Senior Cyber Security Engineer

At LINK, we connect businesses to customers through our communications products and services that drive engagement and satisfaction during each stage of the customer journey.
You're probably already familiar with us: we're behind the messages you receive via SMS, WhatsApp, email, or even to check-in for your upcoming flight, receive delivery notifications, cash in a mobile coupon to your favorite store, and so much more.
You will be joining a security team as the engineer and an equal technical partner. Our environment is a complex hybrid infrastructure combining bare-metal systems and multiple cloud platforms. We are looking for a hands-on engineer who sees technology as a tool to solve real security and operational problems.
This role requires a high level of independence and ownership. You should be comfortable planning and prioritizing your own work, investigating problems without detailed instructions, and taking technical topics from analysis through implementation and documentation.
You will help us build and mature our SOC capabilities, improve threat detection, investigate security incidents, develop automation, and maintain the security monitoring platform.

Key Responsibilities:

- **Maintaining and tuning the Wazuh HA cluster:** Making sure the system doesn't choke. This includes OpenSearch performance optimization, data retention management, tuning queues on managers and workers, and optimizing I/O load and disk space
- **Working with raw logs:** Creating custom decoders and local rules for specific services and edge cases that standard rules can't handle. Fighting false-positives at the detection logic level
- **SOAR Engineering (Automation):** Building integrations and automation around APIs to remove manual workload from the future SOC team
- **K8s Security:** Integrating container environments with the central logging system
- **Incident Response Processes:** Creating pragmatic, technical security procedures and incident response playbooks
- **System hardening:** Working closely with IT and DevOps teams to secure operating systems and services

Your Tech Stack:

- **SIEM/XDR:** Wazuh HA
- **Infrastructure:** Complex hybrid environment (Bare-metal, AWS, Azure, GCP)
- **OS:** Linux (various distributions)
- **Data / Logs:** OpenSearch / Elasticsearch, auditd, syslog, custom decoders, local_rules
- **Containerization:** Kubernetes
- **Automation & IaaC:** Bash, API, Ansible, Python

Must-have Requirements:

- **Advanced knowledge of Polish is an absolute must-have**;
- **Wazuh (SIEM/XDR):** Commercial experience with the system in a large enterprise environment. You need to understand how agents, decoders, and rules work under the hood
- **Deep Linux Adminstration:** Fluent administration and troubleshooting. We are looking for someone who can diagnose issues at the OS level
- **OpenSearch / Elasticsearch:** Proficiency in cluster management (ISM configuration, index lifecycle, troubleshooting queries and database performance)
- **Scripting & Automation:** Fluent scripting and working with REST APIs – you must know

how to "glue" different systems together
•**Understanding Log Sources:** Good knowledge of systems like auditd and syslog
•**English:** B2+ level (to comfortably work with technical documentation and communicate with international IT teams)

Nice-to-have:

•Experience in designing and deploying Wazuh HA clusters from scratch
•Practical knowledge of Ansible for configuration management
•Practical knowledge of Python
•Operational experience in a Security Operations Center
•Deeper experience with Kubernetes security
•Practical experiments using LLMs to support log analysis and automation in a SOC

We offer:

•Hybrid work model after trial period
•Co-financed Medicover care
•Co-financed private life-insurance
•Co-financed MultiSport card
•Extra day off on your birthday
•Team building events
•Extra fee from employer for retirement program (PPK)
•Employee Referral Program
•Summer bonus
•Fruits in the office
•Lunch days: Mondays & Wednesdays
•Free parking (cars & bikes)