Open Position: Cyber Security Analyst - Chicago, IL
Full -Time -Exempt

The successful in this position is responsible for serving as the Single Point of Contact for system related system intrusions and/or data compromises of the Credit Union. Using a blend of computer science education, investigative experience and tools, problem-solving skills, and training in forensics and incident response, incumbent will oversee and direct the investigation of a wide variety of cases. These cases include, but are not limited to website defacement, internal and external account abuse, theft of source code and other intellectual property, click-fraud, hacking and other forms of security breaches. Additionally, the incumbent will be responsible for recommending and implementing improvements to current practices to proactively mitigate security threats. Resources to do the job require reliance on extensive experience and judgment to plan for and reinforce the overall safety and security of the critical data. General direction is received from the Chief Information Security Officer.

Responsibilities of the position will include:

Network Responsibilities:
- Monitor electronic channels for cases of abuse or fraudulent activity.
- Work closely with the information security and fraud departments to proactively mitigate, detect, report, and investigate suspicious activity.
- Be first responder for cyber-security incidents, monitor alerts, events and incidents identified through security event management tools, virtual SOC, etc. and confirm validity of identified incidents.
- Differentiate false positives from true intrusion attempts; track the latest in security vulnerabilities, advisories, incidents, and penetration techniques, review periodic vulnerability scan results.
- Manage issues resulting from investigation, work collaboratively with technical and business leads to follow up accordingly to security incident management procedures and processes, and assist in development and resolution of daily reports.
- Provide comprehensive computer forensic investigations: Acquire, collect, document, and preserve evidence from various forms of electronic media and equipment.
- Conduct highly-confidential internal investigations into violations of Acceptable Use Policies and other activities counter to the organizations success.
- Handle evidence in accordance with company policies and forensic lab best practices.
System Projects and Process Improvement:

- Participate and potentially lead projects to further enhance security technologies, practices, processes.
- Participate in the improvement and development of process/procedure manuals and documentation.
- Participate in the updates and improvements of the Incident Response Plan in conjunction with current threats.
- Provide education to existing staff on the emerging trends of security operations methodology, information security concepts, security analysis and monitoring.

Qualifications:
Completion of a Bachelor’s degree in Engineering or Computer science and minimum five years of I.T. experience supporting complex network architecture at the enterprise level; with significant experience in security oversight and management. Must have a solid understanding of information technology and information security. Security and Network proficiency certification(s) preferred not required (CISM, CISSP, MCSE, GIAC, and CCSP). Must be an articulate and persuasive leader who can communicate security-related concepts to a broad range of technical and non-technical staff. Excellent communication, analytical, troubleshooting, project management and organizational skills are required.

Interested candidates, please submit your updated resume to Terri Demchinski via email at tdemchinski@alliantcreditunion.com. For any questions, please call (773) 462-2106.