Cyber Challenges

IT Operations for commercial and Federal Enterprises are continually seeing new challenges that impact their cyber security stance at an operational level. On the one hand IT organization are dealing with the ever-changing requirements of business units on IT systems to be more responsive to consumers, demanding systems changes from months to response times of days. At the same time the ever-evolving demands to incorporate and respond to emerging technologies to improve interaction with our customer and improve IT operational cost is making security more complicated and riskier. Mobility, Cloud, and IoT are some of these emerging technologies that are extending the boundaries of the enterprise and introducing new risk to the IT Operations. All impact the organizations approach on addressing their Risk Management Framework.

Cauldron Approach

Cyber situational awareness and prioritized remediation planning determine timeliness, cost effectiveness, and success in improving operational cybersecurity. Mission success depends on understanding the evolving

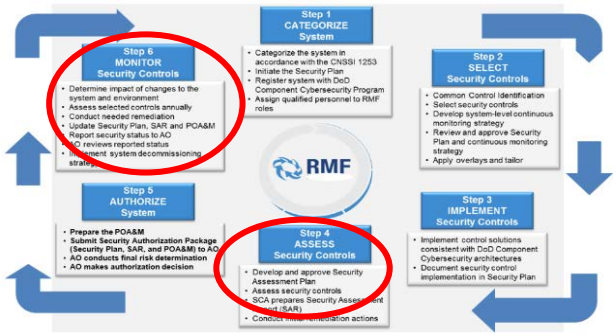
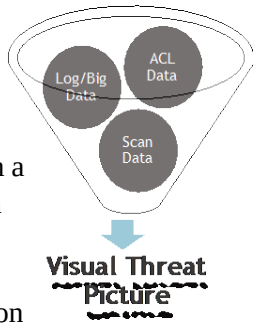


Figure 1 *- Managing Risk with Enterprise Changes at a daily pace.*

and changing computer networks, which are vulnerable to various types of attacks due to interconnectedness. Today, cyber defense capabilities are limited in many ways, such as inaccurate and incomplete vulnerability analysis, failure to adapt to evolving networks and attacks, inability to transform raw data into cyber intelligence, and inability for handling anomalous data.



Cauldron's unique approach maps all paths of vulnerability through networks, by correlating, aggregating, normalizing, and fusing data from a variety of sources. This approach provides transparency of attack vectors within the enterprise. It provides sophisticated visualization of attack paths, with automatically generated mitigation recommendations and prioritized patching reports. Flexible modeling supports multi-step analysis of firewall rules as well as host-to-host vulnerability, with attack vectors inside the network as well as from the outside.

The continued cybersecurity progression relies on the development of improved integration of data elements and advanced analytics at near real time. Technology plays a crucial role in all aspects of the economy and government activities. Ultimately, the goal is to improve overall security by lowering the risk surface area and adopt tools that advance cyber controls in proactive methods. Cauldron™ is design to co-exist in a continuous monitoring ecosystem to allow security team the ability to support independent audits.

To that end, CyVision will implement the advanced analytics tool, Cauldron™, for a partner/customer engagement. This effort will provide the customer with a visual representation of the true state of its cybersecurity posture and a proposed *prioritized* remediation plan and other prototypical reports.

Compliance: Meets 27 NIST 800-53 controls in categories AC, AU, CA, CM, IR, PL, SA, SC, and SI. Generates reports based on NIST RMF.

Pricing: Available in 1-time or subscription licensing. Implementation & training time-to-value is **hours.**

Corporate: CyVision Technologies, Inc.
8619 Irvington Ave.
Bethesda, MD 20817-3603
301.237.0007
www.cyvisiontechnologies.com