Ақпаратты қорғау жөніндегі инженерлер

Бос жұмыс орны 27.09.2026 бастап
11.10.2026 дейін жарамды

Ведущий аналитик SOC

IT және телекоммуникациялар

ЖҰМЫС БЕРУШІ

Товарищество с ограниченной ответственностью "BTS DIGITAL"

Еңбекақы	732 000 теңгеден бастап
Шарттары	толық жұмыс күні, тұрақты жұмыс, еңбек жағдайы қалыпты
Бос жұмыс орындар саны	1

БОС ЖҰМЫС ОРНЫ ТУРАЛЫ АҚПАРАТ

Аймақ	Астана қ. / Астана қ.
Жұмыс орны	Многофункциональный комплекс Абу Даби

Лауазымдық міндеті

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.

ЖҰМЫС ІЗДЕУШІГЕ ТАЛАПТАР

Мамандық бойынша өтілі	2 жыл
Білім деңгейі	жоғары
Меңгерген тілдері	• Орыс - жоғары деңгей

КӘСІБИ ДАҒДЫЛАР

- Web-сервер құрылымының қауіпсіздігін талдау және тексеру
- ОЖ, ДҚБЖ, ҚБЖ қауіпсіздік саясатын теңшеу
- Құпия ақпараттың жылыстауынан қорғау жүйесін теңшеу
- Берілген шаблондар бойынша дұрыс жұмыс істеу үшін антивирустық қорғаныс құралдарын орнату

ЖЕКЕ ҚАСИЕТІ

- Логикалық ойлау
- Көшбасшылық
- Логикалық ойлау

КӘСІПОРЫН ТУРАЛЫ АҚПАРАТТАР

Қызметкерлер саны	272
Байланыстағы тұлға	Наршибаева Анель
Кәсіпорынның аймағы	Астана қ. / Астана қ.
Кәсіпорынның мекен-жайы	Сығанақ көшесі 60/2 15 этаж