Инженер по защите информации

Вакансия действительна с 27.09.2026 по 11.10.2026

Ведущий аналитик SOC

IT и телекоммуникации

РАБОТОДАТЕЛЬ

Товарищество с ограниченной ответственностью "BTS DIGITAL"

Оплата труда	от 732 000 тенге
Условия	полный рабочий день, постоянная работа, нормальные условия труда
Количество вакансий	1

ИНФОРМАЦИЯ О ВАКАНСИИ

Регион	г. Астана / г. Астана
Место работы	Многофункциональный комплекс Абу Даби

Должностные обязанности

Обязанности:

- Проводить углубленный анализ инцидентов ИБ, эскалированных с L1.
- Подтверждать или опровергать инциденты на основе анализа логов и сетевого трафика.
- Проводить расследования, определять вектор атаки и масштаб инцидента.
- Выполнять первичное реагирование: изоляция узлов, блокировка учетных записей, ограничение доступа.
- Создавать и оптимизировать корреляционные правила и сценарии в SIEM.
- Настраивать системы мониторинга и снижать количество ложных срабатываний.
- Подготавливать отчеты по инцидентам и предлагать меры по устранению уязвимостей.
- Пополнять базу знаний SOC новыми сценариями и примерами атак.
- Взаимодействовать с L3, DFIR и Threat Intelligence по сложным инцидентам.

Требования:

- Уверенные знания Windows и Linux, навыки работы с логами и журналами безопасности.
- Понимание сетевой архитектуры и протоколов TCP/IP, DNS, HTTP/S, SMTP, SMB.
- Опыт работы с SIEM: Splunk, QRadar, ELK и другими решениями.
- Опыт разработки и настройки корреляционных правил в SIEM.
- Навыки работы с IDS/IPS, WAF, EDR, DLP, MDM и Sandbox.
- Умение анализировать сетевой трафик и артефакты атак: IOC, PCAP, Sysmon.
- Опыт расследования фишинга, malware, bruteforce и privilege escalation.
- Знание MITRE ATT&CK, Cyber Kill Chain и NIST Incident Handling.
- Навыки Python, Bash или PowerShell для автоматизации расследований.

- Английский язык для чтения технической документации и деловой переписки.

Желательные навыки:

- Опыт реверс-инжиниринга или цифровой криминалистики DFIR.
- Знание AWS, Azure, GCP, Docker и Kubernetes.
- Опыт работы с платформами Threat Intelligence.
- Наличие сертификатов CompTIA CySA+, GCIA, GCIH, ECIH, Splunk или QRadar.

ТРЕБОВАНИЯ К СОИСКАТЕЛЮ

Стаж по специальности	2 года
Уровень образования	высшее
Знание языков	• Русский - высокий уровень

ПРОФЕССИОНАЛЬНЫЕ НАВЫКИ

- Анализ и проверка безопасности архитектуры Web-сервера
- Настройка политики безопасности ОС, СУБД, ППО
- Настройка системы защиты от утечек конфиденциальной информации
- Настройка средств антивирусной защиты для корректной работы ПО по заданным шаблонам

ЛИЧНЫЕ КАЧЕСТВА

- Логическое рассуждение
- Лидерство
- Логическое мышление

ИНФОРМАЦИЯ О ПРЕДПРИЯТИИ

Количество работников	272
Контактное лицо	Наршибаева Анель
Регион предприятия	г. Астана / г. Астана
Адрес предприятия	Сығанақ көшесі 60/2 15 этаж