accendnetworks

FLORIDA NATIONAL GUARD

Mock Command Cyber Readiness Inspection (CCRI)

The Challenge

Client: FLARNG

Location: St. Augustine, Florida

Florida Army National Guard (FLARNG) required a team of Command Cyber Readiness Inspection (CCRI) certified reviewers to pre-inspect the myriad of domains covered during a mock CCRI to include: Web and Database servers, Host Based Security System (HBSS), Assured Compliance Assessment Solution (ACAS), Traditional/Physical Security and Network Infrastructure. The project was to include a certified CCRI Team Lead to provide a full mock CCRI inspection, identify shortfalls, provide hands-on training and written/digital products to FLARNG's IT staff to improve the organization's CCRI score. CCRI is an inspection driven by the Army regulations and DISA guidelines. The domains evaluated are Technology, Cyber Network Defense (CND), and Contribution Factors.

Our Solution

FLARNG reached out to Accend Networks (Accend) with the requirement and Accend was able to provide a team of 4 highly certified and experienced security consultants to assist with the Mock CCRI audit. This was done well in advance of the audit. Due to COVID-19, scheduling had to be rescheduled around and delayed a bit but eventually, we were able to provide a certified reviewer for each area to be covered.

The Results

The Mock CCRI was done in a span of two weeks Monday to Friday. Each assigned certified consultant met with the assigned staff member in their respective domain and went through all the CCRI STIG for that area, assisted with remediating any vulnerabilities discovered so that FLARNG could obtain a high Mock CCRI score, which was needed to ensure a secured and complaint environment. The certified Team lead covered the CND and Contributing Factors.

CND Components are Warning Orders (WARNORDs), Tasking Orders (Orders (TASKORDs), Operations Orders (OPORD), General Administrative Order (GENADMIN) and Fragmentary Orders(FRAGOs) issued by USCYBERCOM and JFHQ-DODIN. USCYBERCOM and JFHQ-DODIN plan, coordinate, integrate, synchronize, and conduct activities to; direct the operations and defense of specified Department of Defense information networks (DODINs) and when directed, conduct full-spectrum military cyberspace operations in order to enable actions across all domains, ensuring US/Allied freedom of action in cyberspace and denying the same to our adversaries.

The Contributing Factors are designed to evaluate the Command's emphasis on compliance of existing Information Assurance (IA) controls during a Command Cyber Readiness Inspection (CCRI). The inspection items/calls in this document link to one or more of the IA Controls as found in NIST SP 800-53. The Contributing Factors evaluate three overall IA areas: Culture, Capability, and Conduct. Each area must be evaluated and discussed during a CCRI.

Accend's team of certified reviewers was able to assist FLARNG achieve a very high Mock CCRI score (above the 90% rating).

It was a successful audit and Accend may likely assist FLARNG with their on-going Mock CCRI every two years.

Contact Us

info@accendnetworks.com

408-784-2345

Headquarters
75 E. Santa Clara Street, Suite 600
San Jose, CA 95113