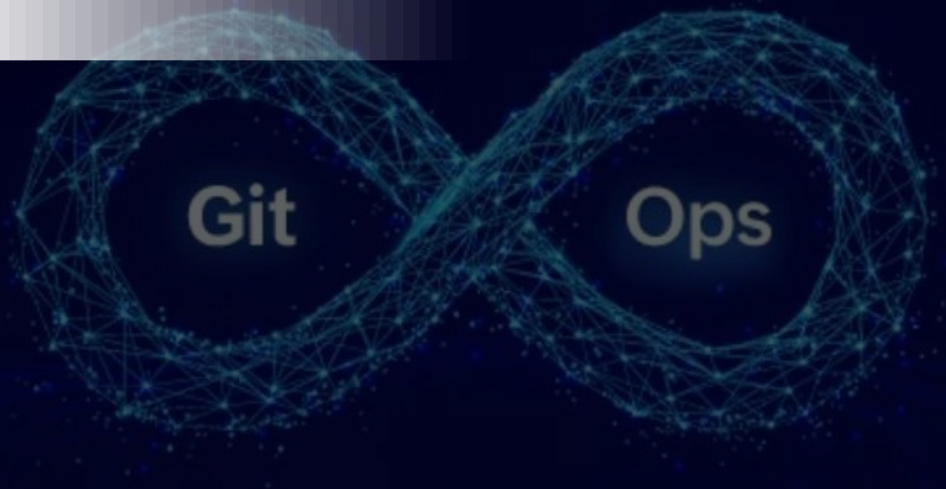
ЭР·ТЕЛЕКОМ

Детектирование атак и подход GitOps



Владимир Звонарёв
Архитектор SOC R-X

vladimir.zvonarev@r-x.team

Кратко о себе

Владимир Звонарев:

- Архитектор коммерческого SOC «ЭР-Телеком Холдинга» (R-SOC)
- Развитие архитектуры SOC, разработка новых сервисов SOC

План доклада

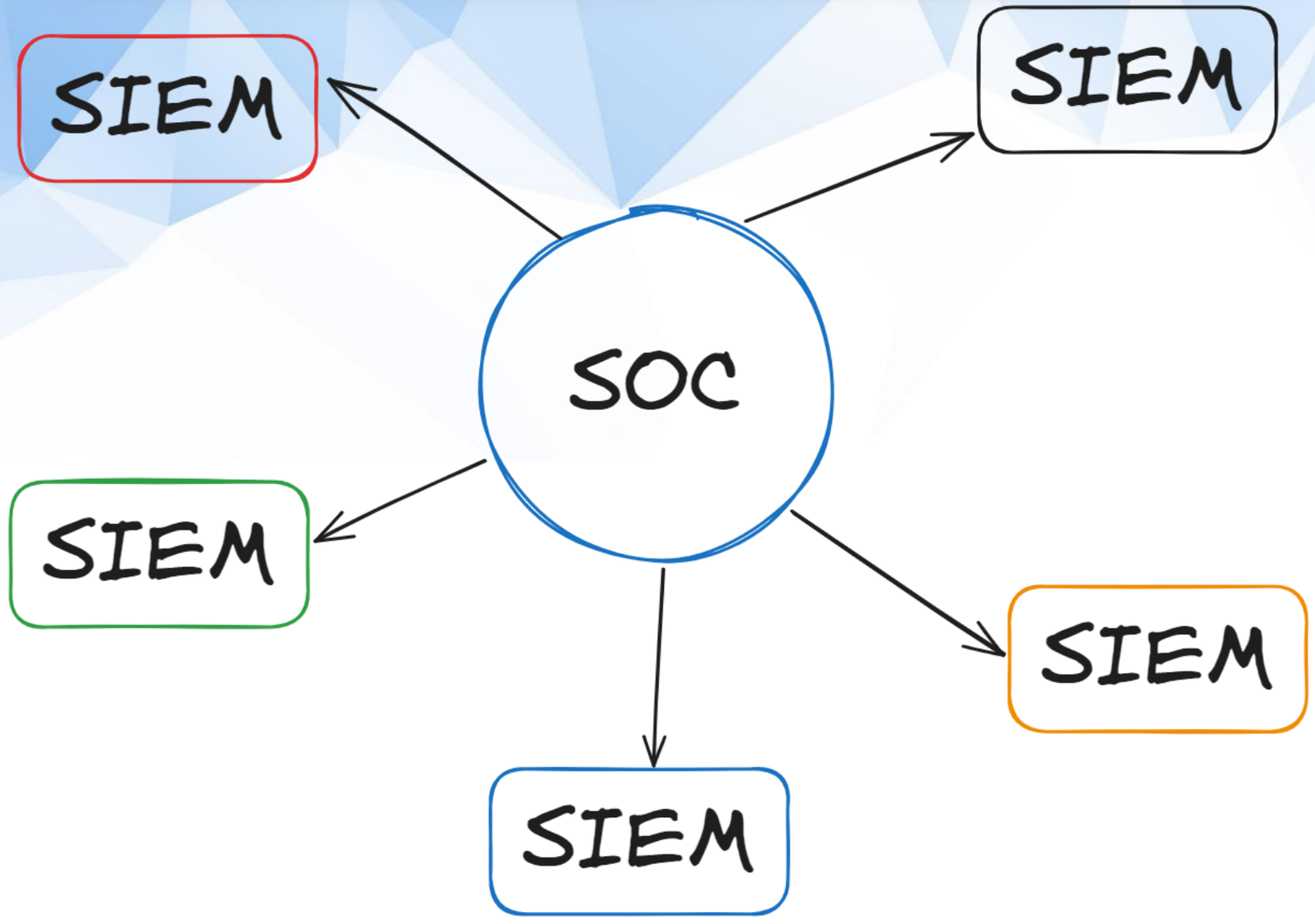
- Актуальность проблематики
- SIEM. Традиционный подход к разработке и управлению правилами
- Что такое GitOps?
- GitOps и SIEM
- Инструменты и методы для автоматизации и контроля изменений в правилах детектирования.
- Пример использования GitOps в SIEM (RuSIEM, Splunk).
- Управление безопасностью в GitOps
- Проблемы при внедрении GitOps в SIEM
- Перспективы развития и рекомендации.

Актуальность SOC растет

ЭР-ТЕЛЕКОМ

- Дефицит квалифицированных специалистов по ИБ
- Нет уверенности в безопасности конфиденциальных данных
- Необходимость соблюдения требований №152–ФЗ, №187-ФЗ
- Большие затраты на организацию собственного SOC
- Рост и повышение уровня сложности кибератак
- Необходимость круглосуточного мониторинга и поддержки экспертов по ИБ

SOC + SIEM проблематика



Проблематика:

- Множество различных SIEM у Заказчиков, подключаемых в наш SOC
- Правил «из коробки» недостаточно
- >10 тысяч различных типов объектов мониторинга, требующих написания своих правил детекции для различных SIEM
- Необходимость быстрого применения новых правил на всех SIEM


Что такое
GitOps?

Определение GitOps

GitOps — методология, основанная на принципах Git и автоматизации в управлении инфраструктурой и кодом.

Преимущества:

- Автоматизация
- Конвергентность
- Детерминизм
- Наблюдаемость
- Аудит
- Безопасность

Примеры инструментов:

- GitLab, Vault, Pipeline
- Dockers
- Custom scripts


GitOps
и SIEM

SIEM. Традиционный подход к разработке и управлению правилами

ЭР-ТЕЛЕКОМ

1. Получение первоначальных данных
2. Проверка наличия необходимых событий от источников
3. Выявление индикаторов компрометации, ключевых слов, критериев сработок
4. Написание правила в соответствии с индикаторами
5. Проверка работоспособности правила, эмулирование атаки
6. Раскат правила в прод
7. Доработка правила, уменьшение количества ложных срабатываний

SIEM. Традиционный подход к разработке и управлению правилами

ЭР-ТЕЛЕКОМ

Правила детектирования в контексте SIEM

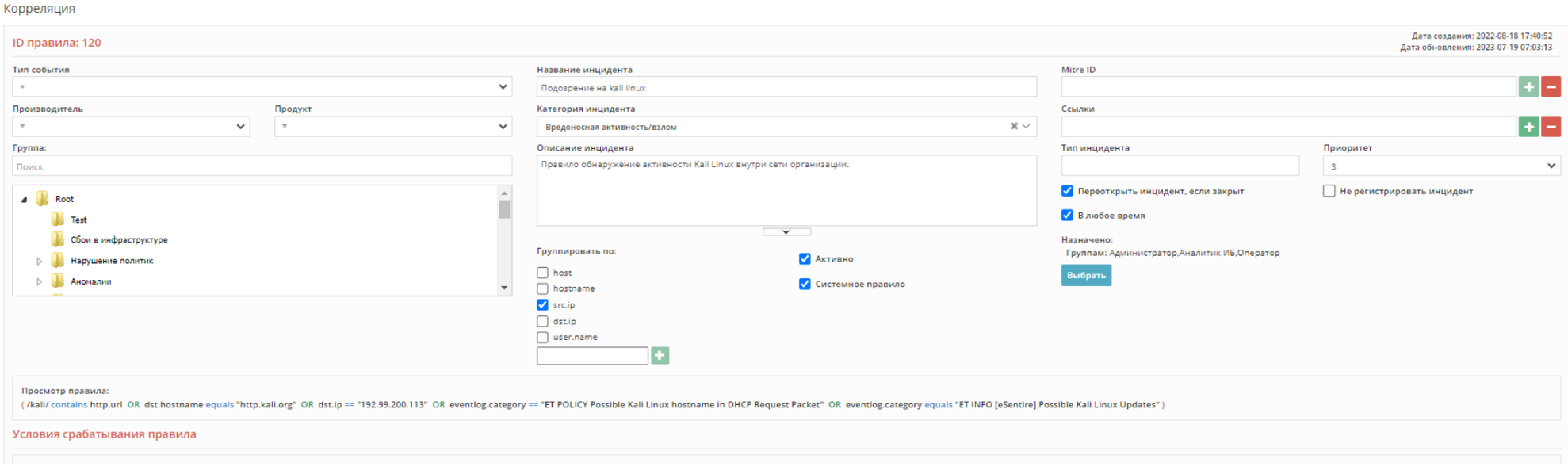
Splunk

Search | Metrics | Datasets | Reports | Alerts | Dashboards

Alert_ERTH_bruteforce_vpn

```
index=paloalto event_id=globalprotectportal-auth-fail OR event_id=globalprotectgateway-auth-fail | stats count by user, src_ip | where count>10
```

RuSIEM



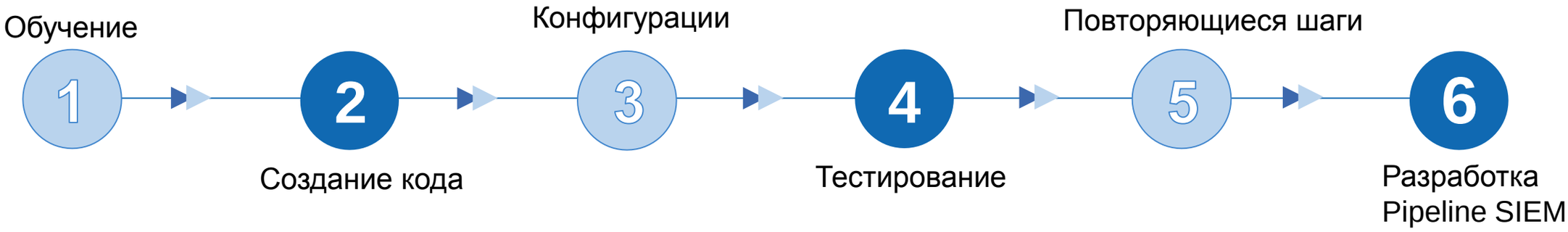
Применение подхода GitOps к разработке контента для SIEM

ЭР-ТЕЛЕКОМ

Использование GitOps в разработке правил детектирования:

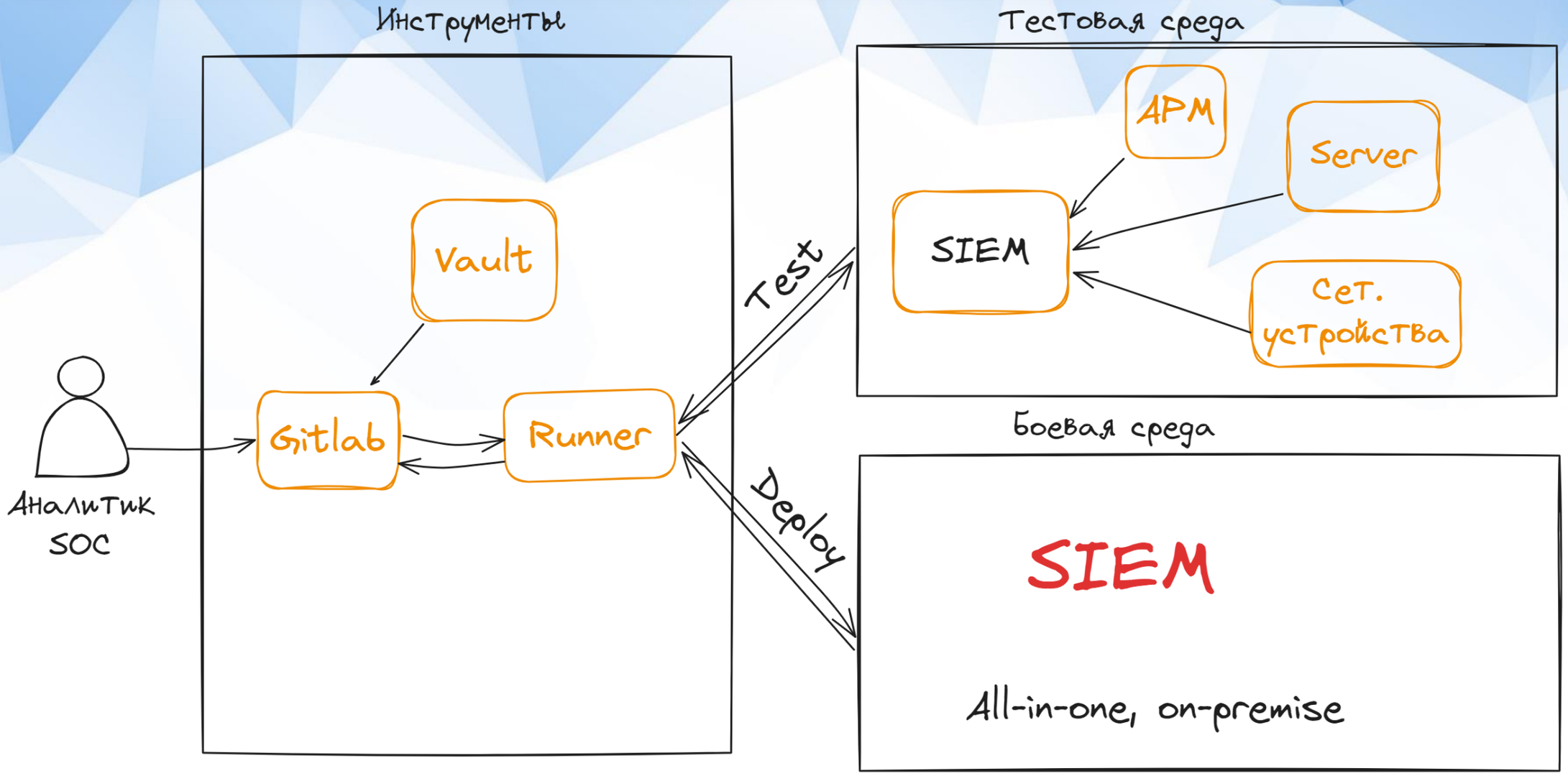
- помогает командам аналитиков сосредоточиться на разработке контента
- оптимизирует совместную работу по разработке сложных правил детектирования угроз
- позволяет быстро и с упором на качество развертывать правила корреляции в различных SIEM
- снижает ручной труд
- создается единая база и максимально полная правил детектирования

Основные шаги внедрения GitOps в процесс разработки SIEM правил детектирования:

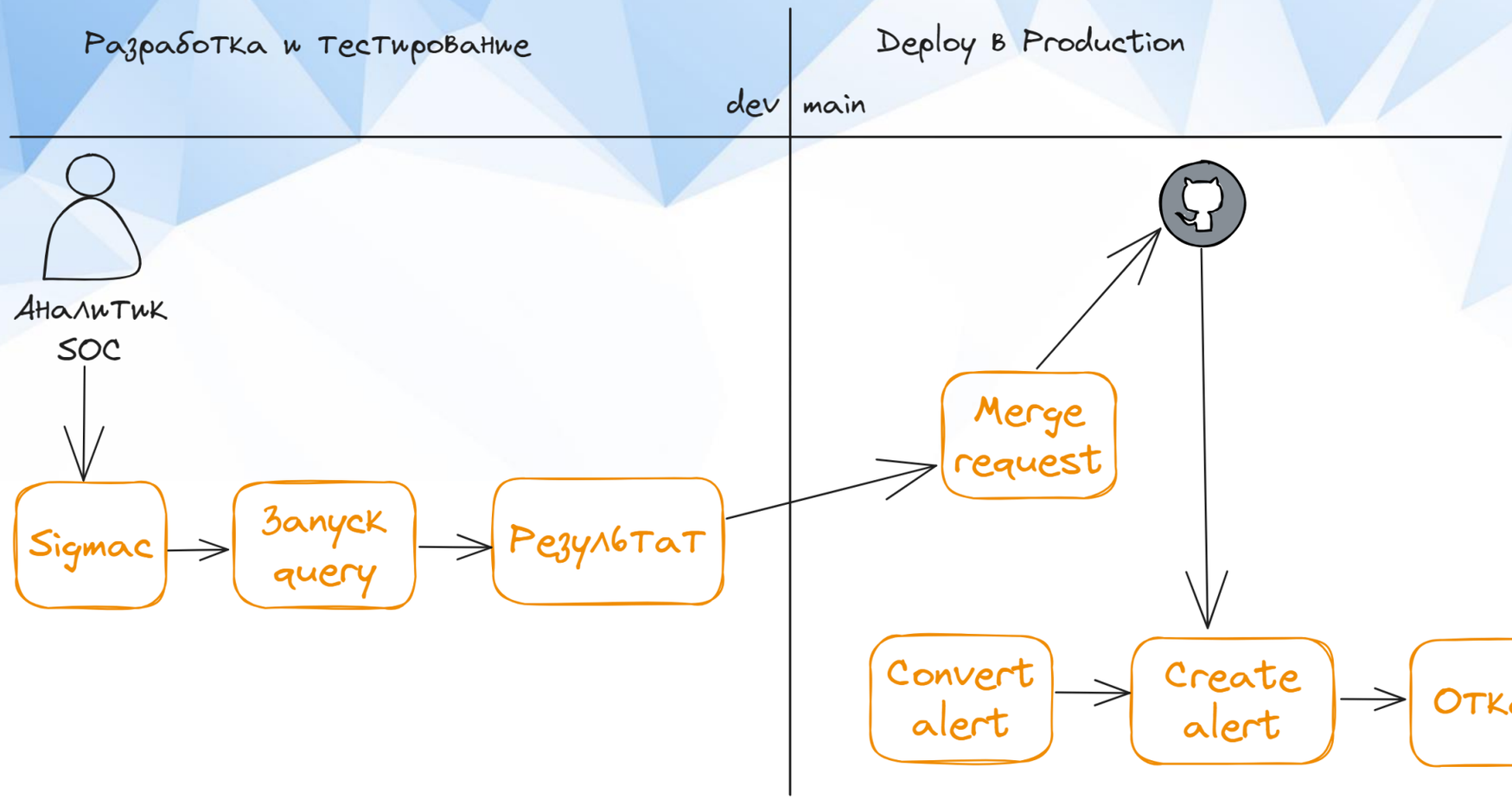


Инструменты и методы для автоматизации и контроля изменений в правилах детектирования

ЭР-ТЕЛЕКОМ

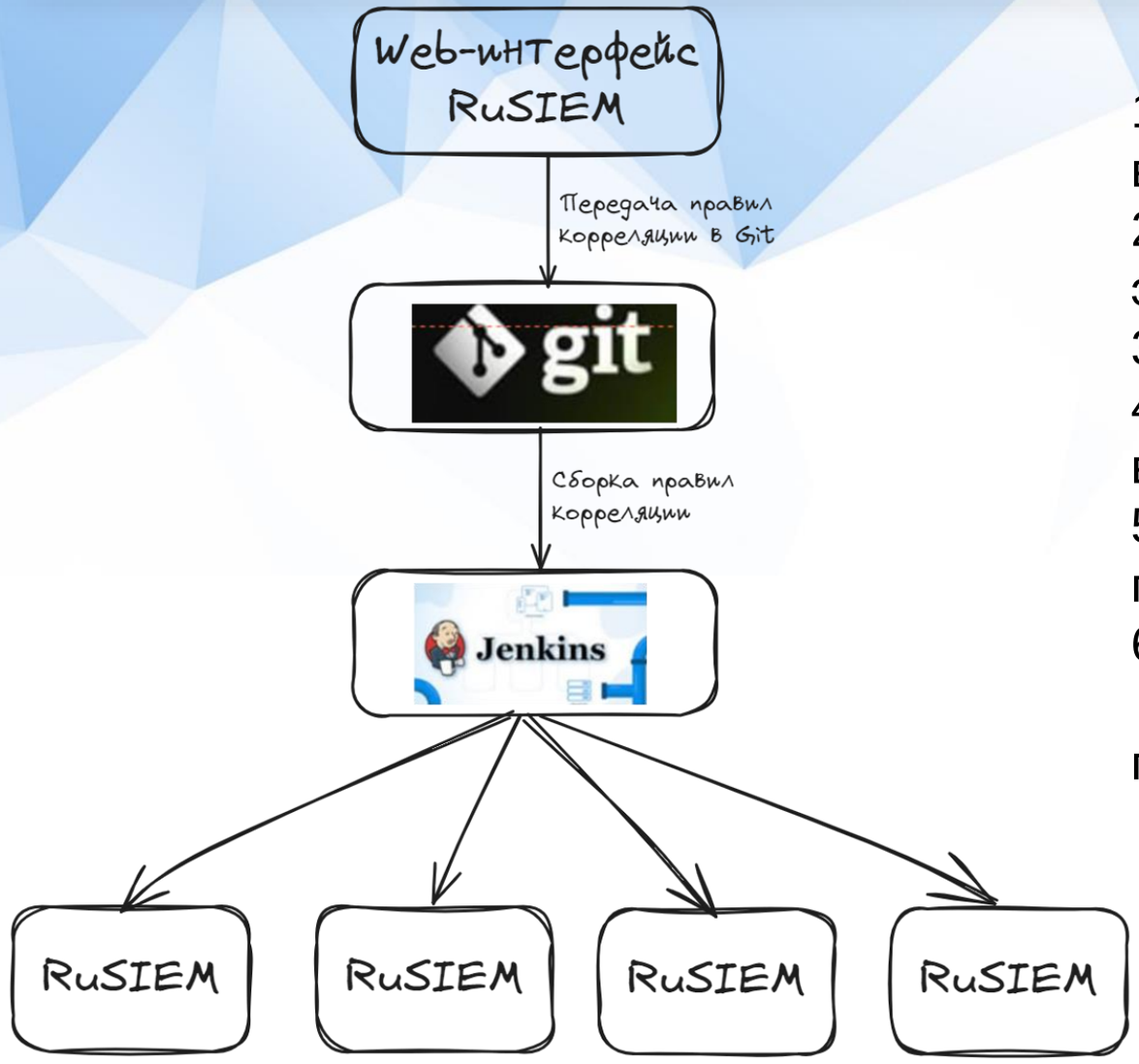


Пример использования GitOps в SIEM



Счастливый аналитик

Пример использования GitOps в RuSIEM



1) Создание правила корреляции в web-интерфейсе Rusiem
2) После все отладок и тестирований экспорт правила в файл (в yaml формате)
3) Размещение файлов в git репозиторий
4) По коммиту автоматическая сборка всех правил
5) Передача собранного файла на сервер, где установлен Rusiem
6) Импорт файла в систему

пункты 4-6 выполняются автоматически

Возможные проблемы при внедрении GitOps в SIEM

№	Проблема	Как решаем
1	Невозможно управлять системными сущностями (правила корреляции)	Используем пользовательские правила
2	Поля событий разные	Создаем систему мэппинга полей источников событий
3	Отсутствие в SIEM функционала по загрузке контента	Выполнение доработок совместно вендором SIEM
4	Собственные форматы описания и загрузки правил у SIEM	Создаем конверторы под типовые SIEM (MaxPatrol и т.п.)
5	Отсутствие знаний персонала по работе с Git	Внедрение практики разработки в Git-е
6	Удаление контента через Git	Запрос вендору SIEM на доработку 2024 год (RuSIEM)

Наш опыт успешных кейсов использования GitOps в SIEM

1. Сокращение времени разработки и применения правил корреляции в разы
2. Организация совместной разработки контента с Клиентом в нашем репозитории
3. Использования подхода для разработки правил для SIEM Splunk.

уже разработано более 400 правил

Перспективы развития

- Разрабатываем продукт, применимый для различных классов решений

ЭР-Телеком - провайдер услуг информационной безопасности

ЭР·ТЕЛЕКОМ

15+ продуктов в линейке

50+ экспертов в команде

>99,7 SLA доступности услуг

45 гбит/с самая мощная отраженная атака в 2022 г.

24/7 экспертная поддержка

3 000+ клиентов услуг ИБ по всей России

Линейка продуктов для всех сегментов клиентов

Для государственных организаций
Реализации программ по ИБ

Для крупного бизнеса
Поставщик комплексных решений по ИБ

Для среднего и малого бизнеса
Поставщик доступных решений ИБ

OTT продукты

- ✓ 14 продуктов доступны вне инфраструктуры ЭРТХ

Импортонезависимость

- ✓ Только отечественные решения
- ✓ Проводим миграции

Все необходимые лицензии по оказанию услуг ИБ

- ✓ Лицензия ФСБ
- ✓ Лицензия ФСТЭК

Собственный коммерческий центр кибербезопасности (SOC)

- ✓ Мониторинг событий ИБ 24x7
- ✓ Реагирование на инциденты
- ✓ > 3,8 млн анализируемых событий ИБ в сутки
- ✓ Взаимодействуем с

БАНК РОССИИ ФИНЦЕРТ

- ✓ Статус Корпоративного центра

ГОССОПКА НКЦКИ

Ваши вопросы

Контакты

Владимир Звонарёв

Архитектор SOC

vladimir.zvonarev@r-x.team

https://r-soc.ertelecom.ru/