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

For OpenMRS, I would employ a two-prong approach to monitoring, which would include scanning and a SIEM working in tandem. I would continuously monitor vulnerability exposure across the server, network, and application stack by running authenticated daily scans for internet-facing assets, weekly full scans for all nodes, with automated app-layer scans on each deployment, and continuous monitoring for new Common Vulnerabilities and Exposures (CVEs).

I would then have the scanners stream/feed their information to the SIEM. The SIEM would then ingest the information from the scanner reports to help prioritize and respond to risks. By using the scans in tandem with the SIEM, it would ensure that OpenMRS would be able to minimize exposure to PHI, while having the right tools to maintain a security posture that would be both proactive and reactive.