Job Title: SOC ANALYST LEVEL 1

J2 Software is an established African security-focused technology business founded in 2006 to deliver practical, world-class security services and solutions to our customers. Using our proven approach of getting things done, we provide real solutions to ever-changing cybersecurity problems.

We are here to make sure that you have enterprise-grade security, no matter the size of your business. J2 Software will deliver managed security services that are tailored to your individual business.

No business is the same and we, therefore, know that there is no one-size-fits-all solution.

By delivering fast to implement, practical solutions we ensure that we are your strategic IT and security partner and will be part of the journey to improved security and effective compliance which goes beyond simply ticking a checkbox. Real security allows our customers to operate more efficiently knowing that information is secured, and their reputation protected.

Job Description:

Your primary objective will be to proactively monitor and hunt through customer environments to detect and respond to information security threats.

You will help to protect organisations by employing a range of bleeding edge technologies and processes to prevent, detect and manage cyber security threats.

This may include protection of computers, data, networks, applications and business operations.

In your role as Security Operations Analyst Level 1 role is tasked with evaluating SIEM (Security Incident Event Management) related events flagged for review by established strategies.

This evaluation is performed with various validation tools, understanding and application of computer security topics and malware infections, and identification of new techniques to make quick decisions with a high rate of accuracy. The successful candidate will contribute to the strategic development of the existing CSC program within J2 Software aimed at further enhancing our world class experience.
The Security Operations Analyst is expected to adhere to numerous Key Performance Indicators to ensure decisions are made balancing factors such as risk tolerance and customer experience.
Key responsibility for this role is to help train machine learning models by labeling transactions, queries, or other entity pairings.

The Employee will be responsible for, but not limited to, the following tasks:

- Acknowledge, analyze, validate incidents and alarms triggered by SIEM solution
- Acknowledge, analyze, and validate incidents received through other reporting mechanisms including Alarms, Email, Chat, Telephone etc.
- Alarms analysis
- False positive mitigation Security event qualification Real-time analysis
- SIEM reports analysis
- Gather and analyze security information

- Drive and support incident notification and escalation Follow ticketing processes according to SLA Investigates and Escalates Alarms as appropriate Launches investigations thanks to detection tools
- Manage Alarms from Tier 1 to Tier 2 analysis as needed Identification and escalation of novel testing approaches
- Raise team awareness on testing trends, including syncs with SMEs on current patterns Propose process enhancements and improved tool functionality
- Work with Customer Support to resolve escalations;
- Adhere to platform KPIs related to accuracy, decision time, and productivity Ability to deal comfortably with daily recurring tasks
- Desire to proactively uncover new attack patterns
- Willingness to raise awareness of patterns, including presentations Excellent spoken and written English
- Ability to make decisions with speed and confidence Self-motivated, strong team player
- Desire to contribute to a highly technical world-class team
- Monitor for attacks, intrusions and unusual, unauthorized or illegal activity
- Use advanced analytic tools to determine emerging threat patterns and vulnerabilities Investigate security breaches and other cyber security incidents and provide incident response. Liaise with stakeholders in relation to cyber security issues and provide future recommendations
- Install security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs.
- Document security breaches and assess the damage they cause.
- Work with security team to perform tests and uncover network vulnerabilities.
- Stay current on cyber security trends and news.
- Research security enhancements and make recommendations to management.

The Employee undertakes (as a J2 stakeholder) to:

- Carry out all roles and duties that are assigned to you that are reasonable and lawful;
- Obey and execute all lawful and reasonable instruction(s) as per the request of your J2 supervisor or management.
- Demonstrate the values of J2 in all business dealings and transactions, protect and promote the business, reputation and goodwill to the best of your ability.
- Devote your time and attention during working hours to company business, and such additional time as your position reasonably requires.
- Maintain an up-to-date knowledge of hardware, software and general IT systems by studying relevant publications and participating in educational programs.

Required Skills & Experience:

- Min 2 years at SOC Level 1 experience.
- SIEM experience and knowhow is essential.
- Security+ is required.
- SSCP is beneficial.