KDM Analytics

PRODUCT INFO

Quantify, Measure, & Prioritize CyberSecurity Risk

Blade RiskManager

Automated CyberSecurity Assessment

Overview

Blade RiskManager (BRM) is a powerful risk identification and measurement product that provides a top-down operational view of cybersecurity risk.

BRM includes an Analysis Engine for automated risk analysis and 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 critical challenge by fully automating risk analysis and identifying multistage attacks and application vulnerabilities regardless of platforms, assets, systems, or sub-systems.

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, and causes system based, bottom-up approaches to be more targeted. This mitigates the *ad-hoc* nature of cybersecurity and ensures that resources are applied to the most impactful areas.

BRM Key Capabilities

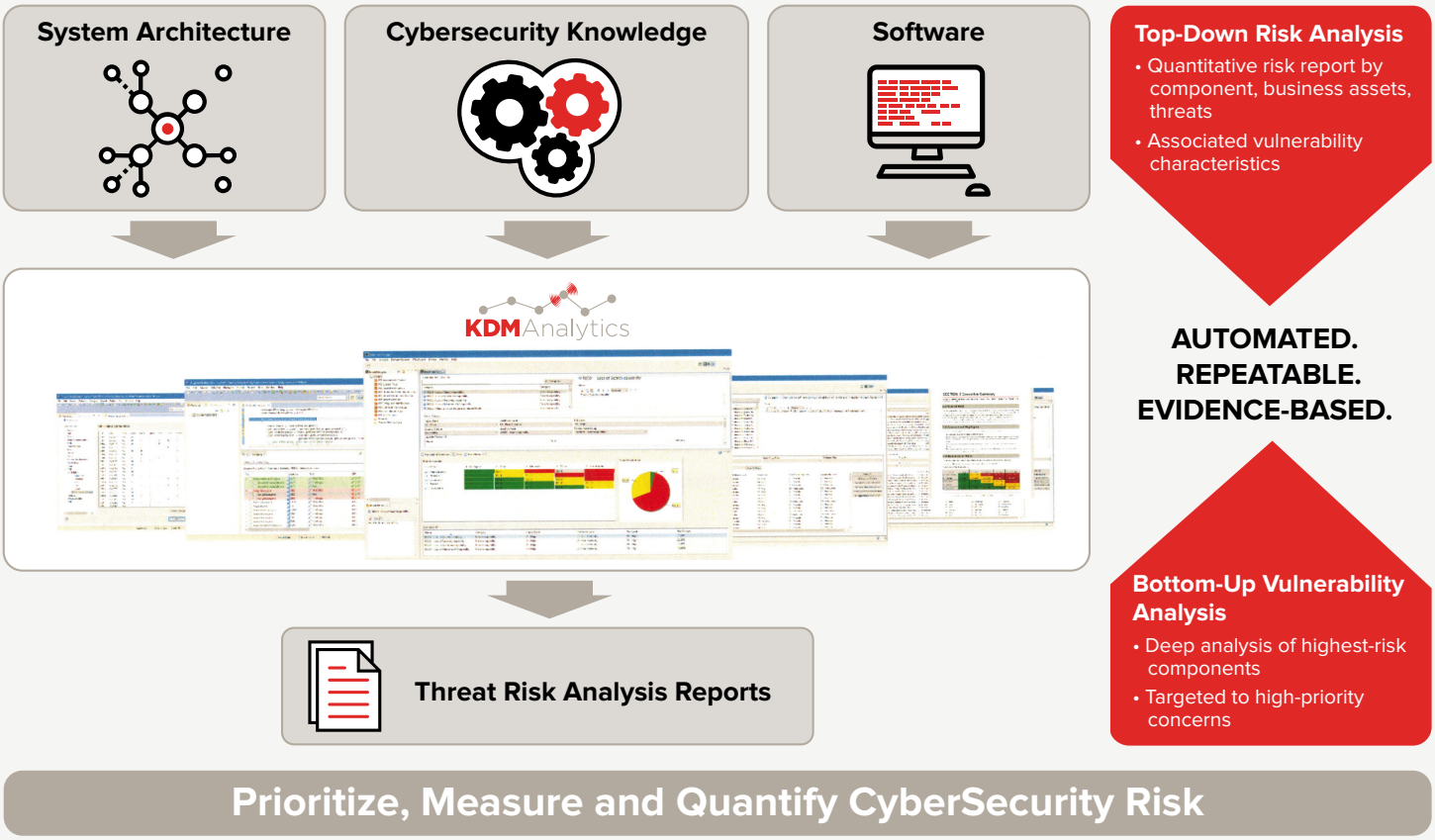
- Evidence-driven risk assessment including multistage attack analysis
- Automation of:
  - Traceability between risk model and system facets contributing to risk
  - Threat Risk Assessment Reports
  - Asset and fault discovery
  - Risk management
  - "Fitness for Purpose" scoring
  - Validation of system architecture document readiness for analysis
- Threat modeling
- DoDAF (Department of Defense Architecture Framework) Analytics:
  - Automated extraction of system information and facts related to risk
  - Automatically synthesized system security view
- Support for non-DoDAF architectures
- System transparency and traceability
- Constructs risk distribution by component, business asset and threat
- Identifies associated vulnerabilities
- Can be integrated into existing management system, e.g., quality and safety systems

KDM Analytics helps to answer the most important question of cybersecurity risk management: where should you focus your budget and resources?

Blade RiskManager

Automated CyberSecurity Assessment

A Unique Approach to Risk Analysis



Prioritize, Measure and Quantify CyberSecurity Risk

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 empirical and mitigates errors and omissions resulting from erroneous interpretation.

Combining BRM with our vulnerability analysis product, Blade TOIF, 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.

KDMAnalytics

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

Washington, DC, U.S.A.
Phone: (202) 756-2488
Fax: (866) 238-0184

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