Information Security Engineer/Analyst

Department: Information Systems

Exemption Classification: Exempt

Location: Full-Remote

Annual Salary Range: $83,723.05 - $125,584.57

Role:

The Information Security Engineer/Analyst is responsible for researching, designing, implementing, and maintaining PFCU's all information security-related hardware or software and technical cybersecurity controls in alignment with business, policy, and compliance requirements. This role also serves as a liaison between vendors and other departments on information security-related projects.

***Compensation is based on a wide array of factors unique to each candidate, including but not limited to skillset, years and depth of experience, certifications, and specific office location. Compensation ranges may differ in differing locations due to cost of labor considerations.**

Essential Functions and Responsibilities:

- Implement, maintain, and monitor IDS/IPS rule sets, alerts, and reports. Identify and fix detected vulnerabilities to maintain a high-security standard. Install security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs.
- Research data security needs and requirements and security enhancements, develop best practices for IT security, and make recommendations to management. Document and present security in an internal meeting to discuss security analysis, findings, and security/compliance responses.
- Build and maintain tools for automation of security events and reporting. Optimize and reconfigure tools to improve security processes. Perform investigations and improve detection processes on various security events from various sources to determine whether they pose a threat.
- Review past incidents and identify attack trends. Fine-tune and reconfigure alerts based on prior incidents to improve detection. Develop, update, and maintain a repository of cybersecurity threat information that may be used in conducting risk assessments and reports on cyber risk trends. Actively participate in developing, documenting, and implementing new processes to expand and mature the organization's capabilities.

- Develop and mature processes and procedures to report, identify, and prioritize risk remediation and ensure ownership of prioritization. Design and implement technology risk and control assurance solutions. Maintain IT policies, standards, and procedures, and work through the process to have them reviewed, approved, and published; lead training and awareness sessions to explain the requirements to others.
- Performs routine audits of security databases including Active Directory, Anti-Virus, Data Loss Prevention (DLP), Group Policy, Remote Authentication Dial-In User Service (RADIUS), and regularly reviews other security logging systems, and audits of Credit Union procedures including new hire/transfer/separation process, configure checklists, firewall changes, Uniform Resource Locator (URL)/Spam filter changes, DLP changes, file permission changes, inventory changes, equipment changes, and system health checks. Designs and/or implements changes to these systems in response to any discovered vulnerabilities.
- Performs other job-related duties as assigned.

Knowledge, Skills, and Abilities:

- Bachelor of Science (BS) degree with emphasis in Computer Science (or similar field) required or achievement of formal certifications recognized in the industry as equivalent to a bachelor’s degree.
- Security certifications include CISSP, CCSP, CEH, GSEC, or equivalent.
- Microsoft Certified: Azure Administrator, Azure Security Engineer, Azure Network Engineer, or Cybersecurity Architect Expert
- Three to five (3 to 5) years of similar or related experience, preferably within the financial services industry.
- Advanced working knowledge with Microsoft 365, Azure/Entra ID, and services within the Microsoft ecosystem.
- Intermediate to advanced working knowledge in configuration and maintenance of endpoint security solutions (e.g., Intune, Microsoft Defender, Bitdefender, Carbon Black, and CIS operating system hardening)
- Subject matter expertise of network security technologies, their implementation, operations, and limitations, including firewalls (CATO, Palo Alto), VPNs, network IDS/IPS solutions, network monitoring solutions (NDRs), network access control solutions, proxies, SIEM, antivirus, penetration testing, vulnerability scans, IPSec and TLS based VPNs, and email security.
- Advanced working knowledge of business, network systems, network protocols, hardware concepts, and applications, including DNS, LADP, TCP/IP, OSI model, virtualization, database design/hardening, email/secure messaging, Data Loss Prevention, endpoint protection.
- Ability to identify and mitigate network vulnerabilities and explain how to avoid them.
- In-depth knowledge of SIEM log ingestion and alert creation.

- Working knowledge of incident response and investigation tools and techniques.
- Working knowledge of information security practices and methodologies.
- Ability to write scripts/code using Python or other scripting languages for automation is preferred.
- Experience in responding to security questionnaires and end-user questions.
- Professional and effective interaction, verbal, and written communication skills.
- Must have excellent written and oral communication skills to communicate technical information to non-technical people and strong interpersonal skills.

Physical Demands and Work Environment:

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions however, no accommodations will be made which may pose serious health or safety risks to the employee or others, or which impose undue hardships on the Credit Union.

While performing the duties of this job, the employee is regularly required to sit and use hands to finger, handle, or feel objects, tools or controls. The employee is frequently required to talk or hear. The employee is occasionally required to stand; walk, reach with hands and arms; and stoop, kneel, crouch, or crawl.

The employee must regularly lift and/or move up to 15 pounds. Specific vision abilities required by this job include close vision, color vision, peripheral vision, depth perception, and the ability to adjust focus.

The noise level in the work environment is usually moderate.

This job description is not a complete statement of all duties and responsibilities comprising the position.