(REMOTE OR OFFICE) SENIOR SECOPS ENGINEER

Striving for excellence is in our DNA. Since 1993, we have been helping the world's leading companies imagine, design, engineer, and deliver software and digital experiences that change the world. We are more than just specialists; we are experts.

EPAM is committed to providing our global team of 36,700+ EPAMers with inspiring careers from day one. EPAMers lead with passion and honesty and think creatively. Our people are the source of our success and we value collaboration, try to always understand our customers' business, and strive for the highest standards of excellence. In today's new market conditions, we continue to support operations for hundreds of clients around the world remotely, with the vast majority of our teams working from home. No matter where you are located, you will join a dedicated, diverse community that will help you discover your fullest potential.

No less important is the safety, well-being and experience of our applicants. Therefore, until further notice, all EPAM employment interviews will be conducted remotely. Our recruitment professionals and hiring managers are standing by to ensure a robust and engaging virtual candidate experience. We look forward to speaking with you!

JOB DESCRIPTION

We are looking for a **Senior SecOps Engineer** to join our team in Hungary.

RESPONSIBILITIES

- Monitor on-prem and cloud (AWS, GCP, Azure) infrastructure for attacks, intrusions and unusual, unauthorized or illegal activity
- Monitor identity and access management, including monitoring for abuse of permissions by authorized system users
- Create SIEM and SOAR detection and remediation scenarios, implement them as rules. Create, test and update playbooks
- Perform threat hunting and support threat intelligence processes

- Along with security monitoring perform other security operation activities
- Generate reports for both technical and non-technical staff and stakeholders
- Use advanced analytic tools to determine emerging threat patterns and vulnerabilities

REQUIREMENTS

- At least 5 years related experience on Agile projects
- Solid technical knowledge of Internet security, networking protocols, and related technologies, including IDS/IPS, firewalls, content filtering, Network Behavior Analysis tool, Anti-malware and packet inspection
- Solid understanding of Windows, Linux, DB and network device monitoring and logging technics
- Solid understanding of host and network security hardening, networking protocols, common intrusion techniques and common risk management concepts
- Solid knowledge of malware detection, intrusion detection and prevention systems
- Experience with 1 or more SIEM solutions (Splunk, QRadar, ArcSight, LogRhythm, ELK, Wazuh, Apache Metron, OSSEC etc.)
- Familiar with 1 or more SIRP/SOAR tool (TheHive, Cortex, Phantom, Demisto, Resilient etc.)
- Experience with network security
- Knowledge of internet security (PKI, LDAP, RBAC, SSL, HTTPS, TLS, DTLS etc.)
- Solid understanding of Identity and Access Management on multiple cloud providers
- Familiarity with existing Security Standards (e.g. PCI DSS, HIPAA, NIST, Common Criteria etc.) and what does it mean to implement compliance with them
- Knowledge of main Security-related activities in development such as Risk and Privacy Assessment, Threat Modeling, Security Code Review
- Knowledge of most common implementations of the Threats (e.g. XSS, SQL Injection, XSRF, buffer overruns, brute force, rainbow tables, DoS etc.) and how they match the general classification
- Good English communication skills (speaking, writing and reading)

WE OFFER

- Permanent job with remote work opportunity
- Widespread training and development opportunities, language courses, soft-skill trainings
- Vast opportunities for self-development, unlimited access to LinkedIn Learning, GAL trainings
- Multilingual work environment
- Competitive salary and benefit packages (private health care, sportcard, fringe benefits)
- International projects, working in hybrid teams with high-skilled peers
- Sport and social teams support, advanced CSR programs