**Cyber Common Operating Picture – How to Efficiently Manage Cybersecurity Risk through Analytics, Automation, and Behavioral Science**

**Jamie Miller**
CEO
MARS Suite, LLC

The MARS Suite©, currently on the Department of Defense Information Network (DoDIN) Approved Products List (APL) – tracking number 1832002), correlates cyber threat and vulnerability data to asset criticality, mission risks, and other operational data to achieve an Enterprise-wide Common Operating Picture – and enable holistic situational awareness to quickly identify and manage risk in an ever-changing network environment. The MARS Suite© solution focuses on enabling this correlation, and advances network monitoring capabilities by moving beyond point solutions to manage to a uniform risk profile. The resulting cyber common operating picture provides leadership and hands-on practitioners with the ability to make more informed, efficient, and effective risk management decisions based on impact, schedule, cost and any other relevant performance criteria.

The MARS Suite© solution is architected and can be configured to integrate with essentially any industry standard data source (such as MS SQL, Oracle, Sybase, etc.), it can also utilize Extract, Transform & Load (ETL) scripts to establish links with most (if not any) other specialized/custom/proprietary sensors or legacy data sources that our clients might possess. This allows the solution to ingest, normalize, and present risk data in an easy-to-understand format and integrates with and supports other enterprise risk scoring models (e.g., Continuous Diagnostics, RMF Workflows, Mitigation Dashboards etc.).
The MARS Suite© solution is unique in that it is focused on changing the behavior of cybersecurity practitioners by incentivizing them to prioritize their workload through risk scoring and the adoption of an overall “risk economy”. Our approach is built on philosophy that not all IT assets are created equal; and that leadership should be tracking key metrics related to those key IT assets (or “key cyber terrain”) and using real-time data (through automated technology) to inform more effective and efficient risk management decision-making.

We achieve this goal by first working to identify the key IT assets within the organization, and defining key cyber metrics that are measurable, actionable, and meaningful to the organization. Simultaneously we work to ensure that each organization possesses the tools/sensors to collect that data that is needed to support the defined metrics. To normalize the data collected from the different automated tools we leverage a common framework and nomenclature called Secure Content Automated Protocol (SCAP). The information collected from these disparate sources is ultimately used to present an organization-wide dynamic risk scoring dashboard and business intelligence analytics. The dashboard scores and tracks progress at the enterprise-level, but also enables the user to “drill down” to unique grades at the component / business unit level, and even the specific IT system-level.