Senior DevOps Engineer in Security Domain

The project and the team

We are looking for a person who is open-minded, passionate about new technologies, thinks logically and takes a creative approach to problem solving. If you are eager to learn, like to design, deploy and troubleshoot network solutions, and want to automate repeatable work, we are offering a great opportunity. You will have a chance to join a team of specialists who know that every problem can be solved. We have already completed numerous projects in the area of networking, cloud or infrastructure automation and monitoring.

We are a team of DevOps and Network Engineers with network automation experience who explore the world of SDN, NFV and work with automated deployments in the public cloud.

What else you should know:

● Our engineers support professional services delivery, customer projects deliveries and at the same time the development automation (incl. open-source).
● We collaborate closely with analysts, architects and developer teams
● Our tech stack for the project include Azure, AWS, GCP and OCI network solutions, especially from the cybersecurity domain, automation tools like Terraform or Ansible, programming languages like Python/Golang and different platforms, i.e. Kubernetes.

We work on multiple interesting projects at a time, so we may invite you to an interview for another project if we see that your competencies and profile are well suited for it.

Your role

As a part of the project team, you will be responsible for:
● Deployment in public and private cloud of various architectures that integrate VM-Series NGFW using automation
● Working in agile methodology and collaborating with the rest of the team (managers, Cloud / Devops Engineers, Solution Architects, Professional Services Engineers)

● Creating Terraform code for cloud based deployments
● Troubleshooting existing solutions and proposing improvements to existing systems
● Working with customers located mainly in US
● Working in US working hours (60-80% of your working time will be expected in the range of 14 - 22 pm CET)
● Mentoring teammates and sharing knowledge

Do we have a match?

As a Senior Cloud Network Engineer in Security Domain you must meet the following criteria:

● Proof of 7+ years of professional, hands-on operational experience in the field of Network, DevOps or SysOps.
● Excellent knowledge of networking and cyber security
● Excellent knowledge of at least two of the public cloud, including advanced cloud networking
● Knowledge of Linux & Linux networking
● Excellent knowledge of at least one of the IaC automation tools (e.g. Terraform, Cloud Formation, BICEP)
● Good knowledge of Ansible
● Experience in writing python scripts or software
● Understanding of SDN and VNF concepts
● Good knowledge of English (C1 level)
● Willingness to learn – you will face challenges that require creativity, individual solutions and teamwork

Important

Each of these will be tested during the interview and the candidate needs to be able to demonstrate by certifications (advanced level), knowledge and experience the requirements above.

Beyond the criteria above, we would appreciate the nice-to-haves:
● Knowledge of Palo Alto Networks solutions
● Knowledge of script language (Python, Bash, Golang)
● Knowledge of of CI/CD tools (Jenkins, GitLab CI, Circle CI, Github actions)

Senior DevOps Engineer in Security Domain - Interview Process

The process involves three interviews and an assignment that needs to be completed by the candidate. The steps are as follows:

1. Implementation of the assignment:

   Create the terraform deployment to host a stateless application containerised here: https://hub.docker.com/r/nginxdemos/hello/

   Create the architecture diagram for the deployment using: https://github.com/mingrammer/diagrams

   If applicable depends on your chosen approach:
   1. Ensure application is deployed behind a load balancer.
   2, On the point of the load balancer the application needs to be HA.
   3, Ensure that the network hosting of the web application is secured.
   4, If application is hosted in a VM build as well the infrastructure for safely access it via ssh,
   5. Make use of service accounts where applicable.
   6. Depending on how your application is hosted, propose options for securing access to the web application itself.
   7. Create all the public/private networks needed to secure unwanted access from the Internet to the infrastructure hosting the web application.

   Use a repository on www.github.com to manage all the code parts of the assignment and provide instructions on how to consume the repository.

2. First interview : Technical interview with team members
   Senior members of the team
3. Second interview : Management interview with the leadership of the team

Alexandru Smeureanu
Konrad Dąbrowski

4. Third interview : Global Solution Architects interview
   Torsten Stern
   Migara Ekanayake

Each interview is eliminatory after the third interview a decision will be made based on the evaluations.