GURUCUL
PREDICTIVE SECURITY ANALYTICS

Threat Analytics Platform™

DATA SHEET

Threat Analytics Platform

Machine learning models can surpass human capability for large volumes and variety of data to find high-order interactions and patterns in data for complex problems such as insider threats, compromised accounts and fraudulent activity. Identity is a threat plane with hundreds of attributes to model in algorithms resulting in predictive security analytics to drive 'find-fix' resources. Identity access intelligence and user behavior analytics data science is a force multiplier for IT security teams.

"A manufacturing company discovered on the second day of use of Gurucul's risk analytics that two of their research accounts had been hijacked."

NETWORKWORLD
May 2015

Why consider Threat Analytics Platform (TAP) ?

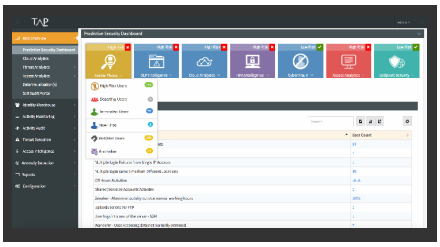
- Predict, detect and deter insider threats and cyber fraud
- Protect intellectual property and prevent data exfiltration
- Detect high privilege account abuse, account hijacking and anomalous activity
- Prevent ID theft through risk-scored event time lines and end user self-audits
- Enhance Security Information and Event Management (SIEM) and Security Analytics intelligence
- Improve Data Loss Prevention (DLP) intelligence with risk-scored alerts based on behavior analytics
- Optimize security resources and time with self learning and training machine learning algorithms

GURUCUL | 222 N. SEPULVEDA BLVD., SUITE 1322, EL SEGUNDO, CA 90245 | 213.259.8472 | INFO@GURUCUL.COM | WWW.GURUCUL.COM

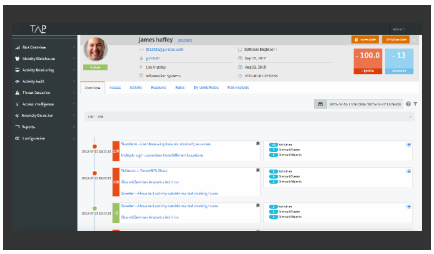
What are TAP features and benefits?

- Risk-scored time line to predict, detect and deter insider and advanced threats
- Identity-based threat plane behavior analysis for account hijacking and abuse
- Proactive and actionable alerting for anomalous behavior and risk scores
- High privilege access anomaly detection for misuse, sharing, or takeover
- Customizable dashboards, configurable policies and risk model optimization
- Work-centric UI with case management, or input to third-party solutions
- Self-audit portal deputizes users for risk awareness to detect identity theft

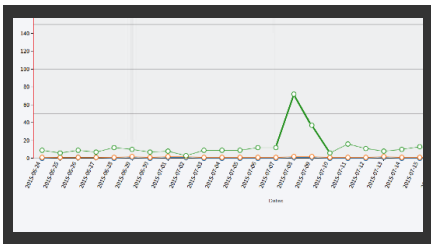
Visualization value from TAP



Predictive security dashboards provide a focused starting point for various use cases.



Risk-scored timelines provide a 360-degree view for identity, access and activity.



Dynamic peer group analysis quickly shows anomalous activity for various data sources.

What makes TAP more effective?

- Core architecture is built on PIBAE™ (Predictive Identity-based Behavior Anomaly Engine)
  - Behavioral machine learning algorithms based on 254 attributes to profile identity
  - Self-learning and training algorithms are contextually aware for transaction scoring
  - Dynamic peer groups improve clustering and outlier machine learning accuracy
  - Awareness to time-based norms such as accepted workflows and operational changes
  - Built for scale with big data foundation and flexible meta data framework
- Inclusion of identity management and privilege account management data sources
- Out of the box algorithms learn anomalous behaviors immediately upon deployment
- Fuzzy logic and linked data analysis automates mapping of activity and accounts to identities
- Big data architecture ingests historical data to speed self-learning and training

About Gurucul

Gurucul is changing the way enterprises protect themselves against insider threats, external intruders and cyber fraud on-premise and in the cloud. The company's user behavior analytics and identity access intelligence technology uses machine learning and predictive anomaly detection algorithms to reduce the attack surface for accounts, unnecessary access rights and privileges, and identify, predict and prevent breaches. Gurucul technology is used globally by large enterprises in finance, banking, insurance, manufacturing, hi-tech, pharmaceutical and retail.

GURUCUL | 222 N. SEPULVEDA BLVD., SUITE 1322, EL SEGUNDO, CA 90245 | 213.259.8472 | INFO@GURUCUL.COM | WWW.GURUCUL.COM