Global Cybersecurity Analyst (CSIRT)

Location: [Africa] [Ghana]

Town/City: Accra

Category: Information Technology

Job Type: Fixed term, Full-time

***Preferred position location: Accra, Ghana. Other possible locations: Indonesia, Thailand, Bolivia or the Philippines where WVI is registered to operate.**

***Please submit your CV in English.**

PURPOSE OF THE POSITION:

Individuals working as Global Cybersecurity Analyst are responsible for working on security projects/issues for one or more functional areas (e.g., data, systems, network and/or Web) across the enterprise, develop security solutions for medium to complex assignments, work on multiple projects as a team member and lead systems-related security components. They provide expertise and assistance to all IT projects to ensure the company's infrastructure and information assets are protected.

Individuals within the IT Security job family plan, execute, and manage multi-faceted projects related to compliance management, risk assessment and mitigation, control assurance, business continuity and disaster recovery, and user awareness. They are focused on developing and driving security strategies, policies/standards, ensuring the effectiveness of solutions, and providing security-focused consultative services to the organization.

Individuals develop, execute and manage data, system, network and internet security strategies and solutions within a business area and across the enterprise. They develop security policies and procedures such as user log-on and authentication rules, security breach escalation procedures, security auditing procedures and use of firewalls and encryption routines. To guide enforcement of security policies and procedures, they administer and monitor data security profiles on all platforms by reviewing security violation reports and investigating security exceptions. They update, maintain and document security controls and provide direct support to the business and internal IT groups. IT Security professionals evaluate and recommend security products, services and/or procedures. They also communicate and educate IT and the business about security policies and industry standards, and provide solutions for enterprise/business security issues.

IT Security professionals require strong technical, analytical, communication and consulting skills with knowledge of IT Security and related technologies. Security certifications (i.e., Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manage (CISM), Global Information Assurance Certification (GIAC) and/or other certifications) may be required.

KEY RESPONSIBILITIES:

Policies, Processes & Standards:

- Maintains an up-to-date understanding of industry best practices.
- Develops, enhances and implements enterprise-wide security policies, procedures and standards.
- Supports service-level agreements (SLAs) to ensure that security controls are managed and maintained.
- Monitors compliance with security policies, standards, guidelines and procedures.
- Ensures security compliance with legal and regulatory standards.

Business Requirements:

- Participates with the project team(s) to gather a full understanding of project scope and business requirements.
- Works with customers to identify security requirements using methods that may include risk and business impact assessments.
- Studies current and proposed business processes to determine impact of security measures on business goals.
- Provides security-related guidance on business processes.

Security Solutions:

- Participates in designing secure infrastructure solutions and applications.

Risk Assessments:

- Works directly with the customers and other internal departments and organizations to facilitate IT risk analysis and risk management processes and to identify acceptable levels of residual risk.
- Conducts business impact analysis to ensure resources are adequately protected with proper security measures.

- Analyzes security analysis reports for security vulnerabilities and recommends feasible and appropriate options.
- Creates, disseminates and updates documentation of identified IT risks and controls.
- Reports on significant trends and vulnerabilities.
- Develops plans to achieve security requirements and address identified risks.
- Follows up on deficiencies identified in monitoring reviews, self-assessments, automated assessments, and internal and external audits to ensure that appropriate remediation measures have been taken.

Security Audits:

- Performs security audits.
- Participates in security investigations and compliance reviews as requested by external auditors.
- Monitors multiple logs across diverse platforms to uncover specific activities as they occur from platform to platform.
- Creates spreadsheets and databases with information in support of security monitoring and account/data access authorizations.
- Consults with clients on security violations.

Problem Management:

- Provides security support to ensure that security issues are addressed throughout the project life cycle.
- Performs control and vulnerability assessments.
- Provides responsive support for problems found during normal working hours as well as outside normal working hours.
- Identifies and resolves root causes of security-related problems.
- Responds to security incidents, conducts forensic investigations and targets reviews of suspect areas.
- Works with teams to resolve issues that are uncovered by various internal and 3rd party monitoring tools.

Incident Management:

- Monitors and analyzes incident data and makes recommendations for process improvement.
- Analyzes reports and makes recommendations for improving reporting structure and content.

Communications/Consulting:

- Collaborates on critical IT projects to ensure that security issues are addressed throughout the project life cycle.
- Informs stakeholders about compliance and security-related issues and activities affecting the assigned area or project.
- Interfaces regularly with staff from various departments communicating security issues and responding to requests for assistance and information.
- Reports to management concerning residual risk, vulnerabilities and other security exposures, including misuse of information assets and noncompliance.

Vendor Management:

- Works with third party vendors during problem resolutions.
- Interfaces with third party vendors to evaluate new security products or as part of a security assessment process.

Research/Evaluation:

- Performs application security risk assessments for new or updated internal or third-party applications.
- Evaluates and recommends hardware and software systems that provide security functions.

Training:

- Assists in the development of security awareness and compliance training programs.
- Provides communication and training as needed.

- May guide users on the usage and administration of security tools that control and monitor information security.

Coaching/Mentoring:

- Mentors less experienced team members.

?

KNOWLEDGE, SKILLS AND ABILITIES:

- Bachelor's Degree in Computer Science, Information Systems or other related field, or equivalent work experience.
- Work experience in designing, implementing, and supporting incident management practices.
- Work experience in designing, implementing, and supporting emergency and data breach response practices.
- Requires knowledge of security issues, techniques and implications across all existing computer platforms.
- Typically has 3-5 years of combined cybersecurity work experience with a broad range of exposure to incident management, audit, risk management, and problem management, and 1 - 2 years of experience with data privacy.
- Willingness and ability to travel domestically and internationally, as necessary.
- Work experience in security incident management, security risk management, and vulnerability assessment.
- Effective in written and verbal communication in English.

Preferred:

- CISSP certification.
- CEH certification.
- Project Management experience.
- Risk Management experience.

- Incident Management experience.
- Problem Management experience.
- Vendor Management experience.

Work Environment/Travel:

- The position requires ability and willingness to travel domestically and internationally up to 20% of the time.