Cyber Security Operations Center – Level-1 Security Analyst

We are looking for SOC Level-1 Security Analysts to provide real time security monitoring services for our corporate clients. The SOC Operator is the first escalation point for all security information and event management (SIEM) service security incidents.

The responsibilities of the Security Analyst will include the following:

- Provide day-to-day expertise on proper handling of security events.
- Provide technical and procedural direction during investigation of an escalated security event.
- Respond to and confirm security incidents within the targeted framework.
- Provide weekly trending and information analysis looking for incident precursors and indicators of potential attacks and/or threats.
- Work with the Security Engineer to build use cases and integrate processes.
- Adhere to documented escalation, process and communication plans.
- Provide technical investigative reports to the management team.
- Track threats and vulnerabilities to SIEM monitored environments.
- Maintain documentation to support security operations.
- Track and document changes to monitored environments.
- Maintain documentation and diagrams supporting all information flows within monitored environments.
- Maintain a list of assets located within monitored environments.
- Identify and track the criticality, confidentiality and owner of each network and system.
- Follow standard operating practices for developing content within the SIEM solution.
- Configure the SIEM solution with the appropriate asset data and information classification.

ENCODE S.A., 141, Georgiou Papandreou, 144 52 Metamorfosi, Athens-Greece, tel. (+30)210-6563880
fax (+30)210-6543576, e-mail: info@encodegroup.com, http://www.encodegroup.com

Required Education and Experience

- Degree in Computer Science, Data / Information Technology, Engineering or similar.
- Excellent verbal and written communication skills, both in Greek and English language.
- The ability to pick new technology or concepts up very quickly required.
- Experience required with Windows operating system, Linux, or UNIX experience preferred.
- Strong communication skills.
- Customer-oriented focus required, with a strong interest in a satisfied client.
- This position requires shift work in a 24/7/365 environment. The capacity to work evening, overnight, and weekend hours is required.
- Analytical and troubleshooting skills on short timeframes.
- Troubleshooting experience in complex environments.
- Ability to fully utilize MS Office products required.

Career Path & Opportunities

ENCODE is committed to staying ahead; as we consider our consultants and engineers to be the core of our service offerings, we ensure that they remain at the cutting technological edge and broaden their knowledge and skills by getting continuous training and through on-going involvement in major projects for leading organizations, as well as in research activities. Regarding Level-1 Security Analysts, top performers will have the opportunity in 1-2 years time to join other cyber security teams, as:

- Cyber SOC Security Engineer, Level-2 Analysts
- Security Assurance Consultants – Penetration Testers
- Security Assurance Consultants – Incident Response

ENCODE S.A., 141, Georgiou Papandreou, 144 52 Metamorfosi, Athens-Greece, tel. (+30)210-6563880
fax (+30)210-6543576, e-mail: info@encodegroup.com, http://www.encodegroup.com