RED VECTOR

PRESS RELEASE

FOR IMMEDIATE RELEASE

Red Vector Launches Tiered Insider Risk Platform at Black Hat 2025

Las Vegas, NV – August 4, 2025 – Red Vector today unveiled its newly enhanced FULCRUM™ insider risk platform, now available in three flexible product tiers: Essentials, Advanced, and Enterprise. The launch, announced live at Black Hat 2025, empowers security teams to deliver early detection of data theft, privilege abuse, sabotage, and negligence through proactive risk mitigation powered by human-centric context, fundamentally transforming how organizations approach insider threat management. Backed by more than 15 years of experience in Fortune 500 and national security programs, FULCRUM™ moves beyond legacy SIEM, DLP, and UEBA tools. Rather than relying on reactive, after-the-fact detection, FULCRUM™ surfaces early indicators of risk and empowers teams to act sooner.

Three Tiers Enable Flexible Growth

- **FULCRUM™ Essentials** provides a streamlined entry point by leveraging identity and HR data to enable early detection of insider risks. It reduces alert noise through contextual signal enrichment and intelligent prioritization, helping teams act faster with greater confidence.
- **FULCRUM™ Advanced** builds on Essentials by integrating alerts from multiple siloed security tools, enhancing visibility and correlation across domains. This results in more accurate detections and a significant reduction in false positives.
- **FULCRUM™ Enterprise** delivers full-spectrum risk fusion through advanced analytics and an expanded range of data sources. Designed for mature programs, it integrates email logs, physical access data, and detailed personnel information to generate deeper behavioral insights and stronger risk context.

How FULCRUM™ Transforms Security Operations

Most traditional tools generate disconnected alerts without context. FULCRUM™ connects behavioral patterns, access changes, HR signals, and even physical activity to identify risk earlier and with greater clarity.

Risk scores can be integrated into SOAR systems to automate graduated responses. This includes enhanced monitoring, temporary access restrictions, or full incident escalation based on the severity and context of the risk.

Organizations using FULCRUM™ report up to a 70% reduction in false positives and significant improvements in operational efficiency. Security teams can now prioritize meaningful threats instead of sorting through thousands of low-fidelity alerts.

Five Core Security Outcomes Drive Our Approach

- **Early Detection:** Identify insider threats before they materialize. FULCRUM™'s Behavioral Risk & Human Context Engine connects IT telemetry, physical access data, and HR information to detect emerging risks at their earliest stages.
- **Proactive Risk Mitigation:** Transform security operations from reactive monitoring to preventive action. FULCRUM™ correlates behavioral patterns, job transitions, access changes, and stress indicators to support early and effective intervention.
- **Reduced Alerts and False Positives:** Eliminate alert fatigue with intelligent prioritization. FULCRUM™ inference-driven analytics reduce false positives by up to 70%, allowing teams to focus on the threats that truly matter.
- **Scalable Implementation:** Deploy quickly across organizations of any size. FULCRUM™'s agentless architecture integrates seamlessly with existing infrastructure, requiring no heavy engineering lift or additional endpoint software.
- **Privacy and Compliance-Ready:** FULCRUM™ supports regulatory frameworks, including GDPR, Critical Pathway, ISO/IEC 27001, NIST Security Publications, and MITRE ATT&CK, delivering security without compromising governance.

The Urgency Is Real

Insider threats now account for nearly 60% of all data breaches, with average incident costs exceeding $17.4 million. Organizations relying on reactive tools often discover risks only after the damage is done.

> *"The cybersecurity industry has been stuck in a reactive cycle, detecting threats only after damage occurs. Our platform breaks that cycle. By combining human-centric context with scalable implementation, FULCRUM™ enables a shift from reactive defense to preventive protection."*
>
> **Stephen Layne, Chief Executive Officer – Red Vector, Inc.**

Experience FULCRUM™ at Black Hat Booth #6428

Attendees can see FULCRUM™ in action through live demos and technical briefings at Booth #6428 during Black Hat 2025. Executive sessions will showcase real-world deployments across government, healthcare, and financial sectors, highlighting measurable outcomes such as faster response times,

reduced alert volumes, and improved compliance posture.

About Red Vector

Red Vector, Inc. is a Risk-Adaptive Intelligence company specializing in insider risk management for enterprise, regulated, and critical infrastructure organizations. Drawing on 12 years of threat detection expertise homed in classified environments, Red Vectors Fulcrum Platform provides context-based risk intelligence, validated by Gartner's March 2026 "Treat Insider Risk as Human Risk" research to prevent insider incidents from escalating into data breaches. Learn more at redvector.ai.

Media Contact:

Victoria Conners
Director of Marketing, Red Vector, Inc.
(484)-631-5061
victoria@redvector.ai