ISSN 2644-237X

CIOReview

CIOREVIEW.COM

The Navigator for Enterprise Solutions

CANADA SPECIAL

RISK MANAGEMENT EDITION

0 74470 91626 0

Certificate

KDM Analytics

*This award is in recognition of **KDM Analytics'** stellar reputation and trust among customers and industry peers, evident in the numerous nominations we received from our subscribers. **KDM Analytics** emerged as a **Top Company** after an exhaustive evaluation by an expert panel of C-level executives, industry thought leaders, and our editorial board.*

Awarded By

CIOReview

ISSN 2644-237X

KDM Analytics

Reducing Financial Risk with Automated Cyber Risk Assessment using AI

Djenana Campara, President & CEO

Manual cybersecurity assessments are increasingly outdated. These methods are slow, susceptible to human error, and cannot effectively process the vast amount of data necessary for cybersecurity analysis. This leads to incomplete or inconsistent results, leaving organizations and their critical systems vulnerable. Companies need a more robust approach. Automated solutions powered by digital engineering frameworks and AI algorithms offer precise and scalable risk assessments. This proactive, structured, and repeatable approach saves time, reduces costs, and significantly enhances security. It's the key to achieving efficient, accurate, and reliable cybersecurity management—a necessity in today's digital risk landscape.

KDM Analytics, a leader in cyber-risk management, stands out for providing a completely automated approach to cybersecurity risk assessment. Its digital engineering framework extends into comprehensive risk assessments, taking a proactive stance against cyber threats.

"We differentiate ourselves through efficient automation, offering a preventive shield against cyberattacks," says Djenana Campara, president and CEO of KDM Analytics.

KDM Analytics utilizes AI-powered algorithms within a digital engineering framework to deliver structured and precise cyber risk evaluations. The company's products automatically generate systematic and comprehensive attack trees. For each attack path in the tree, they identify system exposures that would make the attack successful given a particular threat source—pinpointing potential attack paths and exposures before they can be exploited. By proactively mitigating these attacks, KDM Analytics helps businesses safeguard against devastating financial losses.

The company's Blade RiskManager (BRM) and Blade OneReport (BOR) products go even further. The solution not only identifies at-risk areas and their root causes through comprehensive assessments but also generates detailed attack vector graphs, providing a clear visualization of potential system breaches and recommending courses of action. Security officers can rapidly understand their system's risk profile and focus resources on the most critical assets and their risk mitigations.

BRM reduces the time and cost of cyber risk assessment by automating analysis and serving as a centralized source for managing and tracing evidence related to operational and system risks. Using a model-based system engineering (MBSE) approach, BRM interprets the target system's architecture, incorporating detailed information on hardware, software, data flows, and interconnections.

BRM then automatically creates threat and risk models, develops attack trees that show all possible attack paths, and highlights the conditions for success. It identifies specific weaknesses associated with each attack path and assesses the likelihood and potential damage of exploitation, ensuring mitigation efforts are directed toward areas with the highest impact.

Once BRM has prioritized potential vulnerabilities, BOR takes over. BOR is a vulnerability analysis and detection platform that enhances assessment accuracy and unifies outputs from multiple vulnerability analysis tools into one comprehensive report. The report is imported back into BRM for recalculated residual risk.

In summary, the Blade Suite provides both top-down and bottom-up analyses, assesses systems in an operational context, identifies vulnerabilities, and suggests optimal controls and countermeasures. The detailed report consolidates results into a single view, helping businesses take appropriate action on identified vulnerabilities and informing their clients and stakeholders about how issues are being addressed to prevent future attacks.

We differentiate ourselves with the most efficient and automated approach to cyber risk assessment. Our solution enables organization to be proactive and preventive against cyber attacks by extending a digital engineering framework into their cybersecurity assessments

Based on the insights from BRM and BOR, KDM Analytics customers can develop targeted mitigation strategies to address the most critical areas. These strategies are designed to ensure that resources are allocated to enhance security where it counts most.

KDM Analytics customers include government organizations, defense departments, and critical infrastructure providers. Some large aerospace and defense organizations have used KDM Analytics' BRM to automate risk assessments. Their testimony is that using Blade Suite reduces service costs and man-hours by 80 percent.

One organization, Acquired Data Solutions (ADS), wanted certain capabilities in its solution, including model-driven evidence-based assessments, adaptability in operational technology component assessments, an extensive cybersecurity knowledge base, and capability prioritization for control measures. BRM satisfied these needs in several ways: a user-friendly workflow, comprehensive knowledge about cyber risks, and intelligent reporting capabilities. As Tony Barber, Principal Consultant at ADS, said: "Using BRM, we were able to provide 'More Insight' with 'Less Effort'. We achieved an 80 percent decrease in costs due to reduced resource needs and an 80 percent decrease in man-hours for work performance."

Through risk simplification, ADS identified major attackers and threats, making system architecture and data flows easier to map out. The effectiveness of BRM in reducing risk and enhancing the protection of industrial control systems is demonstrated by quantifiable ROI that validates the technology's value proposition for this purpose.

With the power of KDM Analytics, organizations and the vendors who develop systems for them can now benefit from these products by reducing cybersecurity risks, minimizing financial losses, and safeguarding critical infrastructure—all while achieving substantial cost reductions compared to current risk management practices. CR