PROACTIVE THREAT HUNTING

AI POWERED USER BEAHVIOR ANLYTICS & USER ACTIVITY MONITORING

Cerebral
INSIDER THREAT INTELLIGENCE PLATFORM

Insider Threat security has become the Achilles' heel of many corporate security strategies. Relying on network data (SIEM), or trying to lock down documents (DLP) is simply an incomplete security strategy when it comes to protecting a corporation's critical data from internal threats.

Integrated & Intelligent

Unlike standalone monitoring or analytics tools, Cerebral provides an end-to-end solution, integrating User & Entity Behavior Analytics (UEBA), that immediately identifies insider threats, with User Activity Monitoring (UAM) allowing security to see the related screenshot evidence. This visibility allows security to rapidly react with 100% confidence. Cerebral also provides the essential visual evidence you need to take legal action.

Threat Hunting

The ability to hunt threats by recognizing signs of threat, like changes in an employee's attitude and behavioral patterns, allows you to move your security posture from reactive to proactive.

Daily Risk Scores Cerebral's AI-based behavior analysis, continually tracks each user's activity and language characteristics (psycholinguistics) to create daily risk scores for the organization. The Risk Score dashboard shows high scores for each day, trends, recent alerts, and user details. It provides an immediate overview of high risk, user behavior within your organization, minimizing risk while maximizing productivity by allowing your security team to hunt threats proactively.

60%

of cyber attacks are carried out by insiders

IBM X-Force Cyber Security Intelligence Index

"Advanced forensic data analytics is becoming an indispensable tool to detect Insider Threats."

Ernst & Young Managing Insider Threats, a holistic approach to dealing with risk from within

51%

of CISOs say insider threats are the greatest security threat they are facing.

Cyberark Global Advanced Threat Landscape Report 2018

Risk Score Dashboard

Predictive Analytics powered by AI

Cerebral continually monitors every endpoint and builds a digital fingerprint for each user and group. Additionally, Cerebral is watching for customized keywords and triggers specific to the organization.

When there are anomalies, significant variations from the established behavior baselines, an alert is triggered so that the investigation and remediation can begin immediately, often before the real damage is done.

Because Cerebral also integrates User Activity Monitoring, investigators can immediately review the screenshot videos of the actions that triggered the alert or elevated risk score. This visibility reveals the true context of the incident, allowing the investigator to take immediate action.

To create the dynamic digital fingerprint for all users on a network, Cerebral analyzes:

- Network usage
- Program usage
- File & document tracking
- Geolocation
- Web & Dark Web activity
- Imposter indicators
- Chats & IMs
- Keystroke logging
- Emails activity
- and more…

Psycholinguistics

Veriato's proprietary AI algorithm detects disgruntled users by monitoring email language to identify shifts in sentiment to identify disengagement and signs of threat.

Eyes On Glass

Watch video playback of a user's on-screen actions from 5 minutes ago or 5 days ago. These videos can be exported as JPG or AVI files and used as legal evidence.

The Impact of Veriato Cerebral

The ability to predict and react with speed and confidence is at the core of a mature, internal threat detection & data protection strategy.

Speed of Discovery is critical in minimizing damage. Without AI to rapidly detect anomalies (e.g., imposters in the network or unusual user activities), vast amounts of data can be siphoned over weeks or months. Veriato uses the most advanced machine learning algorithms to analyze and predict risk from the vast amounts of endpoint data that are continually collected. However, discovery alone is not enough.

Speed of Remediation is governed by your ability to determine precisely what's happening. With Cerebral lengthy investigations to determine what a network alert actually means are eliminated. Because you can immediately see the screenshot evidence, you can respond rapidly with 100% confidence, backed by the visual evidence crucial for remediation as well as HR or legal action.