Lesson 30: Planning a Continuous Monitoring Strategy (Task P-7)

Task:

Think of one important thing you would **Continuously Monitor** for OpenMRS and how. You might choose data backups, error logs, firewall logs – whatever you feel is a key security aspect to keep an eye on. Describe your chosen item and why it's important to monitor regularly.

Answer: Server and Network Vulnerabilities

I would run both a bi-monthly application vulnerability scan as well as a bi-monthly network vulnerability scan (because I think a monthly scan is too long a time between scans to really stay ahead of the curve) on the OpenMRS server. I would then have both scanners feed their information to a SIEM. The SIEM would then ingest the information from the scanner reports to help prioritize and respond to risks. By having the scanners work in tandem with the SIEM, OpenMRS would have the right tools to design a security posture that I think would be both proactive and reactive.