R-Vision

SOC: 2 человека на 120 инцидентов в день

Евгений Гуляев
Ведущий консультант по ИБ

01

Проблематика

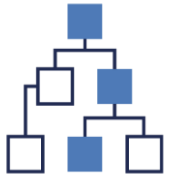
Дано

Отсутствие персонала

для организации дежурной смены SOC в головной организации

Большая распределенная корпоративная ИТ инфраструктура

СЗИ и ИТ системы:
AD, AV, IPAM, SIEM, SOAR



Сложная корпоративная структура

с большим уровнем независимости дочерних структур

Наличие ответственных за ИБ

в дочерних структурах
+ сотрудники ИТ служб

Что хотим

В кратчайшие сроки обеспечить полноценный мониторинг и расследование инцидентов ИБ всей группы компаний имеющимися ресурсами

Построить прозрачный процесс по управлению инцидентами: метрики по процессу, формирование отчетности, проведение аналитики

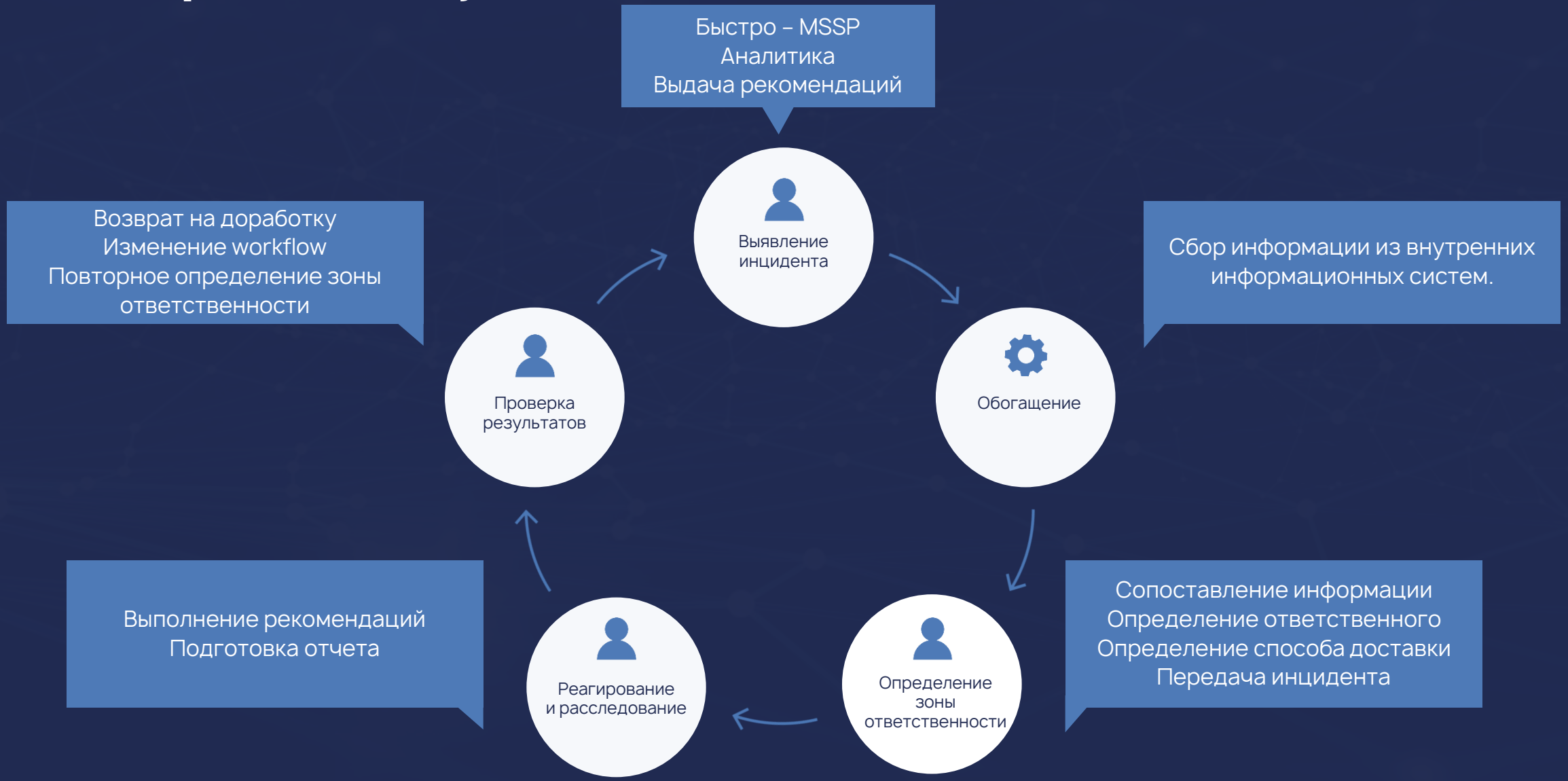
Максимально вовлечь людей в дочерних организациях и филиалах для решения поставленных задач

Минимизировать трудозатраты в головной компании

02

Первый запуск
Первые проблемы

Первый запуск



С чем столкнулись

- **Противоречивые данные** о зонах ответственности в рамках разных информационных систем;
- Необходимость **детализации описания** мероприятий по реагированию на инциденты ИБ;
- Необходимость **вносить изменения** в процесс реагирования без правок сценариев реагирования;
- Разные механизмы взаимодействия. Необходимость **возможности выбора способа реагирования** на конкретный тип инцидента (почта, сервис-деск, telegram и т.д.);
- Необходимость **настройки дополнительных маршрутов** уведомлений;
- **Огромные временные трудозатраты** на определение ответственного за инцидент.

Жизненный цикл инцидента

Возникновение инцидента

Анализ в MSSP и выдача рекомендаций

Передача инцидента в SOAR

Нормализация полученных данных

Агрегация и пост-обработка данных

Обогащение инцидента из имеющихся источников

Уведомление иных заинтересованных лиц по списку

+ ...

Направление инцидента в соответст-вующую зону ответственности

Уточнение данных, кому отправить

Определение способа обработки инцидента (почта, заявка, telegram и т.д.)

Решение конфликтов при противоречивых сведениях из разных источников

Проверка критериев для определения зоны ответственности для каждого из источников

МАРШУТИЗАЦИЯ

90% времени

Проведение расследования в дочерней организации

Фиксация результатов расследования

Проверка достаточности выполненных мер

03

Автоматизация процесса

маршрутизация

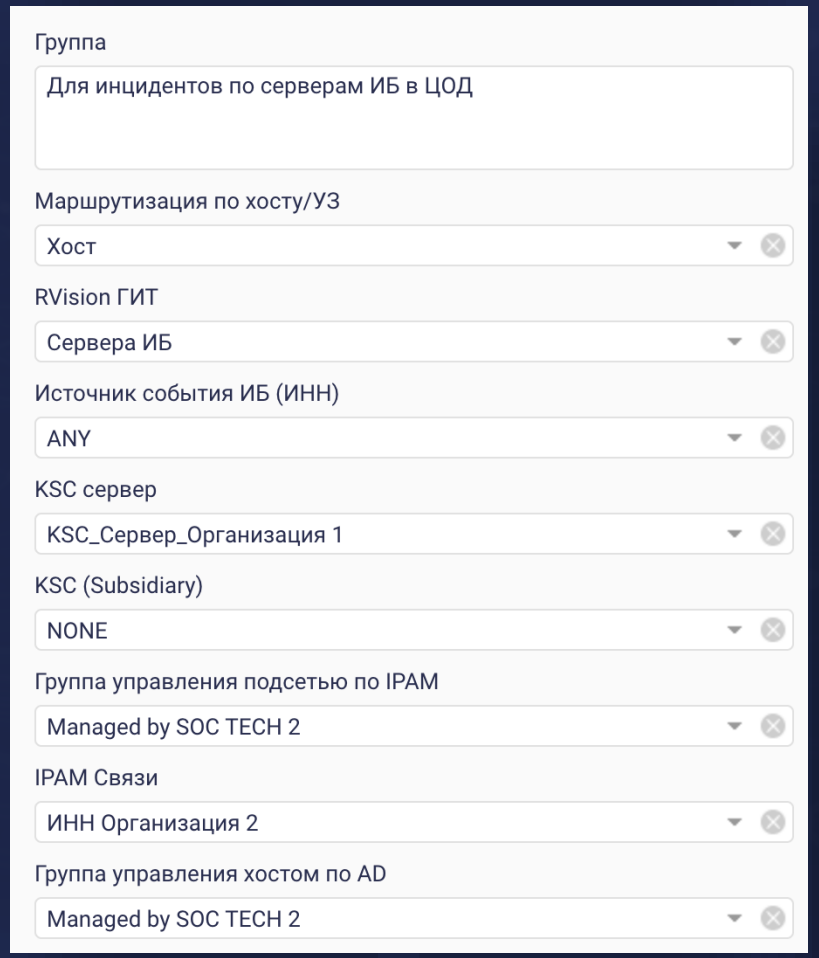
Как решали

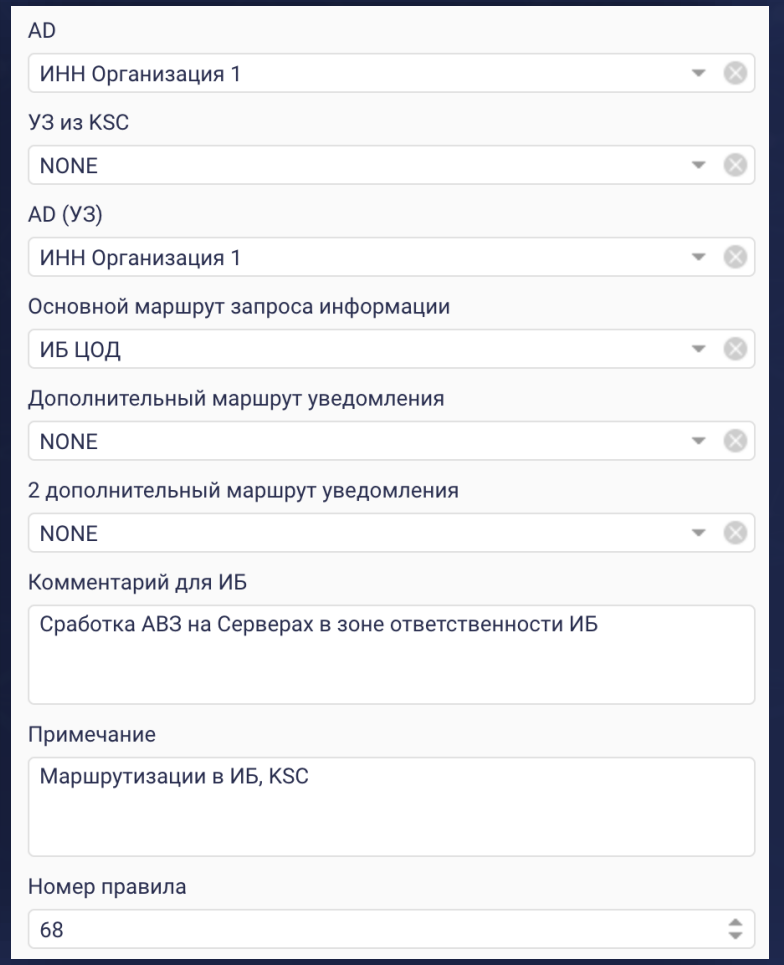
Матрица маршрутизации

Номер правил	Дополнит...	2 дополн...	AD	AD (...	RVision ГИТ	Основной ...	IPAM...	KSC сервер	Группа управления хосто...	Источник...	УЗ из ...	Маршрут...	Группа
51	NONE	ИБ	ANY	ANY	ANY	Subsidiary	ANY	ANY	ANY	ANY	ANY	Хост	Для инцидентов, по котор...
52	NONE	ИБ	ANY	ANY	ANY	Subsidiary	ANY	ANY	ANY	ANY	ANY	Хост	Для инцидентов, по котор...
53	NONE	ИБ	ANY	ANY	ANY	Subsidiary	ANY	ANY	ANY	ANY	ANY	Хост	Для инцидентов, по котор...
54	NONE	NONE	ANY	ANY	ANY	ИБ ЦОД	ANY	ANY	ANY	ANY	ANY	Хост	Для инцидентов по хостам...
55	NONE	ИБ	NONE	ANY	ANY	NONE	ИНН ...	ANY	ANY	ANY	ANY	Хост	Для инцидентов с противо...
56	NONE	ИБ	ИНН ...	ANY	ANY	NONE	NONE	ANY	NONE	ANY	ANY	Хост	Для инцидентов с противо...
57	NONE	ИБ	ИНН ...	ANY	ANY	NONE	ИНН ...	ANY	ANY	ANY	ANY	Хост	Для инцидентов с противо...
58	NONE	ИБ	ИНН ...	ANY	ANY	NONE	ИНН ...	ANY	ANY	ANY	ANY	Хост	Для инцидентов с противо...
59	NONE	ИБ	ANY	ANY	ANY	NONE	ANY	ANY	ANY	ANY	ANY	Хост	Для инцидентов с противо...
60	NONE	ИБ	ANY	ANY	ANY	Subsidiary	ANY	ANY	ANY	ИНН	ANY	Хост	Для инцидентов по источн...
61	NONE	NONE	ANY	ИНН ...	ANY	Subsidiary	ANY	ANY	ANY	ANY	ИНН ...	УЗ	Для маршрутизации по УЗ
62	NONE	NONE	ANY	ИНН ...	ANY	Subsidiary	ANY	ANY	ANY	ANY	ANY	УЗ	Для маршрутизации по УЗ
63	NONE	NONE	ANY	ANY	ANY	Subsidiary	ANY	ANY	ANY	ANY	ИНН ...	УЗ	Для маршрутизации по УЗ
64	NONE	NONE	ANY	ИНН ...	ANY	Продукт Д...	ANY	ANY	ANY	ANY	ИНН ...	УЗ	Для маршрутизации по УЗ ...
65	NONE	NONE	ANY	ИНН ...	ANY	Продукт Д...	ANY	ANY	ANY	ANY	ANY	УЗ	Для маршрутизации по УЗ ...
66	NONE	NONE	ANY	ANY	ANY	Продукт Д...	ANY	ANY	ANY	ANY	ИНН ...	УЗ	Для маршрутизации по УЗ ...
67	NONE	ИБ	NONE		Критичные хосты...	ЦОД	ANY	KSC_Серве...	Managed by SOC TECH 2	ANY	ANY	УЗ	Для маршрутизации по УЗ
68	NONE	NONE	ИНН ...	ИНН ...	Сервера ИБ	ИБ ЦОД	ИНН ...	KSC_Серве...	Managed by SOC TECH 2	ANY	NONE	Хост	Для инцидентов по хостам...
69	NONE	NONE	ИНН ...	ИНН ...	АРМ Управления ...	ИТ: АРМ	ИНН ...	KSC_Серве...	Managed by SOC TECH 2	ANY	ANY	Хост	Для инцидентов по АРМ ЦЭ
70	NONE	NONE	ИНН ...	ИНН ...	ANY	ИБ	ИНН ...	KSC_Серве...	Managed by SOC TECH 1	ANY	ANY	Хост	Для маршрутизации по УЗ ...

Матрица маршрутизации

Маршрут


Группа
Для инцидентов по серверам ИБ в ЦОД
Маршрутизация по хосту/УЗ
Хост
RVision ГИТ
Сервера ИБ
Источник события ИБ (ИНН)
ANY
KSC сервер
KSC_Сервер_Организация 1
KSC (Subsidiary)
NONE
Группа управления подсетью по IPAM
Managed by SOC TECH 2
IPAM Связи
ИНН Организация 2
Группа управления хостом по AD
Managed by SOC TECH 2


AD
ИНН Организация 1
УЗ из KSC
NONE
AD (УЗ)
ИНН Организация 1
Основной маршрут запроса информации
ИБ ЦОД
Дополнительный маршрут уведомления
NONE
2 дополнительный маршрут уведомления
NONE
Комментарий для ИБ
Сработка АВЗ на Серверах в зоне ответственности ИБ
Примечание
Маршрутизации в ИБ, KSC
Номер правила
68

Определение маршрута

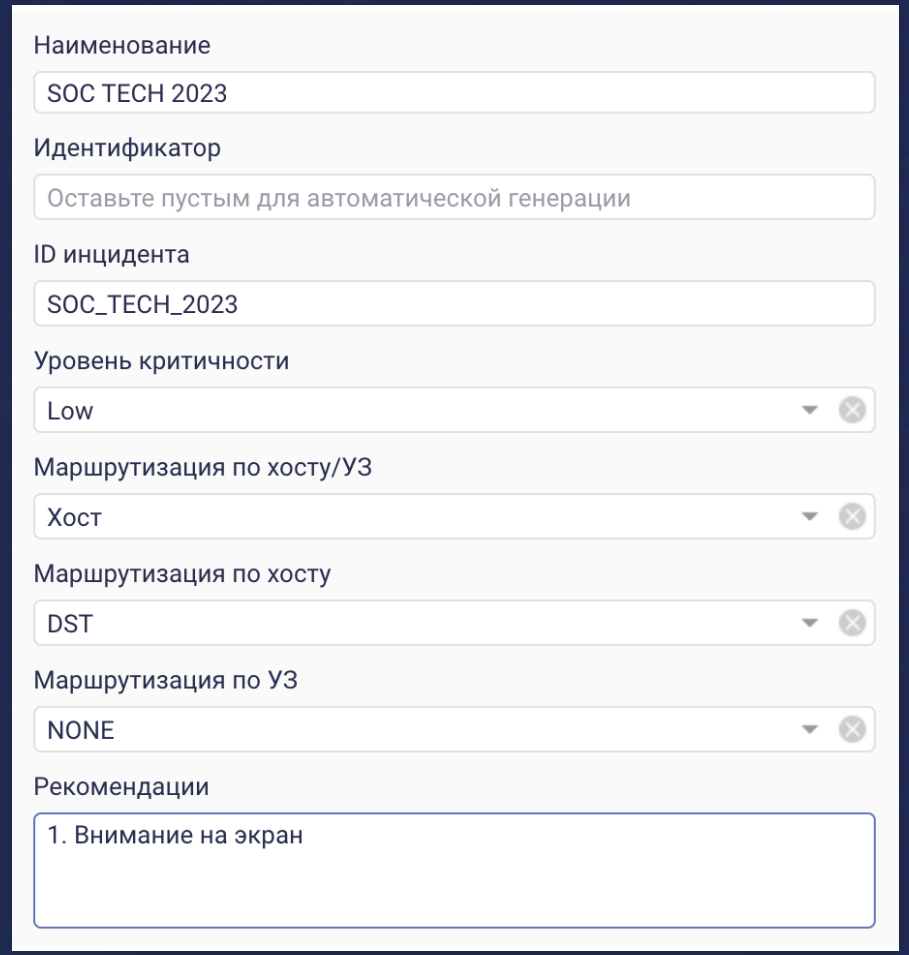
```
ГИТ: Mail service
Исходные данные:
 {
 "field_RouteCustomer": "SOC TECH",
 "field_RouteRvGroup": "Mail service",
 "field_RouteKsc": "KSC_DB01P",
 "field_RouteKscSubsidiary": "",
 "field_RouteIpam": "7710000000",
 "field_RouteADMGMT": "",
 "field_RouteAD": "",
 "field_RouteIpamMngmt": "",
 "field_RouteADUser": "no_matter"
}
Нормализованные данные:
 {
 "field_RouteCustomer": "SOC TECH",
 "field_RouteRvGroup": "mail service",
 "field_RouteKsc": "ksc_db01p",
 "field_RouteKscSubsidiary": "NONE",
 "field_RouteIpam": "INN SOC TECH",
 "field_RouteADMngmt": "NONE",
 "field_RouteAD": "NONE",
 "field_RouteIpamMngmt": "NONE",
 "field_RouteADUser": "no_matter"
}
```

```
route_number: 8
route_name: Mail Service Administration
route_notific: NONE
two_route_notific: IB
Input data:
 {
 "type_inc": "Incorrect authentification profile",
 "customer": "SOC TECH",
 "rv_group": "Mail service",
 "ksc_server": "KSC_ESK-DB01P",
 "ksc_subsidiary_src": "",
 "ipam_src": "",
 "ad_mgmt_src": "",
 "ad_src": "",
 "ad_login_src": "",
 "ipam_mgmt_src": "",
 "ksc_subsidiary_dst": "",
 "ipam_dst": "7710000000",
 "ad_mgmt_dst": "",
 "ad_dst": "",
 "ad_login_dst": "",
 "ipam_mgmt_dst": ""
}
```

«Реестр сценариев»

Пользовательский актив

- Возможность изменения рекомендаций по реагированию
- Возможность вносить изменения в процесс реагирования без правок сценариев реагирования
- Возможность настройки перечня конкретных организаций, куда можно направлять сработки по данному типу инцидентов
- Возможность гибкой настройки дополнительных уведомлений



Другие пользовательские активы

«Дочерние организации или филиалы»

- Базовая информация об организации
- Идентификаторы организации из смежных систем (ИНН или другие)
- Информация об ответственном за ИБ и ИТ
- Информация о способе информирования (email, TG chat и прочее)

«Маршруты»

- Способ обработки инцидента по маршруту
- Принадлежность маршрута к внешней системе
- Наименование маршрута при взаимодействии с сервисами
- Поля триггеры «требуется создание заявки», «требуется запрос информации по почте», «требуется отправка в телеграмм и тд

Активы для обогащения

Специфическая информация, которую необходимо учитывать

Например, средства антивирусной защиты:

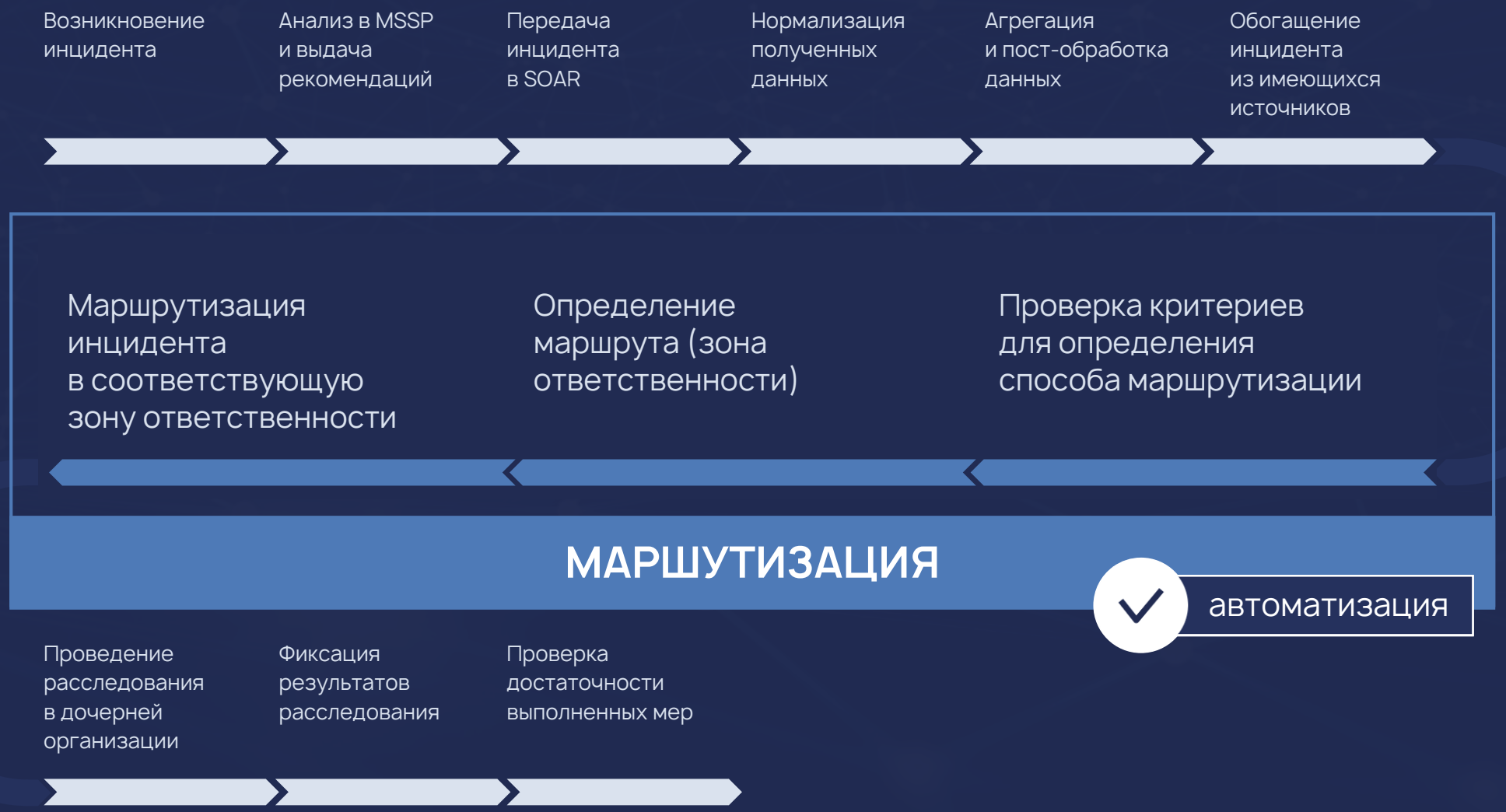
- Имя сервера
- IP сервера
- Вышестоящие сервер
- Имя БД и ее адрес
- Принадлежность к организации

04

Результаты

A - Автоматизация

Жизненный цикл инцидента после автоматизации



05

Дальнейшее развитие

Маршрутизация

По результатам проекта

- **Все цели проекта достигнуты.** Реализован мониторинг и расследование инцидентов ИБ.
- **Сэкономлено значительное количество человеческих ресурсов** и экономия продолжается каждый день функционирования SOC.
- **Высокая скорость** обработки инцидента с момента его выявления до момента начала реагирования и расследования;
- **Единое место хранения** всей информации необходимой для обработки инцидента.
- **Возможность гибкого и быстрого** внесения изменения процессов реагирования;
- **Снижение требований к компетенциям** персонала, эксплуатирующего систему.
- Всего **2 человека в головной организации** обрабатывают более **120 инцидентов** в день;

R-Vision

+ 7 (499) 322 80 40

sales@rvision.ru

rvision.ru

t.me/rvision_pro

vk.com/rvision_ru

Подписывайтесь на наш дайджест ИБ: **rvision.ru/blog**