ANOMALIX

ANOMALIX
WHITE PAPER
Identity And Security Analytics

Identity And Security Analytics

Identity and Access Governance (IGA) solutions have enabled organizations to automate tedious, but necessary, access certification/access review campaigns that span business and compliance relevant access throughout the organization. These access reviews or access certification campaigns are typically conducted quarterly. However, the historical context of access (how it was requested, who approved it, and when was it last reviewed) and access usage (when's the last time the access was used, how often is the access used) are helping organizations to reduce the time performing reviews and providing insight into the data and access that needs to be prioritized.

A true risk-based approach is qualitative and quantitative. Risk scoring alone is fallible as it only considers how many entitlements are associated with a given user, but not how the user interacts with those sensitive entitlements. Most often, you'll find the Identity and Access Governance tools is merely a snapshot of a point in time collection. Therefore, Identity and Access Governance tools are only as good as their last data collection. The data collection is constantly overwritten and only shows what entitlements a particular Identity has, as of the collection.

The reason is that market-leading Identity and Access Governance solutions were never architected for a vast amount of data and rely solely on relational databases, which are not built for machine learning, historical context, or deep analytical insight.

Consider What a Risk-Based Approach Looks Like

Taking an accurate Risk-based approach to Identity and Access Governance starts with a big-data architecture that will consume inputs that identify how access is being used. Anomalix collects Identity data such as HR repositories (PeopleSoft, Workday, Active Directory, etc.), LDAP repositories, and Contractor/1099 Worker Databases (any RDBMS where Identity data is stored). This Identity data is then correlated to:

- SSO/MFA
- IAG
- VPN
- RDBMS Logs
- Application Logs
- Server Logs
- GRC
- DLP
- Virtual Machines
- Malware (FireEye, Palo Alto, Wildfire)
- External Threats (FS-ISAC, Google CIF)
- Cloud (AWS CloudTrail, Mobile Device Logs, Box)EndPoints (App Logs, Security Logs, DB Logs, Server Logs)
- Custom APIs (Java, JavaScript, REST, SysLogs)

We can now establish a holistic baseline of who has access to what sensitive information. More importantly, we now know "who is doing what" with sensitive/high-risk access.

The next step is to build a baseline of "normal" Identity activity based on time, geography, transactions, and session information. That baseline is continuously gauged against a peer group of Identities to further monitor the "normal" baseline for an Identity given their respective organizational responsibilities through credential modeling. Anomalix automatically builds a dynamic baseline of user behavior through profiles of when, where, and how Identities employ credentials to access sensitive company resources. Anomalix then builds peer groups which can be used to centralize user access and efficiently perform access reviews, while streamlining the Joiner, Mover and Leaver process. Once Anomalix detects anomalous behavior, it will reference supervised and unsupervised algorithms to determine if real-time action is warranted. An example might be that most DBAs run queries against production databases after midnight on weekends for routine maintenance. Since this is the norm for that peer group, the activity is logged and associated with a lower risk level.

Anomalix is able to detect Rogue Access or access that did not go through the proper approval and request channels. Rogue access is then routed for action or disablement. Anomalix can help organizations to automatically identify access that should be cleaned up and removed due to inappropriate access or legacy assignment that is no longer valid given current business responsibilities.

Further, Anomalix allows organizations to take a Risk-Based approach to access certifications to focus only on Identities and Access that impact the business. Far too often, organizations are finding themselves in a state of access certification fatigue where every quarter every user and all their access is being reviewed unnecessarily. Anomalix's customers are doing fewer access certifications and simultaneously increasing their audit and compliance posture. Access requests are streamlined because all requests are evaluated for risk and organizational Segregation of Duties violations, only high risk and potential violations are routed for approval. This significantly reduces the amount of business user involvement in the request process.

Anomalix enables accurate Dynamic & Polymorphic Threat Detection by leveraging supervised and unsupervised algorithms that construct a risk profile through a multidimensional lens. Anomalix provides continuous Machine Learning, Graph Analysis and Behavior Analytics for Users and Entities (IoT). Since anomalies don't always pose a risk, Anomalix cuts through 99% of false positives to enable actionable line of sight through the kill chain by leveraging user/entity behavior and identity context.

Benefits

FAST, SCALABLE DATA COLLECTION – Anomalix enables vast data collection through a heterogeneous engine that will span the breadth and depth of required identity and security-related information and data.

USER AND ENTITY BEHAVIOR ANALYTICS – Dynamic user profile and peer group enhancements that provide real-time and historical user behavior context to empower business decisions.

REAL-TIME RISK-BASED POLICY ENFORCEMENT – Detect real threats in real-time and take action by filtering through the 99% of false-positive events and alerts, Anomalix provides the ability to identify suspicious and anomalous threats, internally and externally, and react based on risk to organizational resources.

IDENTITY AND SECURITY DASHBOARD – Anomalix provides an intuitive User Interface that maximizes the user experience. The Anomalix Dashboard (charts, graphs, and organized data points) quickly identifies Identity and Security related anomalies concerning Authentication, Authorization, Geo-location, Vulnerability, Access Requests, Policy Violations and Enforcements, Peer Group Behavior and Security Investigation.

ADVANCED THREAT MONITORING – Anomalix improves threat detection cycles by over 1000% when compared to SIEM capabilities alone. Most SIEM tools do not enable real-time capabilities with organizational, risk-based policy enforcement to predict user behavior and plan for an automated response or manual response.

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

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