Vital Strategies

Building Health Systems Globally

IT Cyber Security Analyst

Vital Strategies

Vital Strategies, based in New York City, is an international public health organization. We develop and oversee programs to strengthen public health systems and address leading causes of morbidity and mortality, providing expertise in project implementation and management, strategic communications, epidemiology and surveillance, and other core public health capacities. Our specific programs include road safety, obesity prevention, tobacco control, and activities to strengthen public health data systems and the use of public health data to guide policy and decision-making. Activities are based in low and middle income countries and cities in Africa, Latin America, Asia and the Pacific. Please visit our website at www.vitalstrategies.org to find out more about our work.

The Position

Vital Strategies is seeking qualified candidates for the position of **IT Cyber Security Analyst (CSA)**. This is a full-time position based in New York City. Applicants must possess a valid work permit to work in New York City.

The IT Cyber Security Analyst (CSA) is responsible for performing security vulnerability analysis and remediation across IT infrastructures and platforms to ensure the confidentiality, availability, and integrity of data across the Vital strategies systems. The CSA delivers qualitative and quantitative analysis of the systems and processes supporting the system's risk management program while managing multiple projects and maintaining technical skills and knowledge with emerging security technology. This role reports to the Director of Information Technology, and works closely with the Network Engineer, other IT staff and applicable business units to prioritize risk and determine the best course of action for risk mitigation. The CSA helps develop and maintain security policies and procedures, as well as the education and awareness program.

Specific Duties:

The skills required in this position include creation, maintenance and monitoring of access control, data integrity, and data loss prevention of Vital Strategies systems, devices and associated information assets.

- Respond to cyber security audit action items that include providing supporting documentation to auditors, evaluating audit results for relevance/accuracy, and working with teams to develop and implement plan to remediate audit findings
- Creating, updating, reviewing department and organizational wide policies and procedures to adhere to industry best practices, laws and organizational requirements
- Responsible for organization-wide information security training and awareness to ensure employees understand the integral role they play in safe guarding the company's information assets against unauthorized use and disclosure
- Performs risk assessments on third party vendors evaluating on security best practices and legal requirements to ensure that Vital Strategies does not inherit unacceptable risk by doing business with that vendor

- Works alongside team members to effectively analyze and assess new technologies and/or ideas that would be considered a security risk and recommend action
- Responsible for the direct oversight and management of incidents that would be considered a security risk including system outages, malicious cyber threats and/or any situation where there is a loss of productivity due to system failure
- Responsible for the development, setup, maintenance, and enforcement of identity access management and multi-factor authentication policies and procedures
- Responsible for the implementation, maintenance and tuning of a data loss prevention program to assure data privacy and security is in compliance with company policies and state and federal laws
- Responsible for vulnerability remediation and penetration testing of the Vital Strategies network to futureproof against potential exploits
- Work with in-house legal counsel to ensure IT systems are in place to abide by GDPR
- Discover and report any systems and/or users that are not conforming to the Vital Strategies usage policy and report their findings
- Responsible for investigating, classifying, documenting, remediating and reporting on cyber security incidents that would be considered a risk to the company
- Audit user activity to enforce compliance with regulatory and policy requirements to mitigate risk and protect Vital Strategies information assets
- Manage and maintain all security software and appliances across the organization.
- Additional duties as assigned as it relates to the position

Qualifications and skill set:

- Bachelor's degree in information technology or related field. Concentration in information security or cybersecurity preferred, or 3-7 years equivalent experience
- Expertise in network engineering or administration, and with Microsoft Productivity Suite
- Preferred Certified Information Security Systems Professional (CISSP), Systems Security Certified Practitioner (SSCP), or Certified Information Systems Auditor (CISA). Information technology, information security, system administrator, or application administrator is a plus
- Understanding of Data Security Standards and information security frameworks such as NIST
- Experience in performing information security risk assessments
- Strong foundation in and in-depth technical knowledge of security engineering, computer and network security, authentication, and security controls
- Strong understanding of most of the following common security compliance frameworks, controls, and best practices: (SSAE 16 - SOC 2 and 3), OWASP Top 10, SANS, NIST
- Critical Security Controls, regulations governing personally identifiable information (PII)
- In-depth understanding of network and system security technology and practices across all major-computing areas
- Experience creating and updating relevant security policies and risk assessment documentation
- Experience managing, documenting and coordinating testing of Business Continuity and Disaster Recovery Plans
- Self-confidence and interpersonal skills
- Proven analytic and problem-solving skills
- Ability to effectively prioritize in high pressure environment

- Planning and organizing skills
- Good administration of cyber security management skills
- Able to operate effectively in a team environment with both technical and non- technical team members
- Ability to operate with minimal supervision
- Ability to manage time effectively
- Ability to maintain professional demeanor under stress
- Ability to operate within customer standard operating procedures

How to apply:

Please send CV and a cover letter, including salary expectations, to hr@vitalstrategies.org. Applications will be accepted until position is filled.

Vital Strategies offers competitive compensation based on prior experience and qualifications as well as comprehensive benefits in order to best support our people. Benefits we offer include: health, dental and vision insurance where Vital Strategies pays generously towards the cost of these benefits for employees and their families/domestic partner; 15 paid vacation days (rising to 20 paid vacation days from fourth year of service and 25 from seventh year onwards), 13 paid federal holidays and paid days off between the Christmas and New Year's holidays; paid sick days; retirement savings plan; commuter benefits and basic life and personal accident insurance.