Job Description

Job Title: SOC Analyst (Associate)
Date: ASAP
Reporting to: Information System Security Manager
Location: Hybrid

Overview

Prioclen LTD is a fast-growing Nigerian based management consulting firm with its head-quarters in Abuja Nigeria. We have a forte in providing strategic consultancy and advisory services to organizations- private, governmental and individual firms, by creating and integrating information technology solutions to enhance their service delivery and ensure sustainable growth and development in niche-based brands to these individuals/ organizations.

Purpose

Our growing company is looking to fill the role of security operations center analyst who will monitor, select and prevent the company from all sorts of cyber-attacks. The SOC analyst protects significant and confidential company data along with the brand integrity and business systems of the company. You might be required to lead a team that will integrate and implement the complete cybersecurity strategy of the organization and become the main point of contact for monitoring and avoiding digital attacks.
You will begin by reviewing incident notifications after which you will run vulnerability assessments and report your findings to the management.

Responsibilities

- Ensures Service Operations processes (incident, request and event) processes are being executed correctly and with quality
- Proactively document and implement correlation opportunities
- Participate in enterprise patching activities to ensure systems are compliant and vulnerabilities are mitigated
- Monitor systems real time to identify issues, problems, and attacks before they impact Duke Medicine services or patient information
- Correlate events across multiple data sources and detect patterns for event correlation
- Reviews and participates in ticket quality activities and address areas that need improvement

- Review operational performance metrics with the management team to determine areas of improvement.
- Resolve complex problems through advanced analysis and troubleshooting with minimum supervision.
- Considered an expert resource in the security operational area
- Demonstrate advanced understanding of security programs, tools and best practices.
- Operate SEIM (Trustwave) consoles in order to monitor the environment for events of interest
- Perform analysis of security logs in an attempt to detect unauthorized access
- Participate in the creation, modification and maintenance of all SOC policies and procedures
- Tier 1 security event monitoring and device-oriented activities in the SOC with guidance of short-term projects such as upgrades, migrations and implementations on the part of the tier 3 and 4 staff
- Monitor IT defense perimeter and scanning infrastructure and communicate security events and incidents to applicable Computer Emergency Response Team personnel and/or management
- Perform reviews/audits of mixed UNIX and Microsoft Windows environments, including network devices, databases, web services, and enterprise applications
- Coordinate with infrastructure support teams to maintain/trouble shoot defense perimeter and monitoring integrity
- Working rotational shifts (1st, 2nd or 3rd)
- Monitoring telephones and operating radios and computer equipment in the security operations center
- Interacting routinely with employees, executives and contractors.

Requirements

Essentials

- Bachelor's degree is required, preferably in Information Technology, Business, Supply Chain or related field
- Minimum of 2 years full-time work experience in IT consisting of at least 1 year doing windows systems administration, and includes experience with Active Directory, DNS, and network routing (Associate)
- 2+ years' experience working in a Security Operations Center (Associate). No experience required for Junior.

Skills

- Strong written and verbal communication skills, must be able to articulate complex technical analysis to both technical and non-technical audiences
- Good knowledge of Windows, Linux and Unix
- Knowledge of Intrusion Detection and Prevention techniques
- Knowledge of vulnerability scanners such as Nessus, Tenable

Desired

- Demonstrated experience with access control systems such as Active Directory and Virtual Private Network (VPN).
- Working knowledge of Tivoli, IBM End Point Manager.
- Take ownership of and troubleshoot tickets generated by the health monitoring system (Tickets).
- Rudimentary understanding of intrusion detection, firewall operations, and other general security.

Summary Terms and Conditions

Contract: 12-month fixed term contract
Salary: Very Attractive
Annual leave: 22 days holidays per annum pro rata excluding public holidays
Pension: Minimum 10% Employer contribution with minimum 8% Employee contribution
Healthcare: Company scheme subject to terms and conditions.
Life assurance: Company life assurance scheme.
Location: Abuja Nigeria
Notes: This post will be subject to background checks. A full statement of the main terms
and conditions of employment will be supplied with any formal offer of
employment. This job description does not form part of your contract of
employment

How to apply

To apply for this job opportunity, please send a CV and covering letter to recruitment@prioclen.com
Unfortunately, because of the volume of applications we are likely to receive we regret that we are unable to respond to every unsuccessful applicant. If we have not made contact with you within 2 weeks of the closing date you have not been selected for interview on this occasion.