SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

SECURITY VISION
АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ИБ

Анжелика Свойкина
Пресейл менеджер
asvoykina@securityvision.ru

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

SECURITY VISION

Российский разработчик

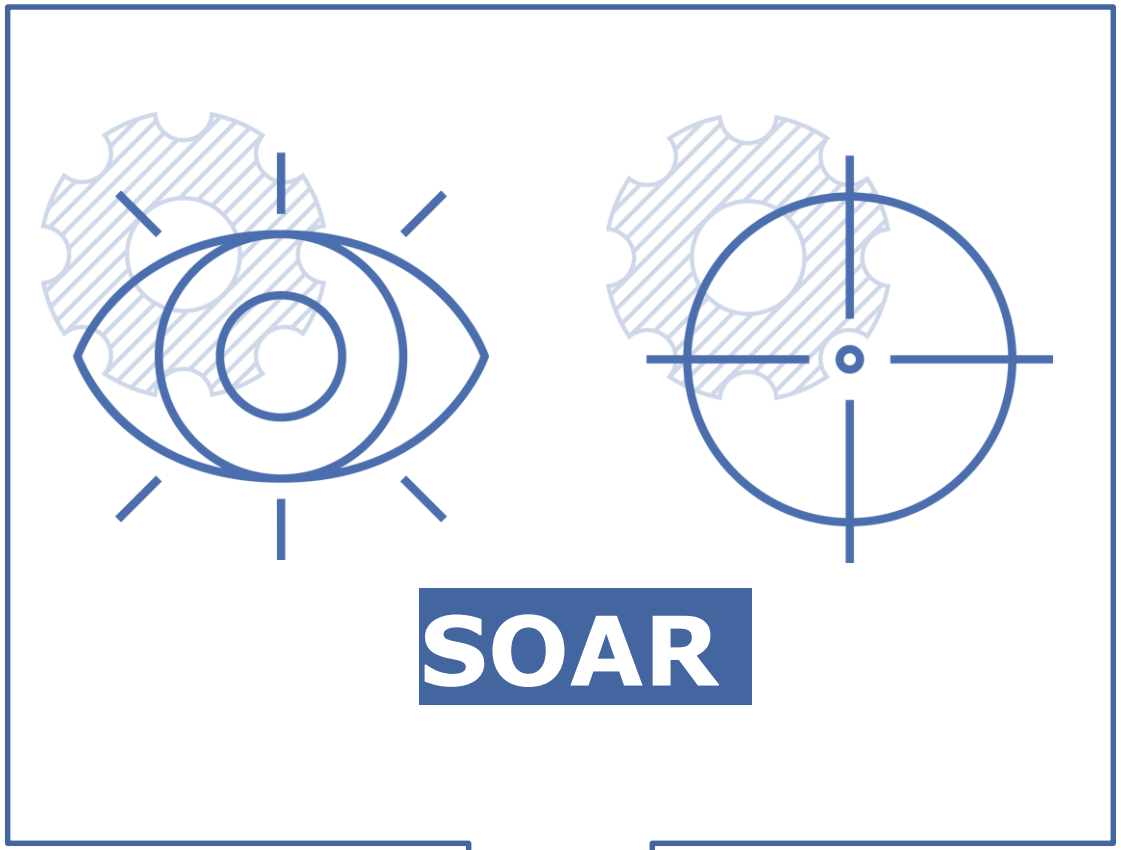
Сертификат ФСТЭК по 4 уровню доверия

Опыт масштабных внедрений

СБЕРБАНК
ПОЧТА РОССИИ
Открытие
ГОЗНАК
ГАЗПРОМ-МЕДИА
ФСО РОССИИ
МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ГЛАВГОСЭКСПЕРТИЗА РОССИИ
РЧС
СДМ-БАНК
Мультикарта
Ростех
Корпорация МСП

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ПЛАТФОРМА автоматизации процессов ИБ

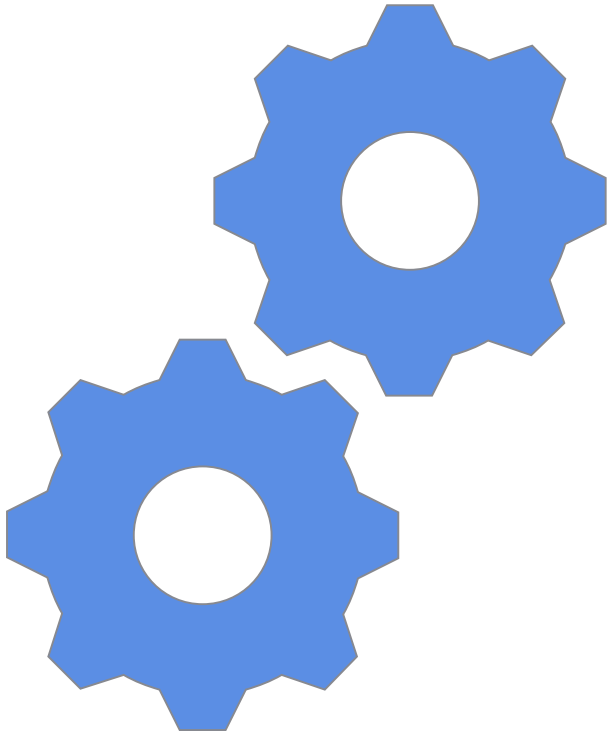


Практическая безопасность

Стратегическая безопасность

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Базовые процессы ИБ



Управление активами

Управление уязвимостями

Управление инцидентами

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

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

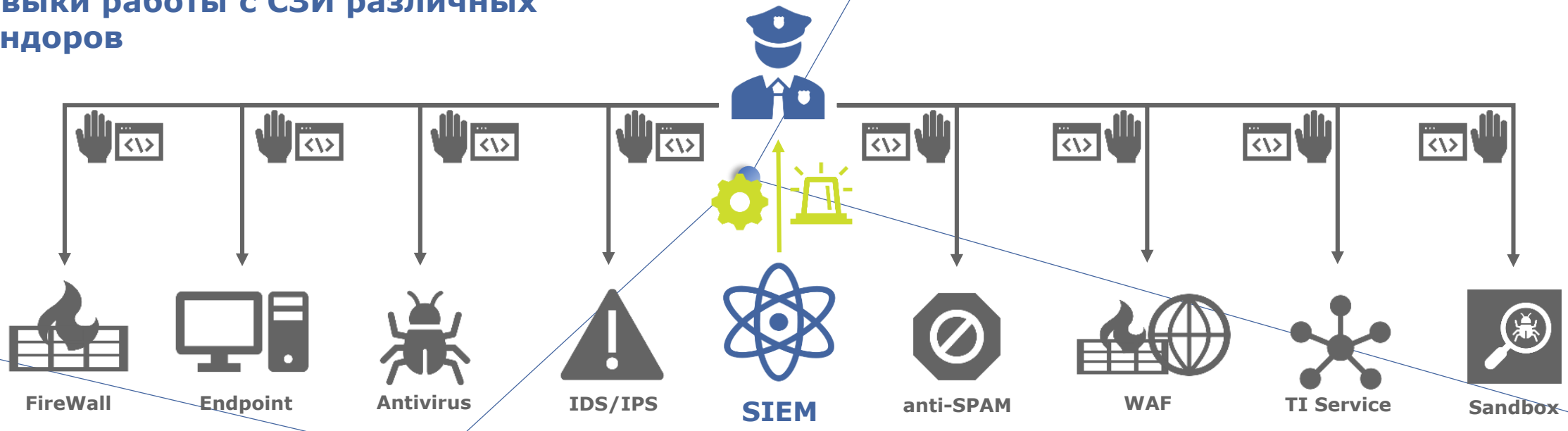
Единый инструмент

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

RESPONSE без автоматизации

 # Нет полной картины по тому как реагируют специалисты ИБ

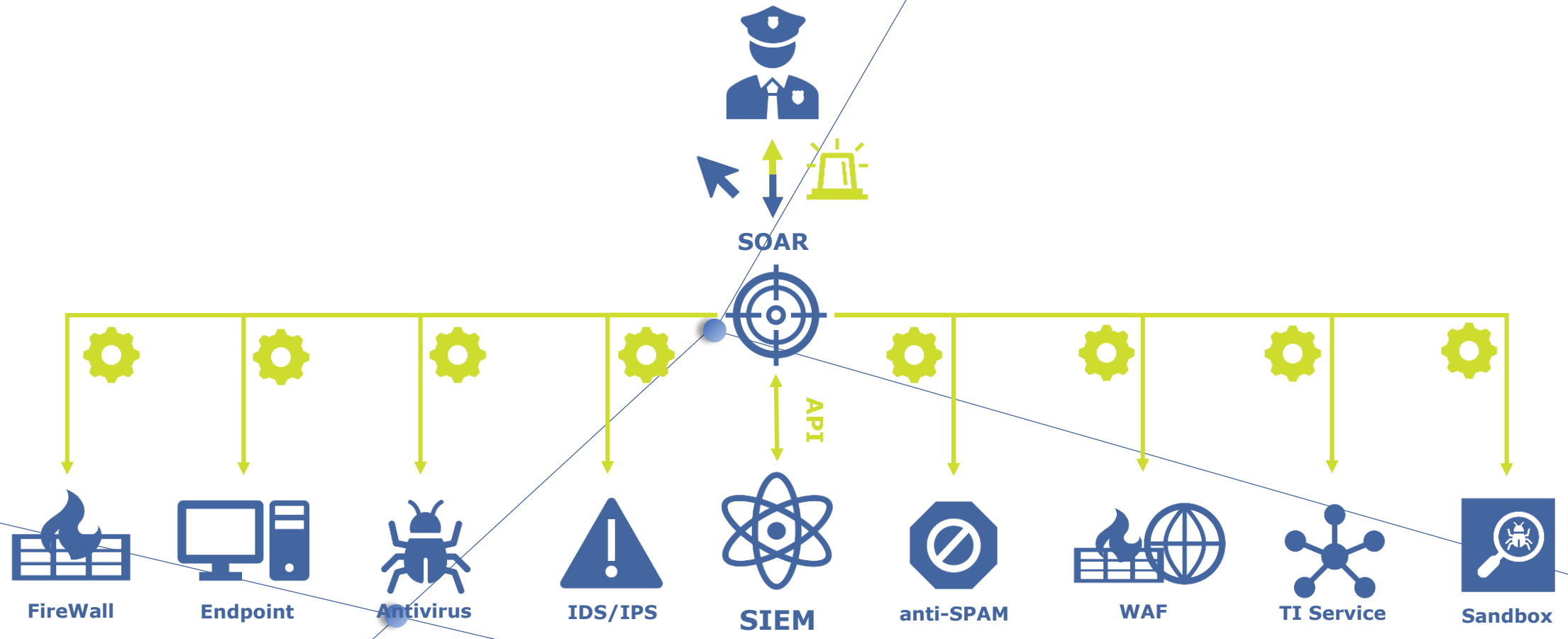
#У специалистов ИБ должны быть навыки работы с СЗИ различных вендоров



 # У специалистов ИБ множество лишних доступов

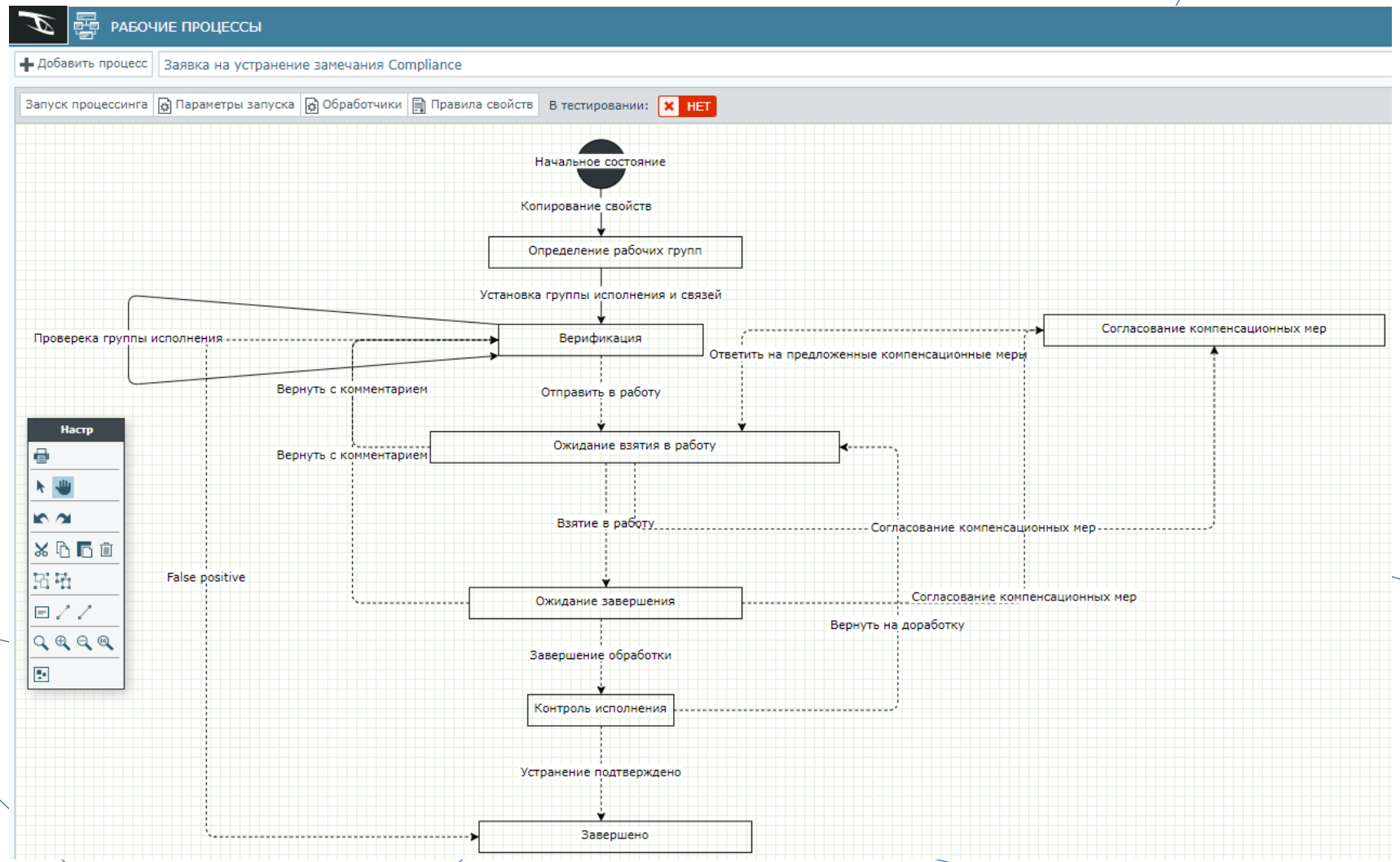
SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

RESPONSE с автоматизацией



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

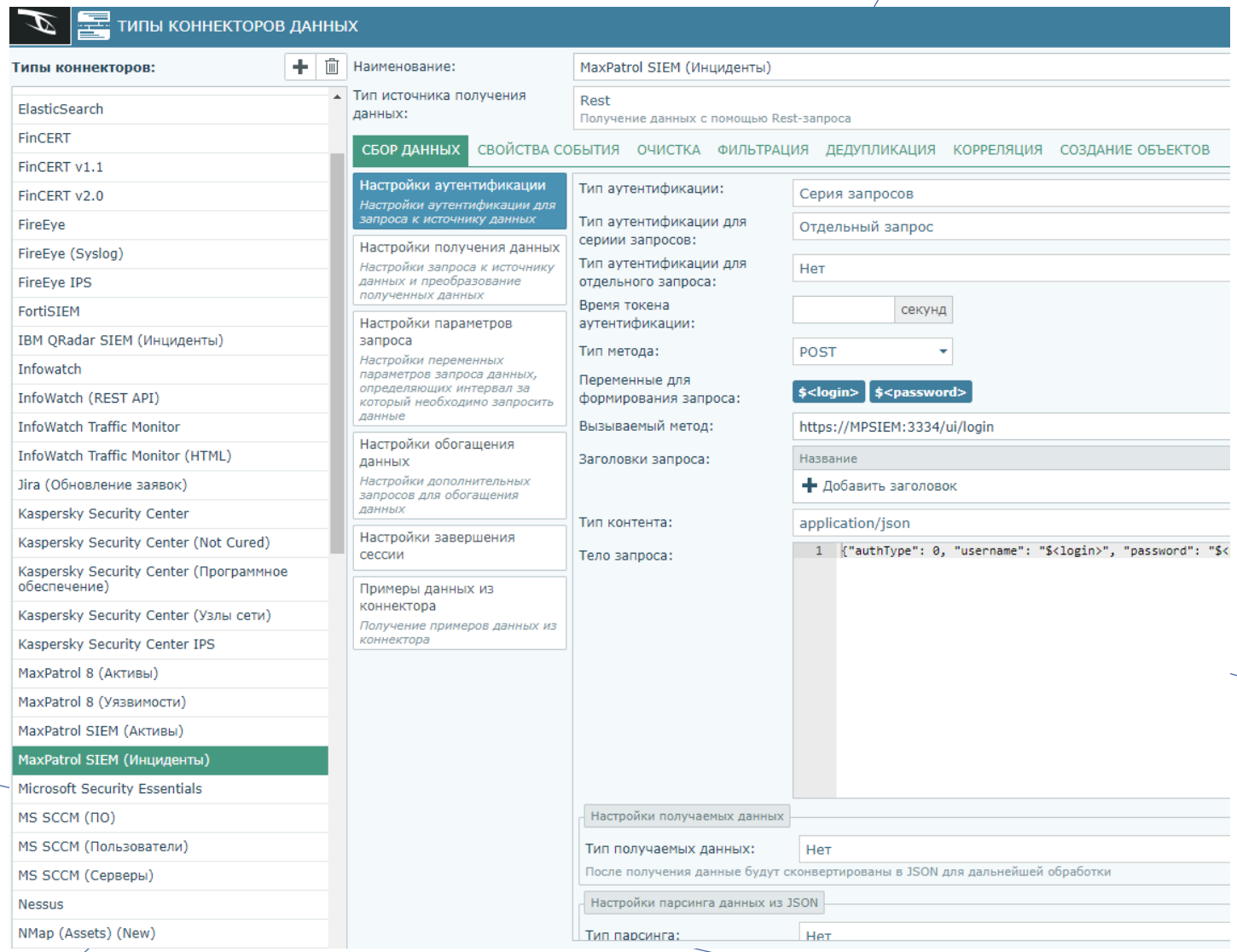
Рабочие процессы



1. **Ручная транзакция -**
2. **Автоматическая транзакция -**

Коннекторы

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ИНТЕГРАЦИИ

Реагирование

UserGate
FORTINET
paloalto NETWORKS
Symantec
KASPERSKY lab
eset
JUNIPER NETWORKS
Check Point SOFTWARE TECHNOLOGIES LTD.
CISCO
Microsoft Active Directory
Exchange
Windows Server
Windows 10
UNIX Linux
VIRUSTOTAL
urlscan.io
НКЦКИ НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ
БАНК РОССИИ ФИНЦЕРТ

Активы

iTop
Service Manager hp
Microsoft System Center Configuration Manager
MaxPatrol 8
KASPERSKY lab
Microsoft SQL Server

События

MaxPatrol SIEM
ArcSight
Check Point SOFTWARE TECHNOLOGIES LTD.
Windows 10
UNIX Linux
Windows Server
НКЦКИ НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ
БАНК РОССИИ ФИНЦЕРТ
GROUP IB

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ФИШИНГ

65 МИНУТ → 5 МИНУТ С SOAR

ДО АВТОМАТИЗАЦИИ

ПОСЛЕ АВТОМАТИЗАЦИИ

5 МИНУТ

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

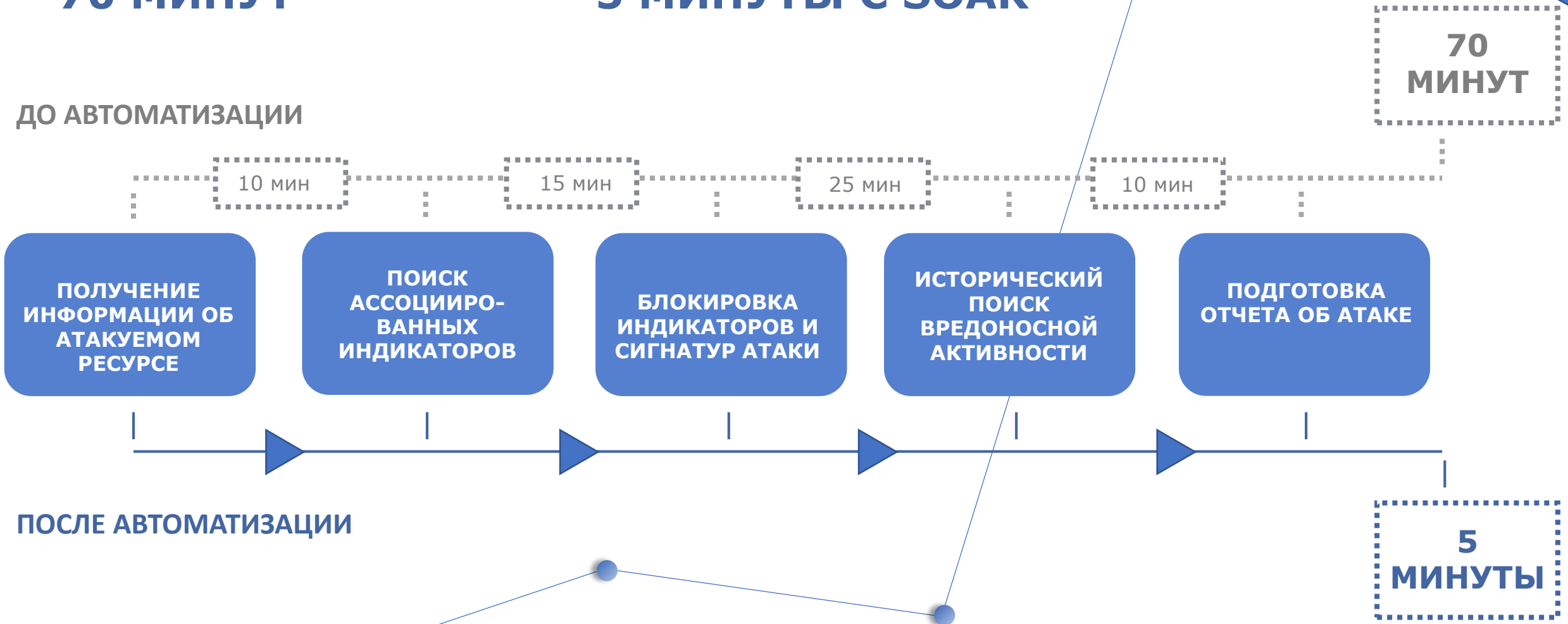
ЗАРАЖЕНИЕ

80 МИНУТ → 10 МИНУТ С SOAR

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

АТАКА НА ВНЕШНИЙ САЙТ

70 МИНУТ → 5 МИНУТЫ С SOAR



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

АНАЛИЗ ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ

85 МИНУТ → 2 МИНУТЫ С SOAR

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ПЛЕЙБУКИ: ДРУГИЕ ПРИМЕРЫ

утечка информации

отправка данных в FinCERT / НКЦКИ

распределенная атака

социальная инженерия

мониторинг изменений

мониторинг ИБ решений

предоставление и блокировка доступа

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

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

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

SGRC

01 Compliance:

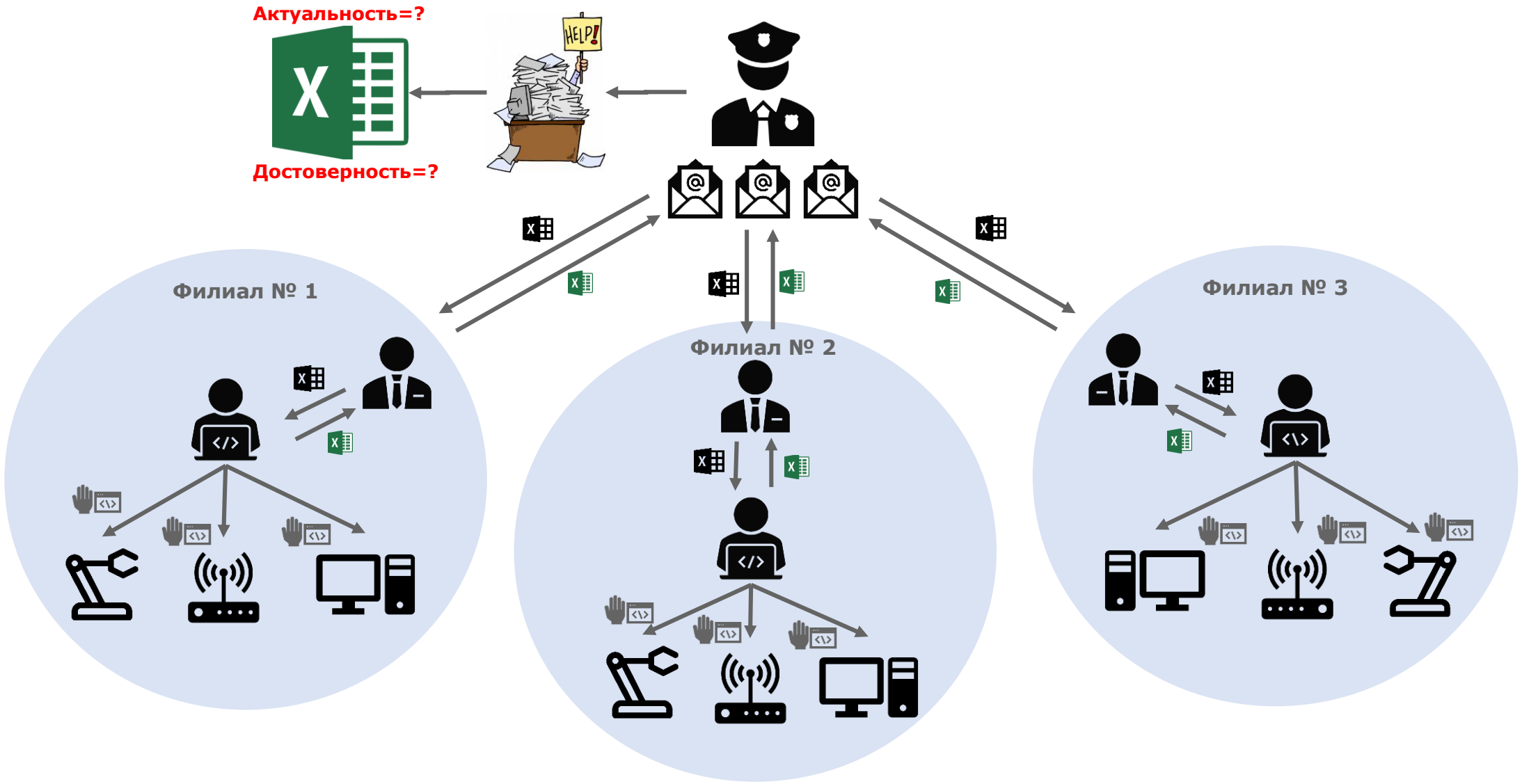
- КИИ
- ГОСТ 57580.x
- ISO 27001
- PCI DSS
- GDPR
- Custom

02 Управление рисками ИБ

03 Проведение аудитов

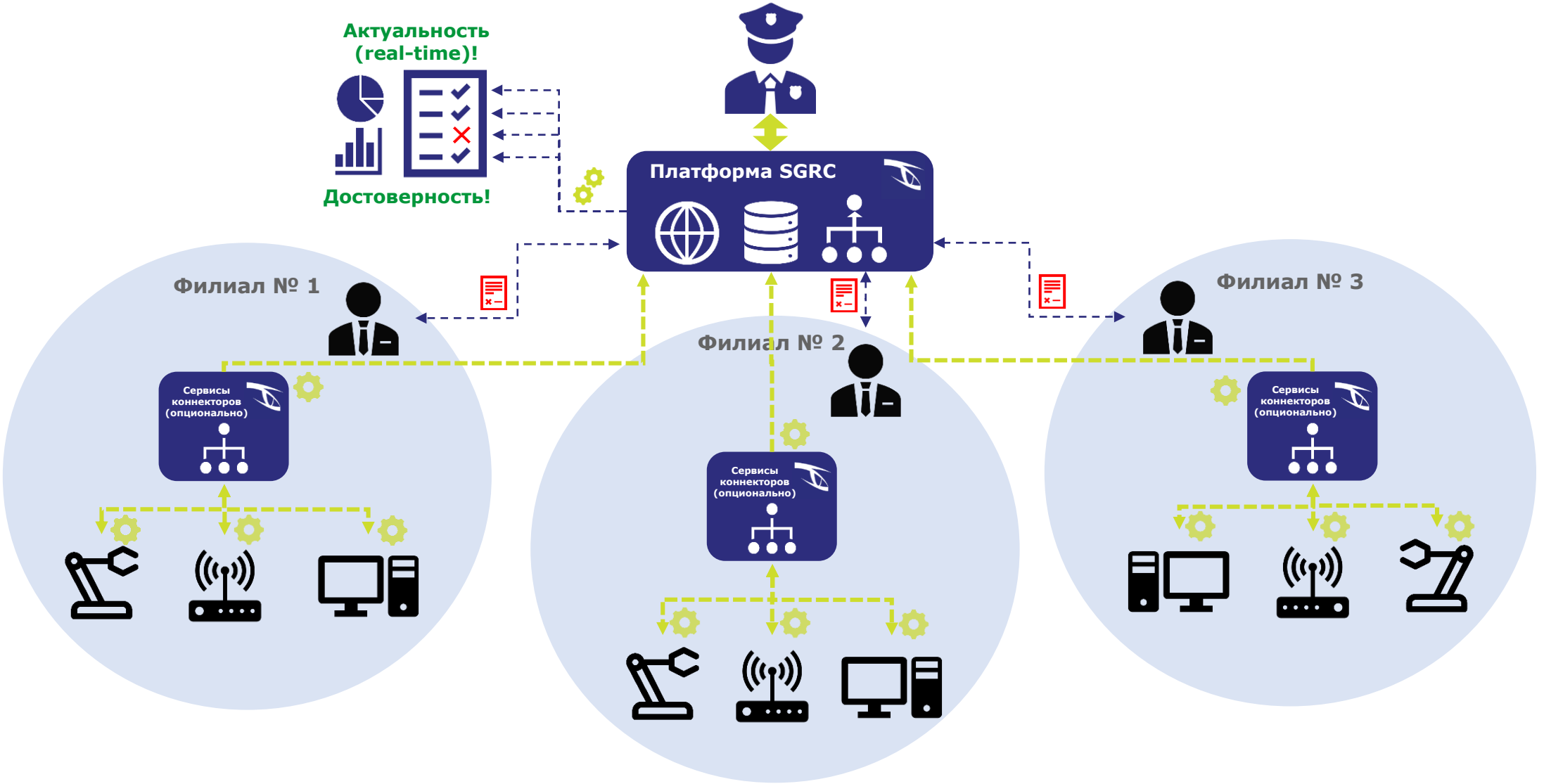
04 Контроль, автоматическая отчетность и визуализация текущего уровня соответствия

SGRC


Актуальность=?
Достоверность=?
HELP!
Филиал № 1
Филиал № 2
Филиал № 3

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

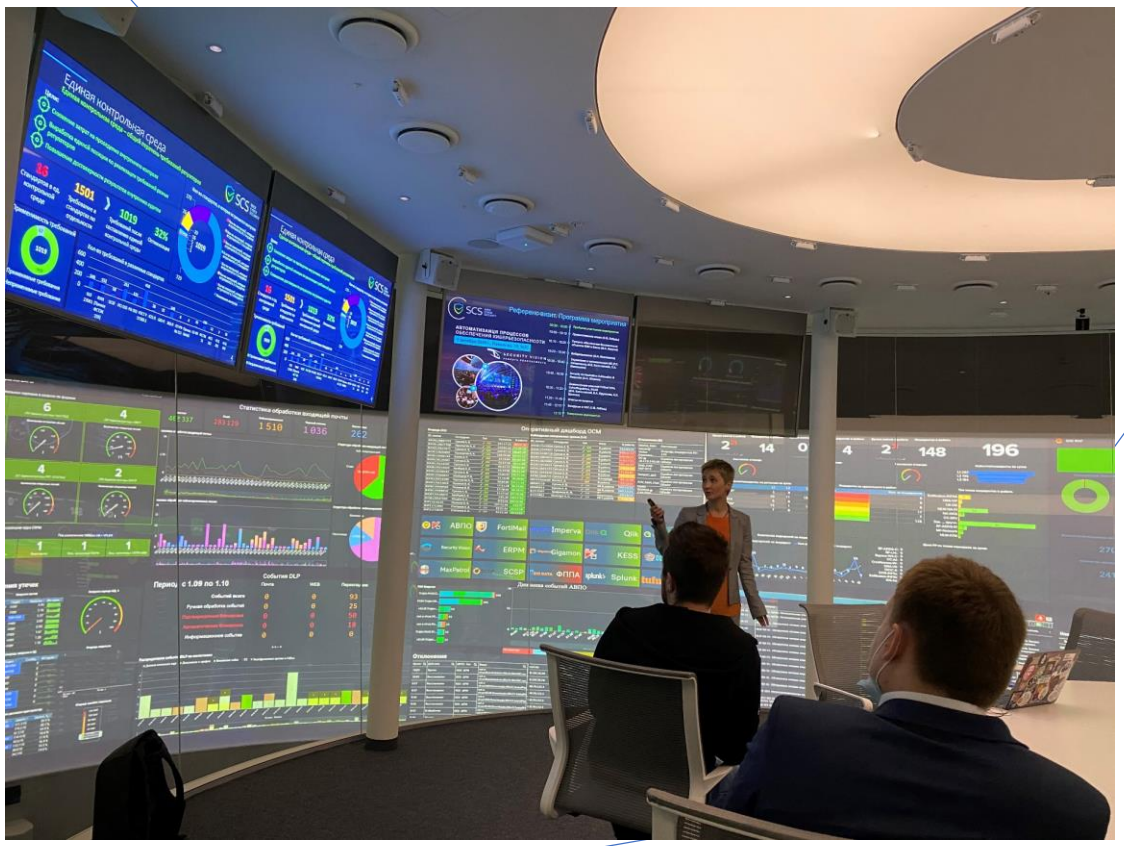
SGRC



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Успешные внедрения

Крупнейший в Восточной Европе SOC использует все продукты Security Vision



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Успешные внедрения

ПОЧТА РОССИИ

Инвентаризация: 300000+ активов

Управление уязвимостями

Управление инцидентами: 15+ плейбуков

Продолжают развивать систему самостоятельно

Custom: Управление проектами

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

СПАСИБО ЗА ВНИМАНИЕ