Operational Security Engineer with French

Hiring organization
EasyDo Digital Technologies

Employment Type
Full-time

Job Location
Bucharest
Remote work possible

Date posted
September 11, 2026

Description

As an Operational Security Engineer, you will play a central role in securing the IT environment. You will be responsible for managing the vulnerability and security compliance process, from vulnerability scanning and assessment through remediation tracking, reporting, and continuous improvement. You will work closely with Security, IT Risk Management, IT, Business teams, and Group Security entities to ensure that vulnerabilities and security gaps are identified, prioritized, and remediated within the expected timelines.

Work Arrangement: Please note that this is a hybrid role (Bucharest), with an expectation to work from the office 50% of the time. This is a mandatory company policy and a non-negotiable requirement for the role. Candidates should therefore ensure they are comfortable with and available to meet this working arrangement.

Responsibilities

o Manage and continuously improve the vulnerability and non-compliance management process, including scan preparation, execution, analysis, and follow-up.

o Identify vulnerabilities, security gaps, and compliance deviations across On-Premises, DMZR, and Cloud environments.

o Coordinate and drive remediation activities, acting as the central point of contact between security and technical teams.

o Define remediation actions, owners, deadlines, and SLAs, and proactively escalate risks and delays.

o Manage security exception requests in collaboration with IT Risk Management, including security impact assessments.

o Ensure the operational maintenance of vulnerability scanning tools, including incident management, lifecycle management, and security patching.

o Ensure comprehensive scanning coverage across all relevant assets and technologies and implement improvements where gaps are identified.

o Conduct technical studies and Proofs of Concept (POCs) for new security solutions and capabilities.

o Produce and monitor operational security KPIs and reporting, aligned with both Local and Group requirements.

o Monitor changes in security standards, requirements, and technologies, and propose convergence plans where gaps are identified.

o Maintain relevant security procedures, operational documentation, and guides.

Technical Environment:

o Vulnerability & Compliance: Qualys, Tanium (Vulnerability/CC, Comply, Self-Assessment, API)

o Reporting & Data: ELK Stack, Power BI, Power Query

o Security Frameworks: NIST, CIS Benchmarks, OWASP, PTES, ISSAF, OSSTMM, ISO 27001

o Operating Systems & Infrastructure: Linux, Windows, Cloud

o Scripting: Python, PowerShell, Regex

o Networking: Strong understanding and analysis of standard network protocols

Qualifications

o Minimum 3 years of professional experience in a similar Cybersecurity, Vulnerability Management, Security Engineering, or IT Security role.

o Strong hands-on knowledge of vulnerability management, including scanning, analysis, prioritization, remediation tracking, and security compliance.

o Experience with Qualys and/or Tanium.

o Good understanding of security frameworks and standards, particularly NIST, CIS Benchmarks, OWASP, and ISO 27001.

o Knowledge of Windows, Linux, Cloud environments, networking, and security technologies.

o Scripting skills in Python and/or PowerShell, with Regex knowledge.

o Experience with security reporting and data analysis, ideally using ELK, Power BI, or Power Query.

o Strong analytical, organizational, and problem-solving skills.

o Proactive mindset, attention to detail, curiosity, and willingness to learn.

o Strong communication and collaboration skills, with the ability to work across Security, IT, Risk Management, Business, and Group teams.

o Ability to manage projects, drive remediation, improve processes, and work in an Agile environment.

o **Fluent French and good written and spoken English**

Job Benefits

o Competitive salary and the opportunity to have a meaningful job where you can make a difference

o The chance to continuously evolve as a professional

o Medical insurance & Meal tickets.

Contacts

Join Us at EASYDO

With a team of 250 dedicated professionals, we combine technological excellence with a people-first culture. We believe in empowering talent, nurturing careers, and building long-term trust with our clients and our teams.

Apply here, or contact our Talent Team by email to hiring@easydo.co