Bay Dynamics

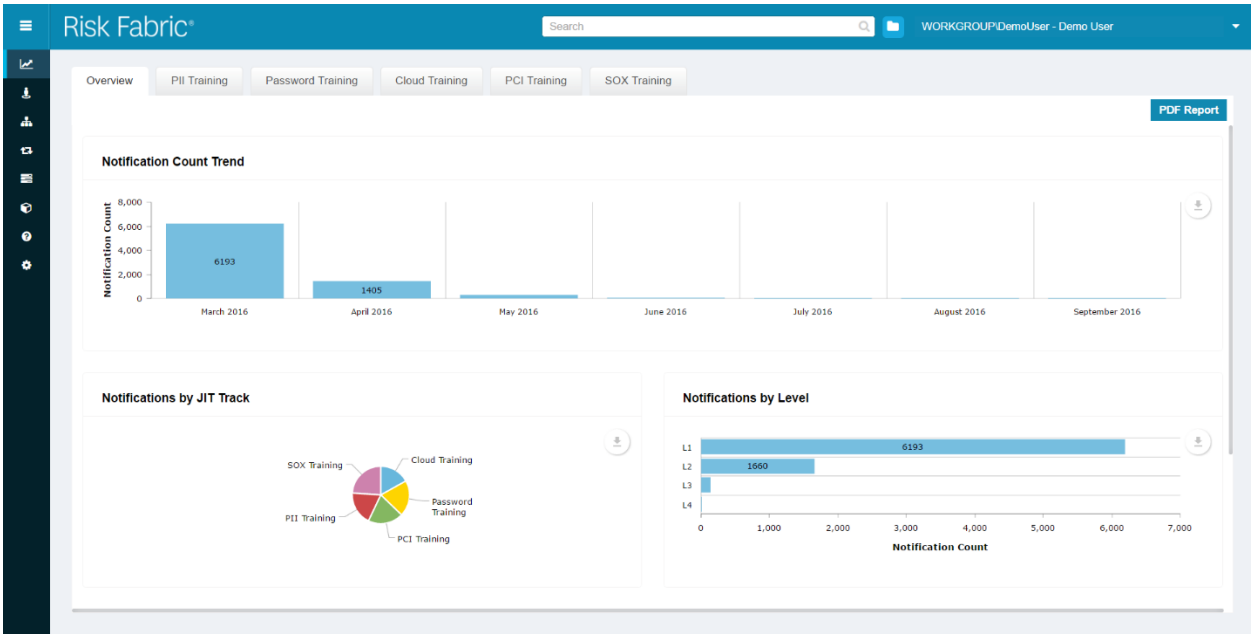
Risk Fabric®

Behavior Based Security Awareness Training Provides Policy Specific Training at the Time of Violation

Not Another Multi-Hour Compliance Training

Employees are on the front lines of data protection. Most just want to do the right thing while getting their jobs done. Unfortunately, due to poor training, carelessness or broken business processes, people take the path of least resistance and often violate policies. This not only puts the enterprise at risk by opening the door to a damaging compromise, but it also adds noise to detection tools, making it that much more difficult to decipher threat alerts.

The typical enterprise security awareness program involves a comprehensive annual training session for all employees, that may last a couple hours and cover the full spectrum of good cyber security hygiene. Although the training checks the compliance box, enterprises have realized that it is not the most effective model for changing user behavior. Employees are overwhelmed by the large body of generalized information being presented. They don't understand how it relates to their day to day work lives and oftentimes don't pay attention during the session.



Training Provided at Teachable Moments Reduce Risk and Reduce Noise

Risk Fabric® identifies risky behavior of non-malicious users, repeat offenders, and third-party vendors, automatically notifies them and their manager, and signs them up for policy-specific Just-in-Time Security Awareness Training. The training is personalized, concise, and focuses on the specific policy the user has been violating.

For example, let's say Risk Fabric flags an employee as a repeat offender of sensitive data handling policies. The system can send a personalized notification to the offending employee, their manager (or vendor manager, if a third party) and sign them up for a 10-minute, sensitive data handling training session. Risk Fabric's Just-In-Time Security Awareness Training tracks the attestation of completion of the required training, and monitors user behavior after completion. In addition to the impact on the users themselves, security awareness management and executives can monitor the effectiveness of training based on actual changes in user behavior.

Targeted awareness and education at the time of violation has proven to be a winning formula for changing user behavior, reducing risk and minimizing noise.