ИНЖЕНЕР ТЕХНИЧЕСКОГО РАССЛЕДОВАНИЯ / FORENSIC

Мы ищем специалиста в команду JSOC CERT на задачи технического расследования атак и инцидентов на инфраструктуре клиента (forensic)

Чем предстоит заниматься:

- Анализ событий и следов инцидента как в рамках анализа журналов, так и непосредственно на целевой системе
- Форензик работы с образом АРМ и памятью скомпрометированной машины – восстановление данных, поиск следов заражения, сбор цифровых доказательств, выявления артефактов работы вредоносного ПО
- Разработка базовых инструментов автоматизации исследований АРМ или вредоносного ПО
- Проведение процедуры технического расследования и реагирования на атаку, участие в выработке компенсирующих мер защиты или сценариев контроля векторов

Наши ожидания:

- Опыт в анализе рабочих станций, дисков, дампов оперативной памяти
- Понимание принципов работы современного вредоносного программного обеспечения
- Навыки программирования на Python/Go для автоматизирования различных задач в ходе работы
- Понимание устройства основных артефактов в операционных системах Windows и nix подобных
- Опыт работы с инструментами по исследованию съемных носителей и образов памяти: Magnet AXIOM, Volatility, TSK, Autopsy, afftools, ewftools и тд.
- Предусматривается обучение по неизвестным и проблемным областям знаний, главное – заинтересованность в тематике и желание развиваться в указанных областях

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