IT PUZZLE RECRUITMENT

We are a technology recruitment partner focused on search and selection of IT experts internationally. Currently, we are looking for an accomplished experts for the role of Cyber Security Analyst. We offer a rewarding and exciting professional experience and opportunity to develop your career in a highly competitive international environment.

Cyber Security Analyst

Location: Warsaw, Poland

Responsibilities / Accountabilities:

The Cyber Security Analyst reports to the Vice President Global Cybersecurity. This role will include engaging in cybersecurity control and process improvement activities, being a key member of the security incident response team, driving and assisting in driving special projects and other cyber security related activities.

This position will serve as the analyst/subject matter expert on all cybersecurity matters, technical and otherwise, involving the security of classified information systems under their purview. This person will perform assessments of systems and networks within the networking environment and will identify where those systems and networks deviate from acceptable configurations or policy. This is achieved through passive evaluations such as analysis from security system data logs and active evaluations such as vulnerability assessments. The position will include support of process, analysis, coordination, security documentations, as well as investigations and emerging technologies. Perform analyses to validate established security requirements and to recommend additional security requirements and safeguards.

- Maintain up-to-date detailed knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors.
- Performs in-depth analysis of security issues and/or vulnerabilities. Ensures compliance to audit, regulatory, and legal requirements.
- Builds and maintains effective relationships with peers and internal business partners.
- Assist in creating effective controls to address security concerns.
- Perform daily cadences, which includes monitoring and reviewing of cybersecurity systems, investigating events and incidents.
- Recommend additional security solutions or enhancements for existing IT solutions to improve overall enterprise security.
- Assist at Implementing and maintaining a formal IT security program and security policies.
- Identifies potential threats and risks and makes recommendations to mitigate these issues.
- Participate in the planning and design of enterprise security strategy, processes and procedures.
- Assists in driving security related projects as applicable.
- Assists in maintaining compliance with various compliance programs, such as PCI, GDPR and Sarbanes-Oxley.
- Manage the remediation and mitigation of security violations to determine if the network environment has been breached, assess the impact and preserve the evidence.
- Maintain and enhance the security education, training and awareness program for the organization.
- Assist in managing, maintaining and executing a continuous incident monitoring program.
- Perform control validation and remediation validation to ensure controls comply with security policies, procedures and technical requirements.
- Assist and partner with IT teams at optimizing and enhancing security tool deployment and continuous monitoring capabilities.

Responsibilities / Accountabilities:

- Create weekly metric reports to demonstrate control effectiveness using monitoring tools.
- Assist with incident response activities.
- Provides project support for both IT and business initiatives requiring security posture and control improvements.
- Perform security risk assessments, share results and recommend a remediation approach.
- Analyze system performance for potential security problems. Prepares system security reports by collecting, analyzing and summarizing data trends.
- Perform vulnerability assessments on internal applications and external facing websites.
- Collaborate with other Teams to ensure appropriate security incident management and threat response processes are followed.
- Perform root cause analysis and create reports based on outcomes of incident investigations.
- Expected to stay up to date on the latest intelligence, including hacker methodologies or the kill chain, in order to anticipate security breaches.

Professional Qualifications/ Experience:

- Bachelor’s degree in information security (or associated discipline) plus at least 2 years of experience working with vulnerability management, incident response; or equivalent combination of education and experience.
- Broad knowledge of networking, infrastructure, and application technologies, including SIEM (Security Incident Event Management) approach to log management.
- General understanding of PCI DSS requirements and controls.
- Security certification is preferred (CISSP, CISA, CEH).
- Work both independently and as part of a team at all levels and across all business units.
- Demonstrate an understanding of business processes, internal control risk management, IT controls and how they interact together.
- Demonstrate solid knowledge of information security risk and countermeasures.
- Specific technical knowledge in Office 365, endpoint security solutions, Checkpoint, Linux, Internet technologies, Networking technologies and Encryption technologies.
- Experience interacting with a Managed Security Service Provider (MSSP) a plus
- Experience with next generation antivirus, email hygiene solutions and next generation firewalls is preferred

Offer:

- Challenging and innovative global projects
- Medical care, sport card
- Flexible work hours
- Competitive salary
- Casual and very friendly environment

Interested candidates should send their resume (CV) to
magdalena.wielgos@itpuzzle.com.pl
with ” **Cyber Security Analyst** " in the subject line.