QazSOC открывает вакансии на позицию аналитиков Т2 и Т3

Для кого это объявление?

- Если Вы выбрали профессиональной областью кибербезопасность (или кибербезопасность выбрала Вас), не боитесь вызовов и постоянно стремитесь стать лучше;
- Если работа в SOC (Security Operations Center), обнаружение и реагирование на кибератаки, расследование инцидентов – то, чему Вы готовы посвятить как минимум, несколько ближайших лет;
- Если Вы считаете, что Вам хватает знаний и опыта, чтобы конкурировать за место в команде лучших защитников в РК!

Если это про Вас, читайте дальше...

Что нужно знать и уметь, чтобы стать QazSOC аналитиком:

- понимание принципов работы и архитектуры операционных систем Windows и Linux;
- понимание инструментов удаленного администрирования Windows - PowerShell, WMI;
- понимание различных методов атак (различные виды ВПО, phishing, social engineering, account takeover, data leakage, vulnerabilities, ransomware, brute force, APT, DoS/DDoS, и т.п.);
- знание сетевых технологий (стек TCP/IP, модель OSI, VPN, NAT, и т. п.);
- знание инфраструктурных сервисов и протоколов: DNS, DHCP, SMB, NFS, и т. п;
- понимание принципов работы основных СЗИ, таких как Антивирусное ПО, EDR, IDS/IPS, Firewall, Proxy, Сканеры безопасности, и т. п.;
- понимание принципов работы SIEM систем (нормализация, агрегация, корреляция, и т.п.), Sandbox, Honeypot, TIP, IRP, NTA;
- опыт анализа логов от различных систем, умение их правильно интерпретировать;
- понимание методологий MITRE ATT@CK, Cyber Kill Chain;
- опыт расследования инцидентов, анализа журналов аудита и других артефактов для выстраивания цепочек причинно-следственных связей и восстановления картины атак.

Каким нужно быть, что нужно иметь, чтобы работать в QazSOC:

- аналитический склад ума;
- способность решать нестандартные технические задачи;
- отличные коммуникативные навыки;
- грамотная речь, умение излагать свои мысли;
- уметь самостоятельно решать сложные задачи, уметь эффективно работать в команде;
- лояльность.

Что повысит Ваши шансы при отборе:

- практический опыт работы в области кибермониторинга;
- опыт работы с разными SIEM системами, опыт разработки правил корреляции;
- опыт работы в области Threat Hunting;
- опыт работы с ELK;
- опыт анализа сетевого трафика, анализа дампов трафика, памяти, жёстких дисков;
- опыт работы с системами класса Sandbox, Honeypot, TIP, IRP, NTA;
- опыт конфигурирования аудита Windows / Linux;
- понимание архитектуры и атак на Active Directory;
- владение инструментарием для тестирования на проникновение;
- наличие навыков программирования на Python/Go для автоматизации задач;
- знание английского языка, способность работать в международной среде, с международными партнерами;
- наличие профильных сертификаций в области информационной и кибербезопасности.

В чем заключается работа аналитика QazSOC:

- участие в стандартных процессах обнаружения инцидентов в SOC, в том числе:
  - анализ нестандартных подозрительных событий и инцидентов (при эскалации с T1);
  - Threat Hunting;
- участие во всех фазах реагирования на инциденты;
- участие во всех фазах расследования инцидентов, подготовка аналитических отчетов для клиентов;
- участие в процессах усовершенствования механизмов обнаружения и реагирования на атаки, в том числе:
  - исследование техник и инструментов атакующих (Threat Intelligence);
  - участие в Purple Team упражнениях на киберполигоне;
  - разработка правил детектирования атак;
  - автоматизация задач в рамках процессов операционной деятельности;
  - создание / обновление технической документации;
  - участие в работе Центра Компетенции SOC;
- участие в проектах по управлению услугами SOC:
  - исследование различных источников событий (от классических СЗИ, до облачных платформ);
  - подключение ресурсов клиентов к платформе мониторинга.

Что такое QazSOC, что Вас там ожидает:

- один из ведущих SOC в стране;
- одна из самих опытных Blue Team команд (все наши ведущие аналитики имеют боле 5-ти лет опыта работе в SOC, боле 10-ти в ИБ);
- возможность быстрого профессионального роста (все зависит только от Вас);
- клиенты из разных сфер экономики;
- возможность участвовать в расследовании сложных инцидентов и APT;
- наши люди, это наш самый большой актив:
  - обучение в профильных направлениях за счет компании;
  - помощь со стороны коллег в освоении технических навыков;
  - коучинг от стороны руководства в софт-скиллах;
  - поддержка в жизненных вопросах, что бы то ни было;
- возможность удаленной работы;
- много совместного труда и побед!

Для резюме и предложений: office@qazsoc.kz