

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 Information Security Engineer. We offer a rewarding and exciting professional experience and opportunity to develop your career in a highly competitive international environment.



Information Security Engineer

Scope of Responsibilities:

- Identify security gaps and vulnerabilities in our systems and identify fit for purpose controls and validate their effectiveness
- Manage, own and perform vulnerability management using market leading solutions
- Hands-on experience managing SIEM tools and the log correlation solutions with knowledge of data sources
- Performing deep-dive incident analysis and assist with any identified incidents
- Performing identification and collection of cyber threats utilising both proactive and reactive threat hunting techniques
- Executing vulnerability & web application assessments, providing analysis and recommendations to mitigate potential threats
- Monitor systems, identify/resolve issues, and prepare status reviews and reports.
- Ability to identify unknown and undetected malicious activity using a wide variety of tools and scripts
- Responsibility for proactively discovering new attacks, or attacks currently underway
- Strong understanding of the security aspects of Active Directory and Microsoft operating systems
- Ability to perform analysis of adversary tactics, exploits, and capabilities
- Understanding of key data exfiltration and attack techniques and how to identify them
- Manage support cases to ensure issues are recorded, tracked, resolved, and follow-ups are done in a timely manner
- A broad knowledge of the key infrastructure technologies such as PAM, MFA, SSO, IPS/IDS, PKI
- Knowledge of securing IaaS, PaaS and SaaS cloud environments
- Recommend defensive cybersecurity architectures, technologies, and tactics
- Participate in on call rota when required

Skills & Experience required:

- Experience across a number of broad security domains
- Able to demonstrate experience with the following : PAM, MFA, SSO, SIEM, IPS, DLP, PKI, and IAM
- Ability to demonstrate experience using all supported versions of Microsoft operating system and Microsoft Office applications and other corporate applications
- Strong understanding of Endpoint Protection, solutions, application whitelisting, proxy technologies, Vulnerability Management
- Knowledge of hardening standards and the role they play in securing devices (NCSC, DISA and CIS)
- Basic working knowledge of penetration testing tools such as Kali Linux, Wireshark, NMAP, Bloodhound
- Working knowledge of SIEM technologies and basic knowledge of SOAR and UEBA and other monitoring technologies

Offer:

- challenge, opportunities to exchange skills within multinational team
- trainings
- health care
- Multisport card
- social fund
- sports sections
- mindfulness and yoga classes

Interested candidates should send their resume (CV) to konrad.witek@itpuzzle.com.pl with „ Information Security Engineer” in the subject line.