Bay Dynamics

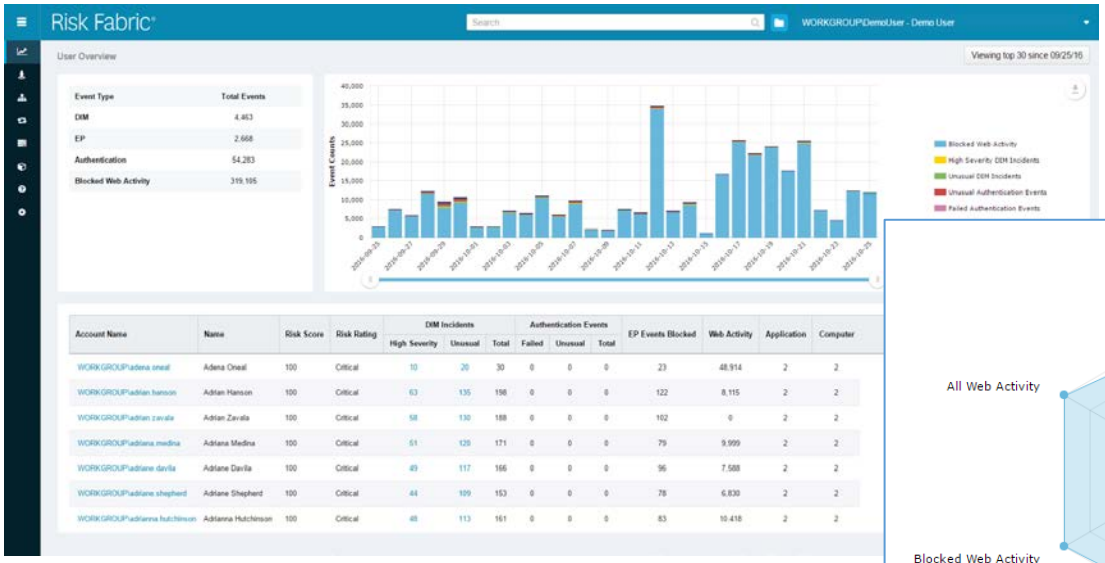
Risk Fabric® for Government

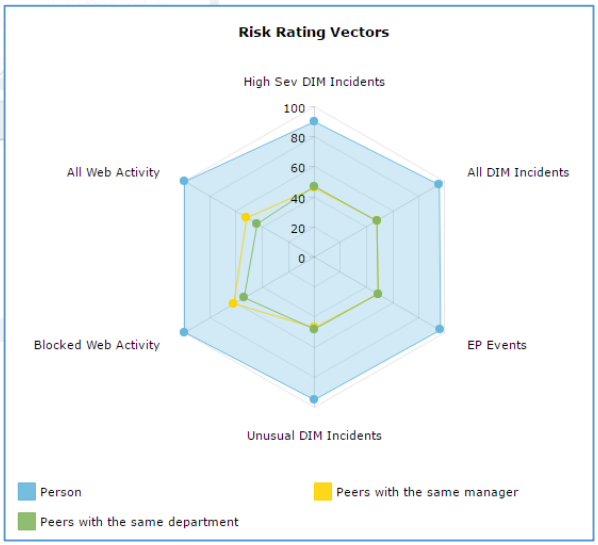
Enabling agencies to prioritize threats based on greatest impact to the mission

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, too often on noise and false positives.

Traditionally, SOCs and responders focus on single dimension tools like data loss prevention or authentication, investigating incidents one by one based on the tool's classification of severity. This approach lacks organizational 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 just a UEBA tool. Risk Fabric is a cyber risk analytics platform that incorporates proprietary user and entity behavioral analytics as one of many analytical tools and data points for identifying and prioritizing people whose behavior may indicate a risk to your agency, like third parties, insiders and compromised accounts.

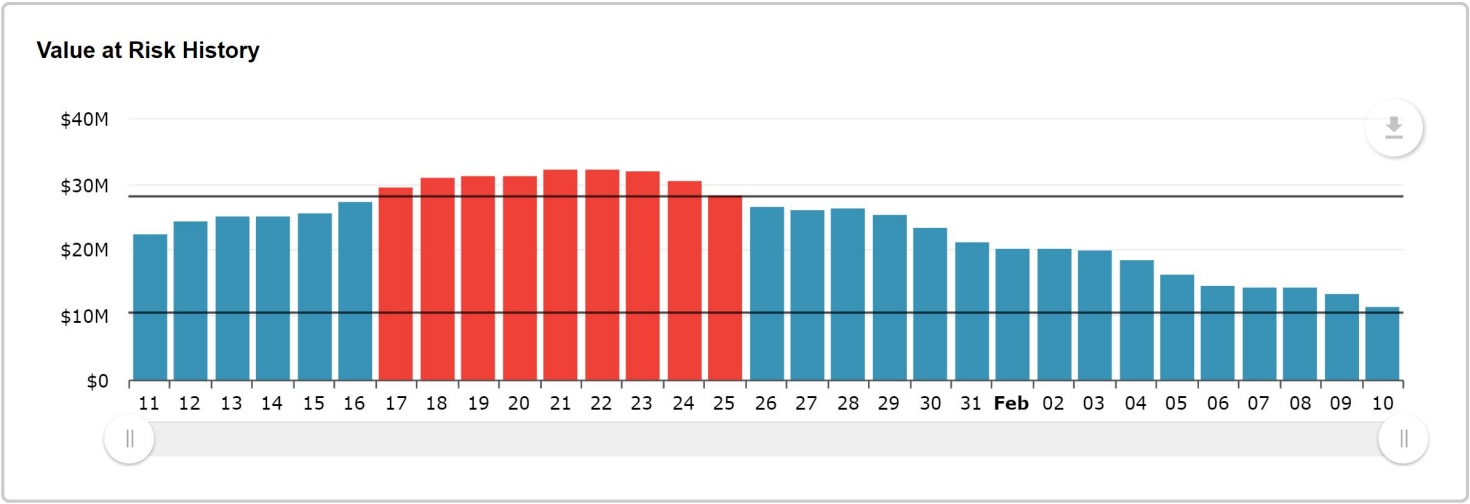
Risk Fabric prioritizes people, users and vendors for investigation based on those that pose the greatest loss impact to the agency mission and associated vulnerabilities that could enable the threat to succeed. The platform integrates security, risk, organization, and asset data from your existing tools,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

Bay Dynamics

Risk Fabric® for Government

Application Value at Risk & Value-Based Remediation

The Risk Fabric analytics platform calculates a value at risk dollar amount, based on dynamic telemetry from cyber defenses and IT systems, to quantify the level of financial risk associated with an application at a given time. Value at risk is calculated daily from actual threats and vulnerabilities detected from existing security tools and business systems.



Name	Value at Risk	Percent of Potential Loss	Credential Risk	Technical Risk	CEP	TEP
FTP	$1,203,700.00	60.19%	$203,700.00	$1,000,000.00	High	Very High
Network Monitoring	$1,194,600.00	59.73%	$194,600.00	$1,000,000.00	High	Very High
Private Cloud	$1,180,800.00	59.04%	$180,800.00	$1,000,000.00	High	Very High
Enterprise Backup	$1,159,300.00	57.97%	$159,300.00	$1,000,000.00	High	Very High
Identity Management	$1,156,800.00	57.84%	$156,800.00	$1,000,000.00	High	Very High
Log Management	$1,151,400.00	57.57%	$151,400.00	$1,000,000.00	High	Very High
Endpoint Backups	$1,145,000.00	57.25%	$145,000.00	$1,000,000.00	High	Very High

Records: 25

Continuous measurement of application cyber risk provide a system of record for the entire agency

About Bay Dynamics

Bay Dynamics® enables enterprises to continuously quantify the financial impact of cyber risk based on actual conditions detected in their environment. The company's flagship product, Risk Fabric®, is a software platform that calculates the value at risk associated with specific threats and vulnerabilities, that when mitigated, measurably reduce cyber risk exposure.

For more information visit **www.baydynamics.com**.

Follow us:
https://www.facebook.com/bay.dynamics
https://twitter.com/baydynamics

Bay Dynamics | 99 Hudson St | New York, NY 10013 | Phone: (646) 527-7280