IT Security Analyst

Reporting to: IT Security Manager

Main activities and responsibilities:

- Internal IT Security point of contact to deal with Managed Security Service Providers (MSSPs), including but not limited to the Security Operations Center (SOC).

- Review alerts, data and reports from the SOC and engage with the necessary stakeholders to solve security issues quickly to mitigate business risk.

- Perform detailed debrief, analysis, follow-up and reporting of security incidents.

- Organize, participate and report incident response exercises/simulations with internal and external stakeholders (MSSPs) under the leadership of IT Security Management.

- Conduct periodic information security audits including but not limited to high privileged accounts, information systems users rights and access, IT security related policy compliance, security configuration hardening compliance and other procedures, standards and processes that are required to maintain the organization's cyber posture.

- Run the IT Security Metrics (KPIs, KRIs, KGIs) generation, control and reporting.

- Work in partnership with IT internal stakeholders to build IT security dashboards in MS Power BI.

- Demonstrable experience in cyber security incident handling processes and frameworks like SANS and NIST, SIEM and Logging Technologies like Azure Sentinel, Log Analytics and Splunk and other leaders in the market.

- Knowledge of IT Infrastructure: Microsoft Server and Workstation Operational Systems, TCP/IP networks, OnPrem and Azure Active Directory. Knowledge in Azure Cloud security related services is desirable.

- Strong communication skills, verbal and written.

- Process oriented and critical thinker being able to connect the dots from diverse security events.

- Ability to communicate complex and technical issues to diverse audiences, in an easy to understand and actionable manner.

- Self-motivated, possessing a high sense of urgency and prioritization.

- Full professional proficiency in English language. French is a plus.

- Knowledgeable in Microsoft 365 collaboration tools, including Power BI.

- Knowledgeable in Cybersecurity frameworks like NIST and ISO 27k.

Education:

- Preferable BA or MA computer science, information security, cybersecurity.
- Fluent English.