Top Financial Services Company: Implements an identity intelligence and analytics framework to monitor identity threat and insider risk of fraud or theft of corporate data

Our client, a global financial conglomerate, was lacking an effective centralized solution to analyze internal user access to their complex, disparate and autonomous set of business critical applications and systems. They contracted SDG to perform an assessment of their environment and to design a solution that would help them collate analytical information to secure their assets against undesirable access from within the enterprise. SDG developed an Identity Discovery Engine (IDE) and a governance framework that would allow them to detect and prevent data exfiltration and breaches through ongoing analysis, rigorous controls and policy adherence and an audit ready access control framework that would help them protect their assets against Internal and Advanced Persistent Threats (APT)

KEY CHALLENGES

In the current environment of increasingly stringent regulatory and audit requirements, identity and access management is critical to business operations and data security. The client has multiple, disparate, mission critical applications that are using manual and inconsistent access controls for highly privileged accounts (HPA) and non-HPA account types. At the systems level the situation is even more dire. Their environment contains HPA that are uncontrolled and inappropriately shared across the operating system and database layers. Current authentication and access controls and processes do not provide the level of protection needed against unauthorized access and potential data loss. Recent audit themes reflect control weaknesses in policies and procedures and account lifecycle management. The combination of all these factors has put them at risk from internal as well as external threats through potentially exploitable applications, platforms and databases.

In an effort to control risk and for audit purposes, the client has an existing process to gather and analyze identity access data from various access management systems. However this process is systemically error prone and inconsistent. The client experienced the urgent need for a new and improved automated solution to aggregate and analyze user identity and access information, so that they could continuously refine their access control and entitlement processes and drive consistent compliance policies andprocedures throughout their enterprise.

BENEFITS

Minimize the likelihood of an APT or Insider exploit by:

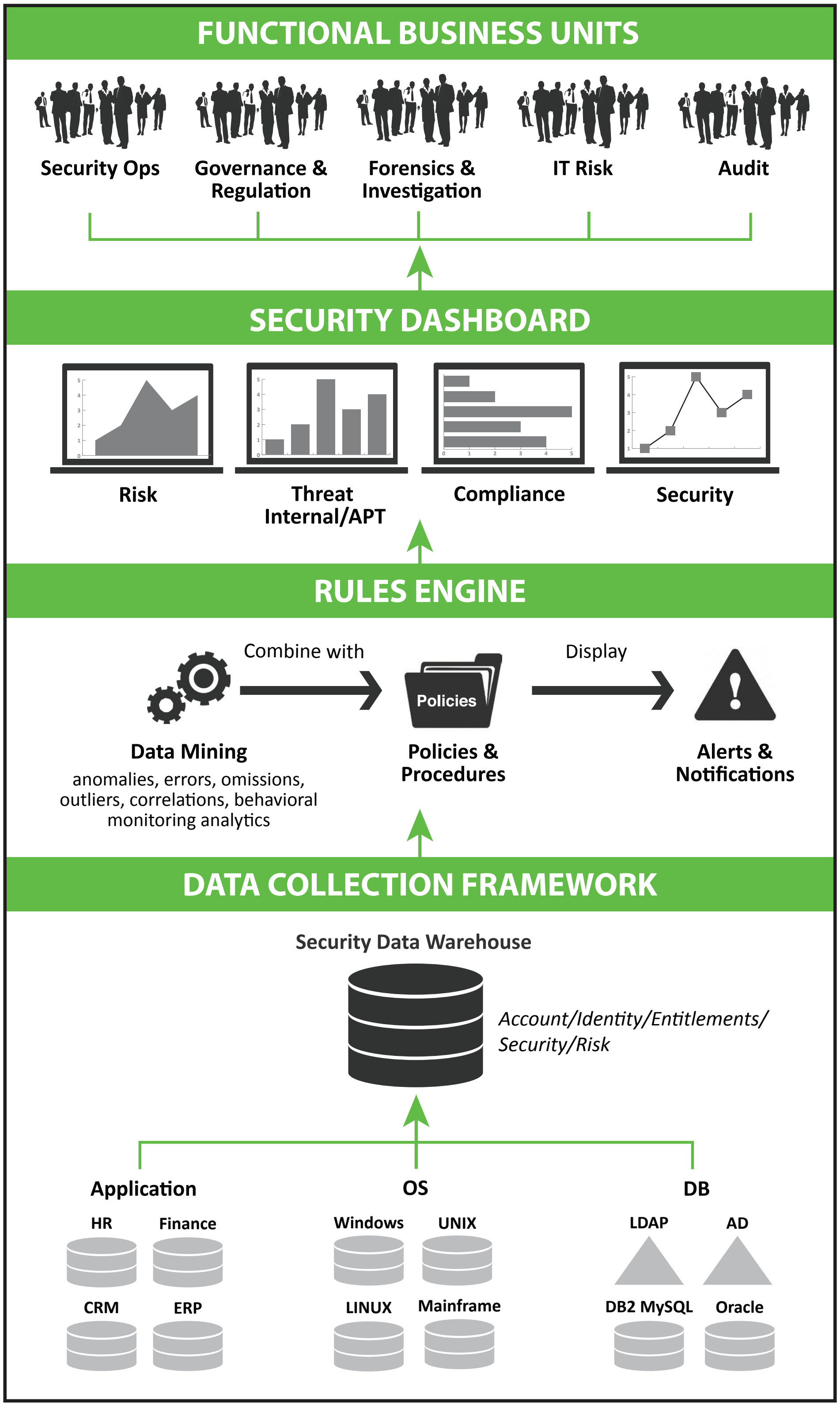
- Enabling account lifecycle monitoring and the timely validation and removal of unneeded or excessive access
- Reducing the risk of sensitive data compromise or theft by proactively detecting threats
- Reducing time for investigation and action by the Incident Response Team
- Improving the effectiveness of compliance policies and procedures
- Enhancing controllership and minimizing data loss
- Eliminating the dependency on inaccurate and error prone manual processes
- Increasing operational efficiency and reducing cost

SDG SOLUTION

The SDG technical team first performed an initial assessment of the current identity and access control infrastructure, systems and processes employed by the client. They analyzed identity access information, and identified data gaps and process risks for each of the systems, and made recommendations for process changes.

They then designed an Identity Discovery Engine (IDE), a rules based engine that will provide an insight into system access data, of authorized users and other identities with elevated privileges/entitlements, across the enterprise. This solution will leverage a Security Analytics Platform and will:

- Discover and collect identity and entitlement information from all the source systems across the enterprise and load it into a centralized repository data warehouse. The data will be used for identity and entitlement governance, regulatory, audit and compliance purposes as well as for threat analysis, modeling and analytics.
- Correlate access patterns and identity attributes and privileges to detect threats in accordance with the client's policies; and generate alerts that will allow the security team to take action. Typical threats include:
  - **Terminated or role change accounts**
  - **Inoperative/dormant accounts**
  - **Uncorrelated/ghost/orphaned accounts**
  - **Rogue accounts**
  - **Uncharted accounts**
  - **High risk entitlement accounts**
  - **Accounts that violate regulatory requirements**
  - **Password policy violations**
  - **Separation of duty (SoD) violations**



[technology + passion] - risk