Leading provider of information security & compliance solutions providing Governance Risks and Compliance Services, Enterprise Security Solutions, Managed Security Services, Training & Awareness Programs, is seeking highly motivated professionals to join our team to cover the following openings:

Cyber Crime Expert (BE-CYE-1001)

A position where you can prevent and fight against cyber criminality The role will see you typically engage alongside Security Solutions Architects, Network Security Architects, and Development team staff. You will be called upon to where a deeper knowledge of your subject is required – Application Security, and secure system lifecycle. You will add the fine detail to all security designs that have a requirement for an in-depth AppSec review and analysis / design. You will be required to provide detailed designs regarding Application Security. An in-depth knowledge of the current threat landscape is essential but more importantly the application security controls and counter-measures that can be used to protect organization's developed and deployed systems and applications.

Main Responsibilities

- *Follow-up activities and control quality of work done by external company:*
  - Qualify escalated events detected by SEM, TSCM, IPS tools (like ArcSight, Tripwire, SourceFire or provided by other sources)
  - Follow-up of security related alerts and recommending corrective actions
  - Validate rules/waivers which filter out all security related events and provide qualification rules
- *Security incidents*
  - Provide L3 support for security incidents: analyze and qualify escalated events, initiate major security incident process
  - Coordinating and conducting IT forensics investigations for the business: Request to identify, collect, analyze and report on various malware related or other threats to security service providers in order to provide actionable intelligence to the organization.
  - Define and implement security incident mitigation solutions
  - Coordinate with other security teams the resolutions
  - Draw lessons learned from security incidents
  - Be part of on call support team (24/7)
- *Cybercrime trends*
  - Research new Cybercrime trends and continuously stay up to date on the latest developments in cybercrime
  - Gather and analyze cybercrime threats (specifically for DDOS & APT)
  - Coordinating efforts to produce actionable plans to mitigate identified risks
  - Make recommendations on solutions to prevent security incidents
- *Cyber Crime Exercises*
  - Define attack scenarios and conduct cybercrime exercises (APT & DDOS)
  - Get insights from previous APT and DDOS attacks to recommend new cybercrime defense initiatives
- *Providing guidance and strategic direction to staff and management, both for projects and incident handling, in accordance with the organization's security policies and local laws & regulations*
- *Develop and document information security procedures to enforce information security standards*

Qualifications and Experience

- Master degree or equivalent by experience and advanced training/certification
- Information technology security (architecture, organization, processes…)
- Network infrastructure and application security
- Firewalls, anti-virus, intrusion detection systems and penetration testing
- Modern malware (trojans, remote access tools, botnets, rootkits…)
- DDOS and APT attacks
- Forensic investigation
- Experience in ethical hacking is a plus
- Analytical and synthetic turn of mind
- Excellent communicator, who can be assertive towards multiple stakeholders
- Team worker but also able to work independently
- Able to work in stressful situations
- Organized and who follows a "problem-solving" and "results-oriented" approach
- Excellent project and time management skills
- Excellent written and spoken knowledge of English, knowledge of Dutch and/or French

Applicants receiving an offer of engagement will be required to complete an application form and sign a disclosure and authorization for a background investigation which may include a criminal check, education and employment verifications.

Candidate must be flexible to relocate to south-west of Europe.

Interested applicants should send their CV by quoting the reference code (BE-CYE-1001) to:

BESECURE
HR Department
133B Franklin Roosevelt
Fax: +357 222 62401
Email : hr@besecuregroup.com

All applicants will be acknowledged and treated in the strictest confidence.