PRESS RELEASE

FOR IMMEDIATE RELEASE

Red Vector Launches FULCRUM™ Case Manager Purpose-Built for Insider Threat Programs

Transforms how security teams assess, investigate, document, and respond to insider risks with built-in security and governance.

VALLEY FORGE, PA — June 10, 2025 — Red Vector, a leading provider of human risk intelligence solutions, announced the general availability of FULCRUM™ Case Manager, designed explicitly for insider threat and human risk programs. This cloud-based solution addresses critical gaps in current insider threat management practices, where security teams are forced to rely on generic project management tools, spreadsheets, and fragmented systems that create significant operational, legal, and security vulnerabilities.

Unlike improvised tool combinations that expose organizations to data breaches, evidence tampering, and compliance violations, FULCRUM™ Case Manager provides a unified, security-first platform engineered explicitly for sensitive insider threat investigations with standardized reporting and analysis frameworks. FULCRUM™ Case Manager includes the option to document cases using CMU's recently released and thorough Insider Incident Data Exchange Standard (IIDES). Insider Threat and Risk Teams can expect major improvements in investigator productivity, a significant reduction in case-resolution times, and the complete elimination of evidence-integrity risks.

"Security organizations worldwide are fighting sophisticated insider threats with inadequate tools," said Stephen Layne, Chief Executive Officer of Red Vector. "Generic project management platforms and spreadsheets were never designed to handle sensitive security investigations, creating dangerous vulnerabilities compromising security and compliance. FULCRUM™ Case Manager transforms insider threat management from a fragmented, risky process into a strategic security capability that delivers measurable business value."

Addressing Critical Market Need

Industry research reveals that 95% of security organizations currently manage insider threat cases using generic tools never designed for sensitive investigations. This patchwork approach creates cascading failures, including a broken chain of custody for digital evidence, inadequate access controls for confidential investigations, manual administrative processes that consume 60% of investigator time, and compliance vulnerabilities that expose organizations to regulatory penalties.

"The consequences of inadequate tools extend far beyond operational inefficiency," explained Ollie Luba, Chief Product Officer. "We've seen organizations lose million-dollar legal cases due to evidence integrity failures, face regulatory sanctions for compliance gaps, and miss critical threats because investigators were overwhelmed with administrative overhead. These aren't minor inconveniences but fundamental business risks that demand purpose-built solutions."

Comprehensive Solution Architecture

Key Features:

- **Centralized Case Management:** Track all insider risk incidents from initial triage to resolution in a secure, unified platform.
- **Customizable Workflows:** Tailor investigation and approval processes to align with your organizational policies and process requirements.
- **Role-Based Access Control:** Ensure sensitive case information is only visible to authorized personnel.
- **Evidence Management:** Add information, notes, and comments directly tied to a person of concern.
- **Audit and Compliance Reporting:** Generate defensible reports to support audits, legal inquiries, and executive oversight.
- **Customizable Standards Options:** Leverage CMU’s Insider Incident Data Exchange Standard (IIDES) or other standards.
- **Growth Path to Automation and Behavioral Analytics:** Correlate case data with any data source with behavioral indicators and risk signals for deeper insights.

Key Benefits:

- **Faster, More Defensible Investigations:** Streamlined workflows reduce investigation time while maintaining thorough documentation.
- **Improved Collaboration:** Secure, compartmentalized collaboration across Security, HR, and Legal teams.
- **Reduced Risk Exposure:** Early detection and consistent handling of insider threats mitigate reputational and operational damage.
- **Stronger Compliance Posture:** Ensure investigations meet legal, regulatory, and organizational requirements

SaaS Delivery Advantages

FULCRUM™ Case Manager is immediately available as a secure SaaS solution. The secure cloud-based SaaS delivery model provides immediate value with minimal implementation complexity:

- **Rapid Deployment:** Organizations can begin using FULCRUM™ Case Manager within days rather than months, with no infrastructure requirements or complex installations.
- **Automatic Scalability:** The platform scales automatically to handle multiple concurrent users and unlimited case volumes without degrading performance or incurring additional infrastructure costs.
- **Continuous Innovation:** Regular feature updates and capability enhancements are delivered automatically, ensuring organizations always have access to the latest insider threat management capabilities.
- **Predictable Costs:** Subscription-based pricing eliminates large capital expenditures while providing predictable operational costs that scale with organizational needs.

Growth

The solution allows you to grow at your own pace to the broader FULCRUM™ Human Risk Intelligence Platform for comprehensive insider threat detection and response capabilities.

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