Tuebora
SELF DRIVEN IAM

Tuebora Machine Learning Platform
Self-Driven Identity and Access Management with Machine Learning

Overview
Machine learning has become popular as a way to detect specific activity patterns in human activities. It usually involves collecting log data from multiple sources, normalizing the data, and then using custom or off-the-shelf algorithms to identify activity patterns in the data. Once machine based analysis is complete, the system will present time-based activity patterns to a human to decide if the pattern indicates normal or outlier behaviors.

There are multiple benefits to using machine learning over static rules. A static approach monitors change through the use of activity thresholding and does not take into account changes in behavioral change due to organizational change. Static models don't react to behavior changes that result from transfers to a new location, promotions, changes in an activity schedule, or changes in responsibility. Machine learning uses algorithms that can identify and measure activity changes in the business environment, identify habitual behaviors, suggest process changes, and provide business decision support. Common use cases for machine learning are found in retail suggestion engines, fraud detection, account take-over detection, and internet advertising applications.

Identity and Access Management (IAM) Machine Learning Use Cases
There are two key IAM metrics where machine learning can have a positive impact. First, due to organizational silos, line-of-business application ownership, and the spread of heterogeneous IAM applications from on-premise to the cloud, it is very difficult to efficiently provision and govern access. As employees wait weeks for many one-off approvals for access, they can't be as productive in the work force as they could be. As they wait for access, employees create tickets adding to support team stresses. At the same time, access provisioning IT teams often do not have the visibility needed to react to the constant addition of new applications and the requirement to constantly analyze and adjust provisioning policies.

For security teams, phishing attacks resulting in employee identity theft makes identity the new security perimeter. Stolen credentials have been found in malware specifically designed to impersonate an employee looking to steal valuable data. This has reaffirmed the necessity for ensuring that employees do not have more access than they need and that unused access is promptly revoked.

Tuebora's Identity and Access Management Platform
Using a vast library of APIs, pre-built connectors, and support for the Cross-domain Identity Management Standard (SCIM), Tuebora's IAM platform scales to collect data from hundreds of business applications and IAM infrastructure applications on-premise and in the cloud. The platform uses algorithms to provide real-time analysis of the activities of provisioning teams and suggests new provisioning rules that increases efficiency. As a result, employee productivity is increased at a quicker pace.

The platform also uses employee access data to analyze access to applications over time. This application of machine learning algorithms to the data allows for accurate judgements about whether or not employees have more access than needed or if access is unused. Removal of unused access supports the business goal of reducing risk (see Figure 1). The same connectors and APIs can be used to automate behavior-based access revocation and provisioning across the organization.

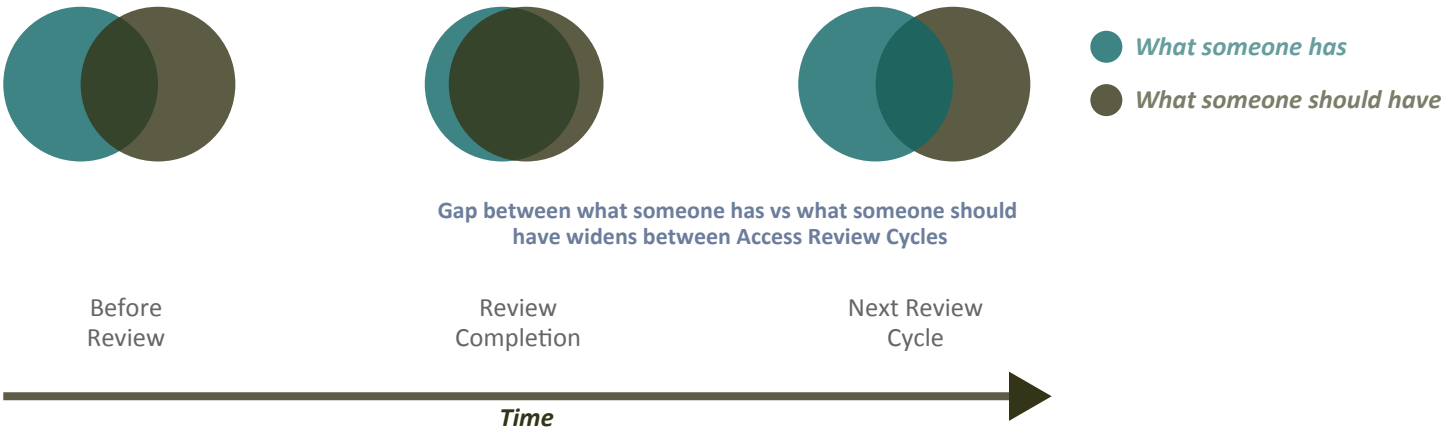

Figure 1 - Organization Access Profile between Review cycles using existing solutions

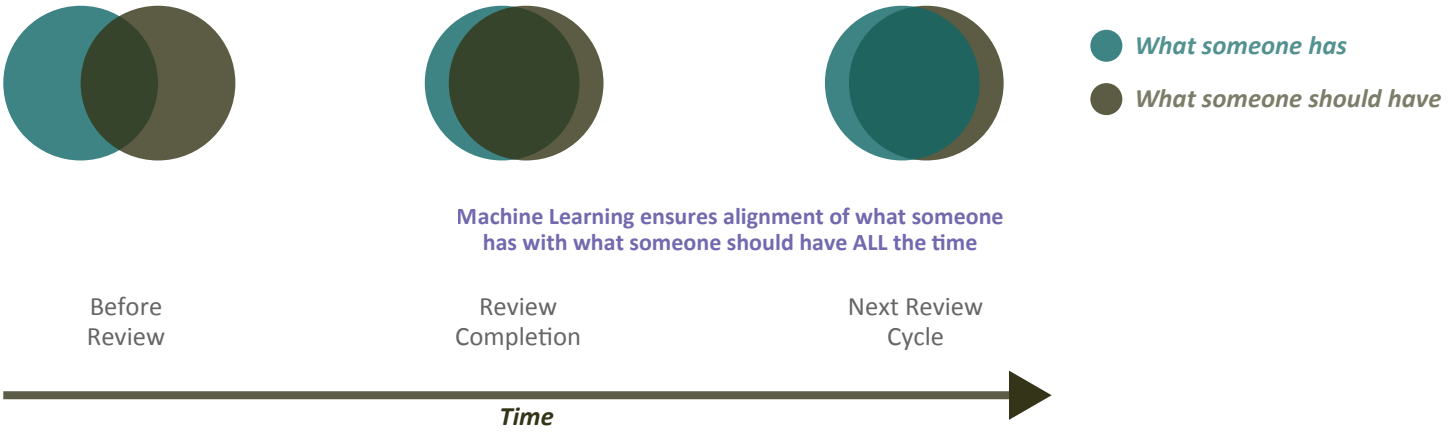

Figure 2 - Organization Access Profile between Review cycles using Tuebora