



ITKey — это команда профессионалов с более чем 12-летним опытом работы в разработке и внедрении решений на базе OpenStack и Kubernetes. Мы успешно реализовали проекты для крупных международных компаний в сферах телекоммуникаций, банковского сектора, а также помогли многим стартапам улучшить процессы разработки и оптимизировать инфраструктуру.

В 2023 году мы представили собственный продукт — **KeyStack**, который позволяет быстро развернуть полнофункциональную ИТ-инфраструктуру «из коробки». Эта платформа обеспечивает безопасность, масштабируемость и управление виртуальными машинами и другими компонентами в рамках подхода Infrastructure as Code (IaC). **KeyStack** уже внесен в реестр российского программного обеспечения.

Подробнее о нас вы можете узнать на следующих сайтах: [ITKey](#) [KeyStack](#)

Кого мы ищем: DevSecOps

В твои обязанности будет входить:

- Разработка и поддержка CI/CD пайплайнов в GitLab.
- Подключение и настройка сканеров уязвимостей, интеграция их в проекты компании.
- Доработка и настройка существующих сканеров безопасности.
- Обеспечение безопасности ОС (Ubuntu, RHEL) и других компонентов ПО.
- Анализ и устранение уязвимостей в процессе сканирования и из сообщений от клиентов (анализ, исправление, патчинг, тестирование).
- Создание и доработка Ansible playbook'ов.
- Участие в разработке процессов информационной безопасности.
- Написание и поддержка технической документации по безопасности.

От кандидата ожидаем:

- Знание и опыт работы с методологиями DevSecOps.
- Опыт построения CI/CD (Jenkins, GitLab).
- Умение читать и писать код на Python.
- Уверенное владение Shell-скриптингом.
- Уверенное владение Ansible или другими системами конфигурационного управления.
- Уверенное владение Docker или другими инструментами управления контейнерами.
- Практический опыт администрирования Linux (Ubuntu, RHEL), включая работу с серверными платформами.
- Понимание принципов безопасности ОС Linux (Ubuntu, RHEL).
- Знание принципов работы компьютерных сетей.
- Опыт работы с OpenStack или другими облачными технологиями.
- Опыт работы с ПО: MariaDB, PostgreSQL, HAProxy, Nginx, Prometheus.
- Опыт работы с системами контроля версий (Git).
- Знание английского языка для чтения технической документации и возможного участия в апстримной разработке.

Будет плюсом:

- Опыт работы с Kubernetes (k8s), Terraform, MongoDB, Redis, RabbitMQ.
- Опыт сборки DEB/RPM пакетов.
- Умение читать и писать код на Go/Rust/Java/Ruby.
- Знание российского законодательства в области ИТ-безопасности (ФЗ, нормативные документы ФСТЭК, ФСБ).

Стек, который используется на проекте:

- OpenStack
- Ansible
- Kolla-Ansible
- Мониторинг: Prometheus, Victoria Metrics, Grafana

- Логирование: ELK (Elasticsearch, Logstash, Kibana)
-

Условия:

- График работы 5/2 с возможностью гибридного формата или полного удалённого участия.
- Бессрочный трудовой договор.
- Бонусная система, включая проектные премии.
- ДМС, программы психологической поддержки.
- Компания оплачивает обучение и сертификацию.
- Возможность профессионального и карьерного роста.
- Преимущества работы в IT-компании.