GURUCUL

Threat Analytics Platform™

DATA SHEET

Threat Analytics Platform

The mean time to detect a breach for organizations is over 90 days, while the average cost per incident in the US is one million dollars. The threat plane continues to expand with growing gray areas where traditional security strategies can no longer cope. There is too much data for humans to manage. Meanwhile, complex problems such as insider threats, compromised accounts and fraudulent activity continue to rise. A force multiplier is required. Machine learning models can surpass human capability for large volumes and variety of data to find high-order interactions and patterns in data revealed as anomalous and malicious behavior. The advanced data science of user and entity behavior analytics (UEBA), along with identity analytics (IdA), delivers the force multiplier needed for IT security teams. Hundreds of attributes modeled in machine learning algorithms result in predictive security analytics to drive ‘find-fix’ resources and provide comprehensive risk-based security monitoring through Gurucul Risk Analytics (GRA).

> ***“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

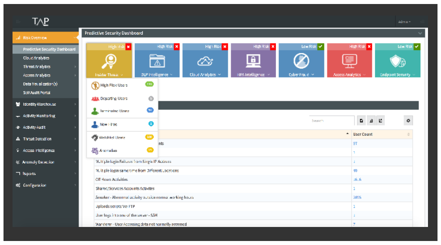
Why consider Gurucul’s Threat Analytics Platform (TAP)?

- Predict, detect and deter insider threats and cyber fraud
- Protect intellectual property and prevent data exfiltration
- Detect high privileged account abuse, account hijacking and anomalous activity
- Prevent ID theft through risk-scored event timelines 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 self-training machine learning algorithms

What are TAP features and benefits?

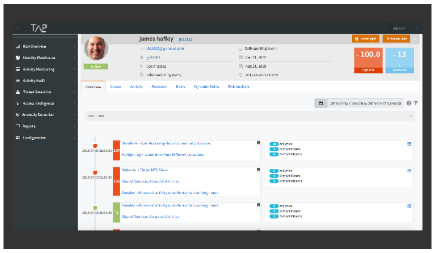
- Risk-scored time line to predict, detect and deter insider and advanced threats
- Identity-based threat plane behavior analysis for account hijacking and abuse
- Proactive and actionable alerting for anomalous behavior and risk scores
- High privileged access anomaly detection for misuse, sharing, 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



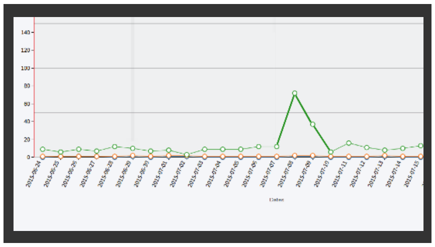
Multiple login Failures from Single IP Address
Multiple login same time from Different Locations | 10
Off Hours Activities
Shared/Services Accounts Activities | 1
Sneaker - Abnormal activity outside normal working hours
Uploads scripts Via FTP | 1
User logs in to one of the server - SSH
Wanderer - User Accessing data not normally accessed | 7

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



Wanderer - User Accessing data not normally accessed
Multiple login same time from Different Locations
Writes to a File on NFS Share
Shared/Services Accounts Activities
Sneaker - Abnormal activity outside normal working hours
Sneaker - Abnormal activity outside normal working hours
Shared/Services Accounts Activities

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



Dynamic peer group analysis quickly shows anomalous activity for a wide range of data sources.

What makes TAP more effective?

- GRA's 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 self-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 metadata framework
- Inclusion of identity management and privileged 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 self-training

About Gurucul

Gurucul is changing the way enterprises protect themselves against insider threats, external intruders and cyber fraud on-premises and in the cloud. The company's user and entity behavior analytics (UEBA) and identity analytics (IdA) 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