Matthew Surratt

Reflection Paper 2

Date: 06/26/2026

ODU Summer 2026

RiverTrail Technology

Professor Teresa Duvall/TA Jade Hines

Internship Reflections

Second 50 Hours

During the second 50 hours of my internship at RiverTrail Technology, I became involved in the company's ongoing vulnerability assessment process by helping verify the security posture of client endpoints. My responsibilities included ensuring that operating systems were fully patched with the latest updates and verifying that antivirus software was current and functioning properly. To complete this work, I was given access to the company's managed service provider (MSP) management platform. This was my first experience using enterprise-level MSP software, and I was impressed by its capabilities. The platform provided centralized visibility into hundreds of devices, allowing technicians to quickly identify systems that were out of compliance, missing updates, or experiencing security issues. This experience also reinforced the importance of proactive cybersecurity. Rather than waiting for a security incident to occur, RiverTrail Technology continuously monitors client systems and addresses vulnerabilities before they can be exploited.

Working with the MSP platform significantly expanded my understanding of how cybersecurity operates in a real business environment. Managing numerous client

endpoints through centralized software gave me a much broader perspective on enterprise security operations and showed me how automation and management tools improve both efficiency and security.

Another significant responsibility I was given during this phase of my internship was researching a better solution for managing client network devices, particularly firewalls and routers. While the MSP management platform does an excellent job managing endpoints such as workstations and servers, it does not provide the level of network device management that RiverTrail Technology would like to have. I was tasked with evaluating remote monitoring and management (RMM) and network configuration management solutions that specialize in managing firewalls, routers, and switches.

This project required me to research several enterprise management platforms, compare their capabilities, and determine how they could integrate into the company's existing workflow. I examined features such as automated firmware management, vulnerability detection, compliance monitoring, and device inventory. I also considered how these platforms could reduce manual administration while improving the security and reliability of client network infrastructure.

What made this assignment especially meaningful was that I was not simply following an established procedure. Instead, I was given the opportunity to help design a new process from the ground up. Rather than being handed a solution, I was encouraged to evaluate different products, identify their strengths and weaknesses, and determine which platform would best meet the company's needs. Being trusted with this responsibility has

been one of the most rewarding parts of my internship. It has shown me that my supervisors value my research and technical judgment. It has also provided me with practical experience evaluating enterprise cybersecurity and network management solutions. Developing recommendations for automating the management of network devices has given me valuable insight into how managed service providers continually improve their operations while strengthening the security posture of their clients. This experience has reinforced my interest in cybersecurity consulting and managed IT services, where identifying better solutions and improving existing processes are essential parts of the job.

One realization that has become increasingly clear during my internship is just how many different career paths exist within cybersecurity and managed IT services. There are so many facets to this profession that I cannot imagine not finding a niche that I truly enjoy. I can see opportunities to continue learning and eventually specialize in an area that matches both my interests and strengths.

I find the work extremely rewarding, even though clients may not always recognize the importance of everything that happens behind the scenes. Much of cybersecurity is preventative in nature. When systems remain secure, updates are installed, vulnerabilities are remediated, and backups function correctly, clients often never realize how much work has gone into protecting their business. This has become especially apparent as I have followed the recent news involving vulnerabilities and cyberattacks targeting firewalls and routers. I now have a much greater appreciation for the importance of proactively managing these devices through continuous monitoring. Knowing that the work I perform contributes

to reducing our clients' exposure to these types of threats gives me a genuine sense of purpose. Even if clients never see the countless preventative measures taking place behind the scenes, I know that our efforts help protect their businesses, their employees, and their customers. That knowledge makes the work both meaningful and highly rewarding.