CYBER SECURITY PER LO SNOC

Our company is hiring a Cyber Security Analyst to be placed within its staff at its headquarters in Bergamo.
The ideal candidate should have a minimal experience in this role.

The candidate will be placed in a highly motivated and rapidly growing context; he or she  ill have the opportunity to develop and consolidate his skills within a team of established professionals in the field and to bring his contribution in the development of new technologies for the identification of cyber threats.

TECHNICAL REQUIREMENTS

? Solid knowledge and experience with Cyber Threats Management (SIEM / SOC; Threat Intelligence and CERT)
? Degree-level education (Computer Science, Engineering, telecommunication engineering, informatics, mathematics, physics. or equivalent);
? Certifications on Information Security (e.g. CISSP, CISM, ISO27001, CISA, ISO22301, GSEC, CEH, CSX etc.) would be a plus;
? Experience in technical security domains (network security, application security, data security, cloud security, etc.)
? Experience on information security governance, IT risk management, regulatory compliance (e.g. Privacy Law) and audit procedures;
? Knowledge of main Information Security standards and framework (ISO27001, ISO22301, ISF, NIST, COBIT etc...);
? Proficiency with Information Sharing tools STIX 1.1/2.0, TAXII, MISP and MINEMELD
? Proficiency with configuration and Management of Splunk Infrastructure (SPLUNK Enterprise Security, SPLUNK Indexer, SPLUNK HEAVY Forwarder, SPLUNK Universal Forwarder, SPLUNK Deployment Server)
? Knowledge of main tools for Security Assessments (Nessus Professional, Burp, Kali Linux)
? Knowledge of tools for Security Monitoring and Analysis (Lastline, CUCKOO, BitSight)

SOFT SKILLS

? Communication skills and ability to manage a wide array of different stakeholders;
? Strong operational focus, ability to drive topics and deliver results even under pressure and time constraints;
? Cross-country team management; ability to work in large international security projects;
? Fluent English, another European language is a plus;
? Advanced problem solving, analytical and communication skills;
? Strong organizational and project management skills;
? Demonstrated ability to work effectively as part of a team;
? Participation in challenges and workshops on Cyber Security (e.g. CTFs) is a plus

ACTIVITIES

? Monitors continuously cyber threats that could potentially affect the Groups evaluating their impacts (vulnerabilities, cyber-attacks etc.);
? Ensures a timely sharing of security alerts, intelligence reports or security bulletins within the Group including necessary countermeasures;
? Supports the evolution of the cyber threat intelligence services by means of the enrichment of intelligence sources (internal and external) and the continuous improvement of the intelligence technical solutions;
? Manage the requests from Group entities related to cyber threat intelligence;
? Support the incident response process in coordination with other relevant entities (e.g. Pirelli Sistemi Informativi).
? Support the execution of red teaming activities (e.g. external vulnerability assessment);
? Continuous Assessment of the company security exposure through Honeynet and Vulnerability Assessments on Company infrastructure and systems
? Analyze and study new cyber threats, new risks and innovative solutions in order to identify the correct and timely defenses against the attack pattern evolution.
? Support in development of the plaform for information sharing together with AGID CERT-PA (CERT Pubblica Amministrazione) with other national CERTs
? Management of SIEM platform to create dashboards and identify meaningful correlation to identify security events

CYBER SECURITY PER LO SNOC

? Continues monitoring on external breaches whenever they involve Company Data
? Perform Forensics Activities in case of incidents
? Management of email protection tools and Fraud Email handling