Toluwanimi Oladeleajose

Toluwaez@gmail.com | LINKEDIN | GITHUB

SUMMARY

Systems-focused analyst with experience in cybersecurity, healthcare IT environments, and enterprise systems support. Skilled in vulnerability analysis, troubleshooting, and root cause investigation, Proven ability to collaborate with diverse stakeholders to enhance security awareness and compliance. Seeking to leverage my skills and experience to contribute to the strategic direction of Union's information security program.

EDUCATION

Stephen F. Austin State University — B.S. Computer Information System, 2024
University of Illinois Springfield — M.B.A. Cybersecurity Management (Expected: 2028)

SKILLS

Splunk, Tenable, Cortex Xpanse | Python, Bash, PowerShell

AWS (basic), Azure, Windows/Linux | Troubleshooting, Data Analysis, Root Cause Analysis, Vulnerability Management

EXPERIENCE

HOPE ER *Sep 2025 – Present*
IT Operations Coordinator

- Collaborate with external vendors (e.g., Nanox, CDMC) to deploy and integrate medicaldevices, ensuring secure and seamless connectivity across networked systems.
- Resolve hardware, software, and network issues to minimize downtime for clinical and administrative staff.
- Support implementation and maintenance of lab and healthcare software systems, improving accessibility and usability for doctors and nurses.
- Assisted in the development and implementation of information security policies and procedures, ensuring compliance with federal and state regulations, including PCI, FERPA, and HIPAA.
- Facilitate integration between third-party platforms (e.g., Medicus Services) and internal systems to streamline clinical workflows and data access.
- Monitor system performance and proactively resolve infrastructure and network connectivity issues to maintain high availability.

CYDEO *Feb 2025 – Aug 2025*
SOC Analyst

- Conducted troubleshooting and root cause analysis of security incidents, escalating issues when necessary to ensure timely resolution.
- Monitored and analyzed security alerts and logs using SIEM tools to identify and resolve system issues, contributing to the overall security posture of the organization.
- Documented findings and supported reporting efforts to improve system monitoring and operational visibility, ensuring that stakeholders are informed of potential risks.
- Collaborated with IT teams to develop and maintain a security roadmap, ensuring alignment with institutional goals and regulatory requirements.
- Reviewed and audited firewall rules and security configurations, enhancing network security and reducing potential vulnerabilities.

Estée Lauder / Provalus *Jun 2024 – Jan 2025*
Threat & Vulnerability Management Analyst

- Analyzed vulnerability scan results using Tenable and Cortex Xpanse, prioritizing remediation efforts based on risk and impact to enterprise systems.
- Developed reports and dashboards to provide visibility into vulnerabilities and system risks for stakeholders.
- Automated reporting workflows using Python, which reduced manual workload by 30%, allowing for more efficient use of resources.
- Partnered with cross-functional teams to track and remediate vulnerabilities, significantly improving the overall security posture of the organization.
- Maintained thorough documentation and supported vulnerability management processes across enterprise environments, ensuring compliance with relevant regulations..
- Conducted risk assessments and vulnerability scans, providing actionable recommendations to improve security measures across the organization.