Вакансия младшего аналитика SOC (Security Operations Center).

МЫ - Platformix.
Работаем на российском ИТ-рынке с 1992 года. Сегодня Platformix – один из крупнейших системных интеграторов в России, успешно помогает предприятиям из различных отраслей создавать надежную платформу для ведения бизнеса.

Станьте частью нашей команды!
По вопросам трудоустройства пишите, пожалуйста, на palenightingale@gmail.com

Обязанности:
- Реагирование на инциденты ИБ с использованием IDR, SIEM, EDR и NTA-систем по существующим сценариям;
- Участие в расследовании инцидентов ИБ;
- Выявление аномальной активности, Threat Hunting;
- Изучение новых типов источников событий ИБ;
- Изучение новых векторов атак и способов их детектирования;
- Помощь в разработке плейбуков по отработке сценариев;
- Участие в разработке сценариев выявления инцидентов ИБ и оптимизации существующих сценариев;
- Проведение исследований и поиска уязвимостей в компонентах и ПО критической инфраструктуры
- Эксплуатация и техническая поддержка существующей инфраструктуры SOC;
- Изучение решений, выполнение сертификационных требований вендоров (обучение, сдача экзаменов).

Требования:
- Выпускник ВУЗа/аспирантуры 2019-2023гг или студент выпускных курсов технических специальностей;
- Знание и понимание основ архитектуры современных корпоративных инфраструктур;
- Понимание принципов функционирования основных технологий обеспечения информационной безопасности (WAF, Sandbox, NGFW, VPN(ГОСТ), IDS/IPS, DLP, AAA, NAC, PIM, AV, PKI, PKI и др);
- Наличие кругозора в сфере технологий обеспечения информационной безопасности;
- Знание и понимание основ ИБ (в т.ч. Cyber Kill Chain, MITRE ATT&CK, TTP) в части векторов атак и защиты от них;
- Опыт работы с подсистемами аудита в различных системах (ОС, СЗИ, сетевое оборудование, прикладное ПО и т.д.), умение корректно интерпретировать различные события и выделять наиболее важную информацию;
- Внимательность к деталям, аналитический склад ума;
- Способность эффективно работать в команде и быстро обучаться новым технологиям;
- Знание английского языка на техническом уровне.

Будет преимуществом:
- Опыт работы с различными СЗИ, в частности АВПО, NGFW, IDS, WAF, NTA, EDR;
- Опыт работы с SIEM-системами, в т.ч. опыт реализации различных бизнес-кейсов с помощью SIEM-системы;
- Понимание базы MITRE ATT@CK, CWE;
- Понимание стандарта CVSS v3.1;
- Опыт расследования инцидентов ИБ: понимание типовых плейбуков по расследованию и реагированию в разрезе основных типов инцидентов ИБ;
- Понимание техник тестирования на проникновение и Red Team, повышения привилегий и закрепления в Active Directory;
- Опыт использования инструментов Kali Linux: metasploit, nmap, sqlmap, w3af, hydra, OpenVAS и т.д.;
- Опыт программирования на Python и одном из скриптовых языков Bash, PowerShell, Batch;
- Опыт работы с одним инструментом виртуализации: Docker, VMware, VirtualBox.

Мы предлагаем:
- Работу в стабильной компании, основанной в 1992 году;
- Достойный уровень оплаты труда;
- Полностью белую заработную плату;
- Работу в дружной команде профессионалов;
- Возможности для развития и профессионального обучения;
- ДМС со стоматологией;