Avint® LLC. Your Vision Achieved

Transforming Cyber Risk Management: The Agile Approach

White Paper

Date: September 16, 2024

Avint, LLC
205 Van Buren St., Suite 400
Herndon, VA 20170
571-287-7715 • www.avintllc.com
CAGE Code: ***7FU49***
Unique Entity Identifier (UEI): ***UW4CUW6QK8N7***

Primary Point of Contact
Marcie Nagel
Founder and CEO
Phone: 571-287-7718
Email: marcie.nagel@avintllc.com

Alternate Point of Contact
Brian Edwards
CGO
Phone: 443-812-1663
Email: brian.edwards@avintllc.com

TABLE OF CONTENTS

TABLE OF FIGURES

1. INTRODUCTION

Traditional cybersecurity approaches often fall behind in today's fast-evolving cyber threat environment. Static methods like the four-quadrant risk matrix cannot capture the complexity or urgency of modern risks. Organizations now need a flexible and scalable solution that adapts to their IT and security environments. Avint's **Agile Risk Enumeration Algorithm (AREA)** meets this need by modernizing risk management through agile principles and advanced technologies.

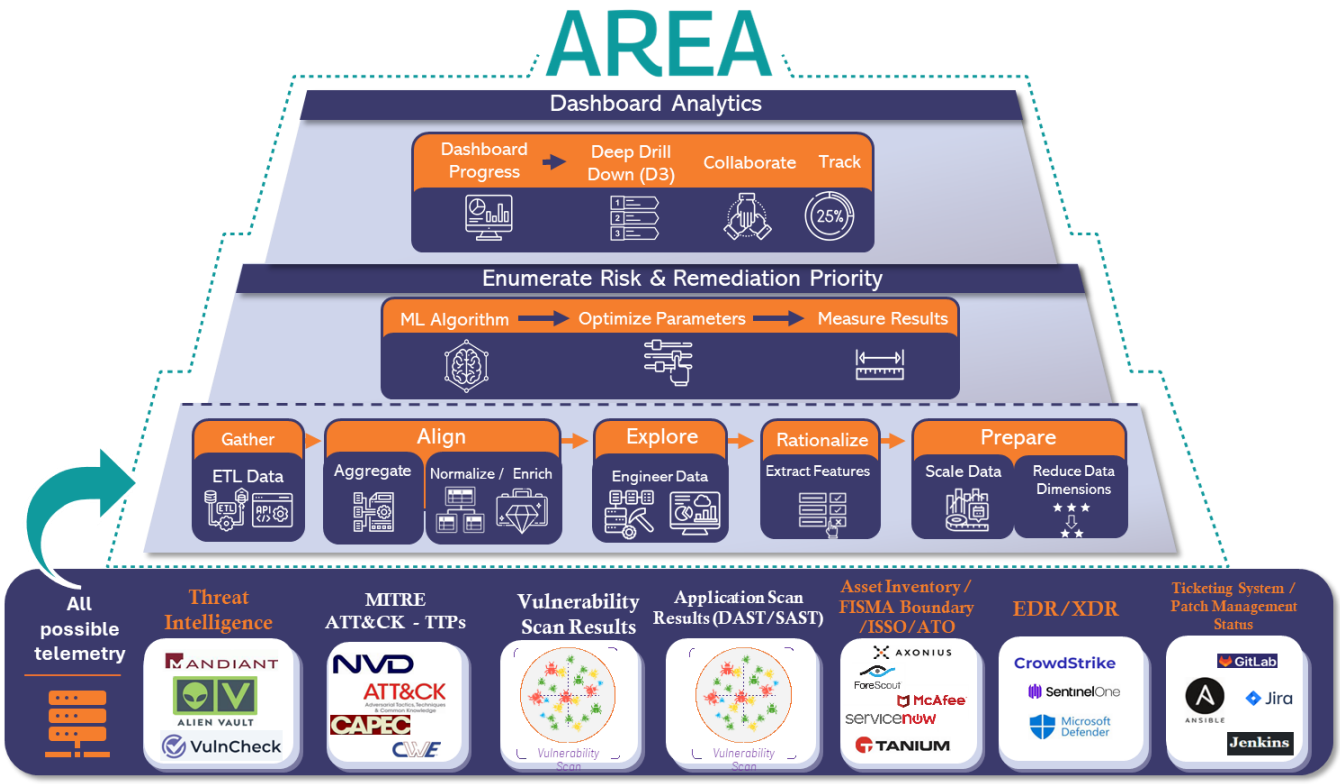

Figure 1: AREA correlates and contextualizes threat intelligence, thus enabling timely mitigation and improved risk management via data-driven remediation prioritization.

With machine learning, real-time threat intelligence, and agile methodologies, AREA enables organizations—especially those with limited resources—to prioritize and mitigate their most critical vulnerabilities swiftly. This increases efficiency and enhances the organization's overall security posture.

2. MOVING BEYOND TRADITIONAL RISK MANAGEMENT

Traditional risk frameworks classify risks statically, failing to prioritize based on threat dynamics. This rigidity is unsuitable for modern, dynamic environments. **AREA** redefines risk management by using an agile, iterative, and flexible approach. Its predictive machine learning capabilities analyze vulnerabilities based on adversarial tactics, techniques, and procedures (TTPs) from frameworks like MITRE ATT&CK, helping organizations focus on the most exploitable risks.

AREA integrates with an organization's existing cybersecurity tools—vulnerability scanning, threat intelligence, endpoint detection—through custom APIs, feeding real-time data into its MongoDB layer for continuous analysis.

3. A PROACTIVE, AGILE, RISK MITIGATION FRAMEWORK

AREA uses agile principles, breaking the remediation process into manageable sprints, allowing organizations to tackle high-priority vulnerabilities incrementally. This sprint-based approach, paired with cross-functional collaboration, allows for efficient alignment between cybersecurity, IT, and management teams. A real-time dashboard provides a collaborative space for decision-making, ensuring that the teams remain aligned, adaptable, and responsive to new threats.

This model allows security teams to make steady, measurable progress by addressing smaller, high-priority tasks, ensuring continuous and sustainable improvements in the organization's security posture.

4. WHY AGILE CYBER RISK MITIGATION MATTERS

By leveraging an agile risk management framework, AREA provides significant improvements in speed and efficiency. Its predictive capabilities allow security teams to quickly assess, prioritize, and respond to vulnerabilities, minimizing exposure to critical threats. Continuous monitoring helps prioritize and address the most dangerous vulnerabilities, significantly improving the organization's security.

AREA maximizes resource efficiency by directing efforts towards the highest-impact risks, making it an essential tool for resource-constrained organizations.

5. THE POWER OF AN INTEGRATED ARCHITECTURE

AREA's technical architecture plays a crucial role in its ability to offer real-time, agile risk management. Through its custom APIs, AREA integrates with existing cybersecurity tools, aggregating data into its MongoDB data layer for continuous, real-time processing. This centralized repository allows for large-scale data processing, continuously updating risk profiles and supporting adaptive security operations as new data sources emerge.

By combining real-time threat intelligence and advanced machine learning, AREA shifts vulnerability management from a reactive stance to a proactive, strategic initiative.

6. THE POWER OF VISUALIZATION

The AREA platform's **MicroStrategy-powered dashboards** are designed with cyber operators in mind, providing a user-friendly way to visualize and interact with complex cybersecurity data. By organizing assets based on **system boundary, location, and organizational unit,** the dashboards help operationalize large datasets, making it easier for teams to assess vulnerabilities within the context of their specific environments. With MicroStrategy's integration of **generative AI**, AREA can generate **ad hoc dashboards** on demand, giving organizations the flexibility to create tailored views that meet their immediate operational needs, ensuring they always have the right insights at their fingertips.

7. CONCLUSION

Avint's **Agile Risk Enumeration Algorithm (AREA)** is the future of cybersecurity risk management, combining agile principles, machine learning, and real-time threat intelligence. It enables all organizations, but in particular those that are "target rich, resource poor", to strategically apply resources to vulnerabilities that will have the biggest security impact. Seamlessly integrating with existing tools and continuously adapting to the evolving threat landscape, AREA helps organizations protect critical assets and improve their overall cybersecurity posture.