Role Profile: Cyber Security Analyst

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 an experienced Cyber Security Analyst to work alongside the Services' Team establishing and providing a critical cyber threat detection and response capability. This role is focused on operational security tasks however, we are looking for a candidate with a broad technical skill-set who can assist in the wider information security and incident management activities.

Your role is primarily to identify, triage and respond to cyberattacks that could disrupt operations or cause harm to the business. Duties will cover but not be limited to prevention and detection, investigation and response to cyber threats.

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

Typical Duties:

- **Prevent and detect**
  - Cyber risk awareness and continual assessment of the threat landscape
  - Undertake vulnerability analysis and limit the impact of known cyber risks with pre-incident planning and preparation activities
  - Support technical changes impacting security, manage external testing like CHECK and assist with any remediation
  - Monitor, analyse and defend against malicious or unusual activity that could be indicative of a security incident or compromise
  - Capture appropriate information for any investigation and develop the supporting forensic processes
- **Investigate**
  - Conduct security incident investigations
  - Analyse suspicious activity to determine the nature and extent of the threat
  - Identify and perform security incident triage by understanding how attacks unfold, and how to effectively respond
  - Understand our network and services, the latest threat intelligence including specifics on attacker TTP (Tactics, Techniques and Procedures) to perform effective triage
- **Response**
  - Provide a first point of contact for security related incidents impacting Services

- As soon as an incident is confirmed, perform actions such as isolating endpoints, terminating harmful processes, preventing them from executing, deleting files etc
- In the aftermath of an incident, work with relevant teams to ensure secure restoration of systems and services
- Coordinate a response to remediate the issue

Requirements

Attention to detail, customer focused, self-motivated, team player, good time management
Willingness to be flexible and assist in other areas of the business where deemed necessary
Must be willing to obtain and maintain a valid UK Security Clearance as required

Desirable

Professional certification such as CISSP, SANS or other information security credentials
Depth of knowledge in security standards such as ISO 27001 / NIST / SANS
Strong knowledge of networking fundamentals and good systems admin knowledge of linux
Demonstrable skills with security technologies including; firewalls, Proxies, SIEM solutions, vulnerability scanning, patch management, endpoint security controls, DLP solutions, mobile device security etc

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