Ensuring the cybersecurity of government networks and systems

Continuous diagnostics and mitigation (CDM)

AT A GLANCE

The pace at which vulnerabilities emerge and threats evolve has changed at such a frenetic pace over the last few years that cyber defenders have had to reconsider the effectiveness of traditional risk management activities.

CLIENT CHALLENGE

The Department of Homeland Security's continuous diagnostics and mitigation (CDM) program provides tools and processes to federal civilian agencies to assist with migrations toward near real-time risk management from previous, less-effective methodologies. In concert with another partner, Coalfire was faced with overcoming two distinct, yet related, challenges pertaining to engineering new solutions into existing department and agency (D/A) environments and developing the governance strategy and processes to support the enterprise risk management paradigm shift.

APPROACH

With our partner, Coalfire analyzed five different existing D/A environments and toolsets to determine the feasibility of repurposing existing tools while implementing new processes to support more stringent risk management requirements in the cyber capability areas of hardware asset management, vulnerability management, software asset management, and configuration setting management.

Based on the information collected during the discovery phase (which included enterprise architectures, license counts, and specific

engineering constraints), Coalfire worked with five D/As to design a solution that leveraged existing tools and incorporated new technology to satisfy program requirements in the aforementioned cyber capability areas. The proposed/finalized solution consisted of a combination of disparate sensors that collected data from agency endpoints (at frequencies not exceeding three days) before forwarding to a data integration layer (Splunk) for normalization. Finally, Coalfire ensured that aggregated data feeds populated the CDM dashboard (RSA Archer) for visualization and risk scoring purposes.

From a governance and strategy standpoint, Coalfire captured existing cyber governance structures across five different D/As for baselining to determine feasibility of repurposing processes and structures to support the CDM program. Feedback on the effectiveness and shortcomings of existing structures and processes was gathered from stakeholders including operations and maintenance personnel and the C-suite. The resulting analysis served as the primary input into devising the "to-be" structure and supporting the CDM governance strategy.

RESULTS

Upon completion of successful engineering and solution deployment activities, the five D/As that comprised the Coalfire task order had the ability to manage risk in a more proactive, centralized manner in the context of the four foundational cyber program capabilities (hardware, software, configuration setting, and vulnerability management). Most importantly, critical mission and business functionality and enterprise system performance were sustained while augmenting cyber situational awareness capabilities.

Lastly, the governance strategy facilitated the transition from point-in-time risk management to the "near real-time" processes that the CDM system provided. The newly established governance structures solidified the foundation of the CDM program through newly established roles, processes, and ongoing strategic working groups. Newly established performance and maturity metrics provided a benchmark for success to measure program progress and performance against established goals on an ongoing basis.

About Coalfire

As cybersecurity risk management and compliance experts, Coalfire delivers cybersecurity advice, assessments, testing, and implementation support to IT and security departments, executives, and corporate directors of leading enterprises and public sector organizations. By addressing each organization's specific challenges, we're able to develop a long-term strategy that improves our clients' overall cyber risk profiles. Armed with our trusted insights, clients can get to market faster with the security to succeed. Coalfire has offices throughout the United States and Europe.
Coalfire.com

CS_CDM_030217

COALFIRE