



SECURITY VISION  
УВИДЕТЬ БЕЗОПАСНОСТЬ

# SECURITY VISION

## АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ИБ

Анжелика Свойкина  
Пресейл менеджер  
[asvoykina@securityvision.ru](mailto:asvoykina@securityvision.ru)

# SECURITY VISION

Российский разработчик

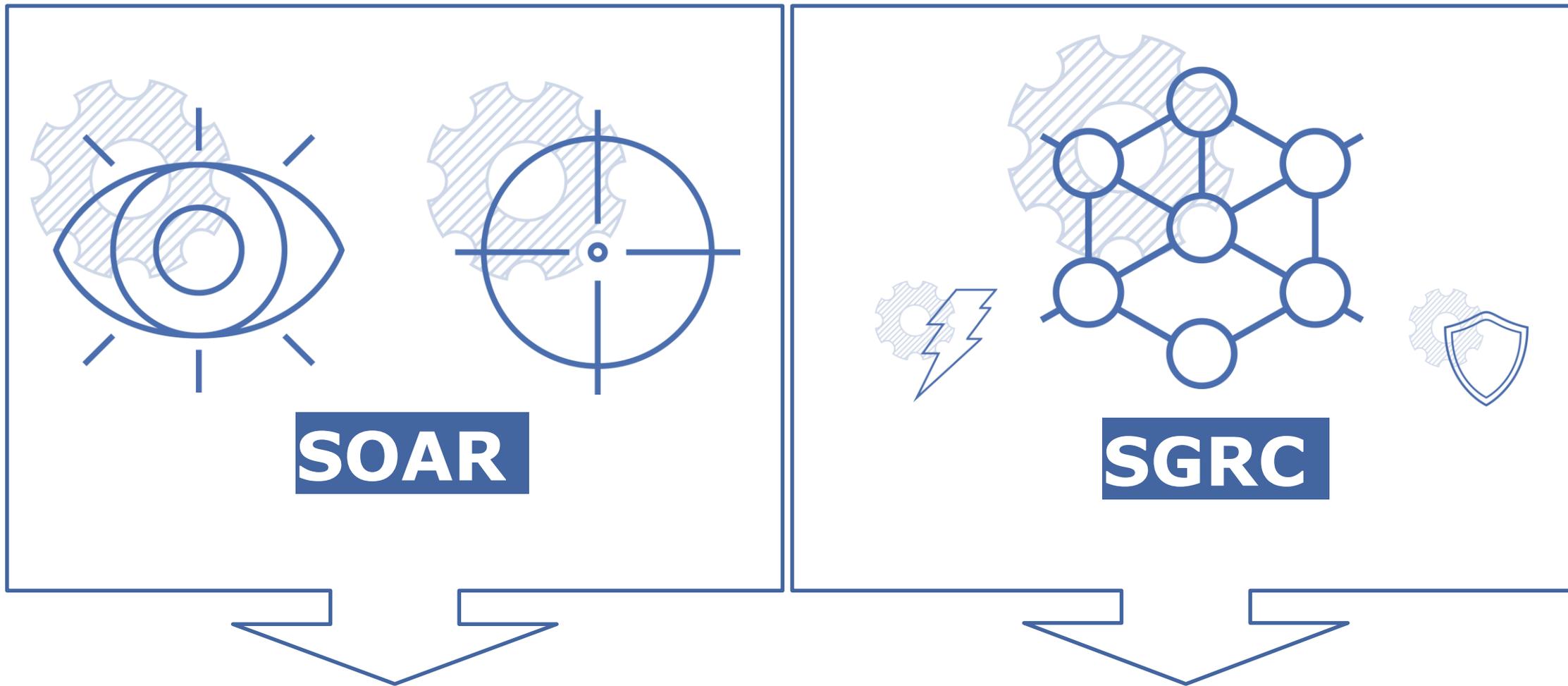
Сертификат ФСТЭК по 4 уровню доверия



Опыт масштабных внедрений



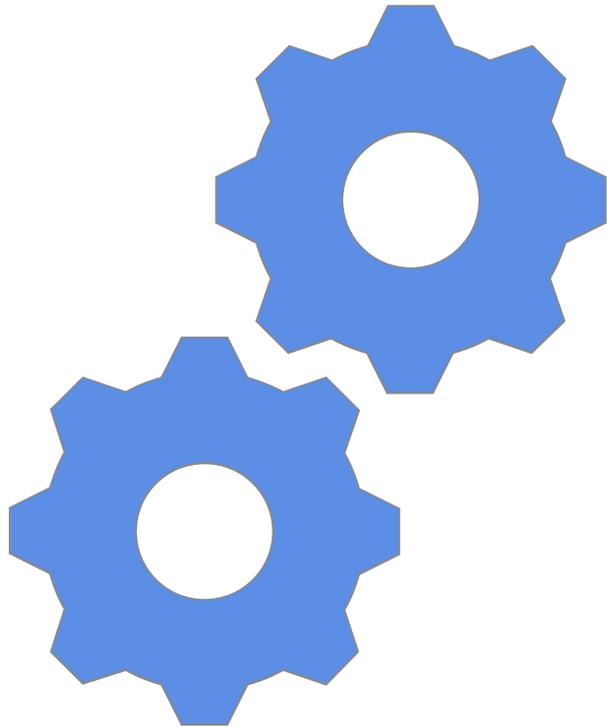
# ПЛАТФОРМА автоматизации процессов ИБ



Практическая безопасность

Стратегическая безопасность

# Базовые процессы ИБ



**Управление активами**

**Управление уязвимостями**

**Управление инцидентами**

# АКТИВЫ

Фундамент процессов ИБ

Интеграции с внутренними системами

- + Учётные записи
- + Сертификаты
- + Бизнес-процессы

Категорирование

Адаптивность модели активов



# Инциденты

SIEM ≠ Incident Management

Playbooks

Сокращение false positive

Обогащения

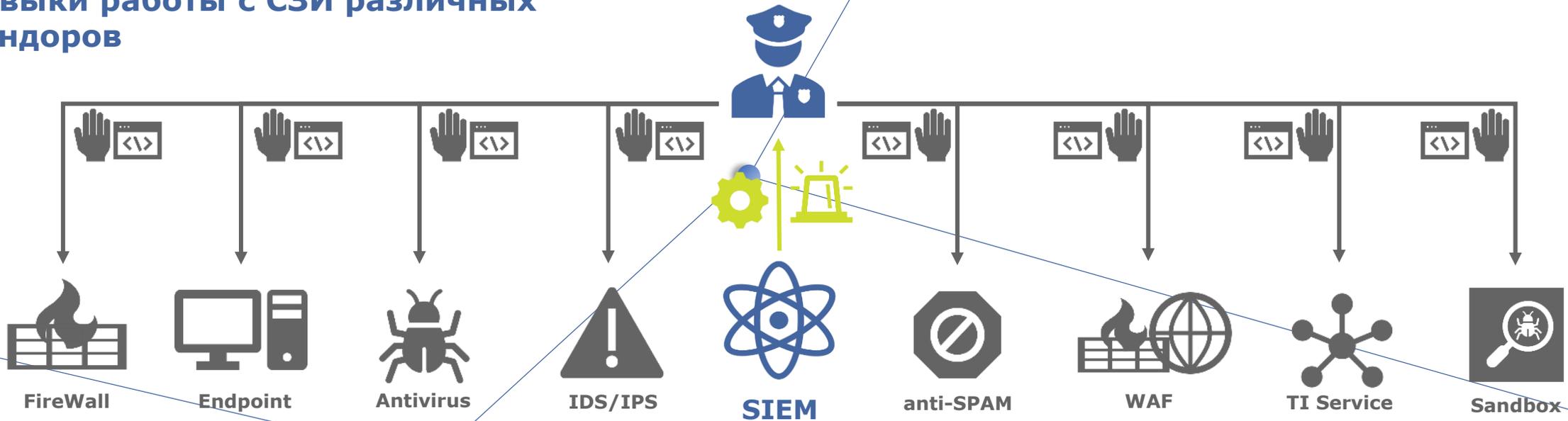
Единый инструмент



# RESPONSE без автоматизации

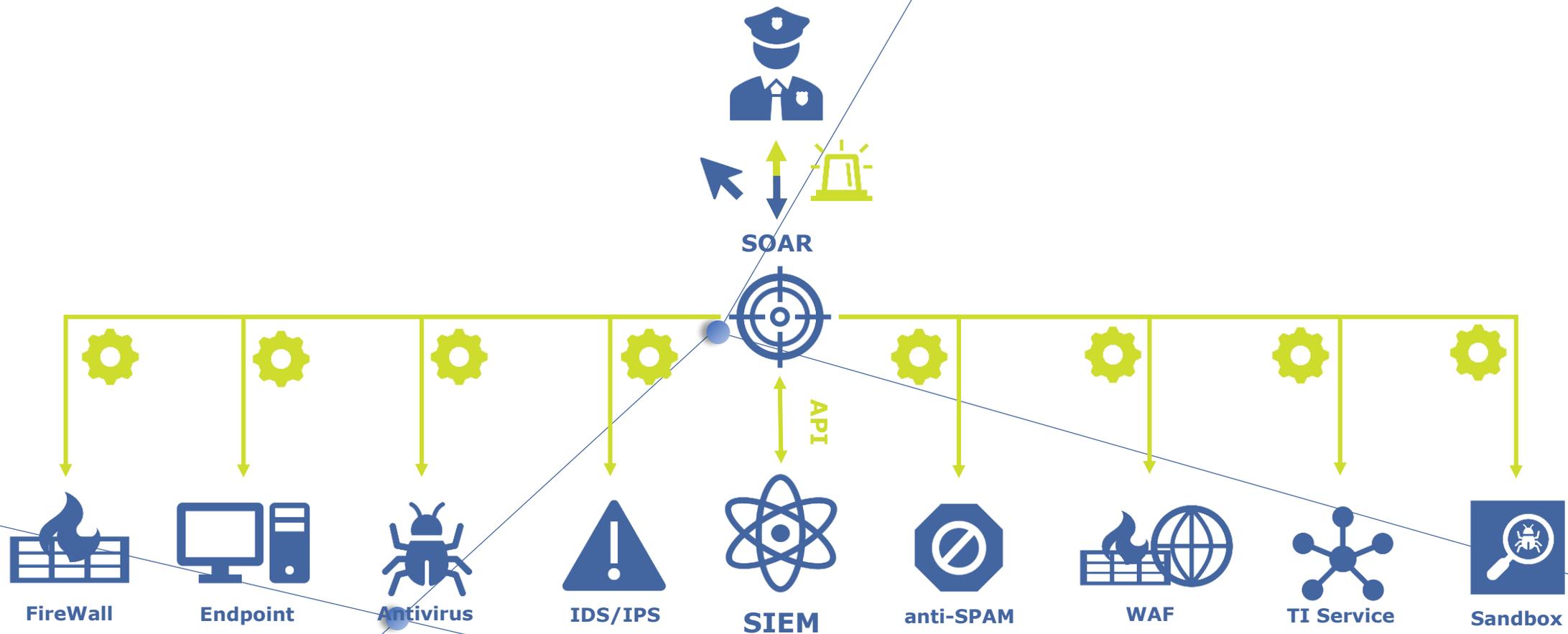
# У специалистов ИБ должны быть навыки работы с СЗИ различных вендоров

# Нет полной картины по тому как реагируют специалисты ИБ

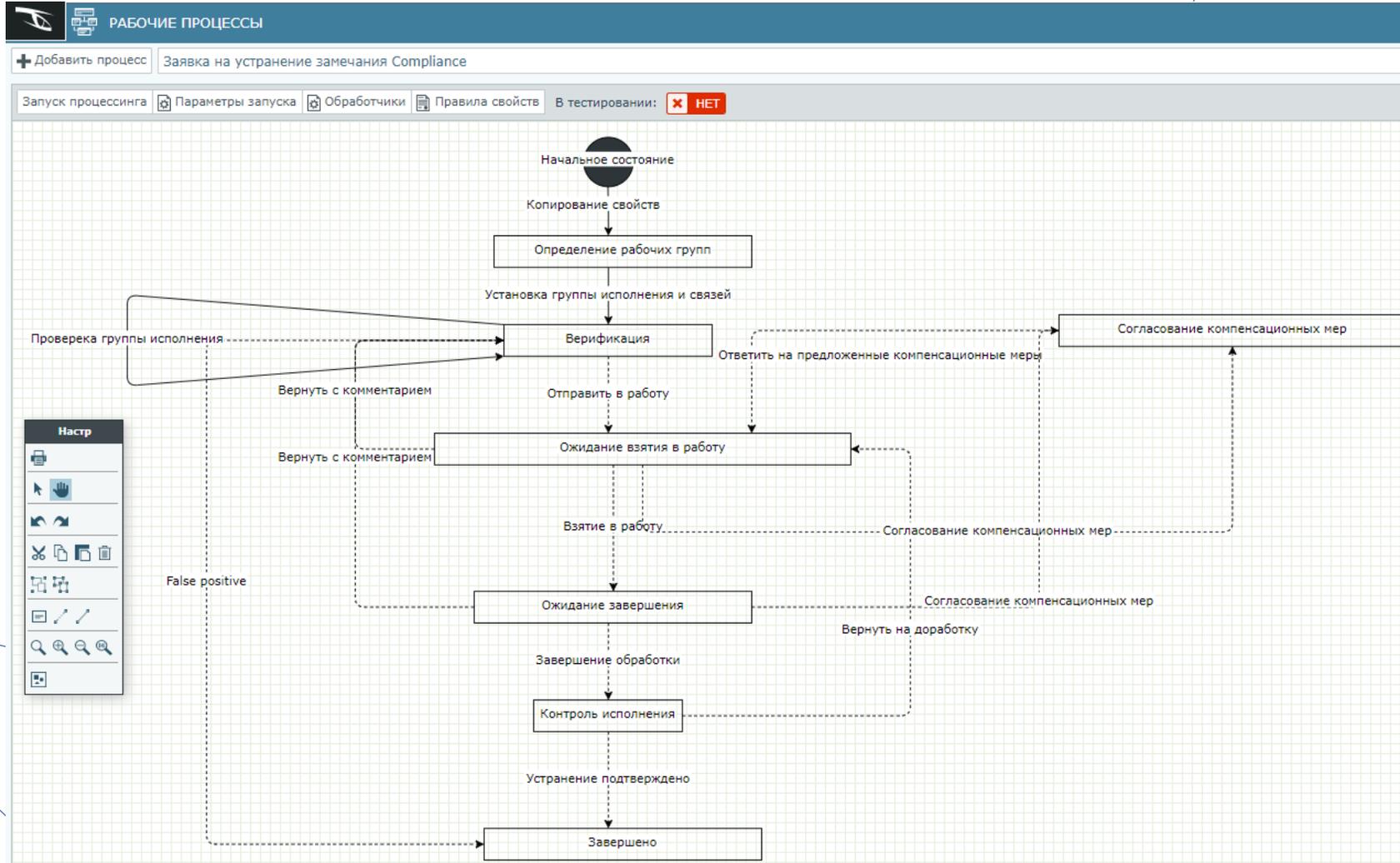


# У специалистов ИБ множество лишних доступов

# RESPONSE с автоматизацией



# Рабочие процессы



1. Ручная транзакция -



2. Автоматическая транзакция -



# Коннекторы

 ТИПЫ КОННЕКТОРОВ ДАННЫХ

Типы коннекторов: + 🗑️ Наименование: MaxPatrol SIEM (Инциденты)

Тип источника получения данных: Rest  
Получение данных с помощью Rest-запроса

**СБОР ДАННЫХ** СВОЙСТВА СОБЫТИЯ ОЧИСТКА ФИЛЬТРАЦИЯ ДЕДУПЛИКАЦИЯ КОРРЕЛЯЦИЯ СОЗДАНИЕ ОБЪЕКТОВ

**Настройки аутентификации**  
*Настройки аутентификации для запроса к источнику данных*

Тип аутентификации: Серия запросов

Тип аутентификации для серии запросов: Отдельный запрос

Тип аутентификации для отдельного запроса: Нет

Время токена аутентификации:  секунд

Тип метода: POST

Переменные для формирования запроса: **`\${login}`** **`\${password}`**

Вызываемый метод: https://MPSIEM:3334/ui/login

Заголовки запроса: Название + Добавить заголовок

Тип контента: application/json

Тело запроса: 

```
1 {"authType": 0, "username": "${login}", "password": "${password}"}
```

**Настройки получения данных**  
*Настройки запроса к источнику данных и преобразование полученных данных*

Тип аутентификации: Серия запросов

Тип аутентификации для серии запросов: Отдельный запрос

Тип аутентификации для отдельного запроса: Нет

Время токена аутентификации:  секунд

Тип метода: POST

Переменные для формирования запроса: **`\${login}`** **`\${password}`**

Вызываемый метод: https://MPSIEM:3334/ui/login

Заголовки запроса: Название + Добавить заголовок

Тип контента: application/json

Тело запроса: 

```
1 {"authType": 0, "username": "${login}", "password": "${password}"}
```

**Настройки обогащения данных**  
*Настройки дополнительных запросов для обогащения данных*

**Настройки завершения сессии**

**Примеры данных из коннектора**  
*Получение примеров данных из коннектора*

**Настройки получаемых данных**

Тип получаемых данных: Нет  
После получения данные будут сконвертированы в JSON для дальнейшей обработки

**Настройки парсинга данных из JSON**

Тип парсинга: Нет

- ElasticSearch
- FinCERT
- FinCERT v1.1
- FinCERT v2.0
- FireEye
- FireEye (Syslog)
- FireEye IPS
- FortiSIEM
- IBM QRadar SIEM (Инциденты)
- Infowatch
- InfoWatch (REST API)
- InfoWatch Traffic Monitor
- InfoWatch Traffic Monitor (HTML)
- Jira (Обновление заявок)
- Kaspersky Security Center
- Kaspersky Security Center (Not Cured)
- Kaspersky Security Center (Программное обеспечение)
- Kaspersky Security Center (Узлы сети)
- Kaspersky Security Center IPS
- MaxPatrol 8 (Активы)
- MaxPatrol 8 (Уязвимости)
- MaxPatrol SIEM (Активы)
- MaxPatrol SIEM (Инциденты)**
- Microsoft Security Essentials
- MS SCCM (ПО)
- MS SCCM (Пользователи)
- MS SCCM (Серверы)
- Nessus
- NMap (Assets) (New)

# ИНТЕГРАЦИИ

## Реагирование



## АКТИВЫ



## События



# ФИШИНГ

65 МИНУТ → 5 МИНУТ С SOAR

ДО АВТОМАТИЗАЦИИ

15 мин

25 мин

10 мин

5 мин

10 мин

65  
МИНУТ

АНАЛИЗ  
ПОЧТОВОГО  
СООБЩЕНИЯ

СКАНИРОВАНИЕ  
РАБОЧИХ  
СТАНЦИИ

ПОИСК И  
УДАЛЕНИЕ  
АНАЛОГИЧНЫХ  
СООБЩЕНИЙ

БЛОКИРОВКА  
ОТПРАВИТЕЛЯ

БЛОКИРОВКА  
ВРЕДНОСНЫХ  
ДОМЕНОВ

ИНФОРМИРОВАНИЕ  
ПОЛЬЗОВАТЕЛЕЙ

ПОСЛЕ АВТОМАТИЗАЦИИ

5  
МИНУТ

# ЗАРАЖЕНИЕ

80 МИНУТ → 10 МИНУТ С SOAR

ДО АВТОМАТИЗАЦИИ



ПОСЛЕ АВТОМАТИЗАЦИИ

 участие человека

10 МИНУТ



# АНАЛИЗ

## ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ

85 МИНУТ

2 МИНУТЫ С SOAR

ДО АВТОМАТИЗАЦИИ

35 мин

25 мин

15 мин

10 мин

85  
МИНУТ

ПОЛУЧЕНИЕ  
ИНФОРМАЦИИ СО  
СКАНЕРА  
УЯЗВИМОСТИ

АНАЛИЗ  
КОНТЕКСТА  
УЯЗВИМОСТИ

УСТАНОВКА  
SLA/OLA  
НА УСТРАНЕНИЕ

СОЗДАНИЕ ЗАЯВОК  
НА УСТРАНЕНИЕ

КОНТРОЛЬ  
УСТРАНЕНИЯ И  
ПОДГОТОВКА  
ОТЧЕТА

ПОСЛЕ АВТОМАТИЗАЦИИ

2  
МИНУТЫ

 участие человека



# ПЛЕЙБУКИ: ДРУГИЕ ПРИМЕРЫ

утечка информации

отправка данных в FinCERT / НКЦКИ

распределенная атака

социальная инженерия

мониторинг изменений

мониторинг ИБ решений

предоставление и блокировка доступа

# OPEN SOURCE SOAR

## 01 Экосистема TheHive:

- Cortex, MISP, N8N
- Linux
- Docker\k8s
- Python\Rest API
- ElasticSearch
- Angular

## 02 Дефицит кадров с соответствующей компетенцией

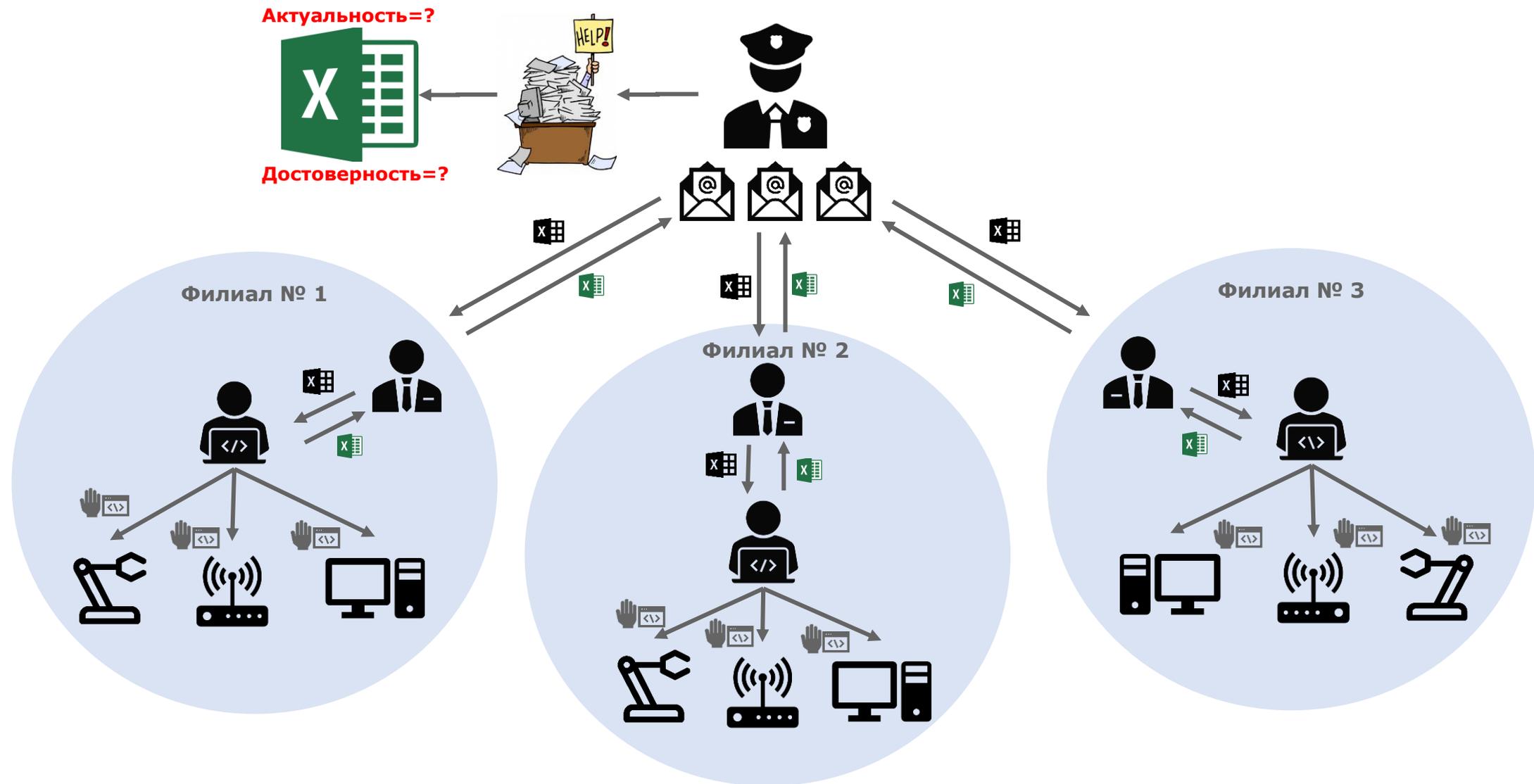
## 03 Кастомные решение требуют детального описания (технического писателя)

## 04 Разработка и актуализация интеграций ложится на внутреннюю команду

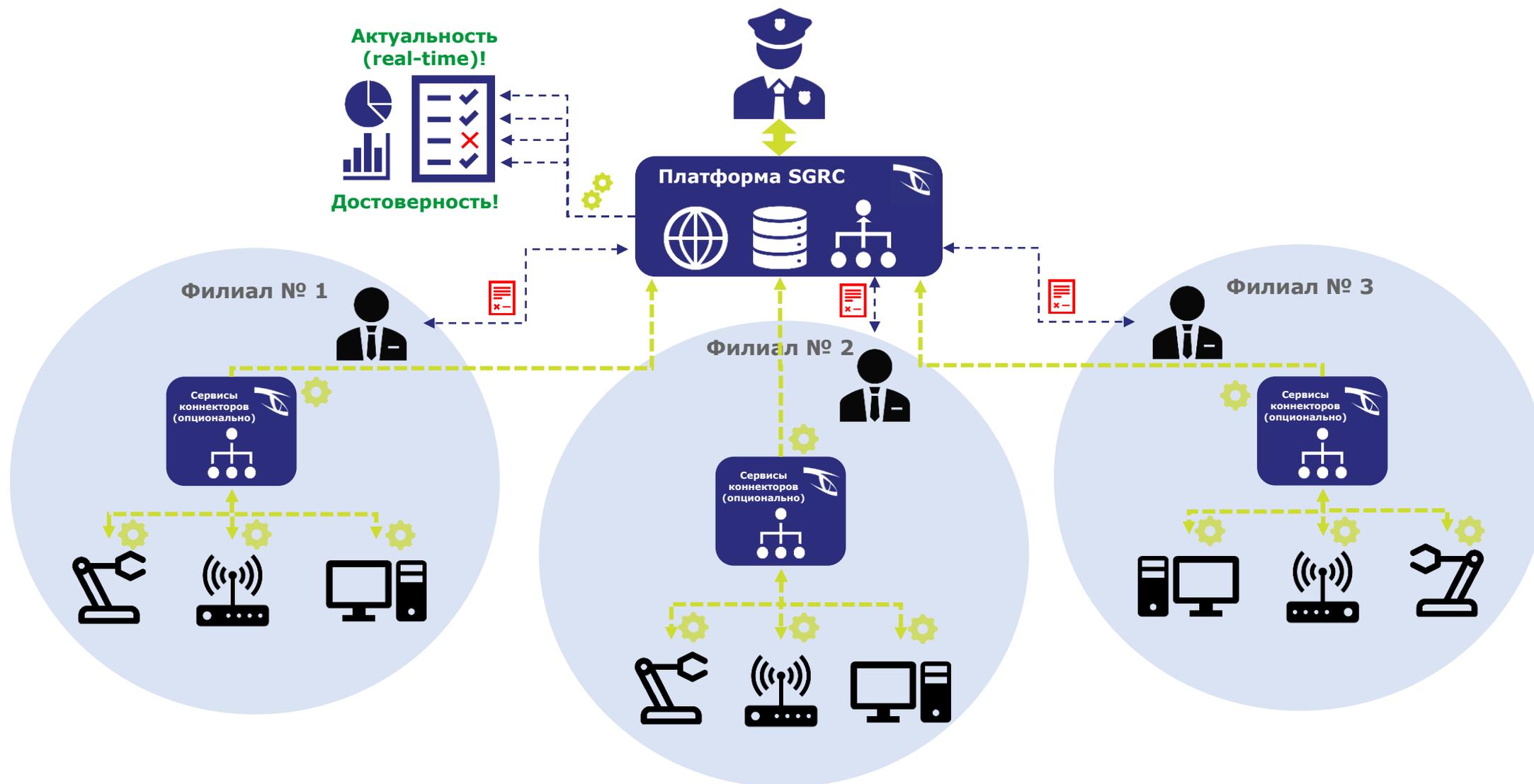
# SGRC

- 01** Compliance:
- КИИ
  - ГОСТ 57580.x
  - ISO 27001
  - PCI DSS
  - GDPR
  - **Custom**
- 02** Управление рисками ИБ
- 03** Проведение аудитов
- 04** Контроль, автоматическая отчетность и визуализация текущего уровня соответствия

# SGRC



# SGRC



# Успешные внедрения

Крупнейший в Восточной Европе SOC  
использует все продукты Security Vision



# Успешные внедрения



**Инвентаризация: 300000+ активов**

**Управление уязвимостями**

**Управление инцидентами: 15+ плейбуков**

**Продолжают развивать систему самостоятельно**

**Custom: Управление проектами**



SECURITY VISION

УВИДЕТЬ БЕЗОПАСНОСТЬ

**СПАСИБО**

**ЗА ВНИМАНИЕ**