Cyber Security Analyst Job Description

Duties and Responsibilities:

- Ensure the identification of required security related issues, and that they are alerted upon by configuring and establishing monitoring, correlation, and alerting solutions
- Correlate all reported events from various multiple systems and network areas where potential security incident is identified; ensure the situation is handled promptly and effectively by starting the process of security incident response
- Carry out proper configuration of security solutions applied in protecting company asset such that the implemented SIEM solution reports all pertinent events
- Carry out configuration and maintenance of the implemented SIEM solution to enable it effectively identify and alert upon potential security events, as well as reduce false positives simultaneously
- Participate in the investigations being performed by the Information Security team
- Participate in maintaining a DLP solution to effectively give notice of violations to affected parties, and to reduce incidences of false positives
- Assist in the configuration of intrusion detection and prevention solutions based in the host and network servers to effectively identify potential security incidents
- Produce and maintain dashboards for monitoring security information for the management and Information Security team, to be able to provide various degree of visibility both real-time and over extended periods of the security events within the environment
- Ensure that all solutions set up for security and monitoring can effectively monitor and report upon security events happening within the environment by assigning security solution agents to devices and systems

- Participate in the process of selecting and reviewing of information security solutions
- Work with major service providers to resolve security issues identified with their managed systems and infrastructure in line with the company's incident response requirements
- Assist in compiling and producing reports on monthly issue and trend for the enhancement of the functions of the Enterprise Security and Support management
- Make recommendations for changes to the environment that can help in the removal of vulnerabilities and reduction in the risk of exploitation that may result in potential incidents
- Participate in ensuring team processes and documentation are effectively documented and maintained
- Participate in designing and implementing efforts towards enhancing ticketing solution so as to simplify monitoring and alerting efforts, as well as streamline incident management tasks
- Recommend and execute ideas to improve processes based on lessons learnt over time in performing assigned duties
- Initiate and produce custom scripts needed to make logging and alerting requirements easy and effective
- Perform as an escalation point for all incidents relating to potential security
- Carry out other enterprise security and support duties that may be assigned by management.

Cyber Security Analyst Requirements – Skills, Knowledge, and Abilities

- Some years of information security experience
- Some working experience with SIEM solutions management
- Deep knowledge and understanding of the various ways attacks are carried out against a system or network and how to effectively detect them
- Possess advanced analytical skills and strong ability to maintain calmness and being diplomatic under highly stressful situations

- Strong multitasking skills to be able to effectively manage multiple activities, including cross-team dependent activities simultaneously
- Strong ability to work effectively in collaboration with other members of a team or/and other professionals with minimal supervision
- Strong ability to quickly learn new processes and technologies, and to adapt to changes in sequences and timelines
- Strong communication skills, including written and verbal, and ability to work off hours when needed
- Possess certification in CEH, CISSP, and GIAC.