






Security Engineer

Role description

Portima has adopted a cloud-first strategy (on Microsoft Azure) to benefit from increased flexibility, innovation as well as cost savings. . At the same time, Portima will dismantle its MPLS network, which was protecting the whole insurance community, and subsequently, all services will be exposed 24x7 to internet threats.


















The Covid situation has also deeply impacted the way we secure out internal IT (which is the entry point to the management of the services we deliver towards our clients), since teleworking has been generalized, not allowing us to rely anymore on a bastion-alike kind of protection.

Information security concerns are numerous in such a context, e.g.:

-  How do we create cloud native solutions that are inherently safe? How do we protect them?
-  How do we securely move our on-prem workloads to the cloud? How do we handle the new 24x7 exposure?
-  How do we keep a secure on-prem infrastructure during the transition?
-  How do we compensate the “safe harbor” of the disappearing MPLS network?
-  How do we secure better our internal IT in a datacenter-less and work from anywhere approach?

Your Role

The security engineer will work in close collaboration with the CISO, the platform chapters, the applicative squads but also with all other entities in Portima to answer to these concerns:

-  Follow up cloud security metrics on a regular base, detect degradation and improvement areas, discuss with concerned parties
-  Follow up the vulnerability scanning, and pen tests performed by 3rd parties with the concerned Portima entities
-  Follow up security KPI, both on prem and in cloud: provide information, detect early the deviation, solve issues, coordination with remediating parties.
-  Monitor and investigate security alerts on multiple platforms
-  External Security Operation Center:
 -  Understand and adapt detection use cases to business requirements
 -  be the first point of contact for all reported incidents
 -  be part of the Incident Response Team
-  Perform Periodical security reviews and control of user management (joiners and leavers, ...)
-  Solve operational Security issues and provide scripts, advice, assistance information and warnings, as well as recommendations based on security controls
-  Provide technical expertise and support to other Portima entities regarding security best practices and overall cybersecurity threats.
-  Manage clients certificate using appropriate tools and issue activation codes to customers
- 
-  Suggest and perform hardening improvements on machines
-  Test the impact of updates on our systems
-  Suggest improvements in terms of processes (such as better controls, better automation, ...) and help during the implementation
-  Learn and assist our application security program, participating in code reviews, pen testing and threat modelling

- ✍ Conduct basic security assessments of applications to identify vulnerabilities and recommend remediation measures
- ✍ Manage the security of endpoints using Microsoft Intune and Defender
- ✍ Assist the team on the red team exercises
- ✍ Feed the Agile backlog of the different squads with stories and tasks, whether they are assigned to the security engineer or to a different person.

Must-have

- 🎯 At least a bachelor's degree in IT is required, with affinity for security-related topics
- 🎯 Understanding of cloud computing technologies, and emerging computing trends
- 🎯 Technical experience or affinity in one or more of the following areas: patching and hardening, network protocols, endpoint protection, user management in (Azure) AD, forensics
- 🎯 Strong attention to detail
- 🎯 Solid understanding of Windows operating systems with a proved experience is preferred
- 🎯 Understanding of Agile principles
- 🎯 You speak at least one of the national languages, and you are fluent in English
- 🎯 You are a team player who is humble, pro-active and people-smart
- 🎯 You are systematic, organised, structured, open to learn, and curious for new security trends
- 🎯 Strong interest in penetration testing and threat detection and response

Familiarity with pen test tools such as Burp Suite, ZAP, and Metasploit is considered an asset for the role.

About Portima

Portima is the n°1 broker tech in Belgium. We provide digital solutions and IT services to the community of insurance brokers, insurance companies and to the customers of the brokers.

We guarantee that the broker channel remains the leading distribution channel for insurance in Belgium with our mission statement: By offering digital, secure and innovative solutions, as partner of the broker and the insurance companies, Portima increases your productivity and sparks customer delight.

Lines of products:

- Portima Connect which is a value-added network for brokers and insurers. We deliver products and services such as private network, security, VPN, single sign-on, EDI message transfer, PC management platform, ...
Target: ~ 4.700 brokers, 13.000 users
- Brio which is a broker management system (a kind of ERP containing customer profiles, contracts, claims, activity log, accounting, document management system).
Target: ~ 3.200 brokers, 11.000 users.
- MyBroker, a mobile app and website for the insured persons

Working @Portima means:

- ✍ Being part of a fintech company
- ✍ Participate in all Agile scrum ceremonies (Product Increments/Sprint planning, PI/Sprint demo, Daily Stand up,...)
- ✍ Collaborate on daily basis with the Product Owner, Chapter leads, etc.
- ✍ Evolve your career in a company that values empowerment and continuous learning
- ✍ Have fun within a strong team and with all the Portimates through many activities organized by our Happiness Team
- ✍ Enjoy a comfortable package with individual and collective annual bonuses
- ✍ Work in a flexible way, with teleworking arrangement (2 days in the Portima office, 3 days Teleworking)

Send your CV via email to lucie.deschrijver@portima.com