

CIOReview

ISSN 2644-237X

CIOREVIEW.COM

SEPTEMBER · 2021

The Navigator for Enterprise Solutions



Awarded by CIOReview

KDM Analytics



Awarded by CIOReview

The annual listing of 10 companies that are at the forefront of providing Risk Analytics solutions and transforming businesses

KDM Analytics

Comprehensive and Systematic Automated Risk Assessment and Vulnerability Analysis

For years, risk management has been a looming concern for business executives. With instances of cyberattacks skyrocketing, it is now a top priority for CIOs, CTOs, and other stakeholders who need certainty about where to focus their risk mitigation efforts, budgets, and resources. Consequently, businesses are turning to risk analytics to measure, understand, quantify, and manage risk.

But, here's the catch! Until now, risk analytics has primarily been a manual process that sucks up time, energy, and labor—with often inconsistent results. The need is an alternate approach to cybersecurity risk assessment, done in a systematic, comprehensive, and repeatable manner.

"This is where we come in," explains Djenana Campara, president and CEO, KDM Analytics. "We provide automated risk and vulnerability analysis solutions that enable companies to find all the possibilities: how a system can be attacked, the threats and undesired events that can lead to attacks, and the impacts of those attacks." An aspect that sets the firm's cybersecurity risk management solutions apart is that its solutions deploy both top-down risk and bottom-up vulnerability analysis, outputting a prioritized list of actions based on solid evidence. This enables KDM Analytics' clients to precisely target risk management budgets and resources.

KDM Analytics' crown jewel is the Blade Suite, which includes Blade RiskManager (BRM) and Blade OneReport (BOR). BRM identifies, prioritizes, and focuses security assessment and risk mitigation efforts on the most critical and risky components of a system. It is the only product to fully integrate and automate risk assessment based on the NIST risk management framework (RMF) assessment workflow. BRM determines and ranks possible system attacks with enabling vulnerabilities, security risks, mitigation options. In addition, it performs automated assessments of each mitigation option to calculate mitigated, compliance, and residual risk. In other words, BRM quantifies a system's exposure to cyberattacks and helps prioritize risk management activities.

"BRM supports the whole lifecycle management experience of a cyber system," Campara notes. "Our clients can thus focus on the path forward from the information that BRM generates rather than focusing on obtaining that information. It is also evidence-based, providing uniformity and objectivity."

BOR complements BRM with a composite vulnerability analysis platform configured based on guidance from the risk analysis provided by BRM. BOR scans and evaluates high-risk software components and assets to identify vulnerabilities

that have the greatest operational impacts. The results can be integrated into BRM to calculate residual risk. Both commercial and open-source tools can be integrated into BOR.

team uses the client's documentation and source code to generate a system model, which is shared with the client for verification. Then, the automated risk analysis is conducted.

"Our sweet spot is when our products are integrated




Together, Blade RiskManager and Blade OneReport are a one-stop source to store, assess, manage, and trace all evidence regarding operational and system risk and identified vulnerabilities

In short, BRM and BOR together serve as a one-stop source to store, assess, manage, and trace all evidence regarding operational and system risk and identified vulnerabilities. With BRM's top-down analysis, noise is filtered out, while BOR prioritizes the vulnerabilities. The product suite provides comprehensive, automated risk assessment that is repeatable across missions and products. Soon, KDM Analytics will add penetration testing and intrusion detection results to gather all possible evidence for risk assessment and take that into account when calculating residual risk.

In addition to these product offerings, KDM Analytics experts can be engaged to provide third-party risk assessment services. Service engagements begin with a client interview to understand the client's focus and objective for risk mitigation. This is followed by information gathering related to the target system's architectural model, which is the primary input for the BRM report. Although most clients do not have a model of their system, this is no problem for KDM Analytics. The

into the digital engineering process and follow system engineering through the whole lifecycle. Engineers create the system model and BRM automatically generates the risk assessment," explains Campara. "Based on the quantifiable risk assessment, the engineering team can then develop a strategy that lowers risk by using the Blade Suite reports to identify the minimum viable mitigation strategy for implementing safeguards and controls. Since the process is fully automated, the client can perform extensive, systematic what-if scenarios with a quick turnaround."

This proven approach plays a critical role in the company's continued success. "How do we know our products are a hit? The proof is in the numbers," states Campara. In a recent instance, BRM was deployed by a client that faced an issue with a mission-critical system under operation. After running BRM, the client was able to pinpoint the smoking gun in a matter of days. Other clients testify to the efficacy of BRM and BOR reducing the cost and hours involved in risk and vulnerability assessments by 80 percent.

The future of KDM Analytics looks bright, as the company puts the finishing touches on its newest offering: a cloud-based, Software as a Service (SaaS) version of Blade RiskManager that will become available in addition to the current on-premise products. "Our goal is to continue to transform the way cyber risk assessments are conducted," Campara says. "We were the first to fully automate the NIST RMF assessment workflow and we'll be first to provide that capability as a flexible SaaS offering." 



Djenana Campara