Cyber Matrix Security Analysis Tool

Intuitive Security Control Baseline Engineering and Analysis

Due to the expanding cyber threat landscape, with attacks increasing in both frequency and sophistication, security requirements are ever-evolving. Changing standards and guidelines, common/inherited security controls sets, and security gaps and weaknesses require technology refreshes. This amplifies the need for a deep understanding of the enterprise's security posture. However, security controls are complex, security posture analysis is difficult, detailed, and time-consuming, and the documentation of an analysis is extensive and difficult to maintain. Cloud and hybrid cloud architectures further complicate a security posture analysis. SAIC's Cyber Matrix Security Analysis Tool (CMSAT) gives customers visibility into their security posture and helps them overcome security compliance challenges and obtain certifications, such as the Cyber Maturity Model Certification (CMMC).

SAIC®

CMSAT IS AT THE CENTER OF ESTABLISHING A "BAKED-IN SECURITY" APPROACH - THE TRUE STANDARD BY WHICH ORGANIZATIONS SHOULD BE MEASURED.

Capability Highlights

- Understand and improve security posture
- Speeds cloud capability development and cloud migration by supporting the cost-effective analysis required to achieve the defined security approach
- Provides complete, extensive analysis
- Reduces analytical errors
- Save costs by reducing wasteful spend on overlap
- Auto-generate documentation
- Reduce risk
- Expedite security product acquisition
- Accelerate ATO by maximizing Risk Management Framework (RMF) reciprocity

CASE STUDY: A LARGE COUNTY GOVERNMENT

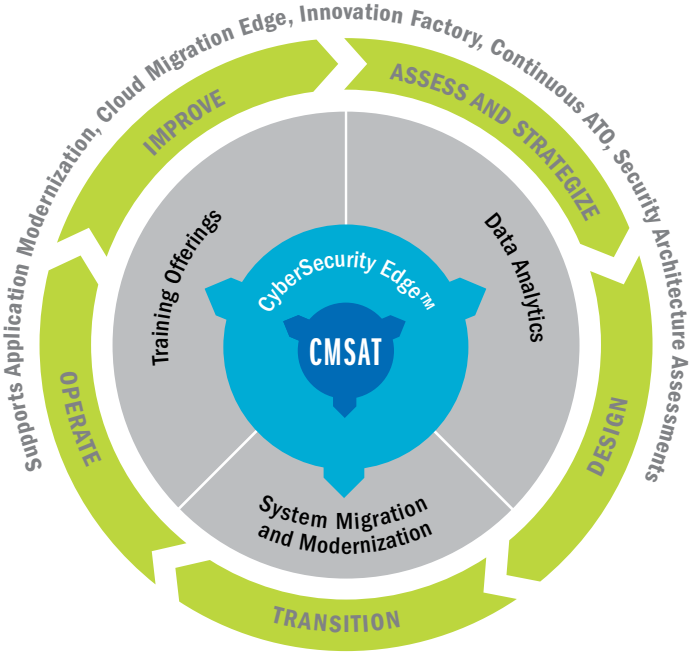
SAIC was tasked to perform an analysis of the security architecture from a security control perspective to identify gaps and deficiencies. SAIC performed the CMSAT assessment in parallel with a penetration test. With no preexisting security control baseline, SAIC utilized CMSAT to create one within minutes by blending a moderate security baseline with the results of the system security categorization data types, including privacy, judicial, and industrial controls.

Working with the customer and on-site staff, our analyst reported a 68% compliance level with the created security control baseline. The results of the 47-page CMSAT report, aligned with many of the findings of the penetration tests. It also identified the strengths and weaknesses and recommended steps forward. It also identified the strengths, weaknesses, and recommend steps forward. SAIC is working with the customer to prioritize and address these findings.

CMSAT is an as-a-service Cyber Situational Understanding (CSU) online tool and methodology that serves as the backbone of a governance, risk, and compliance (GRC) analysis. Its intuitive user interface and application programming interface (API) aid in establishing the security control baseline, identifying gaps in the controls, and recommending mitigations to overcome compliance challenges. Unlike other GRC tools, CMSAT continuously identifies opportunities for security control inheritance and reveals gaps in coverage and compliance.

Security analysts and engineers use CMSAT to model the effects of introducing individual security products and controls on the security baseline of the entire environment – offline and without risk to the operational environment. By mapping security control baselines and security assessments to individual system components, it visualizes dynamic and discrete relationships between vendor products, solutions, and services and security controls, including hidden controls, and conducts dynamic risk calculations. This enables customers to rapidly gauge the risk incurred by the implementation or failure of a security control early in the system development lifecycle, resulting in risk reduction and time savings that reduce long-term costs. With CMSAT, customers reduce their research time and costs of security products by quickly identifying gaps in security controls, decrease wasteful spending on overlapping security products, and expedite security product acquisitions. They can also maximize cybersecurity reciprocity in support of attaining continuous Authority to Operate (ATO).

With CMSAT as a fundamental tool for establishing a baseline, customers can implement a baked-in security approach with continuous visibility into their cyber posture, enabling continuous compliance, risk reduction, increased speed, and cost savings.



Contact

Russell Smith
russell.j.smith@saic.com

Tom Pari
thomas.j.pari@saic.com

20-0414