



READi TECH

Managed Security Analyst

Position Title: Managed Security Analyst	Department: IS
Reports To: Business Intelligence Manager	FLSA Status: Exempt

General Summary:

The Managed Security Analyst is responsible for the real-time identification and alerting of information security events that pose an immediate risk to DRN's employees, customers, or business operations. Regular work hours are Monday – Friday 8 am to 5 pm. Night, weekend and on call work will be required as the business need dictates.

Essential Job Functions:

- Cyber security incident response
- Provide proactive cyber managed services
- Evaluating and analyzing customers' security audits and implementing solutions
- Implement network protection recommendations to improve DRN Security Audit score. (NIST Framework)
- Conduct external vulnerability scans
- Conduct Phishing campaigns
- Responsible for intrusion detection and prevention
- Responsible for security policy administration
- Develop security standards and best practices for DRN and its customers
- Provide ongoing security training for DRN and as a service
- Conduct client facing consulting engagements
- Research and develop new cyber service offerings and the latest information technology security trends
- Conduct penetration testing
- Perform server maintenance such as patching, upgrading, rebooting, active directory maintenance, security permissions and other related server activities.
- Work closely with IS team members, aiding where needed.

- Perform network and general data center maintenance.
- Research and analyze new software solutions as needed.
- Project manage projects for managed service customer installs of new software or hardware. Ensure delivery of timely results that meet customers' timeline and budget needs.
- Track and maintain hardware and software licensing as well as ensuring continuity of software support contracts.
- Involved in regular internal IT projects for DRN.
- Assist in protecting DRN's network via Cyber Security policies, processes and procedures.
- Enforce security policy in daily activities as it relates to the IS team's functions.
- Document IT processes and information as implemented
- Goal & team focused
- Attendance is an essential function of this position. Regular, reliable, consistent and punctual attendance is required.
- Responsible for all other duties as assigned

Knowledge, Skills, and Abilities:

- Knowledge of company policies, procedures, products and services.
- Knowledge of commercial and federal cybersecurity best practices
- Knowledge and hands on experience with security monitoring tools
- Knowledge and experience with firewalls, proxies, incident response, and information security frameworks
- Knowledge and familiarity with configuring and executing vulnerability scans
- Knowledge and experience with system security vulnerabilities and remediation techniques
- Knowledge of Microsoft Active Directory, Exchange Server, IIS, Sharepoint server, System Center Configuration Manager, Terminal Services
- Knowledge of the following protocols/standards: SMTP, POP, FTP, DNS, DHCP
- Knowledge of programming languages
- Skilled in written and oral communication, including presentation skills
- Skilled in supporting clients and serving as a technical advisor
- Skilled in analytic, qualitative, and quantitative reasoning
- Ability to identify and mitigate network vulnerabilities and explain how to avoid them
- Ability to understand network and web-related protocols, operating system security, common attack patterns, and exploitation techniques
- Ability to perform log analysis
- Ability to anticipate and respond to changing priorities and operate effectively in a dynamic demand-based environment requiring flexibility and responsiveness to client matters and needs
- Ability to communicate with customers, co-workers and various business contacts in a professional and courteous manner, keeping them informed of progress, notifying them of impending changes or scheduled outages, etc.

- Ability to organize and prioritize multiple work assignments.
- Ability to make sound decisions using information at hand.
- Ability to develop in-depth knowledge of the service catalog and how it relates to customer's needs.
- Ability to keep current with future technologies emerging in the industry by attending conferences, reviewing IT publications and online materials, etc.
- Ability to document internal processes and procedures related to duties and responsibilities.
- Ability to develop in-depth knowledge of the service catalog and how it relates to customers' needs.
- Ability to contribute in a sales environment.

Education, Experience and Qualifications:

BS in Cyber Security or related degree. Minimum of 2 years working experience.

Physical Requirements:

PHYSICAL REQUIREMENTS	0-24%	25-49%	50-74%	75-100%
Seeing: Must be able to identify by sight maintenance needs on buildings and grounds. Must be able to drive vehicle and operate other machinery such as mowers/trimmers.				X
Communication: Must be able to communicate with co-workers.				X
Movement: Must be able to move around facilities to perform maintenance and other assigned duties.			X	
Climbing/Stooping/Kneeling: Must be able to ascend and descend ladders and work on different levels of the buildings. Must be able to position self to perform maintenance and other assigned duties.			X	
Lifting/Pulling/Pushing: Must be able to lift at least 50 pounds regularly from floor to waist, occasionally overhead, and move heavy equipment.		X		
Fingering/Grasping/Feeling: Must be able to write, type, and use phone system.				X

Working Conditions:

This factor measures the surroundings or physical conditions under which a job must be done and the extent to which those conditions make the job disagreeable. Consider the presence and relative amount of exposure to dust, dirt, heat, fumes, contaminants, cold, noise, vibration, wetness, etc.

Good working conditions with the absence of disagreeable conditions.

Note: The statements herein are intended to describe the general nature and level of work being performed by employees, and are not to be construed as an exhaustive list of responsibilities, duties and skills required of personnel so classified. Furthermore, they do not establish a contract for employment and are subject to change at the discretion of the employer.

This position is an exempt position, not subject to the overtime provisions of the Fair Labor Standards Act. DRN is an Equal Opportunity Employer and offers a competitive compensation and benefits package.