Role Profile: Cyber Security Engineer

Vacancy Description

Amiosec is an exciting and growing UK technology company with innovation, agility and state of the art technology at its core. We work in partnerships with UK government customers and commercial providers to deliver research, technology, products and Services in the communications security sector.

Amiosec is experiencing rapid growth which has in turn opened up an exciting opportunity for a Cyber Security Engineer to build, maintain and assist operating a critical cyber threat detection and response capability for a dynamic mobile service environment.

Your role will be largely focused on constantly evolving our cyber capability, analytics and reporting whilst working alongside an experienced Cyber Security Analyst. The role would suit someone who has previously worked with Elasticsearch, Logstash and Kibana and who has experience of developing complex data ingestion, analysis and visualisation pipelines from multiple sources in varying formats.

Due to the nature of our work, all candidates will be required to obtain and maintain an appropriate UK security clearance.

Duties will cover but not be limited to:

- **Core**
  - Developing and maintaining knowledge of the architecture required to collect data from our deployed systems and services
  - Working with the engineering team to design ingestion and pipeline processes using best practises and open source tools such as Elasticsearch, Kibana, Beats etc
  - Developing and applying quantitative and qualitative analytic methods to identify, collect, process and analyse data sets for specified purposes
  - Develop and provide expertise on the dashboard solution based on ELK (Elasticsearch, Logstash, Kibana) Stack and risk scoring methodology
  - Provide configuration control and change management of our ELK stack
  - Maintain the roadmap for improvement of our analytics pipeline
  - Analyse the impact of changes and provide recommendations for updates
  - Develop reports and presentations that enable decision making
- **Support**
  - Provide training on the dashboard
  - Provide support to Cyber Security monitoring which may include assistance during and post incidents such as presentation of data for decision makers and as part of any investigation process

Requirements

Elastic certified training and/or qualifications
Strong analytical skills, attention to detail, customer focused, self-motivated, team player, good time management
Must be willing to obtain and maintain a valid UK Security Clearance as required

Desirable

Professional certification such as Elastic Certified Engineer
2+ years hands on experience with ELK stack and experience of configuring and maintaining Elastic clusters
A good understanding of networking fundamentals and systems admin knowledge ie Linux
Knowledge of security standards such as ISO 27001 / NIST / SANS

Opportunities

Amiosec is growing rapidly and we are looking for someone who is not only happy to work with existing processes but also to develop these processes and take on more related responsibilities within the organisation
Amiosec will provide relevant training where appropriate and support individual's ongoing professional development