Insider Threat Analytics
&
Anomalous Behaviors

By
Carl Miller
Security Strategist

GURUCUL
PREDICTIVE SECURITY ANALYTICS

Challenge

Too Much Data

Data Volume & Growth → **Data Silos & Expenses** → **Big Data Lake Adoption**

Challenge

Too Few Resources

Staffing, Budget & Talent → **Alert Fatigue & Dead Ends** → **Leverage Machine Learning**

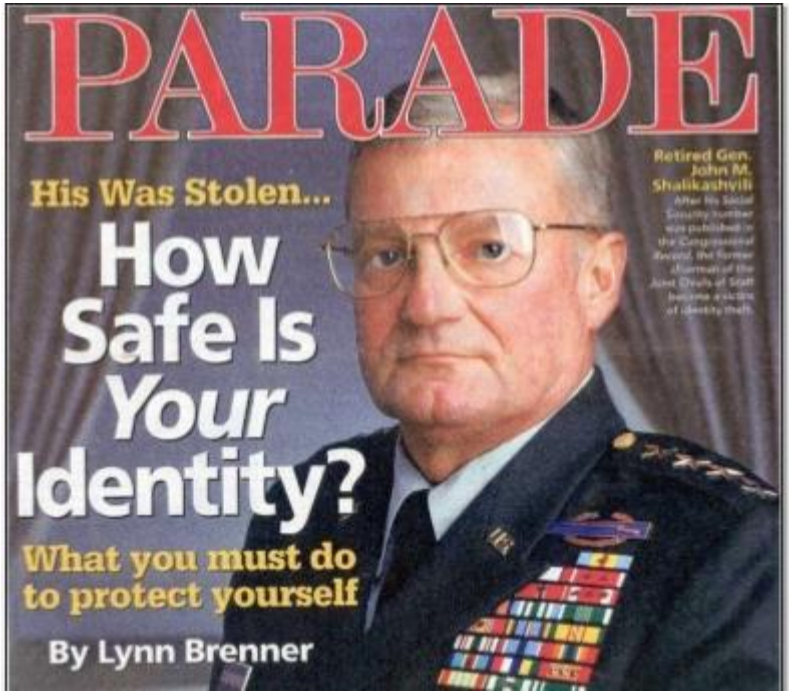
Challenge

Fading Perimeter

Cloud, Mobility & BYOD → User Apps & Data → Identity Attack Vector

Challenge

New Attack Vector



Identity Compromise & Misuse → **Evades Declarative Defenses** → **Core of Modern Threats**

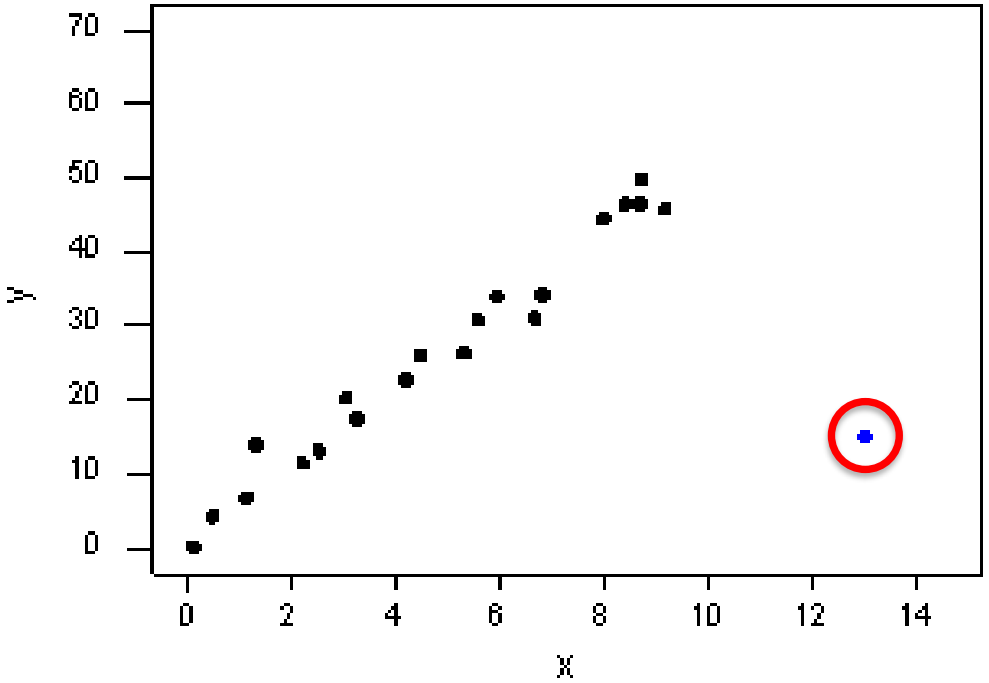
Solution

Behavior Anomalies

Big Data & Data Sources → **Machine Learning Models** → **Behavior Analytics & Risk Scoring**

Anomaly Detection

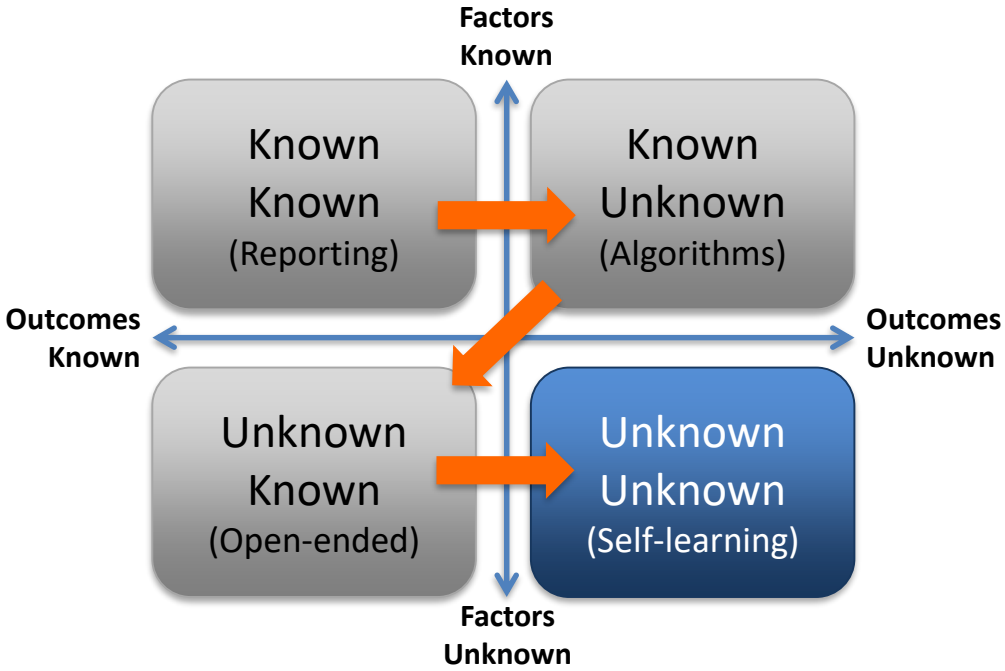
Solution



User Entity Peers → **Access and Activity** → **Clustering w/Outlier Analysis**

Solution

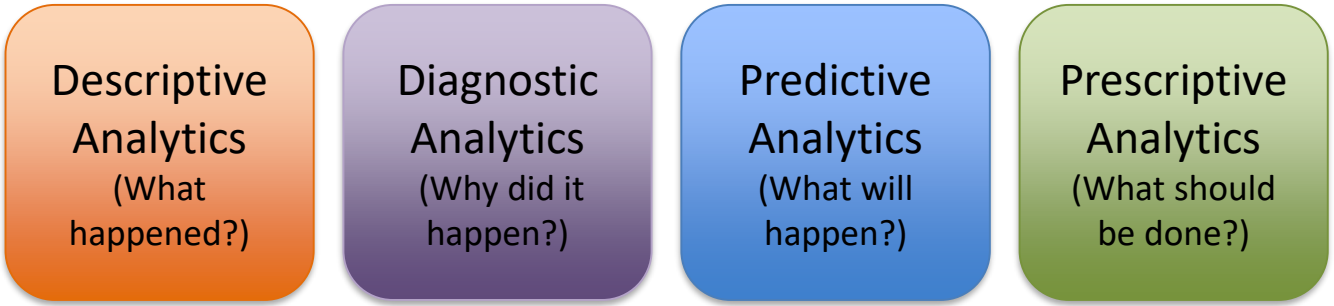
Unknown Unknowns



Declarative Defenses & Rules → **Correlations Causality & Hunting** → **Predictive Security Analytics**

Analytic Maturity Model

Solution



Data Silos
Missing Data
Dirty Data

→

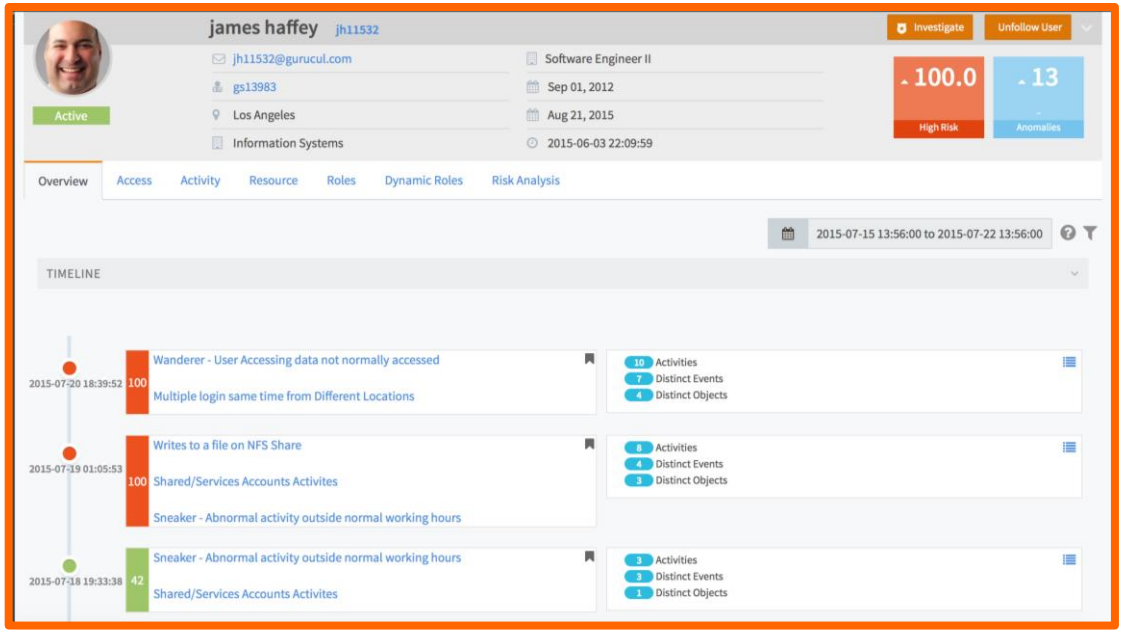
Data Lake
Open APIs
Use Cases

→

Hybrid Visibility
Closed Loop
Auto. Response

User/Entity Behavior Analytics

Solution



Privileged Access Abuse → **Data Exfiltration & Theft** → **Insider Threats & Self-Audits**

Solution

Identity Analytics (IdA)

Excess Access & Outliers → **Risk-based Certs & Approvals** → **Dynamic Access Provisioning**

Privileged Access Analytics

Solution

Hidden Privileged Access → **Outside Lists & Vault** → **Entitlements Determine Privileged Access**

Custom ML Models

Solution

Military
Federal
Financial

→

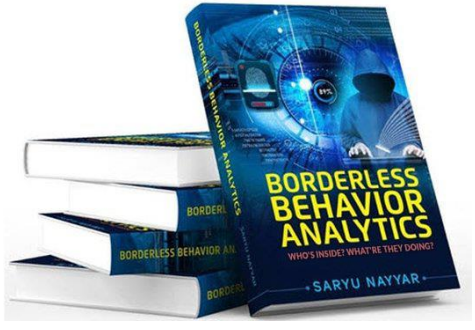
Private
Data &
Use Cases

→

Custom
Model
Creation

Thank You!

To Learn more about behavior analytics:



Available at amazon

www.borderlessbehavioranalytics.com

GURUCUL
PREDICTIVE SECURITY ANALYTICS