1st Capital Bank

Title: Cyber & Information Security Analyst
Reports to: Chief Information Officer
FLSA Status: Non-Exempt
Location: Salinas/Hybrid

The Cyber and Information Security Analyst is responsible for leading and implementing various aspects of Cybersecurity, Infrastructure and Application Security for mission critical enterprise products.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

Conduct Information Security and risk assessments on organizational controls around information security domains including Cybersecurity, on-premises and cloud-based infrastructure, enterprise applications, data security (including privacy), business continuity and disaster recovery, and IAM (Identity and Access Management)

- Monitor, review, analyze and document security alerts and reports generated from various platforms and applications
- Identify threat risks from the reported phishing, malware and virus-related alerts
- Protect 1st Capital Bank from intrusions and all forms of cyber-attacks by proactively profiling internet activities, detecting patterns in intrusion techniques and identifying possible sources of intrusions
- Build automation for detecting, preventing and responding to security events
- Perform vulnerability scans; review and track identified vulnerabilities until remediated
- Establish and coordinate remediation and mitigation activities for identified security risks
- Incorporate Security check processes into existing and new enterprise systems
- Conduct regular quarterly, semi-annual, and annual application user access reviews to ensure banking regulatory compliance (FFIEC, GLBA, SOX)
- Research, analyze, recommend, design and implement network-based, host-based or cloud-based Information Security solutions
- Monitor, track and assess changes to the global threat landscape and evaluate the impact and exposure to 1st Capital Bank and its customers
- Design, implement and maintain Security controls that support NIST, FFIEC, SOC2, PCI DSS, GLBA, SOX frameworks
- Ensure ongoing protection of corporate data and information assets by properly maintaining Information Security policies, standards, procedures and processes
- Manage and assist with the ongoing improvement of the Bank's Information Security awareness training program
- Conduct regular phishing campaigns; track and analyze metrics

- Manage third-party vendors risk assessments
- Assist with gathering documentation to support internal and external audits
- Assist in execution of third-party security testing (pen testing, bug bounty, audits, etc.)
- Continuously update documentation and prepare materials for quarterly IT Steering Committee or other governance entities
- Act as a Cybersecurity and Information Security SME (Subject Matter Expert) to various internal teams on emerging threats
- Continuously learn the latest Cybersecurity and Information Security information by participating in educational opportunities, reading professional publications, and participating in professional events
- Work closely with the IT Team and assist, as needed

MINIMUM QUALIFICATIONS

- Bachelor's degree in Computer Information Science, Engineering, or related field, or suitable combination of education, experience and training
- Information Security certifications such as CISSP, CISA, CISM, GCIA or other SANS GIAC certifications (either currently active or will be completed within 6-12 months).
- 5+ years of experience in Information Security, Risk and Compliance management, preferably in highly regulated industry (financial services, banking)
- Good understanding of the following compliance/security frameworks: NIST, FFIEC, SOC2, PCI DSS, GLBA and SOX
- Medium-to-advanced knowledge of subjects such as infrastructure (network, servers, storage) security design and architecture, endpoint protection, SSO, MDM, BYOD, DLP, IAM, vulnerability management, penetration testing, intrusion detection, risk management, and forensics
- Familiar with cloud Security architecture in Microsoft Azure and Office 365
- Working knowledge of Information Security tools (vulnerability management, Nessus, Rapid7, OpenSSL, NMAP, PAM, SIEM, pen testing, network packet analysis, forensics, etc.) and basic scripting
- Experience performing periodic access reviews to critical systems
- Experience evaluating third-party vendor risks

Ability to:

- Proven ability to lead internal risk assessments, develop and implement remediation and system/application-hardening plans.
- Ability to develop and report on KPIs with solid recommendations for improvements.
- Focused personality, with a demonstrated ability to take initiative, successfully handle and prioritize multiple competing assignments and effectively manage deadlines
- Professional, articulate, and able to use good independent judgment and discretion
- Proven self-starter, requiring little supervision to take initiative and execute above responsibilities

- Strong analytical and excellent writing skills
- Ability to relate complex material in a user-friendly format
- Strong general understanding of banking regulations (specifically security and compliance regulations), federal and state security requirements, bank policies and procedures

PHYSICAL DEMANDS

Physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of the job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

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

- Employee must occasionally lift and/or move up to 25 pounds. Specific vision abilities required by the job includes: close vision, distance vision, peripheral vision, depth perception, and the ability to adjust focus

WORK ENVIRONMENT

Work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

- While performing the duties of this job, the employee is occasionally exposed to the risk of electrical shock
- Noise level in the work environment is usually moderate
- Some occasional travel will be required