

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание услуг мониторинга событий SOC
(на основе сервис-контракта)

№ п/п	Перечень основных данных и требований	Основные данные и требования
1	Место оказания услуг	г. Бишкек, ул. Ибраимова 24.
2	Заказчик	Отдел информационной безопасности.
3	Должностные обязанности	• Мониторинг и анализ событий информационной безопасности со средств защиты информации (SIEM, SOAR, XDR, AV, FW, IPS\IDS, DLP и др.); • Регистрация и расследование инцидентов ИБ; • Эскалация инцидентов на вышестоящие линии; • Посменная работа для обеспечения функционирования SOC в режиме 24x7; • Разработка новых сценариев выявления инцидентов в системах безопасности; • Разработка планов реагирования на инциденты ИБ (playbook) и их автоматизация; • Ведение и поддержание актуальности базы типовых инцидентов информационной безопасности; • Определение ложных срабатываний и предложение рекомендаций для их исключения; • Контроль состояния систем безопасности.
4	Квалификационные требования к исполнителю	Знание языков: • русский – свободно; • кыргызский – свободно; • английский выше среднего (<i>Upper Intermediate</i>) или продвинутый уровень (<i>Advanced</i>). Квалификационные требования: • Знание основ информационной безопасности; • Базовое понимание работы windows/nix систем; • Знание и понимание работы сетевых протоколов (<i>OSI</i> и/или <i>tcp/ip</i>); • Базовое понимание принципов работы Active Directory (<i>механизмы аутентификации, атаки</i>); • Знание и понимание основных тактик и техник злоумышленников (<i>MITRE ATT&CK /Cyber KillChain</i>).
5	Личные качества	• Внимательность к деталям. • Ответственность; • Коммуникабельность и умение работать в команде. • Стрессоустойчивость и способность работать в условиях многозадачности;

		• Аналитический склад ума, ориентированность на результат; • Высокий уровень самоорганизации и способность к принятию самостоятельных решений; • Гибкость и адаптивность к изменяющимся условиям.
6	Контроль и отчетность	Исполнитель обязан предоставлять регулярные отчеты о проделанной работе, в том числе: • Детализированный отчёт инцидентов ИБ по окончанию смены; • Ежемесячный отчёт о проделанной работе.
7	Условия работы	• График: 1х2 (<i>сутки через двое</i>); • 1 смена: 15 часов; • Офис г.Бишкек Ибраимова 24.