

## **NEUROSOFT S.A.**

### **Security Analyst, L2**

Neurosoft S.A., is a leading software, networking and information security provider in financial, telecommunication, transportation, gaming and government sectors, providing solutions and services aiming to increase operating efficiency and security. Listed in the Italian Stock Exchange since 2009, currently employees 200+ highly skilled professionals with in depth expertise in their field.

We have an open vacancy for an experienced Security Analyst position (Level 2) who will join our Information Security Services team to further support the monitoring services provided to our customers and help mitigate security issues on behalf of them. He/she needs to work with a team of skilled professionals to address complex problems, when needed. The role assumes standby monitoring and investigation duties on a 24x7x365 Security Operations Center (SOC).

#### **Main Responsibilities**

- Acts as a point of escalation for Level 1 SOC security analysts in support of information security investigations to provide guidance and oversight on events analysis, incidents resolution and containment techniques
- Coordinates with Senior Analysts and/or Duty Manager for critical incidents
- Communicates with clients and collects useful intelligence and evidence
- Directs remediation / recovery efforts when needed
- Leverages threat intelligence / open source intelligence (OSINT) in order to assess potential attacks / incidents under investigation
- Logs and documents handled incidents and actions taken and reviews closed tickets
- Mentors Level 1 SOC Security analysts regarding risk management, information security controls, incident analysis, incident response, SIEM monitoring, and other operational tasks in support of technologies managed by the Security Operations Centre
- Prepares Monthly Executive Summary Reports for SOC clients
- Defines, creates and maintains SIEM correlation rules
- Conducts research to keep abreast of latest security issues

## **Professional Experience & Qualifications**

- Bachelor's degree in Information Security, ICT, Networking or any other relevant field; a Master's degree in Information Security will be preferred
- At least 2 years prior experience as a Security Analyst
- Excellent knowledge of Linux / Unix / Windows systems
- Solid background in:
  - Networking and associated protocols (TCP/IP, UDP, OSI model etc.)
  - Information Security (Security standards and practices, Security technologies, Security Monitoring, Penetration Testing, Incident Response, Threat landscape etc.)
- Hands-on experience with SIEM - IBM QRadar is mandatory
- Relevant certifications consist a strong asset (e.g. C2150-612 - QRadar Associate Analyst, IBM Certified Associate Analyst, etc.); Certifications such as GCIA, GCIH, GCFA, or GREM would be beneficial
- Understanding or knowledge of software programming with scripting languages is beneficial
- Ability to analyze data, such as logs or packets captures, from various sources and draw conclusions regarding security incidents
- Exposure to security technologies including firewalls, IPS/IDS, and vulnerability management
- Familiarity with Open Source Intelligence (OSINT) / threat intelligence tools is beneficial
- Strong analytical and problem-solving skills, with attention to detail
- Very good organizational and time management skills
- Good communication skills and a customer-oriented approach
- Ability to work efficiently both within a team and independently
- Ability to work under pressure
- Fluency both in Greek and English languages
- The role mandates to work ethically, with high degree of integrity, confidentiality and appropriate use of information

## **We Offer**

A competitive compensation package, a stable and enjoyable working environment, excellent opportunities for professional development, working on leading-edge technology and industry trends.

***For more open vacancies check @ [www.neurosoft.gr](http://www.neurosoft.gr)***