ANOMALIX

ANOMALIX
CASE STUDY

Identity Analytics: Detect and Respond to Anomalous Access Behavior

Identity Analytics: Detect and Respond to AnomalousAccess Behavior

Background –Global Financial Services Client

A Global Financial services company selected Anomalix to build an Identity Analytics engine to detect anomalous access related behavior. Specifically, the client was looking to implement real-time activities that would enable:

1. Correlate Access Related information from disparate sources (HR, CRM, SFA, Applications, Databases, Servers, Firewalls, Logs, etc.) into a single Identity object
2. Establish and Consume Access Related Policies (SoDs)
3. Detect when policies are violated and revoke access in real-time at the Network, Server, Database or Application tier

How We Helped

Anomalix was able to establish a baseline of common access across the various functions (consumer, employee, partner, contractor, vendor) with high turnover.

By identifying specific access "routines", Id Genius was able to identify a common set of access required by user. When the Identity goes outside their routine access, Policies are evaluated and enforced that identify and disable access 1000X faster than the existing Security Information and Event Management tool. An increase of 1000% of anomalous activity is identified in the first 30 days alone.

Conclusion

1. Mined over 2MM Identities to establish an access baseline (the "Access Routine") for each Identity
2. Created 100 basic security policies at the log level to identify:

- Membership Logic for all Job Roles
- Failed Authentication Attempts
- Geographic Boundaries for in each "Access Routine"
- Last Request
- Network Access Behavior mappings

3. Rogue Access – Sensitive (Application, Database or Server-level access) Access Not previously established in Access Routine for an Identity
4. Automated revocation rules disable Network/Perimeter/Application access any high "Threat-Level" account

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144