

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

Copyright © 2014-2017 Coalfire Systems, Inc. All Rights Reserved. Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

COALFIRE