PHDAYS FEST
от positive technologies

SOC
на скорую руку

Внедряем гибридную модель
или наш опыт по выживанию

Сергей Бнятов

1. Больше 9 лет делаю «пу пу пу» в сфере ИБ.
2. Должен был быть разработчиком, но предал братство и ушёл к душным ибэшникам.
3. Начал карьерный путь в пентестах / Red Team, шатая инфру этими вашими mimikatz'ми.
4. На 4 года задержался в AppSec.
5. И вот строю SOC.

Ритейл реального времени в цифрах

Мы делаем ИТ-решения
для ритейла.

На наших технологиях
работают Самокат и Мегамаркет.

711 тысяч

выполненных заказов
из Самоката в день*.

129 городов

быстрая доставка продуктов
и товаров из Самоката.

ecom.tech

* среднее количество выполненных заказов в день в 2024 г.
по данным отраслевого обзора INFOLine E-Grocery Russia TOP №4 2024.

План, о чём поговорим

01 У нас было...

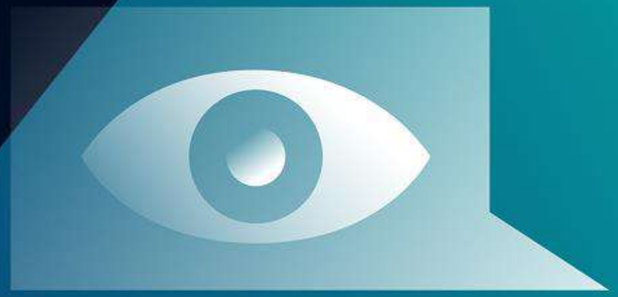
02 Как выбирать MSSP-провайдера

03 Текущая модель нашего SOC

04 Что «под капотом» у нас сейчас?

05 Итоги

Проблемы



Исходная ситуация

У нас было...

3 (сейчас уже 4)

независимых инфраструктуры
с разными ландшафтами.

3

разных команды
эксплуатации и поддержки.

3 месяца

для запуска единого процесса
мониторинга и реагирования
на инциденты.

Основные проблемы

Необходимость выстроить независимый процесс реагирования на кибер-инциденты.

01

Выбрать MSSP-провайдера и интегрироваться с провайдерами, которые уже работали.

02

Ограниченные сроки для реализации единого процесса.

03

PHDAYS FEST
от positive technologies

Как выбрать MSSP SOC?

Какие критерии выбора?

Коммерческие требования

- Условия договора и порядок оказания услуг.
- NDA.
- Возможность гибкого масштабирования.
- etc.

Технические требования

- Возможность самостоятельной регистрация инцидентов.
- Наличие в личном кабинете доступа к данным по API.
- Выделение связанных инцидентов в кейсы.
- Время обнаружения и регистрация инцидента не более 15 минут 24/7 в автоматическом режиме.
- Возможность передачи IOC от заказчика в SOC и правила оповещения при обнаружении указанных IOC.
- etc.

Идеальных SOC

не бывает

Идеальных SOC

не бывает

как и MSSP

Обратите внимание

На отсутствие контекста у аналитика MSSP SOC о вашем окружении и контексте инцидента.

Разный взгляд аналитиков на одну и ту же проблему.

Гибкость вашего MSSP SOC.

Доступ к сырым логам, которые вы отдаёте.

Внимание к деталям, быстрая доработка кастомных правил и кейсов.

Понятный SLA для вас и для MSSP.

Готовую интеграцию с вашей тикет-системой, например, Jira.

Текущая модель SOC

POSITIVE HACK DAYS FEST

от positive technologies

Что такое гибридный SOC?

MSSP

Мониторинг и первичное реагирование 24/7.

Накопленный опыт по триажу и первичному анализу с возможностью масштабироваться.

Свой сильный технический стек.

Единый MSSP на все сервисы

In-house team

Понимание контекста бизнес-процессов.

Понимание и опыт взаимодействия между подразделениями в компании и бизнесом.

Глубокий процесс расследования, атрибутирование.

Команда:

- Направление по реагированию и расследованию киберинцидентов.
- Направление по автоматизации и инженерным практикам.

Цели гибридной модели:

Синергия между командами

Оптимизация процессов

Возможность быстрого старта

Плюсы гибридной модели

In-house SOC

Собственная команда SOC/IR

- Немедленный доступ к информации.
- Полный контроль над расследованиями.

Глубокое знание бизнес-контекста

- Точный триаж, меньше ложных срабатываний.
- Приоритизация критичных активов, возможности примирения мер исходя из бизнес-контекста.

Кастомизация плейбуков и процедур

- Процессы «под нас», быстрая адаптация.
- Оперативное внесение изменений.

MSSP

24/7 мониторинг и первичный анализ

- Непрерывное покрытие без «окон слепоты».
- MSSP берёт на себя рутинный триаж.

Масштабируемые ресурсы и автоматизация

- Быстрое наращивание мощностей.
- Подключение новых интеграций «на лету».

Широкий спектр источников угроз и опыта

- Общая Threat intelligence и IOC.
- Обмен лучшими практиками и накопленный годами опыт по многим клиентам.

Минусы гибридной модели

Категория	Минус	Описание
Процессы	Координация и эскалация.	Требуется постоянно синхронизировать in-house и MSSP, часто неочевидно, кто и когда должен эскалировать инцидент.
	Расплывчатые зоны ответственности.	Чёткие границы между L1 (MSSP) и L2/L3 (in-house) не всегда прописаны — инциденты могут «зависать».
Техника	Интеграция логов.	Согласовать форматы и каналы доставки логов между внутренними системами и MSSP сложно и затратно.
	Обработка кастомных логов.	MSSP часто не умеет «из коробки» разбираться с вашими специфичными продуктовыми логами — требуется ручная доработка.
	Зависимость от SLA провайдера.	Любые сбои или изменения в SLA MSSP сразу отражаются на скорости реагирования и качестве обработки инцидентов.
Управление	Повышенные затраты.	Удержание собственной команды плюс оплата MSSP, а также расходы на интеграцию и администрирование.
	Управленческая нагрузка.	Менеджерам приходится контролировать два параллельных потока работ и держать постоянную связь с внешним провайдером.

В разрезе линий

Линия	Кто	Ключевая роль в приоритизации
L1	MSSP SOC	Первичное выявление, фильтрация, SLA на триаж.
L2	SOC Team	Контекстуализация, приоритизация, эскалация / отклонение. Решение, анализ последствий, корректировки процессов.
L3	Security / IT	Выполнение конкретных технических мер, участие в LLE.

Wake up Neo...

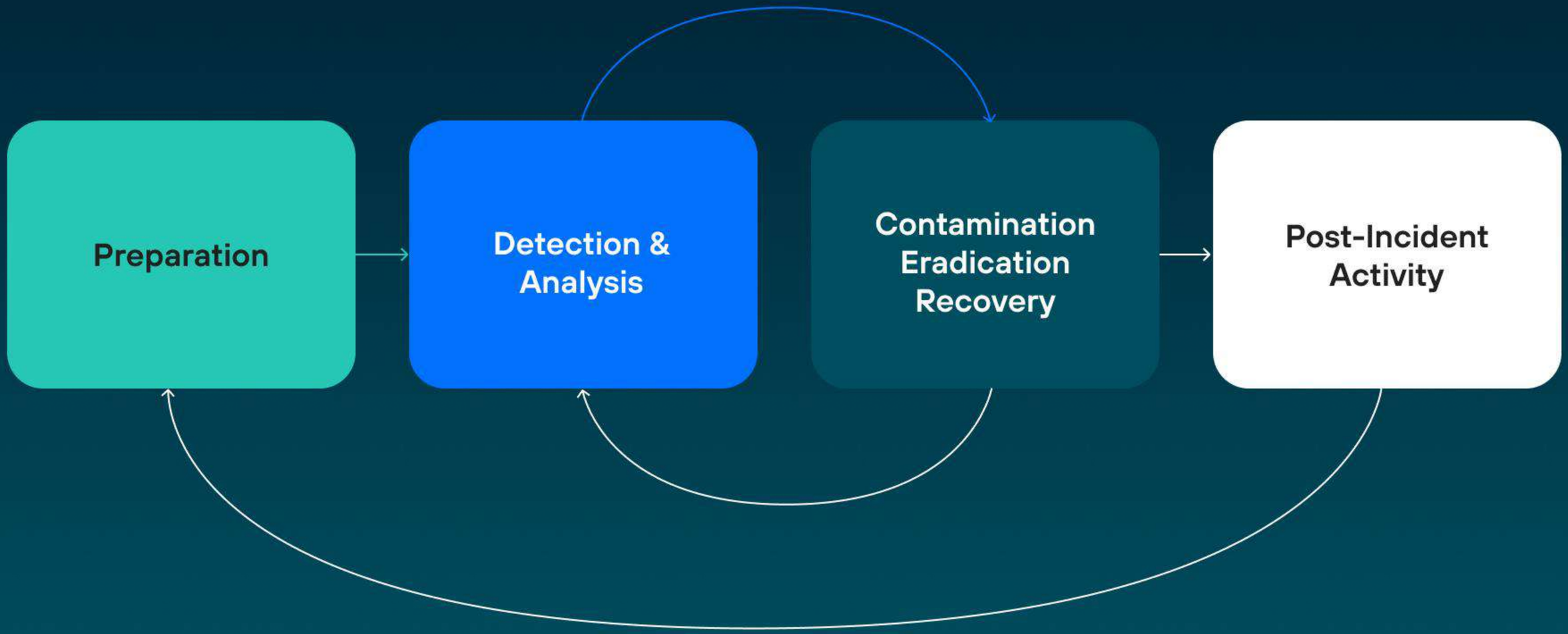
Матрица эскалации

Приоритет / Лицо	MSSP	Support Applications 3-я линия: Infra / products	IT-инфра-структура	ИБ	IRT: ИБ, ИТ, IRT MSSP
Критический	Шаг 1	Шаг 1 →	Шаг 2 →	Шаг 3 →	Шаг 4
K-SLA	SLA MSSP	1 час	1 час	1 час	1 час
Высокий	Шаг 1	Шаг 1 →	Шаг 2 →	Шаг 3 →	Шаг 4
B-SLA	SLA MSSP	2 часа	2 часа	1 час	2 часа
Средний	Шаг 1	Шаг 1 →	Шаг 2 →	Шаг 3 →	–
C-SLA	SLA MSSP	4 часа	4 часа	2 часа	–
Низкий	Шаг 1	Шаг 1 →	–	–	–
H-SLA	SLA MSSP	8 часов	–	–	–

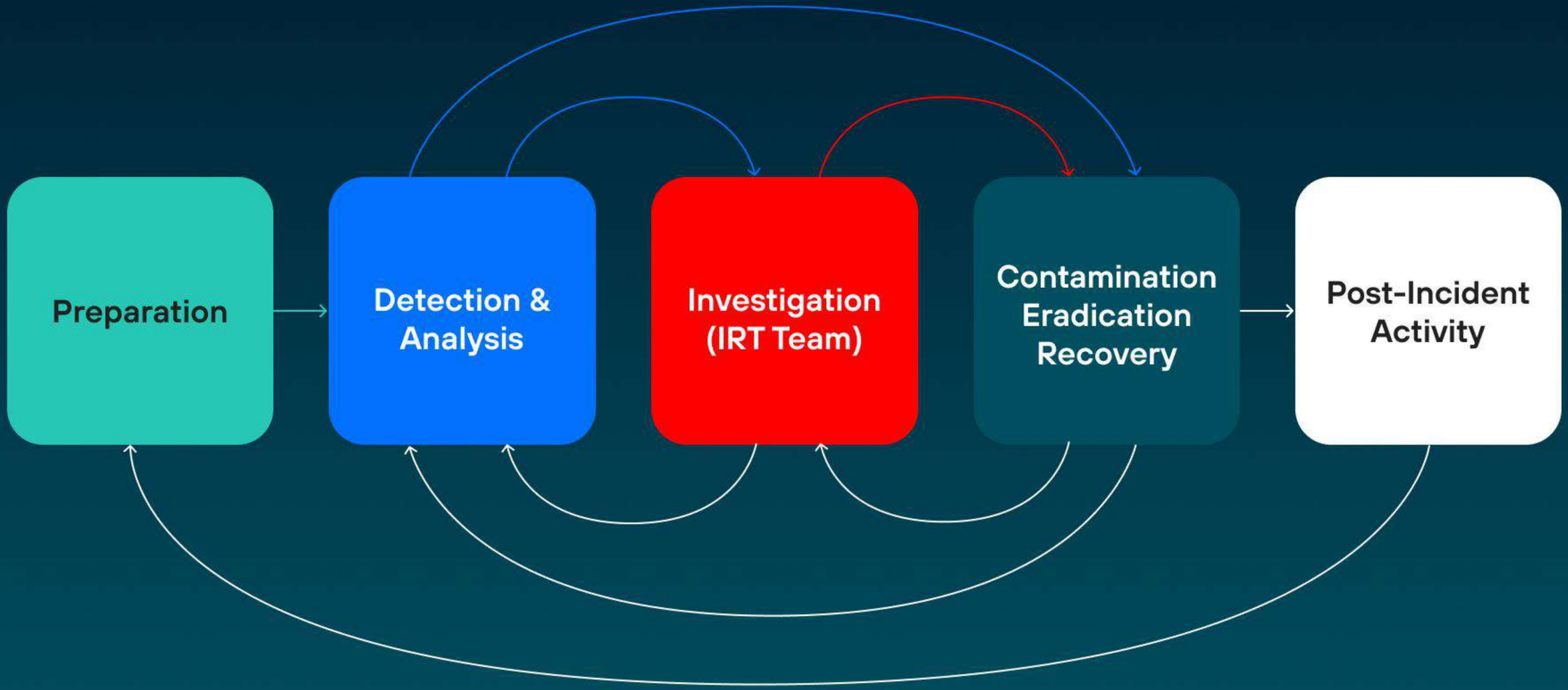
Матрица уведомлений

Приоритет / Лицо	Support Applications 3-я линия	IT-инфра-структура	ИБ	Владелец продукта
Критический	Да	Да	Да	Да
Высокий	Да	Да	Да	Нет
Средний	Да	Да	Нет	Нет
Низкий	Да	Нет	Нет	Нет

Типовой


Preparation
Detection & Analysis
Contamination Eradication Recovery
Post-Incident Activity

Нетиповой


Preparation
Detection & Analysis
Investigation (IRT Team)
Contamination Eradication Recovery
Post-Incident Activity

PHDAYS FEST
от positive technologies

А что «под капотом»?

Я и печник, и плотник, и на мышей охотник...

Необходимо

- реагировать на инциденты
- развивать инженерные практики
- постоянно пополнять базу playbook's и knowledge
- автоматизировать рутину
- оптимизировать процесс реагирования
- управлять командой
- следить за метриками
- пушить задачи команды в другие отделы
- пушить другие команды
- проводить учения
- писать отчёты по инцидентам
- ааааааааааааааа

и так далее...

Автоматизируем

Управление источниками событий

Управление источниками событий в условиях работы с MSSP-провайдером, агрегация информации об источниках, подсчёт покрытия EDR.

01

Управление активами

Агрегация информации о серверах и рабочих станциях в едином окне управления активами.

02

Флоу маршрутизации инцидентов

Путь инцидента от MSSP-провайдера до аналитика, механизм автоназначения инцидентов, управление очередью аналитиков.

03

Подсчёт метрик

Автоматизированный подсчёт метрик, бот для получения метрик по различным параметрам.

04

Управление источниками событий и активами

PHDAYS FEST
от positive technologies

Проблема

Таблица с информацией об источниках заполняется руками.

01

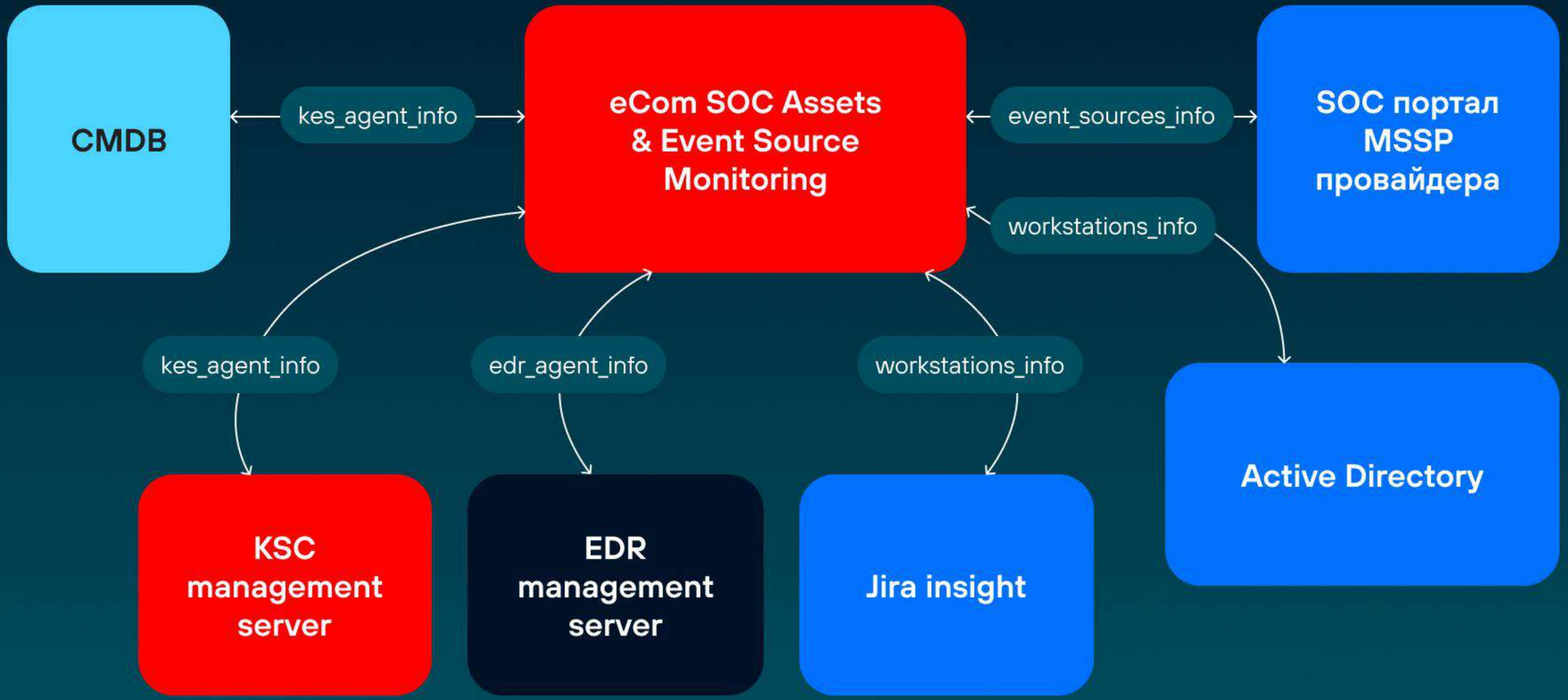
Необходимая нам информация о хостах находится в разных местах.

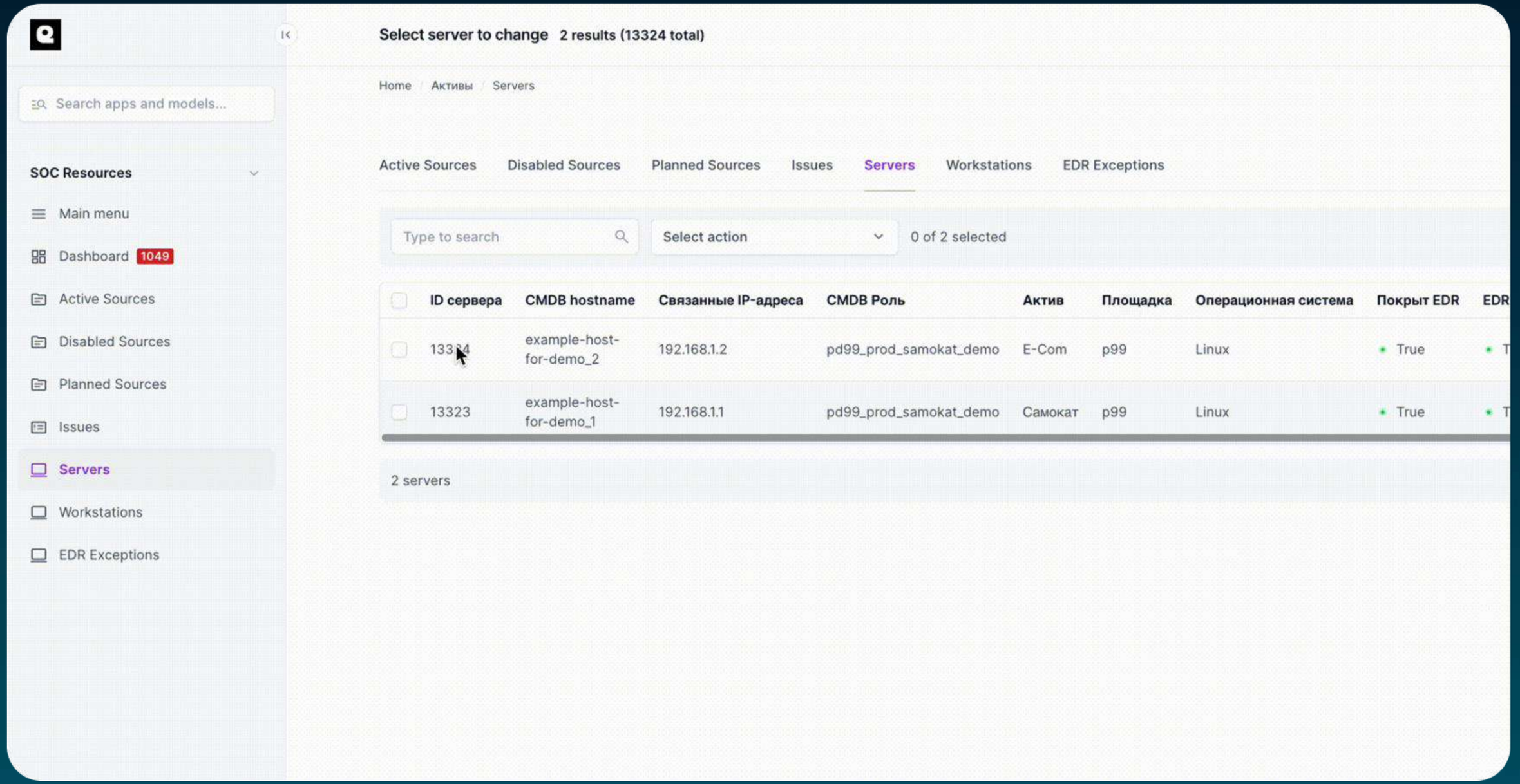
02

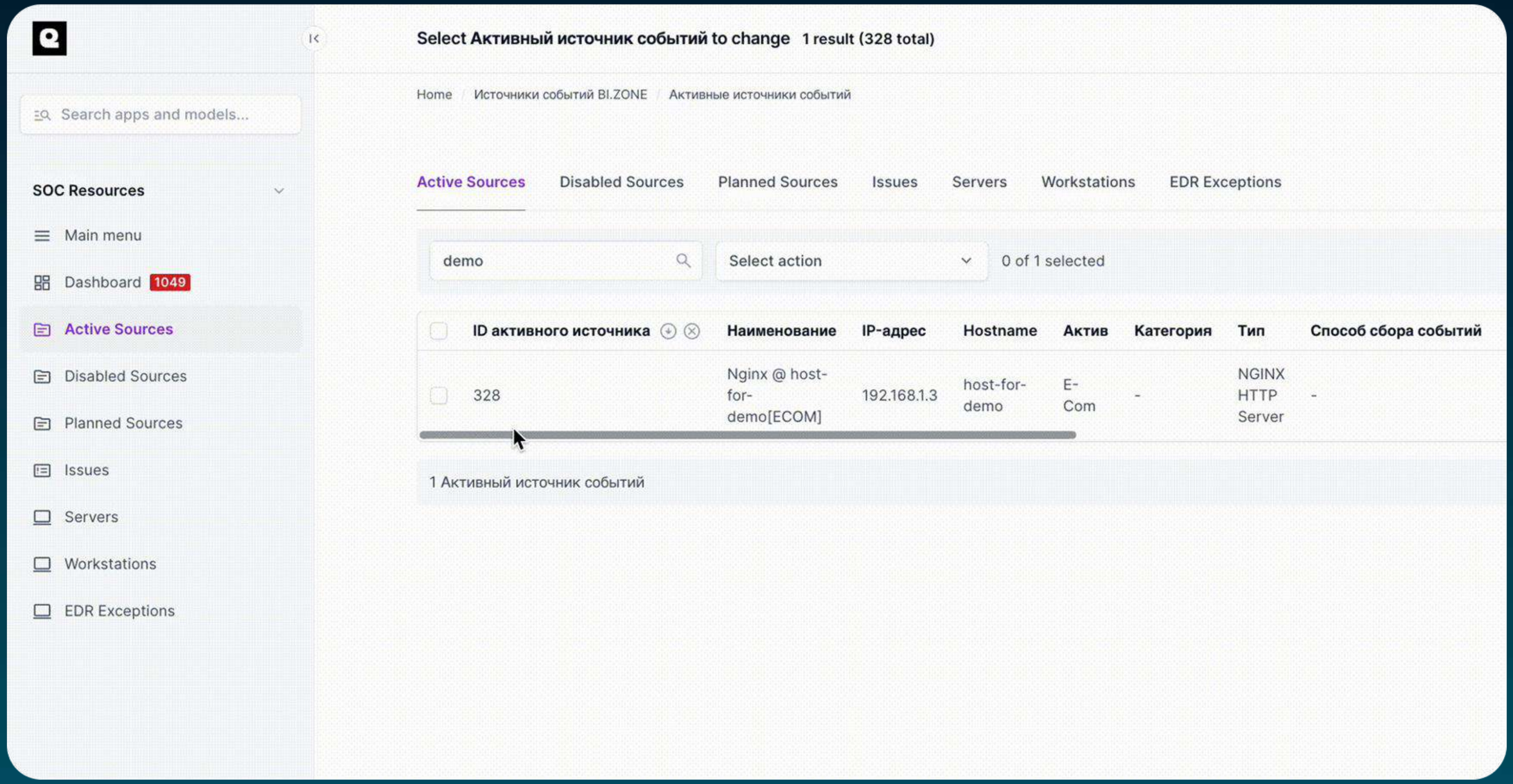
Отсутствие механизма подсчёта покрытия хостов EDR-агентами.

03

Схема приложения




Select server to change 2 results (13324 total)
Search apps and models...
SOC Resources
Main menu
Dashboard 1049
Active Sources
Disabled Sources
Planned Sources
Issues
Servers
Workstations
EDR Exceptions
Home / Активы / Servers
Active Sources
Disabled Sources
Planned Sources
Issues
Servers
Workstations
EDR Exceptions
Type to search
Select action
0 of 2 selected
ID сервера
CMDB hostname
Связанные IP-адреса
CMDB Роль
Актив
Площадка
Операционная система
Покрыт EDR
EDR
13324
example-host-for-demo_2
192.168.1.2
pd99_prod_samokat_demo
E-Com
p99
Linux
True
13323
example-host-for-demo_1
192.168.1.1
pd99_prod_samokat_demo
Самокат
p99
Linux
True
2 servers


Select Активный источник событий to change 1 result (328 total)
Search apps and models...
SOC Resources
Main menu
Dashboard 1049
Active Sources
Disabled Sources
Planned Sources
Issues
Servers
Workstations
EDR Exceptions
Home / Источники событий BI.ZONE / Активные источники событий
Active Sources
Disabled Sources
Planned Sources
Issues
Servers
Workstations
EDR Exceptions
demo
Select action
0 of 1 selected
ID активного источника
Наименование
IP-адрес
Hostname
Актив
Категория
Тип
Способ сбора событий
328
Nginx @ host-for-demo[ECOM]
192.168.1.3
host-for-demo
E-Com
-
NGINX HTTP Server
-
1 Активный источник событий

Результат

Единое окно для управления источниками и активами.

01

Возможность получать агрегированную информацию об активах и источниках из одного приложения по API.

02

Автоматизированный подсчёт покрытия серверов и рабочих станций EDR-агентами.

03

Флоу маршрутизации инцидента и подсчёт метрик

Проблема

Инциденты от MSSP-провайдера видим только в почте и портале.

01

Аналитики берут инциденты в работу в случайном порядке.

02

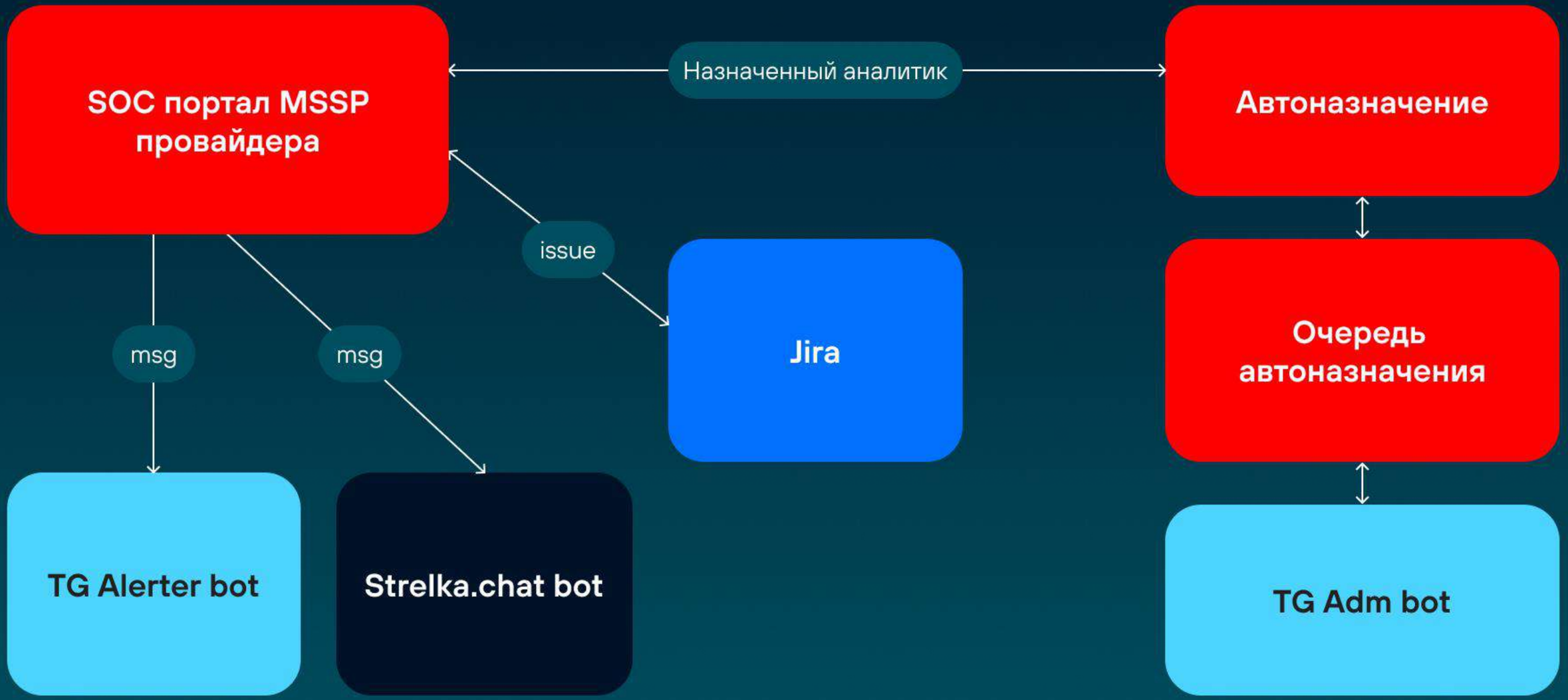
Нет возможности управлять нагрузкой на аналитиков.

03

Нет конкретных метрик работы аналитика и способов их подсчёта.

04

Флоу маршрутизации инцидентов



Alerter bot

Alerter SOC portal
INC
Время создания инцидента:

Критичность: Medium 🟡

Описание: Успешное подключение из сети публичного VPN-сервиса от хоста

Полное описание:

Ссылка на инцидент

Инцидент назначен на :

Аналитик подтвердил авто-назначение инцидента в 2025-05-05 19:03:22

Инцидент назначен на :

Статус инцидента : Customer completed

Adm bot

/get_current_line Получить текущую очередь авто-наз...

/add_to_line Добавить аналитика в очередь авто-назн...

/rm_from_line Исключить аналитика из очереди авто-...

/add_to_duty Назначить дежурного аналитика

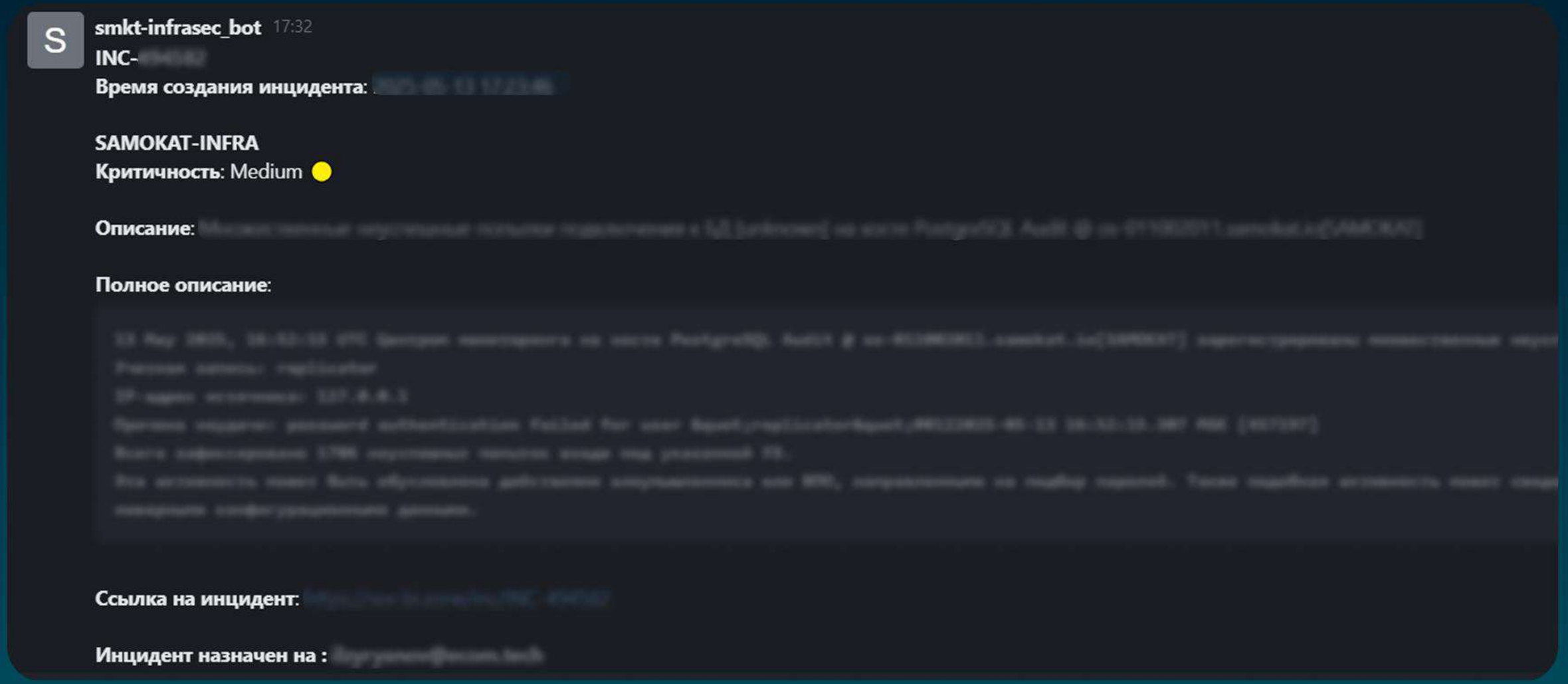
/get_mssp_avg_registration_time Получить метрику MS...

/wh_get_common_avg_solve_time (WH) Получить общу...

/wh_get_common_avg_reaction_time (WH) Получить о...

/get_audit_avg_reaction_time Получить общую метрик...

Когда Telegram было плохо...



Результат

Инциденты от MSSP-провайдера видим в почте, портале, Telegram-боте и корпоративном мессенджере.

01

Инциденты автоматически назначаются на аналитиков, исходя из их доступности и загруженности.

02

Регулярно считаем конкретные метрики работы аналитиков, в любой момент можем получить к ним доступ в Telegram-боте.

03

А что в итоге нужно?

Runbook

«Это как план
на один матч»

- Пошаговая инструкция.
- Чётко описывает стандартные действия.
- Подходит для типовых задач (например, проверка IOC ручками).

Playbook

«Это как стратегия
на весь сезон»

- Описывает все этапы реагирования подробно.
- Подходит для сложных / нетиповых инцидентов.
- Помогает не упустить ничего важного.

Playbook as code

«Это как если бы игроки
исполняли план автоматически»

- Часть мер автоматизирована и выполняется автоматически напрямую в SOAR.
- Код от API СЗИ переиспользуется в разных сценариях.
- Можно встраивать как кирпичики и формировать новые Playbook's, используя уже написанный код или описание действий.

Комбинируем три подхода

01 Стандартизируем сценарии и подходы к ним.

02 Автоматизируем рутину, то, что может сделать код, должен делать код.

03 Сохраняем гибкость и масштабируемость.

Привет!

Испугался?

Я – ~~твой друг~~ продуктовый инцидент

Продуктовые инциденты

Проблемы		Что делаем (и рекомендуем)	
Боль	**Комментарий**	**Действие**	**Эффект**
01. Непонятно, кого звать	Нет закреплённых зон ответственности по продуктам	01. Фиксируем зоны ответственности	Связка продукт ⟷ владелец ⟷ ИБ
02. Информация разбросана	В Confluence, голове и логах — искать сложно	02. Собираем и структурируем инфу о продуктах	Формируем «паспорта» сервисов
03. Сложно вести таймлайн	Непрозрачно, кто и когда делает шаги	03. Автоматизируем таймлайн	Видно, кто и когда действует
04. Инциденты разные, не повторяются	Нет шаблонов, каждый кейс как впервые	04. Настраиваем процесс взаимодействия	Каналы, роли, правила коммуникации с ИБ
05. Неясно, что делать командам	ИБ эскалирует, но все теряются	05. Создаём плейбуки для нестандартных случаев	Быстрые действия по ключевым типам инцидентов
06. Созвоны ради созвонов	Время уходит, пользы мало		
07. Нет модели продуктов	Невозможно быстро понять, что за сервис под атакой	06. Привязываем продукты к инциденту автоматически	По логам, тегам, системам

Результат

Меньше хаоса | Понятные процессы | Быстрее реагируем | Лучше взаимодействуем с командами

На что обратить внимание

Заложите продуктовые кейсы сразу в архитектуру вашего SOC, продумайте, что храните, где и сколько.

01

Продуктовый инцидент — плейбук, это сильно облегчит жизнь.

02

Автоматизация «на коленке» для мониторинга продуктовых кейсов лучше, чем её отсутствие.

03

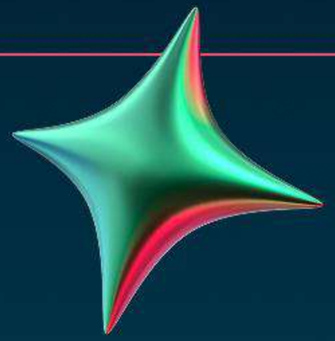
Метрики

Название	Описание	Значение
Coverage EDR	Процент покрытия инфраструктуры EDR-агентами.	> 95% инфраструктуры
Coverage SOC Sources	Процент подключённых источников событий к MSSP для значимых источников (которые имеет смысл подключать).	> 95% значимых источников
Mean time to reaction SOC	Среднее время реакции команды SOC на сформированный инцидент и его первичный анализ.	<= 1 hours
Mean time to contain	Среднее время применения мер по сдерживанию инцидента и его последствий.	CRITICAL – 60 min, HIGH – 120 min, MEDIUM – 8 hours, LOW – 12 hours
LLE time to report \ time to task	Среднее время на создание отчёта по инциденту, Среднее время выполнения задач в рамках пост инцидент активностей.	<= 3 days
Statistic	Статистика по инцидентам.	AS IS

Категоризация инцидентов: от хаоса к системе

phd X pt

Было



- Только две категории:

Manual Incident MSSP Incident

- Все инциденты шли по одному маршруту, не было различий, статистика неточна.

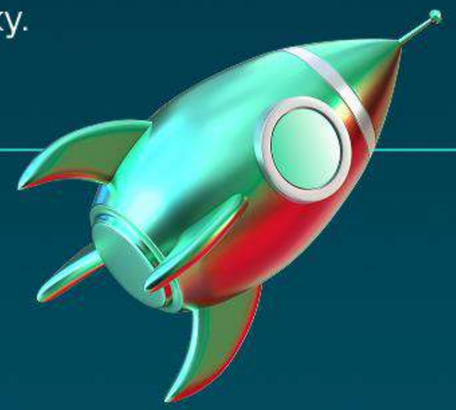
Стало

- 6+ категорий, каждый со своим флоу:

MSSP Manual Incident Internal Leaks

External Leaks Phishing ITHELP

- Каждая категория:
  - запускает нужный плейбук;
  - уходит нужной команде;
  - имеет свой SLA и аналитику.



Категория — это маршрут, SLA и смысл инцидента. Без неё — много шума.

Шесть советов себе, когда только начинал строить SOC

01 Пишите процессы так, как будете потом автоматизировать. Не превращайте playbook в сочинение.

02 Никогда не думайте, что процесс написан навсегда. Он устареет быстрее, чем вы успеете выдохнуть.

03 Развитие команды важно не меньше, чем SLA. Не будет людей — не будет SOC.

04 Инцидент — не лучшее время учиться. Учитесь до пожара или дорого заплатите.

05 Если можно делегировать — делегируйте. Не пытайтесь тащить всё на себе. Это не геройство, это ошибка.

06 SOC — это марафон. Не пытайтесь сжечь всё за квартал. Растите устойчиво. Системно. С холодной головой.

К чему хотим прийти в горизонте двух лет

Технологическая база (фундамент)

- Своя L1 24/7.
- Выстроенная шина доставки логов (для инфраструктуры и продуктов).
- Детектирующее и корреляционное ядро + контент.
- Внедрённый и настроенный SOAR.
- Внедрённая и настроенная TIP.

01

Процессы и инженерные практики

- Непрерывное улучшение Incident Response.
- Развитие инженерных практик: боты, единое окно, внутренняя автоматизация.
- Подняться на уровень абстракции в работе с продуктовыми инцидентами.

02

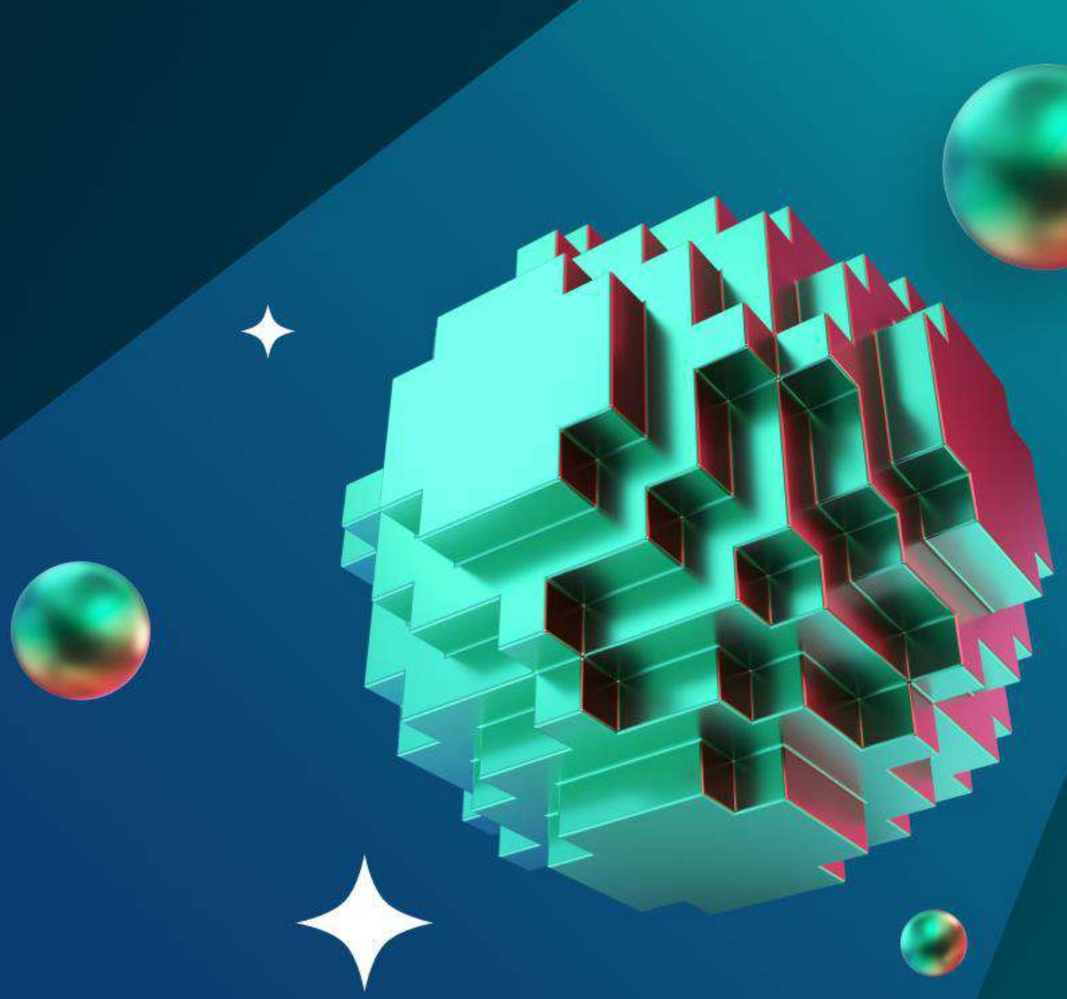
Стратегия и устойчивость

- Масштабируемая SOC-модель.
- Выстроенный баланс операционки и развития.
- И, конечно, выжить.

03

Эти цели — наш компас. Мы понимаем, что путь будет нелёгким, но именно туда мы хотим прийти.

Контакты и QR-коды

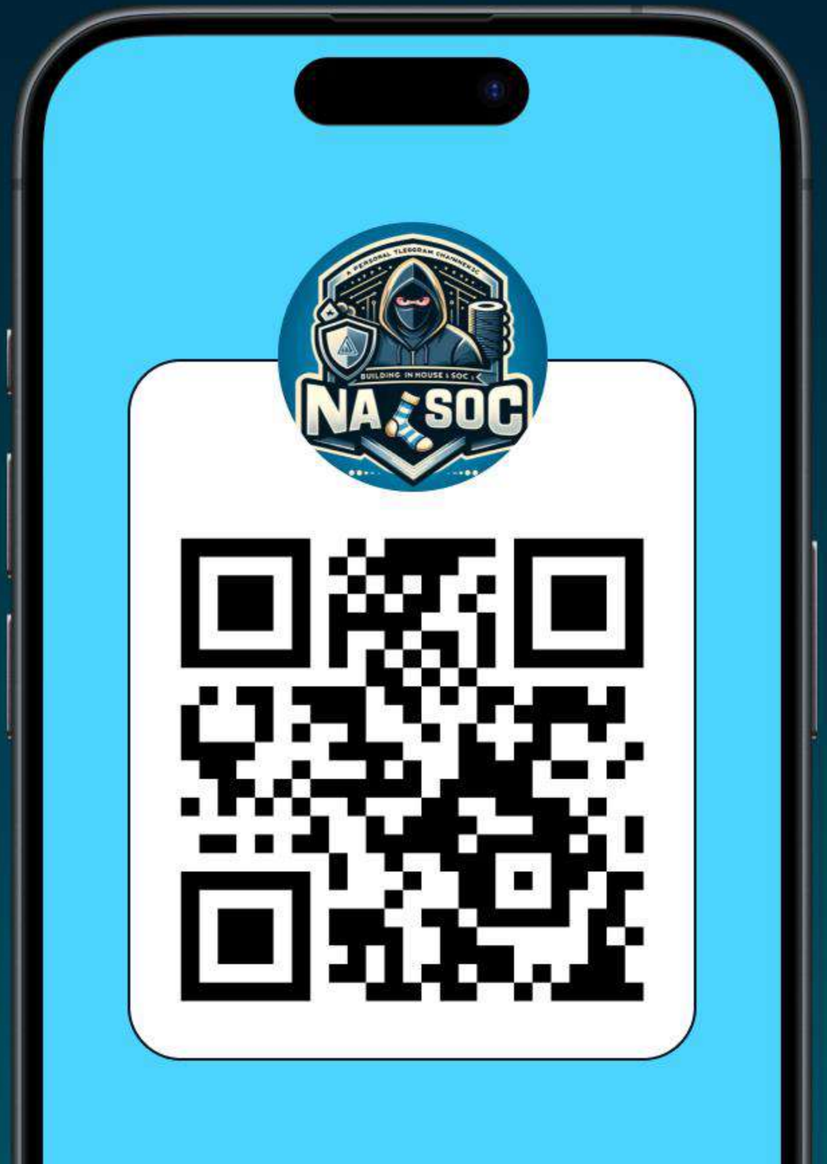


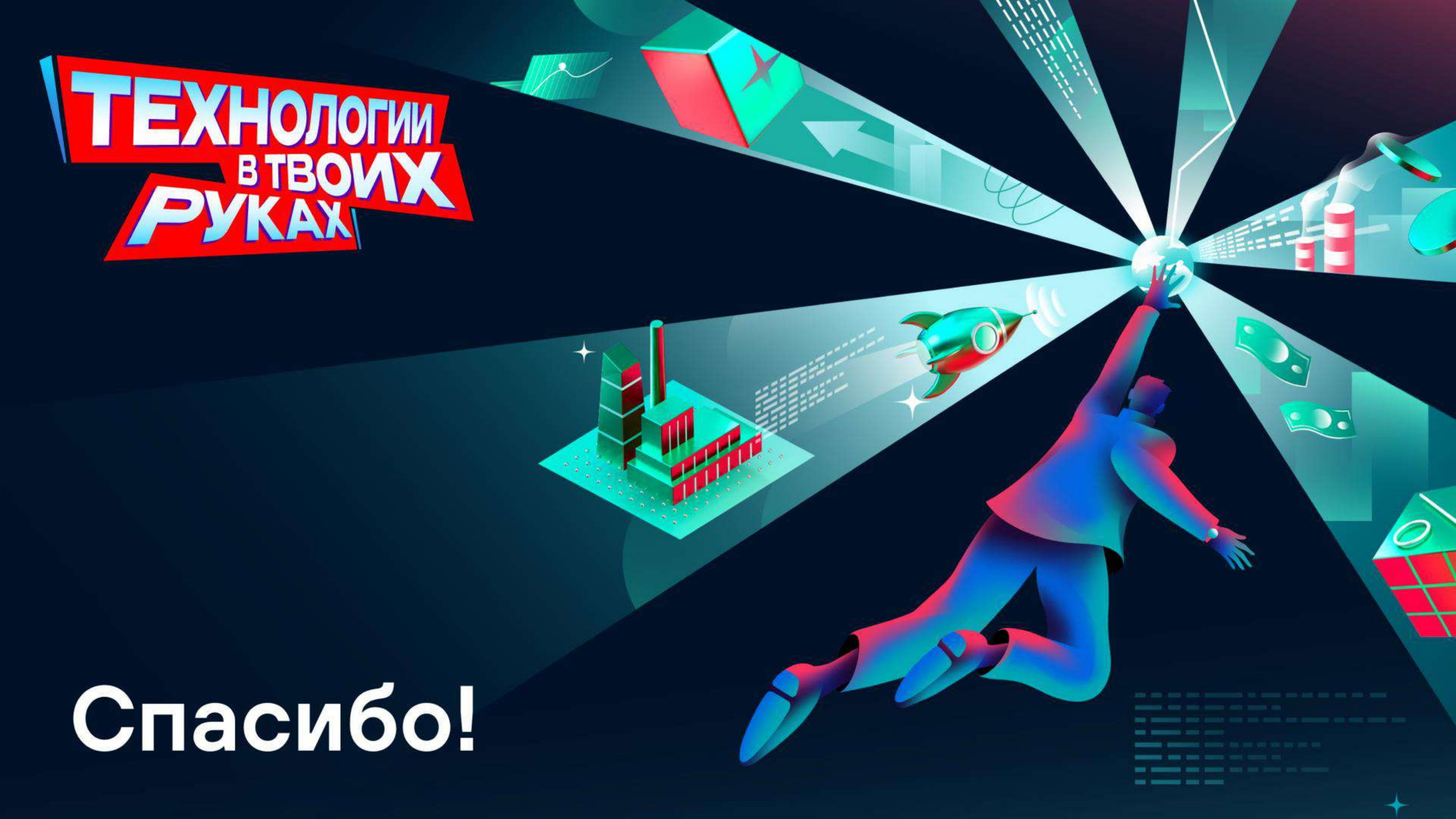
Минутка саморекламы

Веду свой авторский канал в Telegram: *NA_SOC*

- Как строить SOC внутри компании и не сгореть на продакшене.
- Немного про баги, много про людей.
- Тут не «AI спасёт всех», а «вот как оно бывает по-настоящему».
- Шуршим за кибер и за жизнь с этим SOC 24/7.

Подписывайтесь, если хотите без корпоративного маркетинга t.me/na_soc





Спасибо!