John C. Creger

CYSE 368

6/20/2025

UIN 01154971

Mid-Atlantic Regional Maintenance Center (MARMC) Reflection Paper 1

The first 50 hours of my internship are complete, and I can't believe how much I have learned and how much exposure I have received. I was nervous about starting in a field. I have been working in the diving profession for nearly 20 years and starting an internship in cyber security is completely foreign.

The first day was a bit of a whirlwind. I arrived at the cyber security office at 0700 and was meet with a confused look from a man in the MARMC SOC, apparently the supervisor had not informed his team that I was going to be helping over the next several weeks. After the introductions were completed, I was sent down to the IT department to get issued a laptop, and ancillary equipment. I got my workstation organized, computer updated and configured and was now ready for tasking. One of the cyber security analysts, Maurice, pulled me over to help with conducting network scans. The program he used was Tenable in conjunction with ACAS and he explained that this software is used in nearly every federal agency. MARMC has its own network called RMC-Net and is used to communicate with the other RMCs such as Southwest Regional Maintenance Center (SWRMC). Tenable conducted a Nessus scan of the entire network for vulnerabilities and gave a detailed report. I asked how Tenable stayed updated with known vulnerabilities and he showed me DOD patch repository and Defense Asset Distribution System (DADS) on the DISA site. We downloaded the audit files, plugins files and then uploaded the updated files into Tenable to ensure the most up to date CVE were being implemented in security

scans. The last task for the day was to sit in a Microsoft Teams meeting with NAVSEA RMF team to help people with the use of PowerShell and using the Evaluate STIG function. Most of this meeting was beyond my technical experience but was nonetheless interesting to learn about a new tool. Day one was informative, and I am ready for what the rest of the week has to offer.

I met a new member of the team on Tuesday, Nancy, and she has kind of taken me under her wing. She has been working in the office for two years and is mostly responsible for SAAR forms. That has become my new role in the office, processing the SAAR applications sent from the IT department. It's a relatively easy task. The ticket appears on the MARMC IT ticket request portal. I open the ticket, click on the SAAR form and verify the form has been properly completed. So far, the most common errors are personnel not checking the appropriate box for military, government or contractor. After I verify the accuracy of the form, I need to ensure the proper training has been completed for the application. In most cases all that is required is the DOD Cyber Awareness Challenge completed no later the October 1st of 2024. Lastly, I need to ensure the applicant has signed the organizational user agreement stating what they can and cannot do with government assets on government networks. Once training and user agreements are verified, we mark "approved" on the ticket for cyber security and forward the ticket to the physical security office for further processing. Nancy is also responsible for resetting SIPR tokens and is planning on training me in that process next week.

Mr. Fitzsimmons is the Director of Cyber Security and the breach head at MARMC. He provided excellent career training on different paths to take when first getting into the cyber security workforce. He showed me how to navigate USAJOBS website and how to read between the lines so to speak as you try to process these lengthy job listings. He is also helping me coordinate the site visits to NCDOC in Suffolk Va.

Overall the first 50 hours have been very educational, from a technical and personal perspective. I can tell I am just scratching the surface tapping into the wealth of cyber knowledge within the department as well as learning how all the different personalities jive and work together. The next 50 hours will hopefully be just as good and will include a site visit to one of the premier cyber assets in the Hampton Roads area.