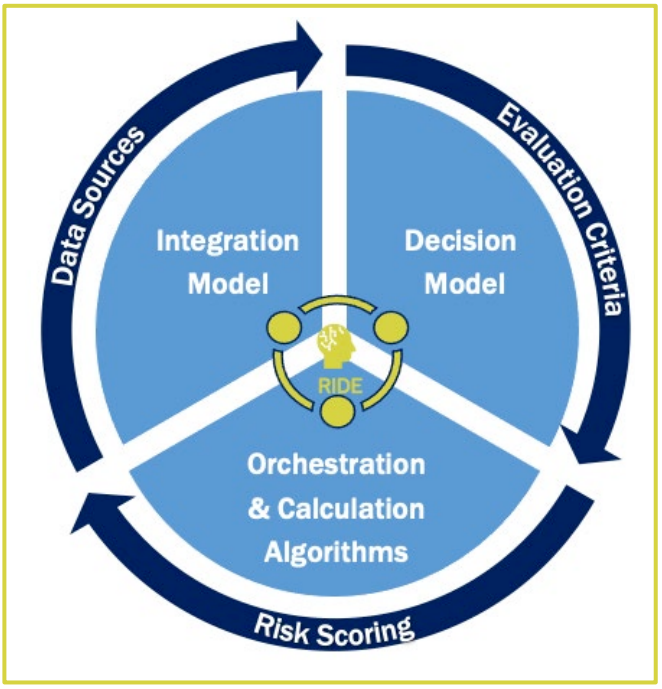
If found as a false positive or mitigable, the alert is dropped, and the profile updated. If the alerted activity cannot be explained, the analyst could recommend escalation, quality review or investigation. Once an alert is escalated, the appropriate investigative authority is integrated as the lead to adjudicate the incident. With the right tools, the Investigator can request a "focused" review of activities using customized triggers. Our tool assists in providing a managed escalation process to ensure accountability, traceability, and adherence to the chain of custody rules. Analysts support the investigator as required to resolve the event. Many of these activities can be automated or set to require manual review; it is a workflow and policy-based implementation decision that may differ across workgroups, programs or across geopolitical boundaries.

AI RIDE

As the value of U.S. Federal Government and Corporate Intellectual Property (IP), reputation, brand, and national interests increase in value, organizations will have to leverage new, cutting edge security technologies and integrations to increase protection from inside and outside threats.

Fresh Haystack innovative AI (Artificial Intelligence) RIDE (Risk Integration & Decision Engine) allows our customers to profit from true integrated risk management and data driven decision making. It is a work in progress and current features already made available are:

- Hyperautomation
- Enables any internal/external system integration
- Event Broker
- Predictive Decision Modeling
- Harmonization of Risk Silos
- Organizational Resilience



CANDA is expanding its AI RIDE capability to provide an automated system to assist any CV program with managing the risk of their enrolled individuals. Our tool imports risk data from various sources and external systems to perform the risk evaluation by both, automated determinations and by manually applying filtering and analytics within the application. Also, both the risk mapping and data sources are setup and maintained within the application. Lastly, tool could use the compliance data vs. risk-based models and apply three (3) main areas of analytics applicable to these models: Complex Event Processing (sees events in context), Predictive Analytics (rule-based matching and risk-based triggers), and Operations Research (Monte Carlo simulation for what-if analysis).

RISK TIERS & DATA PACKAGES

Fresh Haystack ITD integrates with multiple federated third-party data providers like LexisNexis Risk Solutions, ESR, TRSS (Thomson Reuters Special Services), TransUnion, Appriss and IDInsight as examples. Data sources and the criteria they cover are aggregated into sample packages: Bronze, Silver, Gold, Platinum. These data sets can be configured to form a risk factor baseline that provides similar analysis to government investigation standards, but with the capability to add additional data sets commensurate with varying configurable risk baselines across the enterprise and/or personnel population. As an example, a Professional Services firm may want to select the Bronze program for all employees and contractors that are customer facing, gaining access to customer sites, and/or operating company vehicles. Likewise, that same firm may elect to enroll employees with access to Research & Development (R&D), IP or "Keys to the Kingdom" in the Gold or Platinum program for a heightened level of inspection.

CONCLUSION

Fresh Haystack's ITD ecosystem enables the realization of a true Insider Threat Defense previously limited by technology. We believe our solution connected the dots by converging the individuals, their profiles, access, networks and activity into a single glass pane for agencies and corporations to evaluate true Risk exposure by consistently making intelligent data-driven decisions to access, track and capture mitigation opportunities while continuously delivering Trusted Workforce and minimizing Enterprise risk.