

Role: Information Security Analyst

Job Summary:

As an information security analyst, you will be responsible for the implementation and continuous improvement of our clients' cyber defenses. You will accomplish this through the management and refinement of security control measures and by following industry best practices. You will also be responsible for keeping on top of the evolving threat landscape while staying current with leading edge countermeasures.

Duties and Responsibilities

- Provide technical assistance in the selection, configuration and maintenance of both on-premise and cloud security devices/systems including, but not limited to, firewalls, IPS/IDS, SIEM, WAF, network-based malware detection and related platforms.
- Maintain and monitor sensors and data sources to ensure all security events are being logged, monitored, correlated and escalated to the appropriate parties.
- Investigate security breaches and other cyber security incidents.
- Perform vulnerability testing, risk analyses and security assessments.
- Remediate detected vulnerabilities to maintain a high-security standard.
- Develop company-wide best practices for IT security.
- Adhere to, improve and manage IT security policies.
- Help educate staff on cyber security best practices.
- Work with project teams to advise on and ensure security best practices are incorporated throughout the project lifecycle.
- Participate and gather requirements in single sign on projects.
- Facilitate, configure and roll out security self-awareness solution programs.
- Assess and ensure vendors are compliant with organizational data protection policies and practices.
- Research security enhancements and make recommendations to management team.
- Stay up to date on information technology trends and security standards.
- Perform regular reporting to assess the overall security posture within the organization.

Qualifications

- Bachelor's degree in computer science or related field.
- Extensive experience in information security.
- Cyber security training and certifications such as those from SANS or ISC2.
- Detailed understanding of firewalls, SIEM, antivirus, IDPS and CASB concepts.
- Demonstrated experience in creating conceptual, logical and physical security diagrams.
- Thorough understanding of vulnerabilities and countermeasures.
- Excellent knowledge of the tools and techniques used by ethical hackers including vulnerability scanners and network mapping tools.
- Excellent communication skills including the ability to clearly communicate risks and risk management issues to technologists and non-technologists.
- Experience with connected technologies such as public cloud infrastructure, internet of things, sensors and integrated platforms.

What RTS gives back to you:

- A collaborative and creative work environment that truly values and cares about their employees as people
- Bonus Program
- Comprehensive benefits package
- Training and education opportunities
- A fun and inclusive team building environment

If you have any questions, please contact our resident Senior Talent Acquisition Specialist - [Marny Barnes](#) or visit our [Career Page](#) for more opportunities! We are not able to hire (or sponsor) out-of-country applicants that do not have a current Permanent Resident Status or Work Visa.