SOC Analyst Level 1

Location – Banja Luka
Job type – Full time

Company description

GaliaIT d.o.o provides security monitoring services to some of the most recognized companies and brands in the world. We take a proactive approach to solving business challenges and our customers are the heart of everything we do. It's the reason we love rolling up our sleeves and getting down to work – and it's why we're so successful. It takes an entire team to stand behind something big. Interested?

Key duties & responsibilities

- Monitoring organization using Cortex XDR (24/7/365) - working on Cortex platform to solve incoming incidents, ingested from multiple sources like PAN NGFW, endpoints etc.
- Creating monthly reports and statistics
- Generating Status Page reports for the client, to track progress on all failures of the services Threat hunting in Cortex XDR - actively searching for the vulnerabilities using XQL query language, discovering new vulnerabilities.
- Working with Microsoft Defender (24/7/365) - dealing with incidents on Microsoft Defender 365 platform, performing investigations, searching for vulnerabilities in network etc.

The ideal candidate should possess the following attributes:

- An intuitive and methodical approach to problem-solving
- A team-oriented approach (both immediate and wider team) to working and the ability to work equally as well independently
- A confident and proactive approach in furthering technical knowledge and imparting this knowledge to other members of the team
- A positive attitude, setting standards of excellence and achieving them
- The ability to manage time effectively and prioritize cases/projects to ensure goals are met
- Enthusiasm and willingness to learn new technologies
- Able to work in shifts and able to work on rota basis for on-call remote work (weekdays nights and weekend)

Rewards and benefits

- We have fun while we're at work!
- Competitive and regular earnings
- Opportunities to grow and develop your skills on a professional level
- Exciting client working with the latest technologies
- Stimulating environment with excellent work conditions