Senior Risk Analyst, Cybersecurity

Position Summary

Farmer Mac is a vital part of the agricultural credit markets; therefore, protecting its infrastructure, systems, and data from cyber threats is paramount. Farmer Mac is seeking a risk professional who has experience in implementing, maintaining, and monitoring security systems and processes. The Senior Risk Analyst role includes planning and implementing security measures to protect endpoints, networks, applications, and data. A primary daily responsibility of the job is to detect, investigate, and respond to incidents.

In addition, the Senior Risk Analyst is expected to stay abreast of the latest intelligence, trends, and technologies, including hackers' methodologies, to anticipate security breaches.

The role is also involved in planning and implementing preventative security measures and assists the Infrastructure team with building disaster recovery plans. Also, the role will be tasked with preparing and participating in information security audit and compliance efforts.

The Senior Risk Analyst will possess a combination of business knowledge, technical skills, and communication skills to define and guide information security strategy. This individual will initiate and manage projects and communicate issues and risks to management. With demonstrated success, there is certain opportunity for career advancement.

The People You Will Work With

The position will report directly to the Enterprise Risk Officer. The position will primarily liaison with members of the Farmer Mac Infrastructure, Development, Enterprise Data, Business Analysts, Operations, and Compliance teams. The role will also interreact frequently with third-party vendors tasked with securing Farmer Mac's environment.

Where and When You Will Work

Work is to be conducted at Farmer Mac's headquarters at 1999 K Street NW, Washington, DC. Core business hours are Monday through Friday 8:30 am to 5:30 pm Eastern Time. Work outside of these times may be required for planned and unplanned activities for the purposes of completion of a time sensitive project or attendance of off-site meetings or events.

Primary Responsibilities and Duties

- Evaluates, designs, monitors, administers, and/or implements information security systems, policies and processes
- Executes system vulnerability scanning, remediation process oversight, including reporting and governance oversight
- Reviews the development, testing, and implementation of security plans, products, and control techniques
- Consults with client and development area management and staff in the design and implementation of new or modified information security processes
- Implements, administers, and maintains systems and network access
- Performs routine and complex end-to-end support of a variety of security users and applications
- Performs development and maintenance activities for security applications and tools
- Troubleshoots complex systems and networking problems
- Performs investigative research, analysis and troubleshooting to identify, resolve, and report highly complex security issues and may evaluate and monitor system or tool performance
- Monitors system and network configurations to ensure compliance with information security policies, standards and procedures
- Performs technical evaluations and testing of security hardware and software
- Identifies operational inefficiencies and potential risks, executes and improves operational processes, and mitigates risk
- Defines and adjusts processes required to detect, analyze, and respond to security incidents
- Processes requests to design, modify, and grant security accesses, and other security requests as assigned
- Provides guidance to team on complex role provisioning scenarios
- Performs routine and complex project support for security and infrastructure efforts
- Provides audit support and prepares for information security audit and compliance efforts
- Collects, compiles, and generates information security reports on system and network accesses based on established KPIs
- Reports and prepares briefing packages for presentation to customers, management, and senior leadership
- Performs an annual cybersecurity risk and threat assessment and creates a strategic information security plan

- May perform or assist with network and host-based penetration testing using internal and commercially available tools and/or coordinate and manage third-party penetration testing activities
- Participates in the evaluation of new technologies and vendor proposals, conducts process analysis, reviews information security architecture and recommends modifications to the information security operations that reduce costs and improve service
- Performs security impact analyses prior to introduction of software changes to test and production environments
- Performs security review of third-party hosted or developed applications
- Coordinates with the managed services providers (MSP) to ensure that the MSP meet contractual obligations
- Participates in business continuity and disaster-recovery activities
- Performs related duties as assigned or requested

Desired Skills and Qualifications

- Strong understanding of Microsoft technologies including Windows Server, SQL Server, Office 365, Azure, and .Net development
- Strong understanding of multi-factor authentication and data-loss prevention tools
- Understanding of networking, including topologies, data flow, firewalls, and routing
- Hands-on experience in writing reports, risk/threat metrics using data analytics tools
- Ability to provide subject matter expert guidance to business units on DLP usage strategy, remediation workflow, monitoring, blocking, alerting, and reporting
- Ability to manage an incident response and recovery event
- Preferable experience executing information security tasks within a regulated financial institution
- Familiarity with SSAE 18 and SOX404
- Excellent oral and written communication skills to interact effectively in a team setting as well as cross-team and cross-organization setting
- Strong ambition for career development and growth

Education and Experience

- Bachelor's Degree in Information Systems, Computer Science or related field – Required
- 6+ years of related experience in Information Security and/or Information Technology

- 6+ years' experience of dedicated systems administration, virtualization, and technical support
- CISSP or GIAC – Required

About Us

At Farmer Mac, everything we do is inspired by our mission, our promise and our values. We are a diverse group of talented, engaged, and passionate individuals who are committed to bringing vitality to rural America through innovation, collaboration, and excellence. This team embodies these principles that have guided Farmer Mac since its inception and help us to serve as a champion for rural America. Candidates for this position must share the same appreciation for rural America and should want to devote a career to serving those who help set the global standard in agriculture and rural utilities while advancing the livelihood of rural communities.

Farmer Mac's Mission

Farmer Mac is committed to help build a strong and vital rural America by increasing the availability and affordability of credit for the benefit of American agriculture and rural communities.

Farmer Mac's Promise

To build a strong and vital rural America through innovation, collaboration, and excellence.

Farmer Mac's Core Values

Stewardship

Innovative Thinking

Unrelenting Excellence

Passion for Rural America

Unparalleled Service

Collegial Collaboration

Absolute Integrity

One Farmer Mac

Farmer Mac is an equal opportunity employer.

NO EMPLOYEE OR JOB APPLICANT WILL BE DENIED OPPORTUNITIES OR BENEFITS AT FARMER MAC BASED ON RACE, RELIGION, COLOR, SEX, AGE, NATIONAL ORIGIN, DISABILITY, VETERAN STATUS, CITIZENSHIP STATUS, GENETIC INFORMATION, OR ANY OTHER BASIS PROHIBITED BY APPLICABLE LAW.