

**Daniel Akpovi**

**CYSE 368**

**Spring 2026**

**Professor Teresa Duvall**

**TA Joshua Russell**

**McDonald Army Health Center / Information Management Division**

**Reflection # 2**

### **Second 50 Hours**

I spent most of my time these weeks working hands-on as compared to the first 50 hours because I began to make the transition from just learning about the environment to being involved in supporting it. I still asked questions and took notes, but now I am doing the work with more confidence. I was no longer only hearing how security relates to networking, I was seeing that relationship at work every day, especially when something looked wrong and I had to verify it prior to escalating it.

I spent a lot of time getting hands-on experience working within the actual tools I was using, most notably SolarWinds. Initially, I thought SolarWinds was simply an endless stream of metrics and alerts, and I did not have a clue as to which were important. Now I think of SolarWinds as more of a running log of what the network is doing, so I now can explain what I am viewing instead of staring at it. I use it to monitor the overall health of all the devices connected to the network, and the status of each network interface. I compare the data I see to a normal baseline to determine if there are any items that are moving away from their expected

behavior. When I observe either a spike or drop, I do not automatically attribute the change to the tool; rather, I verify the observed data, and look for trends over time, and compare the data across multiple devices. Lastly, I document the results of my investigation in a way that allows anyone else to easily review and follow along. Honestly, the documentation aspect has made the largest difference, because troubleshooting is much faster and easier to manage when documentation is both consistently clear and easily accessible. The fact that the documentation I provide helps other technicians and engineers easily troubleshoot issues makes me feel more productive and useful to the organization.

On the firewall side, my job was more about verifying and requesting process than actual configuration. Since I have read-only access to the Palo Alto Firewall, I can login, but I cannot modify any rules myself. I instead use Siphon to submit and monitor firewall requests, and I focus on verifying whether the requested access is proper before it is implemented. I review the source and destination information, ports, purpose and whether the request can be narrowed to the minimum access required. If I notice anything that seems overly broad, outdated or unnecessary, I document the concern and request the necessary modification through SIPHON so the proper security personnel can implement the correct changes. This experience taught me that firewall rules are not a "yes quick" decision. A small misconfiguration in a rule can open a long-term vulnerability if it is not thoroughly reviewed.

Segmentation also became hands-on. I assisted in verifying Virtual Local Area Networks (VLANs) configurations as well as their naming convention, and Access Control Lists (ACLs) purpose during normal operations and troubleshooting. It was a good reminder that segmentation is a security boundary as it is a design concept. One poorly executed exception can potentially

allow a compromised system to communicate with other systems beyond its intended scope. This made me rethink the extent of a breach every time that I have to review a configuration.

These hours also tested my ability to communicate as well as my ability to be technical. I wrote tickets resolution notes, summaries, and notes that had to be short, but complete. I developed the ability to explain what I did and why it matters, without taking for granted that the person I am communicating with understands "network" and "security."

T.A. Russell's reflection questions in the feedback he provided on my "Reflection 1" helped me to think more critically about the experience. Of those questions, he wants me to reflect on whether I see myself growing in this field. Yes, I am, because I like working in a role that has a defined goal and real implications. Another question he asked was what attributes do I bring to the table professionally? Consistent, patient and detail oriented, especially in documentation and troubleshooting, are some of the professional attributes that I feel I bring to the role. The final question he asked was to reflect on whether the work I am doing is meaningful. Yes, I feel that it is. I contribute to the operation of a healthcare computer network and therefore I contribute to the care and health of individuals that depend upon it. That motivates me to complete my job duties correctly every day, including the days that seem to repeat themselves.

Going forward, I would like to continue to develop my hands-on skills. I also wish to continue to refine how I express my rationale behind the technical decisions I make. Lastly, I would like to continue to develop the practice of critically evaluating the access and changes made to the systems from a security perspective versus just an operational perspective.