Our innovative and growing company is searching for experienced candidates for the position of advisor information security. Please review the list of responsibilities and qualifications. While this is our ideal list, we will consider candidates that do not necessarily have all of the qualifications, but have sufficient experience and talent.

Responsibilities for advisor information security

- You will apply technical know-how to deliver asset classification models, risk analysis reports, security solution scenarios, implementation plans, security services and procedures
- You will maintain and administer exception management process to track, monitor, report and ensure proper closure on security policy deviations
- You will facilitate and promote activities to create information security awareness within the organization, including awareness of information security technologies and related regulatory issues that have a potential impact to the environment
- You will review the security of newly developed or acquired information systems and business applications
- Expected to take on future team lead/leadership accountabilities
- Build and drives a successful and growing SOC consultancy business in South Europe in close collaboration with sales, presales, and product partners
- Own key SOC pre-sales, consultancy and service delivery deliverables as directed by the Regional Practice Leader
- Act as a SIEM advisor from either a Management or Technical perspective, capable of understanding and resolving complex SIEM issues
- Articulate the business benefits of SOC to business/technical clients as appropriate, helping them to identify potential future opportunities and

- Demonstrate SIEM industry awareness including market leaders and key business drivers

Qualifications for advisor information security

- Plans security systems by evaluating network and security technologies
- Knowledge of all areas of IT Security, including Identity and Access Management
- Proven track record of experience in developing and driving the commercial characteristics of security solutions designing security architecture based on unit cost targets
- Must have demonstrated efforts to keep current with changing and emerging IT and security technologies
- Intrusion Detection configuration, implementation, maintenance, and analysis
- Firewall Management, rule creation and security evaluation