FACT SHEET

Cyber-Crime Prevention

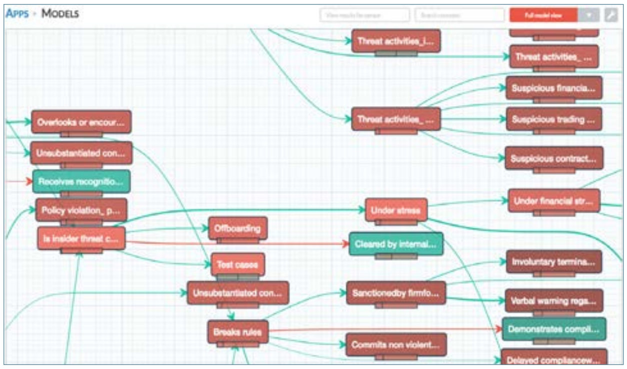
Redefining account-compromise and fraud detection

haystax

Investigating cyber-crimes can be tedious and time consuming. Security operations center (SOC) analysts are often overwhelmed with alerts, many of which are false positives. Haystax helps SOC investigators proactively connect the dots, rather than respond after an incident has occurred. Expert models of user and entity behavior, representing hundreds of key risk factors, analyze diverse data sources to identify and rank indicators of account compromise and fraud. Critically, the system pinpoints risk even when the signals are weak or the data is sparse.

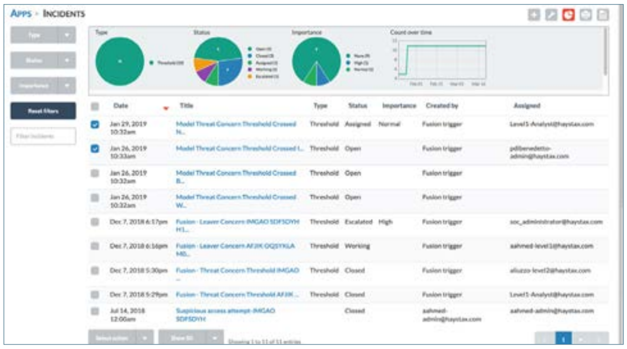
Model-driven analytics

Cyber-crime subject matter expertise is a scarce commodity, and conventional data analysis techniques used to distinguish real threats from false positives are time-consuming and rarely add value. At the heart of the Haystax solution is a probabilistic model that 'reasons' like multiple cyber-crime specialists. The model, which mathematically represents hundreds of key risk behaviors culled from subject-matter expertise, is what enables our system to detect user and entity behavioral risk indicators well in advance of an adverse event.



Holistic risk management

Under the covers, the Haystax platform does the heavy analytical lifting. Automated threat identification, triaging and prioritization ensure that analysts are presented only with their highest-priority risks, while false positives and minor alerts are filtered out. Incident alerts are automatically generated every time an individual's risk score changes by a certain percentage, and each alert can be linked to specific individuals. The system produces a transparent record of each investigation, while protecting individual privacy through redaction of names and other personally identifiable information.

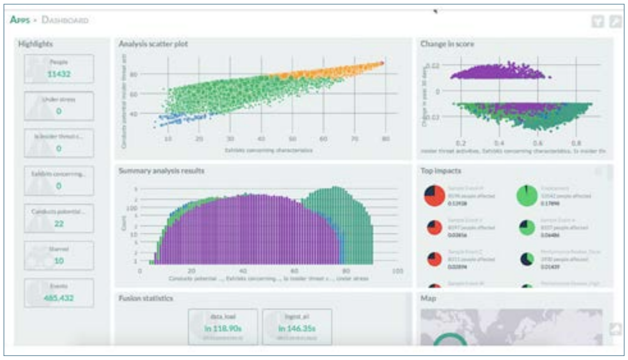


	Date	Title	Type	Status	Importance	Created by	Assigned
☑	Jan 29, 2019 10:32am	Model Threat Concern Threshold Crossed N...	Threshold	Assigned	Normal	Fusion trigger	Level1-Analyst@haystax.com
☑	Jan 26, 2019 10:33am	Model Threat Concern Threshold Crossed I...	Threshold	Open		Fusion trigger	pdibenedetto-admin@haystax.com
□	Jan 26, 2019 10:32am	Model Threat Concern Threshold Crossed B...	Threshold	Open		Fusion trigger	
□	Jan 26, 2019 10:32am	Model Threat Concern Threshold Crossed W...	Threshold	Open		Fusion trigger	
□	Dec 7, 2018 6:17pm	Fusion - Leaver Concern IMGAO SDFSDYH H1...	Threshold	Escalated	High	Fusion trigger	soc_administrator@haystax.com
□	Dec 7, 2018 6:16pm	Fusion - Leaver Concern AFJIK OQSYKLA MD...	Threshold	Working		Fusion trigger	aahmed-level1@haystax.com
□	Dec 7, 2018 5:30pm	Fusion - Threat Concern Threshold IMGAO ...	Threshold	Closed		Fusion trigger	aliuzzo-level2@haystax.com
□	Dec 7, 2018 5:29pm	Fusion - Threat Concern Threshold AFJIK ...	Threshold	Closed		Fusion trigger	Level1-Analyst@haystax.com
□	Jul 14, 2018 12:00am	Suspicious access attempt-IMGAO SDFSDYH		Closed		aahmed-admin@haystax.com	aahmed-admin@haystax.com

Showing 1 to 11 of 11 entries

Modernize the SOC

Enhancing the SOC's ability to stay ahead of evolving cyber threats is challenging, given the vast amount of data to be collected, processed and analyzed. Working in close collaboration with some of the world's largest banks, Haystax developed a suite of integrated tools that support analysts in quickly identifying new or previously hidden compromised accounts and other fraudulent activities. SOC automation is enabled via apps that ease analyst overload and support streamlined investigations and responses as part of a SOC's daily workflow.



FACT SHEET

Customer Success Stories

haystax

Haystax's solution for detecting cyber-crimes was developed in close collaboration with some of the world's leading financial institutions.

For example, National Australia Bank (NAB) has always been at the forefront of research to ensure the security of the bank and its customers, including the use of big-data technologies to identify malware and fraud. NAB worked with Haystax to test its analytics technology in relation to real-time malware identification on millions of daily transactions. The results demonstrated that encoding diverse analyst expertise and judgment in an automated system can identify multiple anomalies that have a high likelihood of indicating compromise. According to a senior NAB security official, "the Haystax security analytics platform is allowing us to move to a more dynamic and predictive risk posture." Similar results were obtained from a cyber-risk management program at a top U.S. bank, which unmasked several previously undetected inside perpetrators of fraud using the Haystax system.

> *"The Haystax security analytics platform is allowing us to move to a more dynamic and predictive risk posture."*

The Haystax Advantage

Holistic
Blends multiple artificial intelligence techniques to automate detection and response

Intuitive
Simple apps and interface mirror current workflows for rapid SOC team adoption

Focused
Highlights the biggest risk indicators, while filtering out 97% of all false positives

Adaptable
Scales to the volume and velocity of existing threats, and adapts to new threats as they emerge