Bay Dynamics®

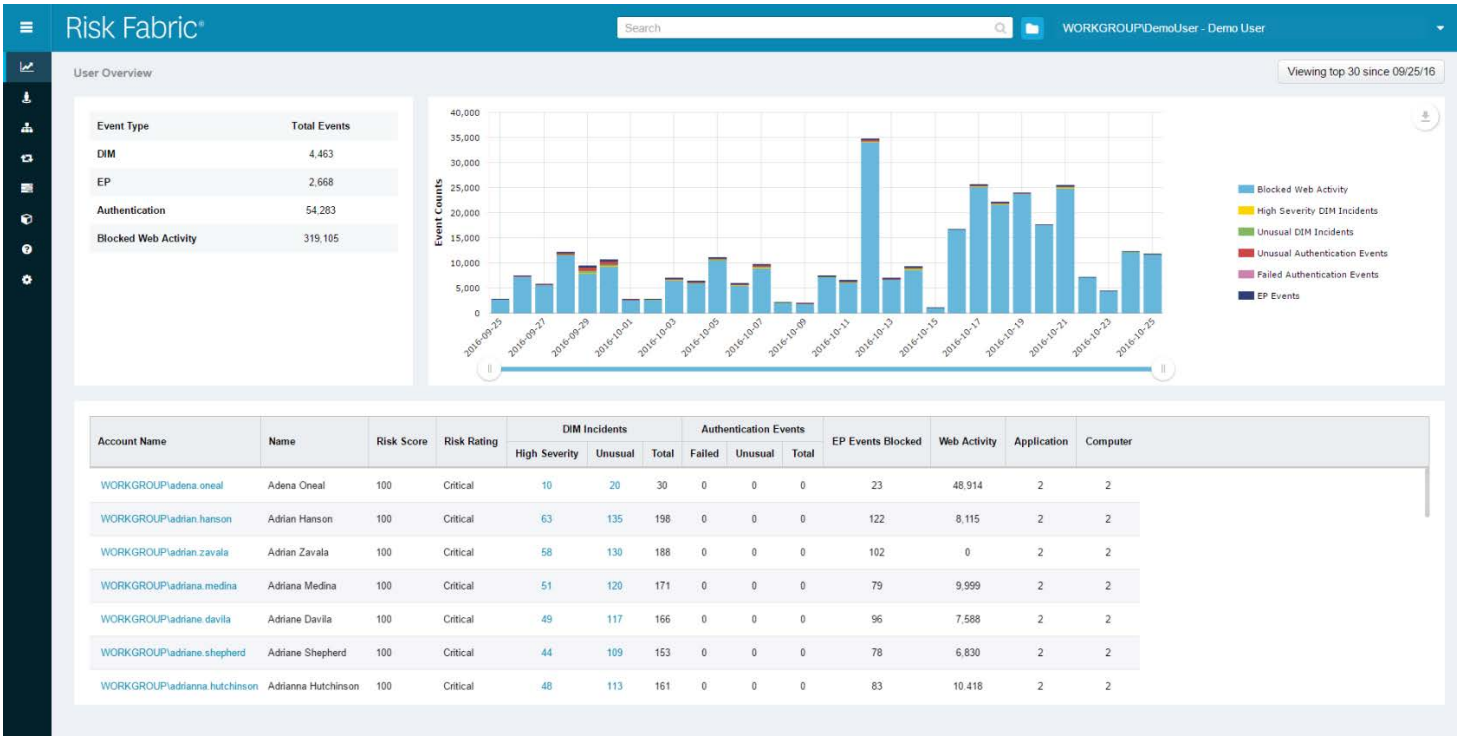
Risk Fabric®

Enabling enterprises to prioritize threats based on greatest financial impact to the business

The Insider Investigation Challenge

Security Operations Centers (SOCs) are flooded with countless threat alerts. Responders don't know which ones to investigate first. Once a potential threat is identified, the investigation process is manual, costing time and resources, oftentimes on noise and false positives.

Traditionally, SOCs and responders focus on isolated dimensions like data loss prevention or authentication data, investigating incidents one by one based on the tool's classification of severity. This approach lacks business context such as the value at risk, and focuses on incidents, not people, endpoints and applications. Even those who add a "UEBA" tool to the mix, are just adding more alerts to the stack.



Prioritizing Insider Investigations

Risk Fabric® is not a UEBA tool. Risk Fabric is a cyber risk analytics platform that incorporates proprietary user and entity behavioral analytics as one of many tools and data points for identifying and prioritizing people whose behavior may indicate a risk to your business, like insider threats, compromised accounts or careless users.

Risk Fabric prioritizes threat alerts based on those that pose the greatest financial loss to the business and associated vulnerabilities that could enable the threat to succeed. The platform integrates security, risk, organization and asset data from your existing tools, identifies anomalies, prioritizes threats using behavioral and value at risk analytics plus lightweight input from application owners to qualify the severity of threats before its they are sent to the SOC. Risk Fabric also provides easy to use tools for investigations, dashboards for visibility and workflows for response automation.