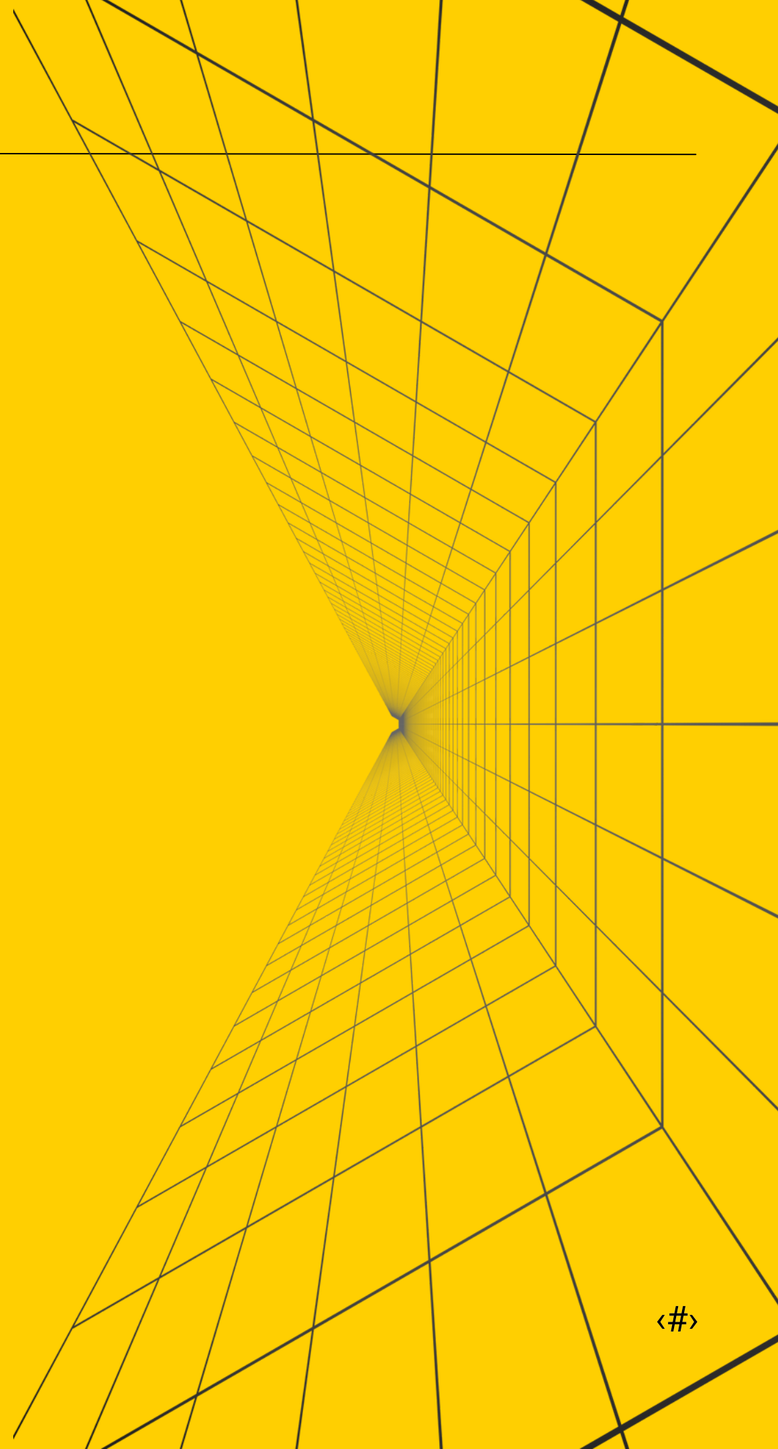
# GitOps from security perspective

By Aleksandr Sungurov



exness

06.09.2023

# Спикер


## Александр Сунгуров

Архитектор по информационной безопасности

alexander.sungurov@exness.com

@Banzay021


# Эксперт


## Антон Туренский

Инженер по информационной безопасности

anton.turenskiy@exness.com

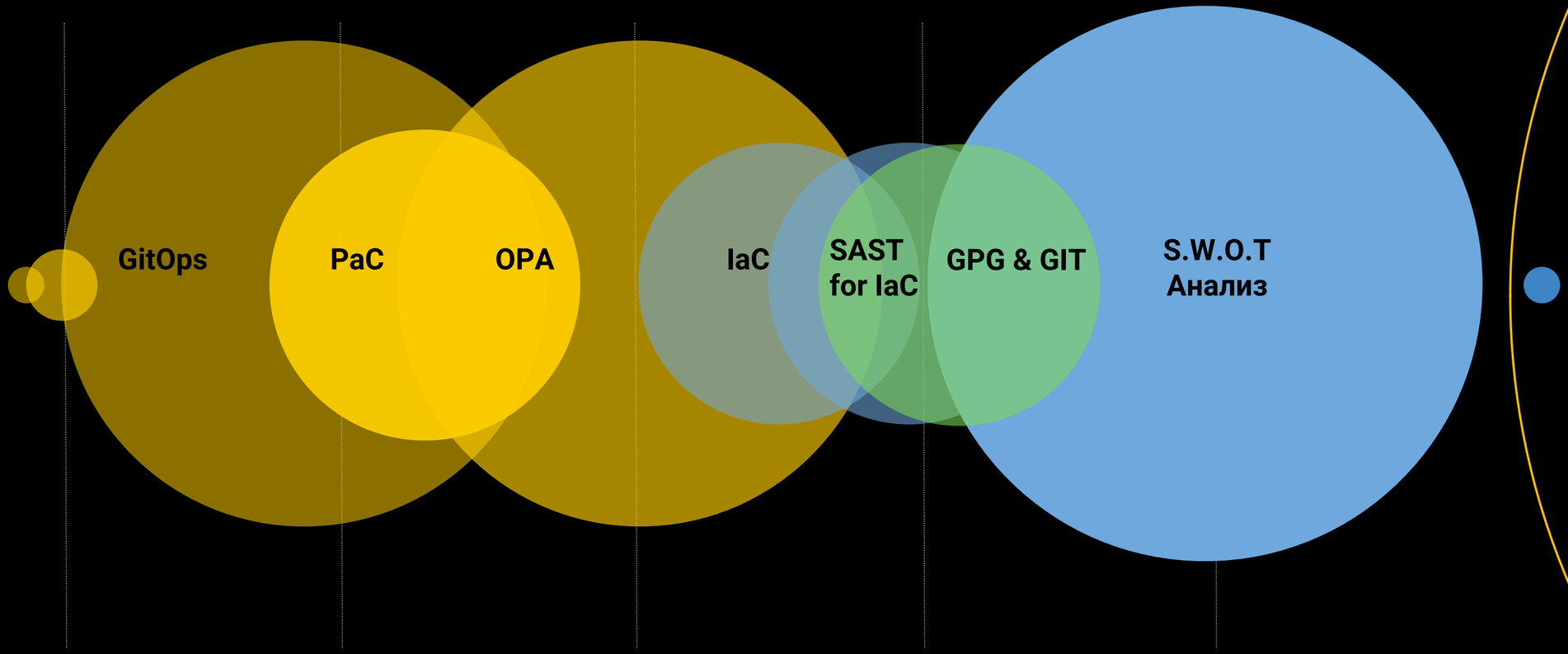
@totofka


# Зачем все это нужно?

Необходимо создать новую безопасную среду.

- Удобную для разработчиков
- Контролируемую
- Прозрачную

# Содержание



# GitOps

**GitOps** предлагает структурированный и автоматизированный способ управления инфраструктурой.


- совместное управление изменениями кода
- тестирование и валидация изменений перед развертыванием
- фиксируются только авторизованные изменения
- возможность отслеживания изменений
- масштабируемость
- аварийное восстановление
- аудит действий
- возврат в консистентное состояние

# GitOps


Development and Version Control Repositories
Infrastructure, Automation & Security
gitops
CI/CD
Project Management
argo

# IAC

**Инфраструктура как код (IaC)** - это способ управления технологической инфраструктурой и ее подготовки с использованием сценариев и конфигураций.

- надежное управление инфраструктурой
- минимизация рисков ошибок
- ускоряет время развертывания
- гибкость инфраструктуры
- быстрая адаптация к меняющимся требованиям бизнеса
- автоматическая инвентаризация

# Policy as code

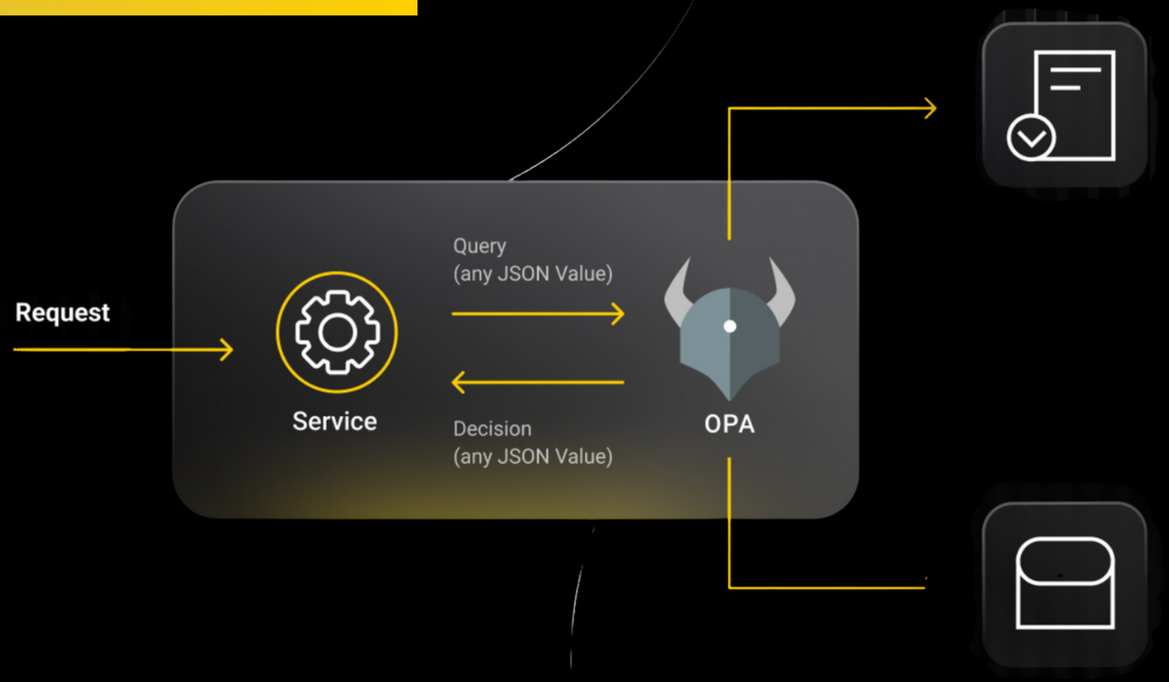
**Политика как код (PaC)** - это способ декларативного описания контролей в виде кода и автоматизация валидации конфигураций на соответствие политике.

- Согласованное развертывание имеет жизненно важное значение для обеспечения единообразного развертывания инфраструктуры в различных средах
- Автоматизированное тестирование изменений инфраструктуры, включая тестирование безопасности
- Возможности отслеживания

# Open Policy Agent (OPA)

**Open Policy Agent** - это механизм разработки политик общего назначения с открытым исходным кодом, созданный Cloud Native Computing Foundation. Он обеспечивает основу для политики в виде кода в любом домене, основанную на декларативном языке высокого уровня под названием Rego.

- Применение декларативной политики
- Улучшенная безопасность и управление
- Быстрое и согласованное развертывание
- Улучшение взаимодействия и документирования



# Open Policy Agent (OPA)

```
  msg_init := concat("",["init ", msg])
}
general_violation[{"msg": msg, "container_type": container_type, "image": container.image}] {
  container := input_object_container_spec[container_type][_]
  not is_exempt(container)
  parts := split(container.image, ":")
  count(parts) == 1
  msg := sprintf("container <%v> does not have image tag <%v>", [container.name, container.image])
}

general_violation[{"msg": msg, "container_type": container_type, "image": container.image}] {
  container := input_object_container_spec[container_type][_]
  not is_exempt(container)
  parts := split(container.image, ":")
  count(parts)==2
  parts[1]=="latest"
  msg := sprintf("container <%v> has an invalid image tag <%v>", [container.name, container.image])
}
```

# SAST for IaC

## Checkov

Он поддерживает различные языки IaC, такие как Terraform, Cloud Formation, Kubernetes и другие. Checkov фокусируется на обеспечении безопасности и проверке соответствия шаблонам IaC.

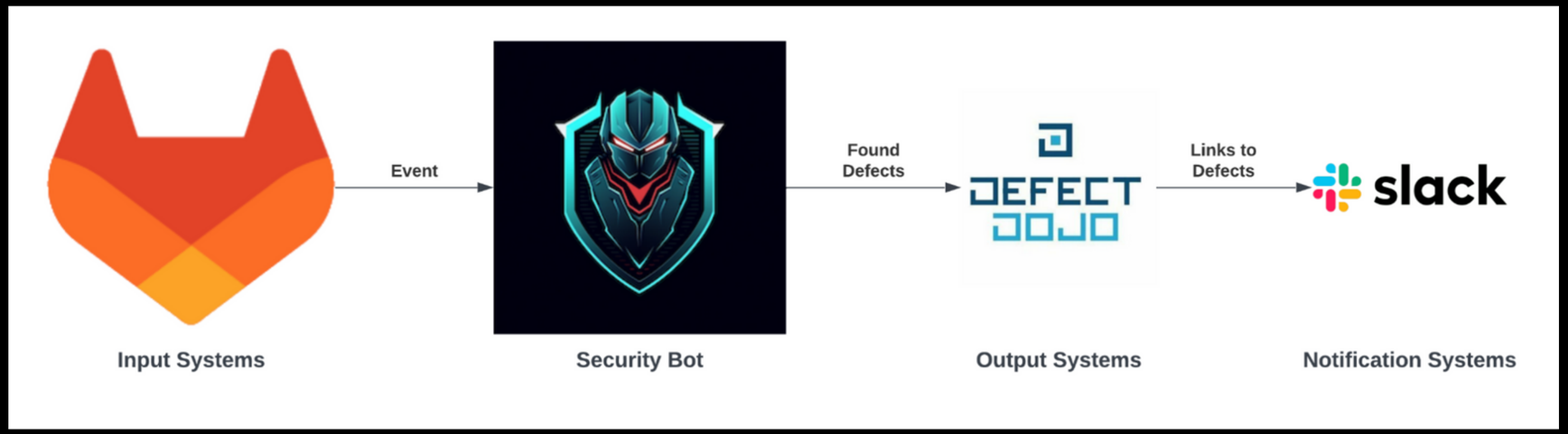
## KICS (Keeping Infrastructure as Code Secure)

Он поддерживает несколько языков IaC и направлен на то, чтобы помочь разработчикам выявить уязвимости безопасности в коде их инфраструктуры.

## Terrascan

Он поддерживает сканирование на наличие широкого спектра рекомендаций по обеспечению безопасности и уязвимостей.

# Sec Bot




Opensource repository

# GPG (GNU Privacy Guard) & GIT

**GitLab предлагает встроенную поддержку подписей GPG, позволяя пользователям легко подписывать свои коммиты с помощью пары ключей, привязанной к их учетной записи GitLab.**

- Подпись GPG помогает предотвратить несколько типов атак, включая атаки с внедрением кода, несанкционированные изменения кода и атаки "человек посередине".
- Требуя использования подписей GPG для коммитов, организации могут значительно снизить риск инцидентов безопасности на основе кода и утечек данных.

# Request approval policy

Overview 0 | Commits 1 | Pipelines 1 | Changes 1

👍 0 👎 0

Pipeline #2131098 passed for 41abe90c on feature/python-main… 4 weeks ago

Approval is optional

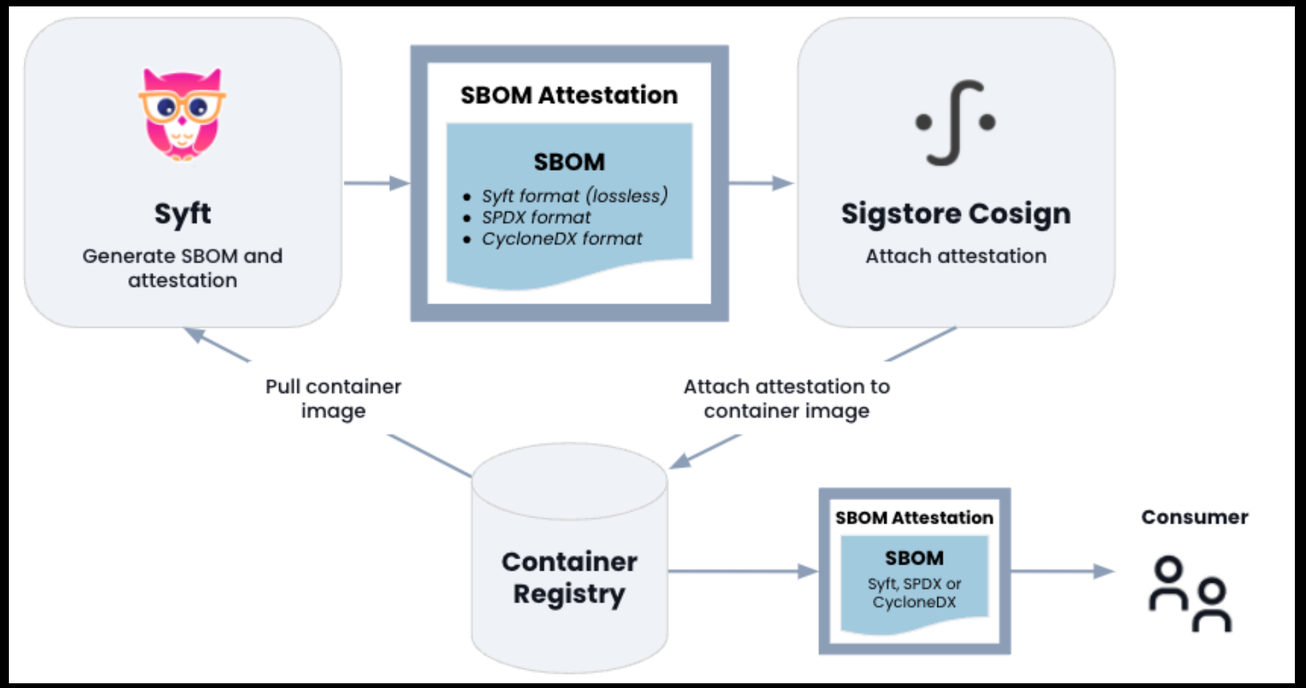
| Approvers | Approvals | Commented by | Approved by |
|---|---|---|---|
| All eligible users | Optional | | |
| **Code Owners** | | | |
| *.py | Optional | | |

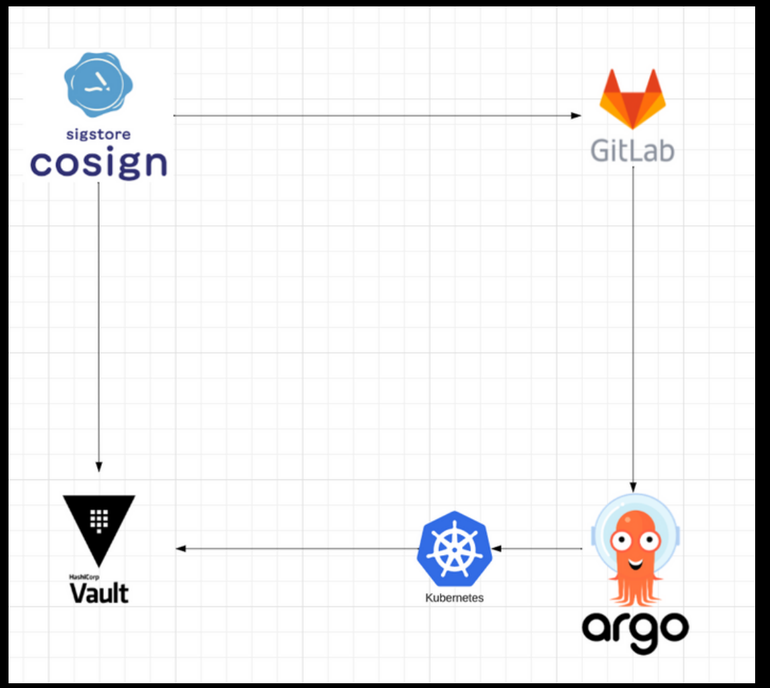
Revoke approval **Requires 2 more approvals from QA and Frontend.** Approved by

Collapse

| Approvers | | Pending approvals | Approved by |
|---|---|---|---|
| QA | 1 more | 1 of 2 | |
| Frontend | | 0 of 1 | None |
| Backend | 4 more | 1 of 1 | |

# Image signing



# S.W.O.T Анализ

## Сильные стороны

- Инвенторизация из коробки
- прозрачность
- аварийное восстановление (DR)
- сведение к минимуму человеческого фактора

## Слабые стороны

- нужен опыт в командах
- затраты на внедрение
- сложности интеграции с собственной автоматизацией

## Возможности

- внутренний IaC с открытым исходным кодом для компании
- Ревью и QA
- уменьшение ttm

# Риски и угрозы

- Git - единая точка доступа
- FP в отчетах SAST
- Ошибки конфигурации
- Управление зависимостями

- Внутренний нарушитель
- Сложно внедрить
- Единая точка отказа

# В реальной жизни

## Экспертиза

Существует много новых подходов, которые необходимо изучить

## Процессы

Специфика процессов внутри компании

## Имидж “бренда”

Восприятие организационных проблем как проблем подхода


Q&A

# Thank you for attention!

alexander.sungurov@exness.com

@Banzay021

anton.turenskiy@exness.com

@totofka

Opensource repository