NEUROSOFT S.A.

Security Operations Center Manager

About Neurosoft

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 within depth expertise in their field.

We have an open vacancy for a Security Operations Center (SOC) Manager to lead the 24x7x365 Security Operations Center (SOC) and the relevant monitoring services provided to our customers. He/ She will work with a team of skilled information security professionals to offer guidance, direction and address complex issues, when needed.

Main Responsibilities

- Leads and manages the Security Operations Center (SOC)
- Is primarily responsible for security events' monitoring, management and response; ensures incident identification, assessment, quantification, reporting, communication, mitigation and monitoring
- Acts as an escalation point and assists in resolving High/Critical incident tickets and attacks
- Drives containment strategy during data loss or breach events
- Acts as the central point of contact for all communications with SOC Clients, when it comes to dealing with information security incidents
- Ensures compliance to SLA, process adherence and process improvisation to achieve operational objectives
- Leads/reviews/maintains the onboarding process for each SOC Client, based on the agreed onboarding plan
- Is responsible for the optimal allocation of human resources and shifts' scheduling, the training and development plans of the SOC Team and the team's management overall
- Develops processes to further improve the current Security Operations Center working Framework and provides recommendation for SOC Infrastructure's optimization
- Performs threat management, threat modeling, identifies threat vectors and develops use cases/ rules/playbooks for security monitoring
- Creates and updates reports, dashboards and metrics for SOC operations
- Conducts research to keep abreast of latest security issues

Professional Experience & Qualifications

- BSc in Information Security, ICT, Networking or any other relevant field; an MSc in Information Security will be preferred
- At least 3-5 years prior experience as a Security Analyst L2/L3
- Proficient in Incident Management and Response; working experience with a SIEM tool, preferably IBM QRadar
- Excellent knowledge of various operating systems including but not limited to 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.)
- Knowledge of applications, databases, middleware in order to effectively address security threats
- 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
- Excellent organizational and time management skills with the ability to prioritize effectively clients' requirements
- Strong analytical and problem-solving skills, with attention to detail
- Excellent interpersonal and communication skills, internal and client facing
- Customer-oriented approach and ability to handle high pressure situations with key stakeholders effectively
- Ability to work efficiently both within a team as well as independently
- Proven experience in reviewing/preparing reports/dashboards/documentation
- Excellent written and verbal skills both in Greek and English
- Works ethically, with high degree of integrity, confidentiality and appropriate use of information

Preferred Skills and Qualifications

- People management experience
- Relevant certifications consist a strong asset such as CISSP, GCIA, GIAC, Advanced Digital forensics and Incident Response - FOR 508 (Optional GCFA)
- Experience in information security risk assessment
- Familiarity with adversary tactics frameworks, such as Mitre Attack Framework
- Knowledge of software programming with scripting languages

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