Bryant Watkins

Reflection Paper 3

Date: 06/12/2025

ODU Summer 2025

Professor Teresa Duvall

TA Ashley Robinson

Internship Reflection Paper: Third 50 Hours

Virginia Dept of State Police

The latest 50 hours as a communications technician provided me with another hands-on experience as well as learning some insight on some of the operational functions of networking hardware for the Virginia Department of State Police. I underwent the learning process to comprehend the full installation and troubleshooting of various alarms. I also would review published material outlining the operations of Juniper firewall devices as well as Motorola Moscad remote terminal units. These experiences work to further my understanding of the integral role that firewalls, alarm maintenance, and remote monitoring communications play in cybersecurity.

For practice in troubleshooting site alarms, I was instructed on how the steps of that process and then got to get hands-on experience doing so. My team would intentionally put random devices in alarm momentarily while I would be tasked with finding the culprit and rectifying the issue. The first and most important step was to identify the device affected, this can be difficult as there are commonly up to 50 different alarms at each site. Identification is done by either viewing the Motorola Moscad device or contacting the Network Operating Center, and then visually tracing the alarm cabling from the phone block directly to the device to ensure a

secure connection is in place. If the connection is fine, then comes the most difficult part – communicating with the device and identifying the issue.

Once connected via ethernet cable, I am then able to type the internet protocol address into a web browser and log into the respective device software maintenance site. These maintenance sites keep a comprehensive log of alarm events, making it relatively easy to identify an exact cause. Since my team obviously doesn't want to cause true damage to these devices, I often would be able to rectify the problem by resetting the module data for the respective device(s). This scenario was just to simulate under duress how the process would play out, in instances of true damage (i.e. lightning strike or vandalism) a ticket would be put in for the local State Police division communications team to respond with possibly our division's assistance as well to repair the device back to functionality.

I also learned the functions provided by the Juniper Networks SRX380 firewall and Motorola Moscad SDM 3000 RTU devices. The Juniper Networks device operates by providing large area network systems with multiple firewall features to ensure the security of network communications. Some of these firewall features provided include – antivirus software, malware detection, intrusion prevention, and encrypted network traffic. These devices are found at all sites and are vital to the cybersecurity of Virginia Department of State Police network communications.

The Motorola Moscad SDM 3000 RTU devices serve an important role as in cybersecurity operations. This is the device I used when identifying alarms in my earlier exercise, as the Moscad visually displays lights representing all 50 alarms. The Moscad is optimal for data collection and remote monitoring capabilities, thus meeting the needs of the Virginia Department of State Police. The Network Operating Center for the State Police is the

entity tasked with monitoring all the data collected from these devices. In collaboration with my team, when alarms arise as indicated by the Moscad – the Network Operations Center will communicate this to us while at any site. Our collaboration under this circumstance is why my earlier alarm troubleshooting exercise is all the more important for effective cybersecurity management for the Virginia Department of State Police.