

Семь инструментов для управления инфраструктурой? Достаточно одной КОНСОЛИ.

PAM, аудит, комплаенс и SIEM для банков — в одной консоли.

Что это

Proxima Console объединяет управление привилегированным доступом (PAM), журнал аудита с доказуемой целостностью, контроль соответствия требованиям и выгрузку для SIEM — вместе с инвентаризацией, мониторингом и дежурствами. Разворачивается on-prem, в вашем ЦОД в Узбекистане.

Что заменяет

Привилегированный доступ (PAM)

Вместо: Отдельной PAM-системы, VPN и общих SSH-ключей

Контроль соответствия

Вместо: Таблиц Excel перед каждой проверкой

Инвентаризация

Вместо: CMDB в таблицах

Мониторинг доступности

Вместо: Отдельного сервиса проверок

Дежурства и оповещения

Вместо: Отдельного сервиса оповещений

Регламенты (runbooks)

Вместо: Скриптов на чьем-то ноутбуке

Журнал аудита

Вместо: Журналов доступа, разбросанных по системам

Интеграция с SIEM

Вместо: Ручной выгрузки журналов для SOC

Живая топология

Вместо: Нарисованных от руки схем сети

Метрики и логи

Вместо: Отдельных систем метрик и логов

Инциденты и ИИ-анализ причин

Вместо: Догадок в «штабе» инцидента

Сервис-деск + Jira

Вместо: Переходов в портал Jira ради каждой заявки

Безопасность и контроль

Жёсткая изоляция клиентов

Метрики физически разделены по клиентам, а не отфильтрованы запросом, о котором приложению нужно не забыть.

MFA и ключи доступа

Ключи доступа WebAuthn, TOTP и вход через Google Workspace с ограничением домена. При сбое — отказ в доступе.

Идентичность агента под контролем брокера

У каждого агента свои учётные данные с ограниченными правами. Агент не может выдать себя за другой сервер, даже если попытается.

Цепочка аудита проверяется каждый час

Записи аудита связаны хеш-цепочкой SHA-256; независимая задача каждый час проверяет всю цепочку.

Роли на уровне окружения

Выдавайте роль на одно окружение одного клиента. Действует для пользователей, команд и сервисных учётных записей, полностью аудируется.

Секреты в Vault

Учётные данные агентов, TLS-сертификаты и хранимые секреты выпускаются и шифруются через HashiCorp Vault. В конфигурации приложения ничего длительного не хранится.

Изменения — только после согласования

Исправления и разрушающие регламенты выполняются только после согласования человеком с нужной ролью, и согласование записывается.

Записано и воспроизводимо

Выдача доступа, терминальные сессии, выполнение регламентов и административные изменения записываются, воспроизводятся и доступны для поиска.

Как проходит пилот

01

Подключите одно окружение

Установите агент на серверы одного окружения, которое выберете.

02

Посмотрите карту и мониторинг

Инвентаризация, топология, проверки доступности и оценки соответствия заполняются по мере поступления данных от агентов.

03

Разберём находки вместе

Мы вместе с вашей командой пройдем по тому, что нашёл Console, и договоримся о следующих шагах.

Свяжитесь с нами

Запишитесь на звонок на console.proximaops.io или напишите на sales@proximaops.io.