Lockheed Martin

Cyber Resiliency Scoreboard® (CRS®)

Michael Hankins, Fellow, and Jason Johnson, Associate Fellow
Lockheed Martin Corporation

From concept through delivery to retirement, Lockheed Martin integrates full-spectrum cyber solutions into everything we do. We introduced the Cyber Resiliency Level® (CRL®) Framework (see Figure 1) in 2019 as the world's first standard method to measure the cyber resiliency maturity of a weapon system[1]. In support of the CRL® framework, we created the Cyber Resiliency Scoreboard® (CRS®) tool to assist customers in making informed decisions in selecting courses of action (CoA) and prioritizing their resources for maximum effect against cyber attacks.

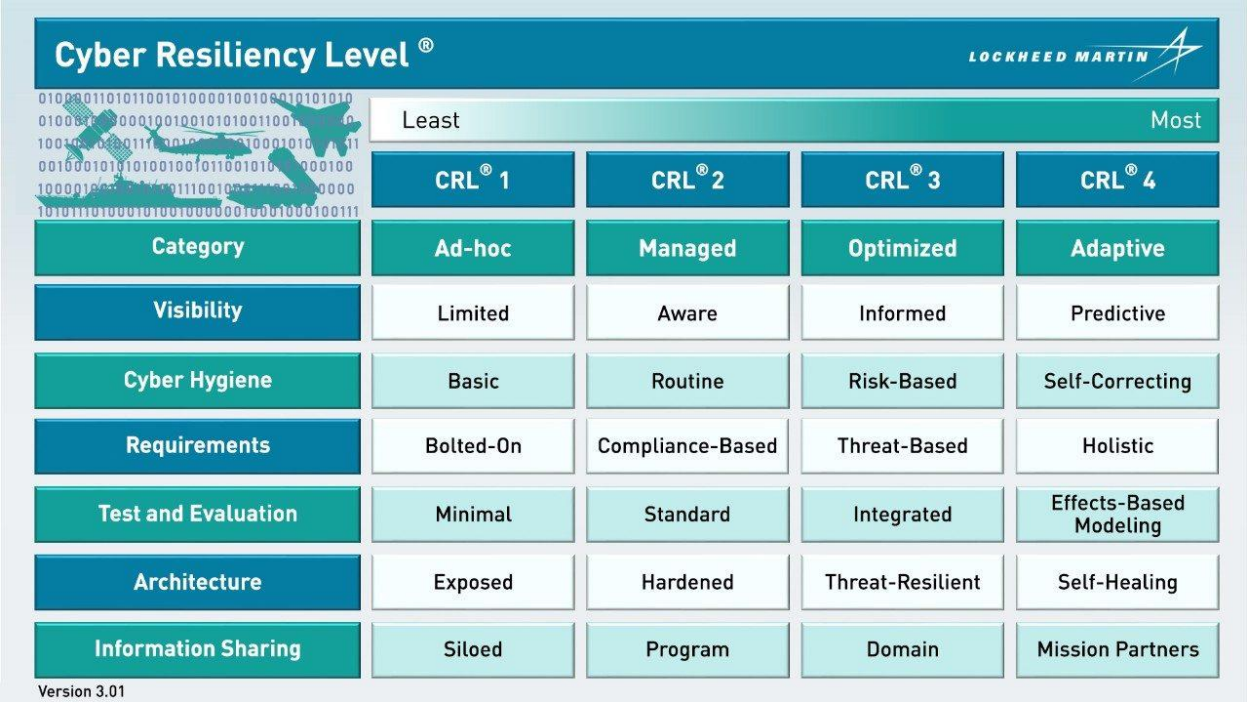

Figure 1. Cyber Resiliency Level® Framework V3.01

Overview

The CRS® tool captures inputs from subject matter experts (SME) about a system's state of cyber resiliency. These inputs are used to calculate key metrics corresponding to each of the six CRL® framework categories: Visibility, Cyber Hygiene, Requirements, Test and Evaluation, Architecture, and Information Sharing[2]. CRS® consists of a questionnaire and dashboard.

The questionnaire provides qualitative and quantitative cyber performance measures leveraging CRL® category criteria and maturity level descriptions. The questionnaire is divided into two sections:

[1] The term "weapon system" refers to major acquisition programs. These include a broad range of systems such as aircraft, missiles, ships, combat vehicles, sensors, and satellites, as well as their associated ground systems, simulators, and training systems (GAO, 2018).
[2] These six categories form the major recurring concerns of the Department of Defense and were pulled from across their strategy, policies, practices, testimonies, and conference proceedings (Beyer, Nance et al., 2020)

Demographics and Question Responses. These sections gather the data needed to perform measurements for each of the CRL® categories as well as information from each individual respondent. CRS® then performs data analytics on each of the responses and measurements to identify any discrepancies between respondents. The questionnaire responses are used for back-end analysis and are represented via the dashboard. This analysis provides valuable insight for measuring a system's current level of cyber resiliency and identifying specific opportunities to improve a system's cyber resiliency.

The dashboard consists of charts and data sets. The CRL® category measurement is calculated, and results are displayed via a radar chart. The radar chart (see Figure 2) provides visualization comparison of measurement data. Category levels are measured along their own axis, and overall differences displayed by the size and shape of the polygons. Another advantage of this chart is that the "as-is" and "to-be" measurements can be represented next to each other while still giving each category the same resolution.

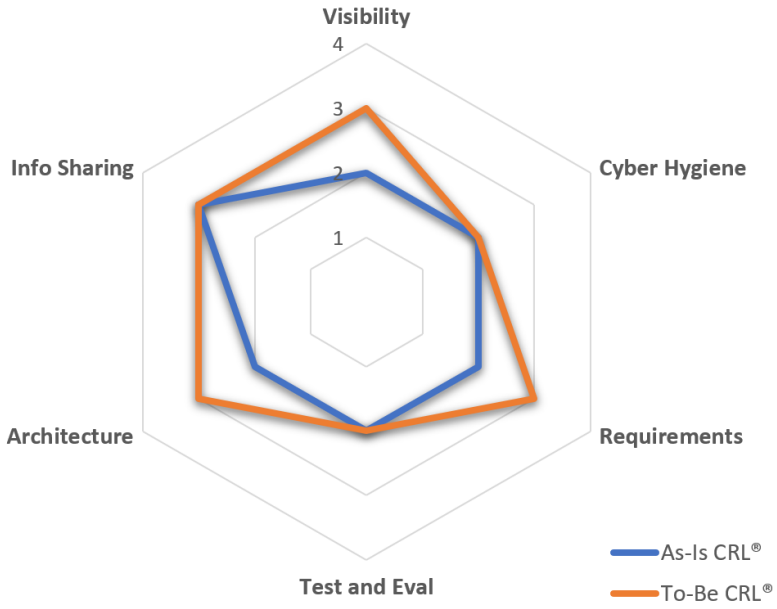

Figure 2. Cyber Resiliency Scoreboard® Radar Chart

In addition to the radar chart, program strengths and opportunities to improve the cyber resiliency of a program are highlighted in individual data sets within the dashboard. The data sets can be leveraged to identify CoAs and investments needed to achieve the "to-be" state.

Usage

The CRL® whitepaper (2020) outlines the recommended process steps programs should follow to use the CRS® tool. The CRS® is designed to be utilized in a variety of different scenarios. CRS® can either be used in a facilitated environment (such as a Cyber Table Top or an individual cyber resiliency measurement activity) where a trained cyber lead can help gather subject matter expertise into a single set of responses, or it can be used by having multiple cyber SMEs respond to the questionnaire. Statistical analysis from usage of CRS® have shown that in the multiple respondent use case, leveraging three to five cyber SMEs (respondents) can reduce measurement subjectivity. Once all respondents have completed the questionnaire, the data is exported from the questionnaire tool into the dashboard tool where it is processed using statistical analytics and is utilized to create the metrics showcased in the dashboard. One of the dashboard views is showcased in Figure 3 below. Within this view, cyber engineers can analyze the areas of exceedances (resiliency responses that are above the target CRL®

levels), watch items, and CRL® resiliency criteria that need to be satisfied for each category to reach the specified target CRL® levels. The content displayed in the dashboard was designed to be assessed by cyber SMEs. The program's cyber lead is responsible for summarizing this information and presenting results to program stakeholders.

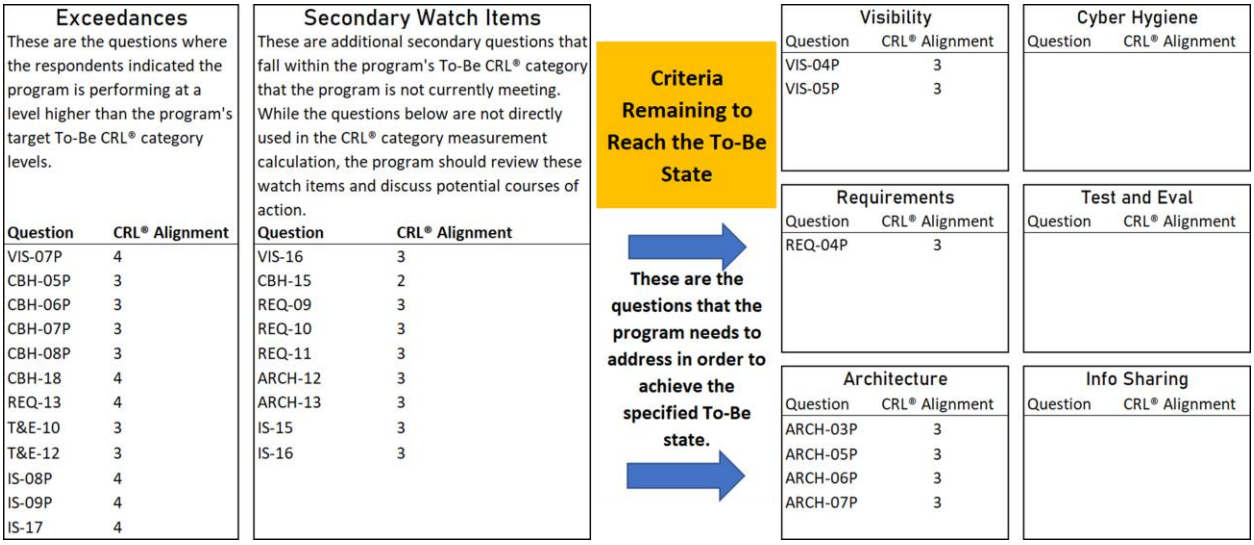

Figure 3. Cyber Resiliency Scoreboard® Dashboard

The CRS® data, along with risk assessment results, can be leveraged to identify and evaluate candidate CoAs. A cost-benefit analysis should be performed to estimate CoA strengths and weaknesses to determine which CoA will provide the best approach to achieving estimated benefits, preserving cost, and mitigating risks while increasing resiliency.

Summary

The Lockheed Martin CRS® tool measures CRL® category maturity levels of mission, training, and weapon systems. CRS® allows stakeholders to prioritize and select CoAs to improve cyber resilience. It includes a questionnaire and dashboard. The tool can be used in any phase of the acquisition lifecycle.

CRS® is easily adaptable and has been successfully applied to numerous programs within Lockheed Martin's business areas. Feedback from programs is used to validate CRL® category criteria, determine metrics and data representation, and improve tool performance. Program feedback is also leveraged to streamline the measurement process, making it more simplistic, understandable, and easier to discuss results with stakeholders. The update of CRS® to version 2.1 has incorporated multiple years of lessons learned and feedback and has added improvements and enhancements to the original tools and methods.

CRS® is a proven tool in mitigating risks and performing cost-benefit analysis for determining which mitigations provide the most cost-effective benefits. To learn more about CRS®, visit https://www.lockheedmartin.com/crs.

Acknowledgements

David Harrison, Shaun Thomas, Dr. Dawn Beyer, Jacque Blanchard, and Orion Strimenos provided significant contribution to the original work presented in this paper. Michael Hankins and Jason Johnson have developed substantial updates and currently maintain the CRS® tools and content.

Edited on 01 August 2023, Version 2.1. Points of Contact:

Michael Hankins, Fellow, & Jason Johnson, Associate Fellow

References

Beyer, D., Nance, M., Lardieri, P., Roberts, N., Hale, R., Plummer, T., Johnson II, J. (2020). *Lockheed Martin Cyber Resiliency Level® (CRL®) Framework V3.01 for Weapon, Mission, and Training Systems.* https://www.lockheedmartin.com/crl

GAO. (2018). *GAO-19-128: Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities.* https://www.gao.gov/assets/700/694913.pdf