Steven Gills

Reflection Paper 1

Date: 02/08/2026

ODU Spring 2026

Blue Wireless

Professor Teresa Duvall / TA Joshua Russell

Reflection Paper #1

First 50 Hours

The first 50 hours of my job as a Senior Network Engineer at Blue Wireless has been very productive towards my Cybersecurity learning goals. My work week is the typical 40 hours per week, but 25 hours each week is dedicated towards my responsibilities in the company's IT Security. Blue Wireless is a subsidiary of Wireless Logic, and as a result we have much more resources available through our parent company. I had an introductory call with David Wilson, the Chief Information Security Officer, and he provided me with the roadmap and resources for obtaining the ISO 27001 certification within Blue Wireless. This included specific security policies to implement surrounding network security, asset management, physical security, and supplier security.

Alongside the introductory call with Wireless Logic’s CISO, I helped to implement a conditional access policy for our Microsoft environment. This conditional access performs a device posture check before allowing any access to anything in our Azure and Office environment. The device posture check ensures that the device has the latest security updates, the company's configuration patching software, as well as the endpoint security software. Additionally, sign-ons from non-compliant devices or web browsers are prohibited. This helps to

prevent unauthorized access to any user's account. During this rollout, I provided assistance to my colleagues by assigning the correct attributes to the workstations and phones within Microsoft Intune to ensure that all employees had uninterrupted access to their accounts.

Moreover, I was able to fully implement access control policies to our global core infrastructure. This allows only specific IPs, controlled by Blue Wireless, to access the management interfaces of our equipment. Alongside the access control policies, I reviewed each physical and virtual server in our self-hosted and cloud environments to ensure that they had automatic security updates, the latest access control policies, as well ensuring that insecure management protocols are disabled. In addition to the access control policies, I ensure that security and audit logs of each server and appliance were sent to our SIEM (Security Information and Event Management) log server.

Overall, the first 50 hours of my cybersecurity responsibilities have been productive with the introduction to the policies surrounding the ISO 27001 certification, assisting with the rollout of a conditional access policy for Microsoft accounts, as well as implementing access control policies. I believe that each of these actions were deeply involved in my learning objectives. I believe that terminology and cybersecurity policies learned from my coursework greatly helped me perform these tasks.