Fact Sheet

Constellation for Insider Threat

Analyze whole-person behavior, not just network activity

A malicious insider is often too well concealed to be detected using conventional data analytics solutions, and many organizations lack the internal tools to monitor risks associated with employee negligence. Among the most critical challenges currently facing security decision-makers are:

- Organizations typically become aware of threats only after an adverse incident has occurred
- Current detection solutions focus mainly on network activity and often fail to spot low-level threats, or those with no precedent, that would be evident in non-network data sources
- Analysts are overwhelmed by an excessive number of false positives, and bogged down by conflicting results
- Most big-data technology solutions don't distinguish between malicious, negligent and inadvertent events

Haystax Technology's insider-threat solution gives organizations actionable intelligence on their highest-priority threats, in time to take the preventive measures necessary to address these challenges.

Predict and prevent

Based on our Constellation Analytics Platform, the Haystax insider-threat solution continuously measures the trustworthiness of personnel in an organization, pinpointing early indications of the most serious risk from IP theft, sabotage, fraud, policy violations and other damaging behaviors. Starting with an expert model of insider risk behaviors, our platform integrates a wide array of data that's analyzed using our patented technology, and prioritized against the model. The system then displays the results in an easy-to-use interface, minus the excessive false positives generated by many network monitoring tools.

Model-first analytics

Haystax data scientists have captured the judgments of diverse insider-threat experts and transformed them into a probabilistic 'whole-person' model named Carbon, which mathematically represents over 700 distinct human behaviors as trustworthiness indicators. Data fed into the model can come from internal repositories such as HR records, access control logs and network security devices, and from public sources like news reports, social media feeds and criminal and financial records. Constellation establishes a 'pattern of life' and continuously analyzes new information to quickly discern when an individual starts deviating from the norm or trending in a negative direction.

Enterprise-compliant workflows

Constellation is designed to reason like a team of insider-threat experts and 'connect the dots' like a team of analysts – all in real time. Our solution is built to support collaborative analyst workflows and adhere to existing corporate guidelines and best practices. It enables users to create, view and edit data on individuals, conduct personnel risk assessments and manage incidents and scheduled events. With our purpose-built dashboard, a decision-maker or analyst can monitor and quickly identify the riskiest outliers, drilling down into their histories and records, viewing top areas of concern, identifying emerging behavioral patterns and viewing timelines of new incidents and organizational events. And because Constellation runs at machine scale and can be reconfigured on the fly, organizations don't have to hire more analysts as their insider threats increase or evolve.

Haystax
TECHNOLOGY
Security Analytics **Redefined**

Fact Sheet

Customer Success Stories

A large defense agency needed a more robust way to identify trusted insiders at risk of becoming active threats. The agency's complex data-management, access-control and computing solutions made monitoring personnel both extremely challenging and absolutely essential.

Haystax deployed its Constellation Analytics Platform, an innovative model-based solution for identifying risk indicators, to continuously evaluate and rank insider threats. In the initial operational pilot 4,000 highly cleared personnel were analyzed, and the group was expanded to 100,000 personnel in a subsequent operational deployment. Our model was then validated by the agency, and Haystax is now working to expand the system across the entire agency, so that all of its personnel can be continuously evaluated. As a result of this deployment, the agency has gained tighter control over its evaluation processes – while improving threat alerting, investigation timelines and information sharing across multiple functional areas. According to a recent evaluation briefing by the agency, the Haystax solution represents the "only known system for prioritizing personnel according to positive and negative nodes of trust."

Key Features

Adaptable

Model is extensible and adaptable, so it can accommodate new or evolving threats

Holistic

Connector framework makes it easy to integrate third-party data and existing detection systems quickly

Intuitive

Easy-to-understand interface minimizes user training and streamlines workflows

Mission-ready

Highly secure cloud-based software platform; can also be deployed on-premises

Key Benefits

Preventive

Focuses on individual behaviors rather than network activity, enabling users to anticipate rather than react to threats

Actionable

Decision-makers get immediate, continuously updated intelligence on high-risk individuals

Intelligent

Platform can discern even weak signals and slight anomalies, at machine scale

Transparent

Carbon model allows user to know exactly how a particular individual's risk score is calculated