Adventist Risk Management
Career Opportunity

Information Security Analyst

As the official insurance and risk management company for the worldwide Seventh-day Adventist Church, Adventist Risk Management®, Inc. (ARM) is devoted to finding Adventist professionals who are committed to the success of our clients and our organization.

Working at ARM means you are joining a diverse global team of professionals who are focused on providing timely, real-world insurance products and innovative risk management solutions for minimizing risk within Adventist ministries. Beginning in 1936, our team has grown with the Church and now serves over 21 million adult members, 86,000 churches, 8,515 schools, 527 hospitals/clinics, as well as many other ministries. We also provide underwriting, claims, financial, and risk management services for two captive insurance companies that collectively write over $100 million in premium annually

Joining ARM allows you to be part of a team of professionals committed to extraordinary customer service, a culture of diversity and inclusion, while working in a Seventh-day Adventist Christian environment. You are encouraged to visit our website www.adventistrisk.org to learn more about ARM. We don't view what we do as just a business; our ministry is to protect the ministries of the Seventh-day Adventist Church.

We currently have a full-time **Information Security Analyst** position open on our Information Technology team. The Information Security Analyst's primary role is to provide day-to-day operational support to the ARM suite of security application layers in the cloud, WAN and LAN. This position is inclusive of our company benefits package which offers healthcare, employer matching 403(b), paid vacation, professional training, and other programs. This position is telework/remote eligible.

What is in it for you?

- An opportunity for long-term and upward growth potential with an organization that emphasizes opportunities for current team members.
- You will have the knowledge that your work is meaningful and valuable.
- Exceptional benefits, great paid time off and additional perks that come with working at ARM.

We will count on you to do:

- Manage and support an organization's security measures such as anti-virus software, passwords, and firewalls to identify any areas that might make information systems vulnerable to attack. They also analyze reports generated by the monitoring system to identify anything that may indicate a future risk.
- Manage and support security systems, such as firewalls, email filtering, DNS filtering, MFA systems, SSO systems, SLDAP systems, LAN segmentation controls, data protection controls, patching, encryption, vulnerability scanning, pen testing, and so on. Includes overseeing the proper deployment, configuration, and functioning of these systems.
- Monitor all security operations and infrastructure, working with the ARM SIEM to analyze alerts and logs to keep an eye on your organization's digital security footprint
- Collaborates with users to discuss computer data access needs, to identify security threats and violations,

and to identify and recommend needed programming or process changes.
- Uses data encryption, firewalls, and other appropriate security tools and applications to conceal and protect transfers of confidential digital information.
- Develops and implements plans to safeguard digital data from accidental or unauthorized modification, destruction, or disclosure; adheres to emergency data processing needs.
- Reviews violations of security procedures; provides training to ensure violations do not recur.
- Monitors and restricts access to sensitive, confidential, or other high-security data.
- Modifies security files and applications as able and necessary to provide specialized access, allow new software to be installed or integrated, or correct errors.
- Performs risk assessments (internal and third-party partners), audits, and tests to ensure proper functioning of data processing activities and security measures.
- Safeguards system security and improves overall server and network efficiency by training users and promoting security awareness.
- Determines when to update virus protection systems by monitoring current reports of computer viruses; facilitates or performs needed updates.
- Performs other related duties as assigned.

Security Operational Responsibilities

- Management of network security suite of systems.
- Management of access control for infrastructure systems.
- Monitor and test system performance and provide performance statistics and reports.
- Management of security upgrades, patches, and updates for security level systems.
- As needed, work with network engineers to execute modifications to infrastructure router/switch, backup and security server environment in order to improve efficiency, reliability, and performance.
- Develop and maintain training materials and related documentation.

What you need to have:

- Bachelor's degree in computer science, information technology security or related fields with at lease three years required
- Six years related experience and/or training; or equivalent combination of education
- CCNA, CCNA-Security, CCIE, CISA, or other relevant certifications preferred

KNOWLEDGE AND SKILL:

- Thorough understanding of computer-related security systems including firewalls, encryption, and password protection and authentication.
- Experience with Cisco security platforms such as Cisco ASAs and FTDs, Cisco AMP, Cisco Firesight and Firepower, Cisco ISE, Cisco TrustSec, Umbrella, Wireless infrastructure, etc.
- Experience with Cisco routers and switches, vlan design and support, etc.
- Experience with virtual hypervisors such as Citrix, VMWare and KVM.
- Experience with enterprise level email security protection and filtering layers.
- Experience with enterprise backup systems such as Unitrends, Veam, HYCU, etc.
- Experience with APC power infrastructure components such as cabinets, racks, power distribution units, online ups systems, etc.
- Project management skills a definite asset.
- Strong understanding of the organization's goals and objectives.
- Good written and oral communication skills; good interpersonal skills.

- Ability to present ideas in business-friendly and user-friendly language.
- Highly self motivated and directed, with keen attention to detail.
- Proven analytical and problem-solving abilities.
- Ability to effectively prioritize tasks in a high-pressure environment.
- Strong customer service orientation.
- Experience working in a team-oriented, collaborative environment.

What makes you stand out:

- Self-starter, resourcefulness, with the ability to work independently without daily supervision.
- Ability to work in a fast-paced environment and ability to prioritize work.
- An ideal team player who is hungry, humble, and smart.
- Ability to think critically and to plan and develop strategy for serving our clients

Interested in a Career:

Please contact our Human Resources team by August 22nd at 301-453-6983 or email your resume to rfiddis@adventistrisk.org. Please reference the Account Executive position.