KDM Analytics

PRODUCT INFO

Automate, Prioritize and Quantify CyberSecurity Risk

Blade RiskManager

Automated NIST Risk Management Framework (RMF) Assessment

Overview

Blade RiskManager (BRM) is a fully automated risk analysis and risk measurement product that provides organization with a top-down operational view of cyber-system risk.

The product uses artificial intelligence techniques and leverages a cybersecurity knowledge base of more than ten years. It automates risk analysis and is a one-stop source to store, manage, and trace all evidence regarding operational and system risk.

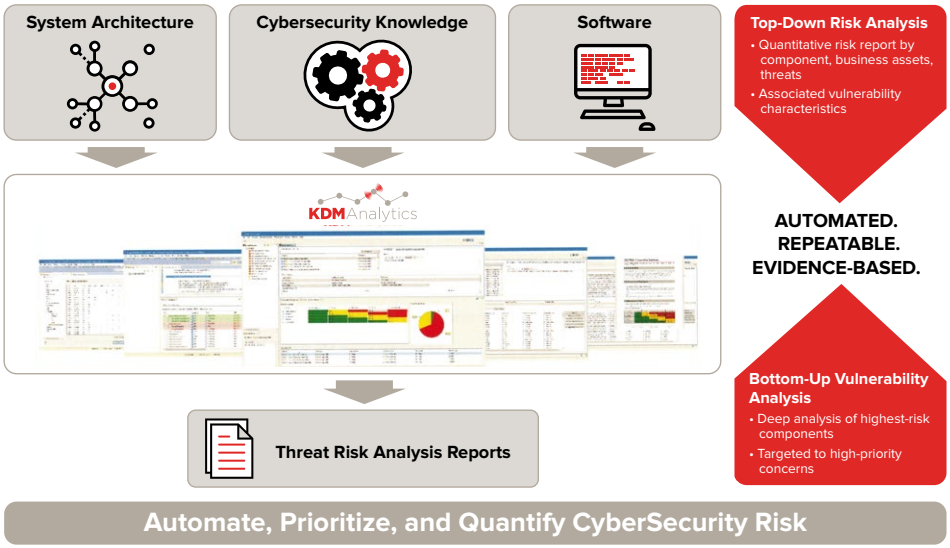
Organizations benefit from a risk assessment solution that is proven and repeatable across a variety of systems, assets, and components. BRM effectively reduces overall lifecycle development costs and improves confidence in decision-making related to cybersecurity risk management and mitigation.

Repeatability for Cost Effectiveness & Reporting

Understanding, assessing, and managing risk for today's complex cyber systems can be costly and laborious. In many instances, the process is *ad-hoc* and unique to every system, organization, or risk assessment professional.

BRM solves this by automatically, systematically, and comprehensively identifying multi-stage attacks and application vulnerabilities regardless of platforms, assets, systems, or sub-systems.

A Unique Approach to Risk Analysis



Automate, Prioritize, and Quantify CyberSecurity Risk

BRM Key Capabilities

Automated RMF Assessment

- Evidence-based risk assessment

Support for automated import formats

- System Facts: DoDAF/UAF; CSV; MS tables
- Security Controls: CSV

Automated import validation

- Provide error reporting on system's input data

Support for System Diagrams

- Automated generation and manual creation of OV2 System Diagram with multiple layout formats
- Categorized target icon library and properties panel
- Shareable Icon mapping to target nodes

Support for safeguards

- NIST 800-53 Security Controls & mitigations
- Automatically generates Security Requirements Reports including on a per identified risk

Automated graphical attack tree

- Automatically displays a graphical representation of direct & multi-stage attacks and attack paths

Automated risk computation

- Outputs DoD 5x5 risk matrix
- Residual and non-compliance risk

Automated risk distribution

- Per Component, Assets, Attackers ...

Automated identification of vulnerabilities

- Detects & characterizes operations/systems susceptibility
- Integration with software vulnerabilities

Customizable knowledge base

- Tailoring to industry, family of systems and individual system

Support for manual adjustments

- Group and adjust multiple attacks & undesired events by various characteristics

Automated report generation

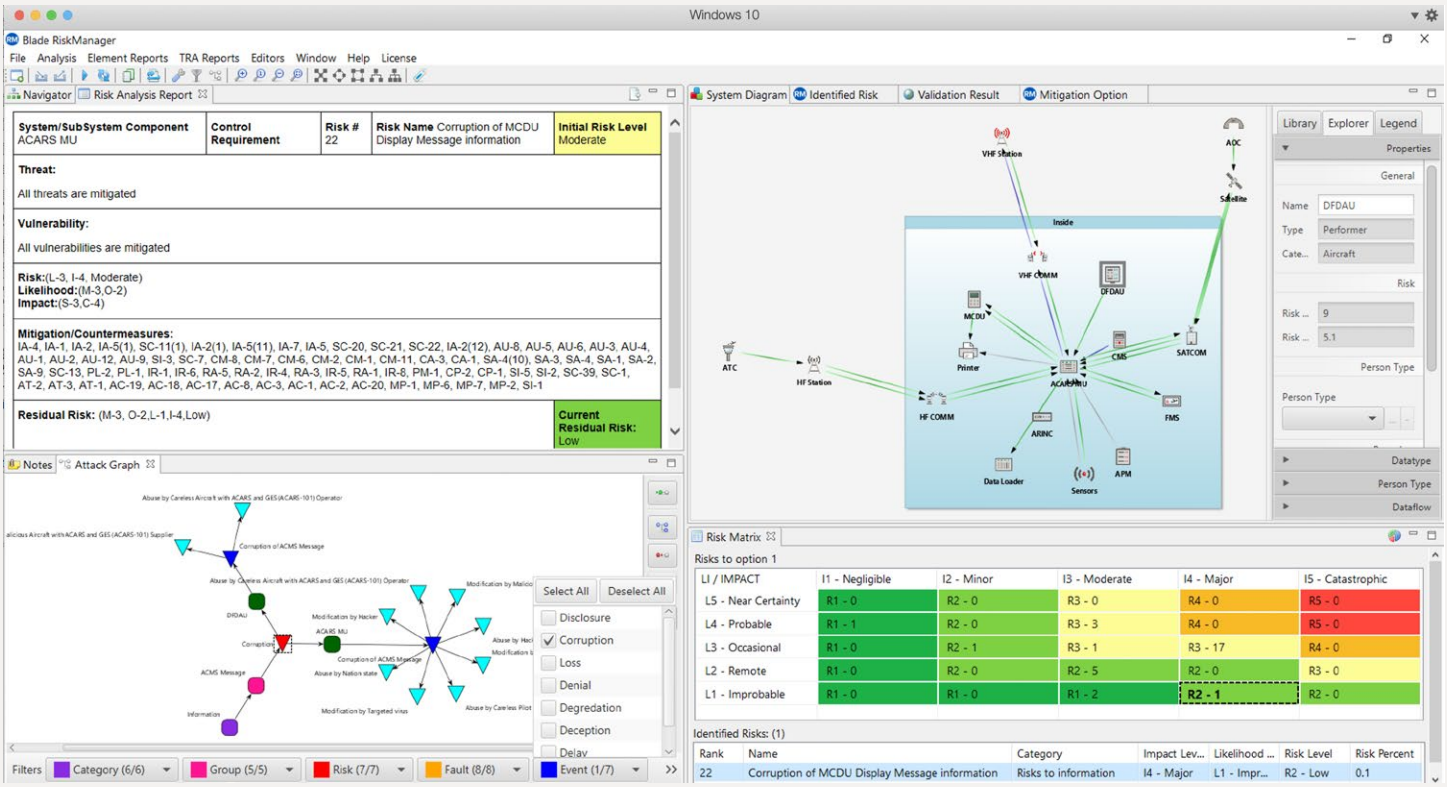
- Template-driven & customizable

"The USAF benefits from KDM Analytics automated risk management tools by cost-effectively assessing cyber threat, vulnerability, and risk for our Aircraft Systems."

— Mr. Harrell Van Norman, Cybersecurity Tech Expert/SCA for Aircraft Systems, United States Air Force

Blade RiskManager

Automated NIST Risk Management Framework (RMF) Assessment



Prioritization for Better Resource Management

BRM's operational perspective enables organizations to identify and focus security assessment and risk mitigation to the most critical and risky components of a system. An operational perspective also provides a better means of prioritizing the importance of risks and threats. It also makes system-based, bottom-up vulnerability scanning approaches more targeted. This mitigates the ad-hoc nature of cybersecurity and ensures that resources are applied to the most impactful areas.

Automated Analysis for Improved Prioritization

To ensure that threats and vulnerabilities are quantified and prioritized, BRM minimizes human interpretations, which can be influenced by a lack of knowledge, personal bias, errors and omissions, and discretionary misconceptions. BRM's automated analysis is evidence-based and mitigates errors and omissions resulting from erroneous interpretation.

Combining BRM with our vulnerability analysis product, Blade OneReport, builds a comprehensive cybersecurity management solution that includes:

- Automated risk analysis
- Automated vulnerability detection and analysis
- Traceability
- Measurement and prioritization that make it easy to plan how to best leverage the risk management budget and resources for greatest impact.

KDM Analytics automates, speeds, and reduces the cost of cyber risk management.

KDM Analytics

For more information, please visit www.kdmanalytics.com or contact us at info@kdmanalytics.com

Ogdensburg, NY, U.S.A.
Phone: (315) 605-1059
Fax: (866) 238-0184

Ottawa, Ontario, Canada
Phone: (613) 627-1010
Fax: (866) 238-0184