Reflection Paper 2

Importance of Cybersecurity Tools

Amari Fisher

10/17/2025

Second Reflection

After completing 100 hours of the cybersecurity internship provided by COVA CCI, I have learned more about the tools and techniques utilized in cybersecurity. I learned about tenable and its significance as a vulnerability management tool, and learned to differentiate Microsoft Defender and Windows Defender. As the former provides way more general policy and security options and the latter mainly just provides an antivirus system. Microsoft defender would be more important in the context of large organizations that often require multiple endpoints to be secure within multiple networks, similarly, tenable is also useful in the context of large organizations that manage more than just ~25 endpoints. Although both tenable and defender serve distinct purposes, I learned that there are some overlaps between the two because defender also can serve as a simple vulnerability management tool but its main purpose lies in policy creation, and ids/ips systems. In one of the meetings with my chosen company, we spoke about having multiple tools to fall back on which I linked to the cybersecurity concept of having no single point of failure meaning that if one tool is down, you can fall back to multiple other secondary tools for a reasonable amount of time. Tenable's importance falls on its capabilities as an efficient vulnerability management tool, during the meeting, we saw that tenable could host thousands of end systems without issue and even offers options to configure cloud scanning and monitor cloud systems. Its diverse tool set allows for cybersecurity professionals to quickly solve issues that rely on known vulnerabilities.

SIEM Importance

Although not explicitly mentioned during the internship, we spoke about SIEM tools such as splunk. SIEM is also an important aspect of cybersecurity because it allows for forensic analysis and centralized collection of all logs for multiple reasons such as third party auditing, or log retention compliance(regulatory compliance). Splunk is one of the most popular tools regarding SIEM because of its capabilities, and ease of access. I have worked with splunk before during out of class research and loved that it was brought up during the meetings.

Ethical Cybersecurity

In regards to ethical cybersecurity, I have learned more, but since my chosen employer leans more toward the technical sides of cybersecurity there may not be much ethics going on within simple scans. During the next session of design thinking with dr. baki, we will probably touch more upon ethical cybersecurity considerations.

Conclusion

In conclusion, tools like tenable and defender are important toward achieving a better security posture in large organizations. Tenable's importance lies in its ability to scan endpoints for known vulnerabilities, and Defender's importance relies on its ability to serve as a IDS/IPS tool and its policy driven security features. SIEM has a significant impact on cybersecurity because it's the main component that allows for forensic analysis. Additionally, ethics remain a serious concern within cybersecurity, and I hope that in the future during another design thinking session we will further discuss the ethical dimensions of cybersecurity. All of these tools and aspects of cybersecurity are very important toward establishing a strong security foundation/posture.