Position Title: Cybersecurity Specialist

Ecb Non-Esg 39.13(2) Nte 81-03

Location: Madison, WI (Onsite)
Division: Engineering, Educational Communication Board (ECB)
Reports to: Chief Information Security Officer (CISO)
Employment Type: Part time, 20 hours per week (PTT) (.50 FTE - Unclassified)

Position Summary:

The Educational Communications Board (ECB) is committed to maintaining strong cybersecurity practices that align with the Wisconsin Department of Enterprise Technology (DET) security standards. DET security standards are based upon the National Institute of Standards and Technology (NIST) security standards. The Cybersecurity Specialist plays a key role in supporting this mission by analyzing security logs, identifying vulnerabilities, and recommending remediation strategies. This position is instrumental in helping ECB mature its cybersecurity posture through proactive threat detection, risk assessment, and the development of effective monitoring tools and dashboards.

The Cybersecurity Specialist works as part of ECB's security team, reporting to the agency's CISO and collaborating closely with the Core Engineering Team. This position is expected to be on site at ECB's Madison location.

Goals And Responsibilities:

60% Goal A: Contribute to the continuous improvement of ECB's cybersecurity maturity through assessments.

1. Contribute to the continuous improvement of ECB's cybersecurity maturity through assessments and proactive recommendations.
2. Analyze security Nessus scan results and SIEM data regularly, identifying threats, anomalies, and vulnerabilities.
3. Recommend and document actionable remediation strategies based on log analysis and DET security standards.
4. Create and maintain dashboards, risk assessments, and security monitoring reports to support efficient log and risk review.
5. Monitor patch management systems for security threats and run software and operating system updates as needed.
6. Support security infrastructure and perform system upgrades when authorized.

30% Goal B: Proactive cybersecurity recommendations.

1. Recommend and document actionable remediation strategies based on log analysis and DET security standards.
2. Review network and system configurations against DET security standards and identify areas for improvement.

3. Research, evaluate, and recommend additional security technologies or systems to enhance ECB's defense capability.
4. Apply basic knowledge of Incident Response techniques and principles to support security operations

10% GOAL C: Perform miscellaneous job duties.

1. Participate in weekly security team meetings and contribute to ongoing cybersecurity initiatives.
2. Perform all job duties with prescribed industry-standard and ECB health and safety procedures and guidelines.
3. Perform other duties as assigned.

Knowledge, Skills and Abilities

1. Security Tools: Knowledge of security monitoring and management platforms such as CrowdStrike, Tenable, NinjaOne, or equivalent.
2. Frameworks & Standards: Familiarity with the NIST Risk Management Framework (RMF) and familiarity with Wisconsin DET or public-sector cybersecurity standards.
3. Network Security: Knowledge of network security architecture (topology, protocols, components) with the ability to implement or support secure environments.
4. Technical Analysis: Ability to perform log file reviews, vulnerability assessments, and apply core principles (CIA triad) to risk management.
5. Automation & Scripting: Basic scripting, coding, or query language skills (e.g., Python, SQL, PowerShell) with knowledge of report automation.
6. Education & Outreach: Ability to support cybersecurity education, awareness, and training initiatives.
7. Professional Skills: Strong analytical and written communication skills, ability to produce high-quality technical documentation.
8. Ability to work effectively both independently and as part of a collaborative team.