Security Gate: централизованное управление безопасностью приложений

Антон Юрищев

Архитектор, VK Cloud

tech

VK – лидер в DevSecOps

- 40K репозиториев
- >1,5 млрд строк кода
- 2000+ разработчиков
- Сотни продуктов
- Десятки ДЗО
- Все популярные языки и парочка непопулярных

VK Secure Inside

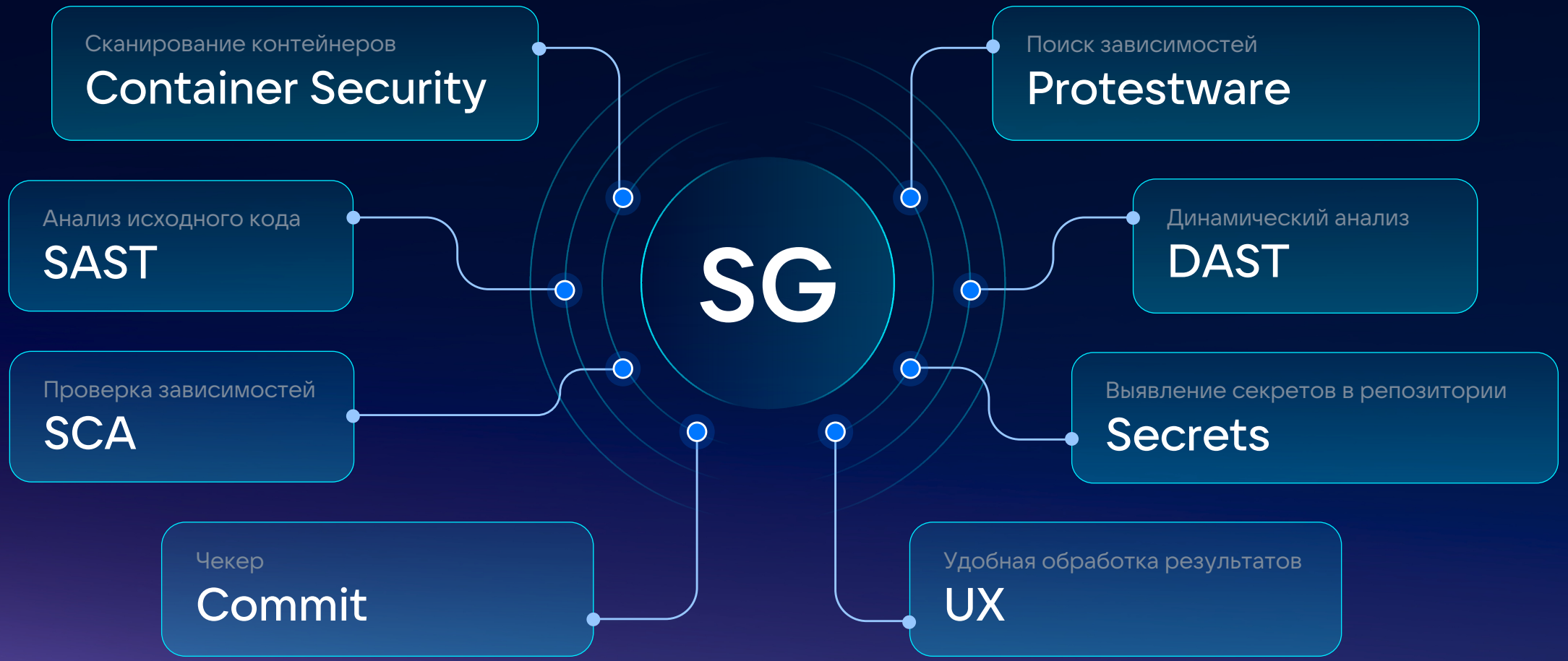
Powered by

Security Gate

Реализовано на единый DevSecOps платформе Security Gate

tech

Security Gate



tech

Security Gate отвечает на запросы ИТ и безопасности

Компании с большим количеством in-house разработки

Компании в процессе внедрения практик DevSecOps

Сложности в масштабировании практик безопасной разработки во всех проектах

Запрос на внешнюю экспертизу, методологии, лучшие практики

Необходим выбор инструментов для разнородной кодовой базы

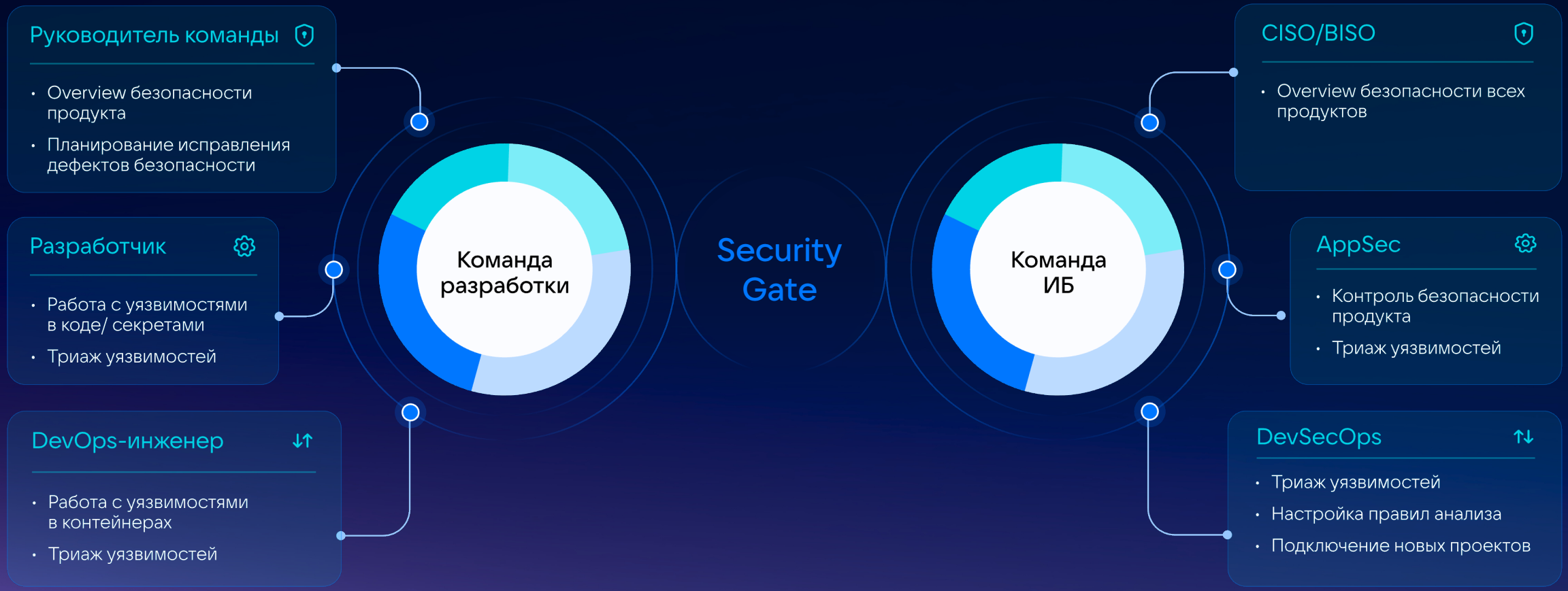
Рассматривается привлечение продуктовых команд к совместной с ИБ работе над безопасностью кода

tech

Популярные функции!

- Все сработки дедуплицируются и нормализуются
  → не надо сидеть и разбирать отчёты. Результаты в удобном UI
- Встроен поиск секретов
- Интеграция с Jira и аналогами
- Умная приоритезация сработок
  → не будет ситуации с 100 критическими сработками и подбрасыванием монеты что фиксить первым. Самое важное подсвечено
- LLM триаж сработок. ИИ поможет сделать правильный выбор

Типовые потребности команд



VK Cloud

Почему появился Security Gate

tech

Почему появился Security Gate

Множество языков программирования

- Java
- Php
- C#
- Go
- Python
- Scala
- JS/TS
- Ruby
- ...

Множество технологий

- Gitlab
- Gitlab CI
- Bitbucket
- Jenkins
- SVN
- Team City
- Самописные системы

Разные производственные процессы

- Релиз из master
- Релиз из daily-веток
- On-prem релиз
- ....

Решаемые задачи

Полное покрытие кодовой базы

40 k
репозиториев в VK

> 10 k
сканирований в день

> 1 млрд
строк кода

Максимально быстрое подключение

- Встраивание в CI/CD
- Авто-сканирование из VCS
- API

Независимость от конкретного анализатора

Подключение новых анализаторов plug&play, без изменения CI/CD

Снижение затрат на анализ

- Многофакторная дедупликация
- Приоритезация уязвимостей
- Кросс-веточная обработка результатов

tech

Интеграция с Security Gate

tech

Максимальная дедупликация

- Все уязвимости по сканированным веткам можно посмотреть и обработать в одном месте
- Вердикт по уникальной сработке указывается 1 раз в рамках кроссветочного триажа
- Реализован специальный механизм дедупликации для режима кроссветочного триажа

tech

Приоритезация уязвимостей

Множество анализаторов переоценивают критичность обнаруженных дефектов в коде. Это приводит к проблеме «мусорных» сработок на уровнях High+ и скрывает наиболее значимые результаты

Первоначальные результаты

	Crit	High	Medium	Low
SAST	40	56	70	1
SCA	250	472	355	10
Secret	47	35	10	2

SG - приоритезатор

- Приоритезация правил SAST
- Оценка критичности CVE
- Динамическа приоритезация Secret

Итоговые результаты

	Crit	High	Medium	Low
SAST	10	22	100	35
SCA	16	37	702	322
Secret	12	10	70	2

tech

Процесс сканирования

VK Cloud

Как работает Security Gate

tech

VK Cloud

securitygate_multi_mcs
mcs4117005902

0 ₽

i.ignatyev@vk.team
Суперадминистратор

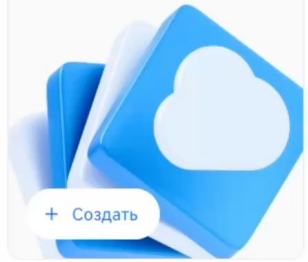
- Главная
- Облачные вычисления
- Виртуальные сети
- Cloud Backup
- Data Platform
- Мониторинг
- CDN
- DNS
- Объектное хранилище
- Магазин приложений
- Контейнеры
- Сервисы безопасности
- Базы данных
- Аналитические БД
- Большие данные
- Графические адаптеры
- ML Platform
- Cloud Desktop
- AI API
- Готовое рабочее место
- Специальные сервисы
- Управление доступами
- Баланс

Настройка меню

Сервисы и возможности

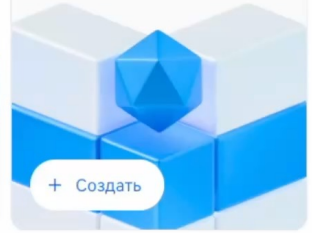
Все возможности

Виртуальные машины
Размещение IT-сервисов в облаке



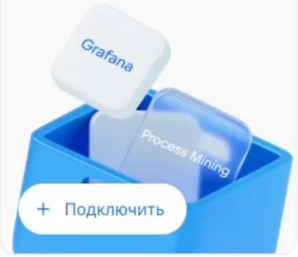
+ Создать

Кластеры Kubernetes
Разворачивание и запуск приложений



+ Создать

Магазин приложений
Подключайте ПО мгновенно в маркетплейсе VK Cloud



+ Подключить

Базы данных
Перенос базы данных и управление системой в облаке

+ Создать

Объект
Хранение д
доступом

+ Созд

Общая информация | Детализация расходов | Безопасность | Журнал событий | Цены

Бесплатный курс →
Курс о работе с платформой VK Cloud

С чего начать →
Базовая информация об облаке, обращении в поддержку, правовая информация и реквизиты

Доступы и роли →
Участники проекта

A I D F D M +5

Ваша роль в проекте

Суперадминистратор

Миграция →
Перенос существующей виртуальной инфраструктуры в облако VK Cloud

Биллинг →
Учет использования ресурсов, оплата и получение финансовых документов

Квоты

Добавить квоты

Виртуальные машины	0 из 15 шт.
vCPU	0 из 48 шт.
RAM	0 из 73728 МБ

Главная
Облачные вычисления
Виртуальные сети
Cloud Backup
Data Platform
Мониторинг
CDN
DNS
Объектное хранилище
Магазин приложений
Контейнеры
Сервисы безопасности
Security Gate
Базы данных
Аналитические БД
Большие данные
Графические адаптеры
ML Platform
Cloud Desktop
AI API
Готовое рабочее место
Специальные сервисы
Управление доступами
Настройка меню

Security Gate

VK Sec

Начать сканирование

Demo | Мой Продукт

Название	Дата сканирования	Critical	High	Medium	Low	Статус
vuln-nodejs-app	25.06.2025 20:28	24	59	67	83	В процессе
dvsa	25.06.2025 20:28	23	71	83	150	В процессе
railsgoat	25.06.2025 20:28	16	47	116	105	В процессе
webgoat	25.06.2025 20:28	6	55	119	33	В процессе
govwa	25.06.2025 20:28	2	24	27	10	В процессе

Проекты

mcs4117005902

Начать сканирование

Demo > vuln-nodejs-app (Кроссветочный разбор)

Показать ветки

SCA 150 | SAST 47 | Secrets 36

Все 14 8 26 46

ejs:3.1.6	Подтверждено
ip:1.1.5	Не обработано
json5:1.0.1	Не обработано
json5:2.2.0	Не обработано
jsonwebtoken:8.5.1	Подтверждено
loader-utils:1.4.0	Отклонено
mysql2:2.3.3	Не обработано
node-serialize:0.0.4	Не обработано
qs:6.9.3	Не обработано
qs:6.9.6	Не обработано

1 2 3 4 5 ... 10

loader-utils:1.4.0

Раскрыть

Подтверждено | Не обработано | Отклонено | Исправлено

Подробнее | Комментарии 1 | JIRA | История | Ветки

Не обработано

test

dev

master

VK Cloud

Главная
Облачные вычисления
Виртуальные сети
Cloud Backup
Data Platform
Мониторинг
CDN
DNS
Объектное хранилище
Магазин приложений
Контейнеры
Сервисы безопасности
Security Gate
Базы данных
Аналитические БД
Большие данные
Графические адаптеры
ML Platform
Cloud Desktop
AI API
Готовое рабочее место
Специальные сервисы
Управление доступами

Настройка меню

Security Gate

VK Security Gate

Начать сканирование

Demo | Мой Продукт

Название	Дата сканирования	Critical	High	Medium	Low	Статус
my_project	25.06.2025 20:33	2	1	27	5	Завершена

Спасибо за внимание!

Антон Юрищев

Архитектор, VK Cloud

tech