АНАЛИТИК УГРОЗ / THREAT HUNTING

Мы ищем специалиста в команду JSOC CERT на задачи проактивного поиска угроз в инфраструктуре клиента (Threat Hunting)

Чем предстоит заниматься:

- Анализ публичных и приватных инцидентных отчетов различных компаний и вендоров с целью выработки рабочих гипотез по проактивному поиску угроз
- Анализ угроз и трендов в тактиках и техниках атакующих
- Участие в эмуляции действий атакующих в тестовом окружении
- Проверка выработанных гипотез в инфраструктурах заказчиков с помощью различных SIEM, EDR и NTA решений
- Участие в процессе перевода проверенных и рабочих гипотез в детектирующие правила SIEM, EDR, NTA решений

Наши ожидания:

- Желательно: опыт работы с какими-либо системами класса EDR, SIEM, NTA (IDS)
- Знаниями современных тактик и техник атакующих (MITRE ATT&CK) и способов их детектирования
- Глубокое понимание событий аудита Windows, утилиты Sysmon и Linux Auditd
- Понимание принципов работы современного вредоносного программного обеспечения
- Опыт работы с инструментами по анализу сетевого траффика
- Знаниями устройства и функционирования ОС Windows и Linux
- Понимание принципов Baseline и выявлений аномалий при анализе и интерпретации событий ОС Windows и Linux

Мы предлагаем:

Обращаем ваше внимание, что компания отменяет испытательный срок для специалистов по информационной безопасности и информационным технологиям. Сотрудники, которые придут в компанию с 3 марта по 1 сентября 2022 года, с первого дня работы будут пользоваться всеми преимуществами и льготами компании.

- Конкурентная зарплата + бонусы
- Работа в команде с ведущими специалистами в стране, много новых знаний, большой объем задач и ответственности, быстрый профессиональный рост
- Гибкий график и индивидуальный подход к возможностям и потребностям каждого
- Современный офис с видом на Кремль в 5 минутах от метро Охотный ряд
- Социальный пакет: ДМС, оплата обучения, скидки на фитнес и другие партнерские программы, бесплатный доступ к корпоративным библиотекам с сотнями книг, врач в офисе и 10 дополнительных дней оплачиваемых отгулов
- Хороший кофе, вкусности на кухне, автоматы с едой

Юлия Морозова

руководитель группы подбора Solar JSOC

+7 (903) 747-79-17

@YuliaMorozova

SOLAR WORK