Validating DoD CMMC Compliance Effectiveness

The Challenge of the DoD Cybersecurity Maturity Model Certification (CMMC)

The U.S. Department of Defense (DoD) relies on the defense industrial base to produce everything from logistics management to weapons platforms to computer networks. As cyberspace expanded into the defense industrial base, powering defense innovation for the country, hostile actors began to penetrate DoD contractor-built networks to steal and manipulate DoD data on a massive scale. In response, the Department has for years sought to elevate cybersecurity requirements for its contractors, and this winter launched its Cybersecurity Maturity Model Certification (CMMC) requiring that every DoD contractor that handles unclassified DoD-related information achieves a specific security certification.

If you are a chief information security officer working for a defense contractor, you now need to be able to prove that your cybersecurity program works as it should under the CMMC. To do so you need real, granular performance data to show security auditors that you are operating at the level of effectiveness required. That is what the CMMC is about. And that's what AttackIQ's Security Optimization Platform does for you.

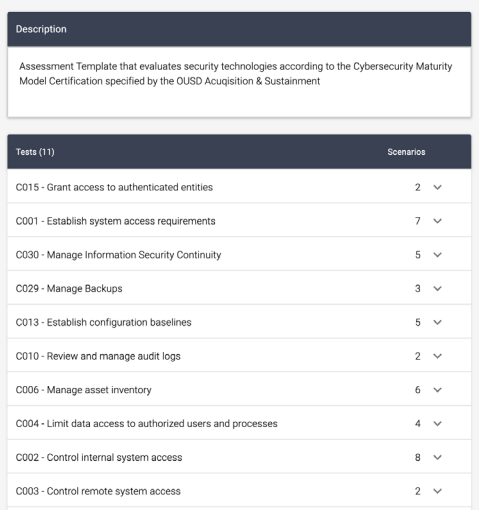

Fig. 1. CMMC Assessment Template

How AttackIQ's Security Optimization Platform Helps You Achieve Compliance with DoD's CMMC

The AttackIQ Security Optimization Platform operates at scale, in production environments, and across your security program to test, measure, and validate your security program effectiveness continuously and in an automated fashion. Through automated testing, the Security Optimization Platform discovers gaps in your security stack (in people, process, and technology) that teams may otherwise miss. It discovers misconfigurations. It reveals operator errors. It helps you make the most of your scarce resources by driving up effectiveness, sharpening your defenses and identifying areas for investment. This is transformative in any management environment—but especially when you have a baseline certification to meet and you need data to prove your cybersecurity maturity to DoD auditors.

AttackIQ has introduced new Assessments into the Security Optimization Platform to validate CMMC security controls. On the basis of MITRE ATT&CK®, these Assessments take adversary behaviors from the AttackIQ Library to guide your testing and produce empirical data so that you can understand how well your defenses perform to the CMMC standard. They provide evidence about how your organization's defenses comply with a specified CMMC control against a specific ATT&CK technique, reading "[CMMC control] mitigates [ATT&CK technique]", and generating analysis about how well your technologies detected and prevented attacks. Finally, the platform produces a remediation report with data and guidance to help you configure your technologies to produce a more effective result. Testing can happen as often as you like to ensure compliance effectiveness.

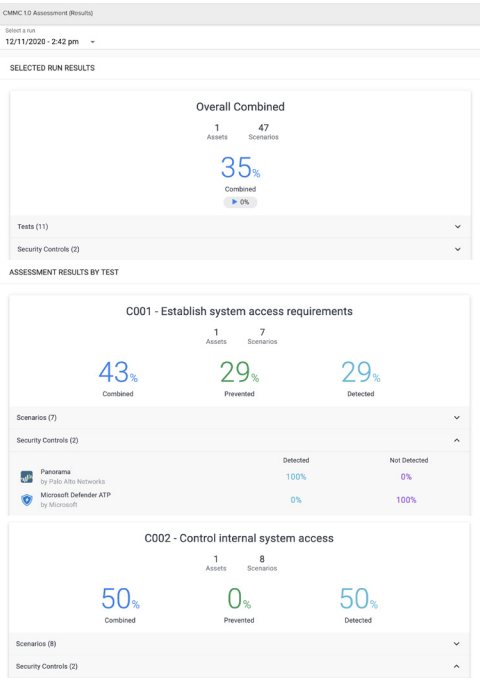

Fig 2. Detection and prevention results

The Net Result: CMMC Compliance and Improved Security Performance

With data from AttackIQ's Security Optimization Platform, defense contractors that design their security infrastructure around CMMC can prove compliance, turning the Security Optimization Platform into a CMMC compliance validation platform with data at the center. Click here to download the CISO's Guide to NIST 800-53 compliance to support this analytic work and here for a free course on how to achieve compliance effectiveness with AttackIQ.

Fig. 3. Remediation Report