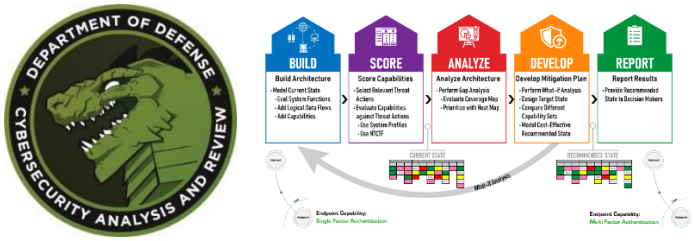
Cyber Security & Information Systems Information Analysis Center

2019 Success Story



"DoD Cybersecurity Analysis and Review (DoDCAR) Proliferation"

Customer: National Security Agency/Central Security Service (NSA/CSS)

Challenge:

As cybersecurity compliance requirements continue to grow in quantity and complexity, security goals/objectives tend to shift to a compliance-based focus. One of the observed results, identified in a recent OMB report, is stated below:

> "Agencies continue to allocate their limited cyber funding to acquire single point solutions to provide capabilities for perceived security gaps, rather than allocating funds to address gaps that threat actors are actually exposing."[1]

The same report suggests the NSA/CSS Technical Cyber Threat Framework (NTCTF), a standardized threat model mapped to the adversary life cycle, be employed to provide defenders with an improved awareness of the threat landscape. NSA/CSS mechanized this strategy for cyber investment with the DoDCAR framework, but lacked the resources to raise awareness among cybersecurity practitioners, let alone provide intensive training.

Approach: Under the Core Analysis Tasks (CAT) program, NSA/CSS tasked CSIAC to develop a five-day experiential training workshop to: (a) educate users on the NTCTF and DoDCAR fundamentals; (b) train participants to employ this strategy within the context of NIST's Cybersecurity Framework (CSF); and (c) provide first-hand experience performing a real-world DoDCAR analysis through exercises. The course culminates in a project-focused capstone exercise to apply course concepts in the evaluation of a notional network based on key system attributes, enabling students to produce a set of observations, recommendations, and assertions to inform architectural and investment decisions.

Value: The NSA/CSS DoDCAR team's mission is focused on refining DoDCAR processes and tools, while also performing high-value DoD cybersecurity acquisition analyses. Given the demand, CSIAC has been tasked to provide eight additional workshops. Per the sponsor, the vision is to integrate the content provided via this training into additional outlets, such as NSA's National Cryptologic School (NCS) and the Defense Acquisition University, to reach a broad scope of stakeholders.

[1] "*Federal Cybersecurity Risk Determination Report and Action Plan*", Office of Management and Budget (OMB), May 2018.

Distribution Statement A: Approved for public release; distribution unlimited.