GARMIN

Cyber Security Administrator

We are looking forward to meeting any Cyber administrator eager to manage Garmin's Cyber-Data Lake and other Threat Intelligence tools at Garmin Cluj office.

This is not your typical application development job.

At Garmin, we work with hardware that communicates to mobile applications and other devices. Garmin is a great place to work if you love developing products that make a difference and are passionate about technology.

Our benefits are designed to lead an evolving marketplace, support innovation and encourage a healthy balance between work and life. They allow our associates to make their own decisions about their wellbeing and future and consistently rank Garmin as a top tier benefits provider when compared to other high-tech employers.

Your role would be to analyze logs from Garmin's Crown Jewel systems looking for signs of criminal intent.
Other essential functions include:

- Add services and systems to the Cyber Data Lake
- Validate and continually review that all Garmin Crown Jewels are incorporated into Cyber Data Lake
- Become expert level resource for client, server, and data requirements of Cyber Data Lake
  - LogStash, Filebeat, HDP, Hortonworks
- Work with application and infrastructure teams worldwide to ensure logs are stored in a consistent manner
- Solicit feedback from Security Operations Center (SOC) and Cyber Data Scientists to identify opportunities to continually improve Cyber Data Lake abilities
- Collaborate with Cyber Data Scientist to implement and continuously improve data visualizations for stakeholders such as management and SOC
- Execute release management using an approach that minimizes disruptions/negative impact
- Continually tune Cyber Data Lake to ensure optimal health
  - Update Big Data software platform such as HDP, LogStash, Filebeat, and Hortonworks
  - Monitor and remediate performance limitations
  - Plan and execute Cyber Data Lake capacity management\scalability efforts
  - Plan and execute Cyber Data Lake Data Retention efforts
- Identify and improve behavior context queries for further efficiency, performance, and awareness of nefarious actions
- Collaborate with Data Lake stakeholders such as Web and Infrastructure teams to ensure optimal health of Cyber Data Lake resources

- Collaborate with Cyber Data Scientist to tune Cyber Data Lake to maintain and take greater advantage of threat intelligence feeds
- Implement enrichment sources
- Collaborate with management, data scientist (leader), SOC, and other stakeholders to develop and execute Cyber Data Lake roadmap
- Application administration for additional Threat Intelligence tools (Nexpose, Nessus, and others as necessary)
- Assist penetration team with operational aspects of hacking