SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

SecOps - это не только про события

Александр Падурин
apadurin@securityvision.ru

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

SecOps – это про

- События
- Состояние

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Активы

Фундамент процессов ИБ

Интеграции с внутренними системами

+ Учётные записи
+ Сертификаты
+ Бизнес-процессы

Категорирование

Адаптивность модели активов

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Уязвимости

Диалог ИТ и ИБ

Обогащение

Приоритезация

Конвертация уязвимостей в патчи

Проверка SLA

Верификация

Emergency Patching

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

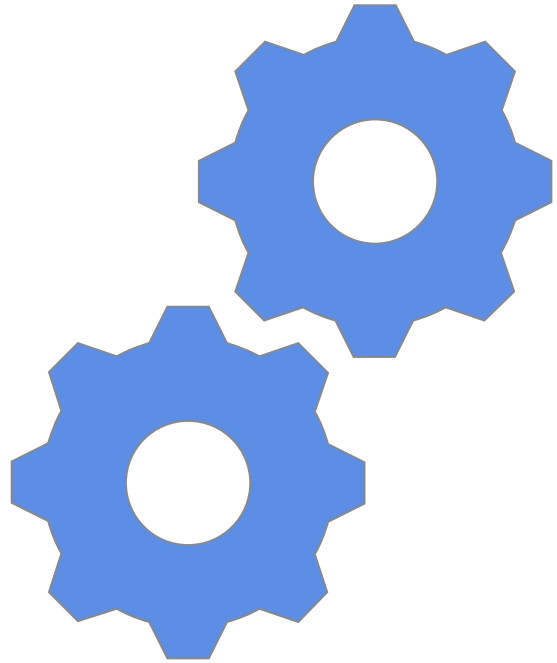
Регулярные контроли

Управление учетными записями

Управление сертификатами

Управление установленным ПО

Управление потоками данных



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Log Management

Приоритезация при сборе логов

Управление доступностью логов

Управление глубиной хранения логов

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Инциденты

SIEM ≠ Incident Management

Playbooks

Сокращение false positive

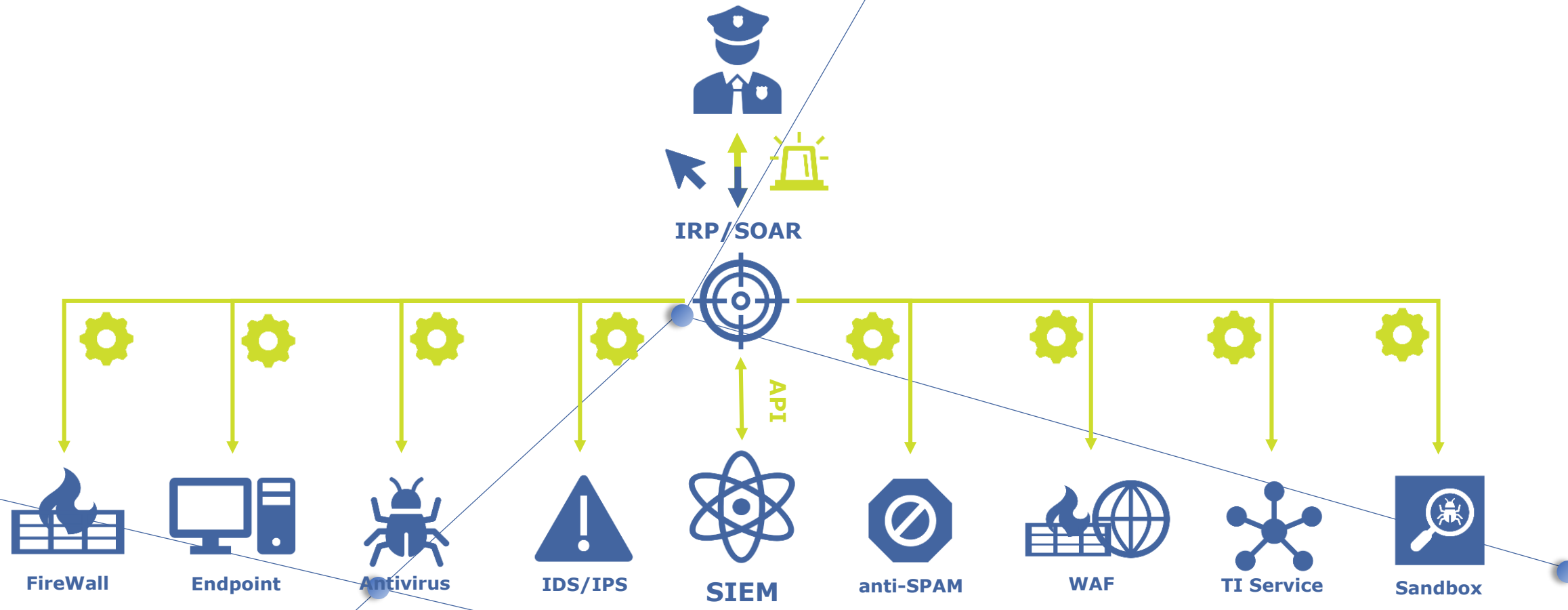
Обогащения

Единый инструмент

Оценка загруженности аналитиков

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Автоматизация



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ФИШИНГ

65 МИНУТ

ДО АВТОМАТИЗАЦИИ

15 мин	25 мин	10 мин	5 мин	10 мин
АНАЛИЗ ПОЧТОВОГО СООБЩЕНИЯ	СКАНИРОВАНИЕ РАБОЧИХ СТАНЦИИ	ПОИСК И УДАЛЕНИЕ АНАЛОГИЧНЫХ СООБЩЕНИЙ	БЛОКИРОВКА ОТПРАВИТЕЛЯ	БЛОКИРОВКА ВРЕДОНОСНЫХ ДОМЕНОВ	ИНФОРМИРО-ВАНИЕ ПОЛЬЗОВАТЕ-ЛЕЙ

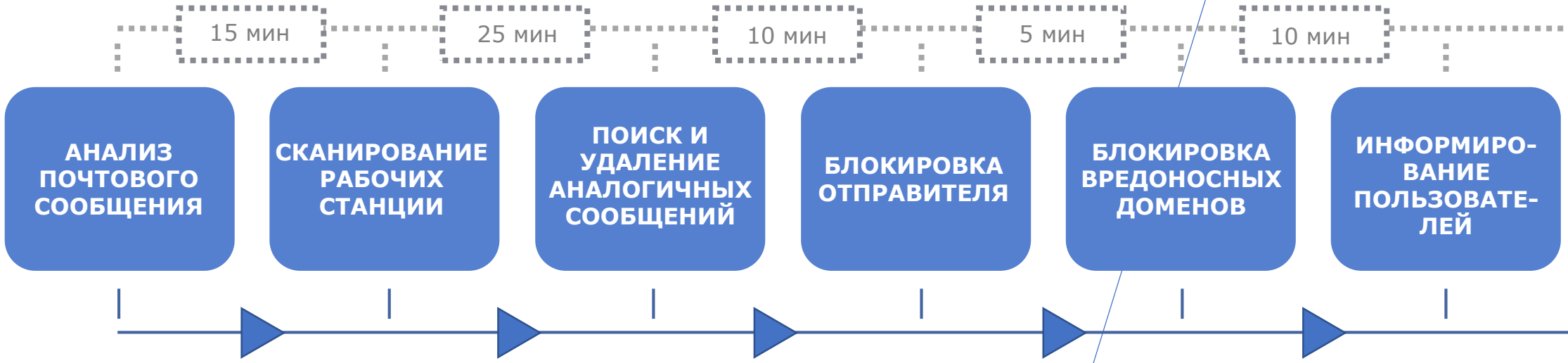
SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ФИШИНГ

65 МИНУТ → 5 МИНУТ С SOAR

65 МИНУТ

ДО АВТОМАТИЗАЦИИ

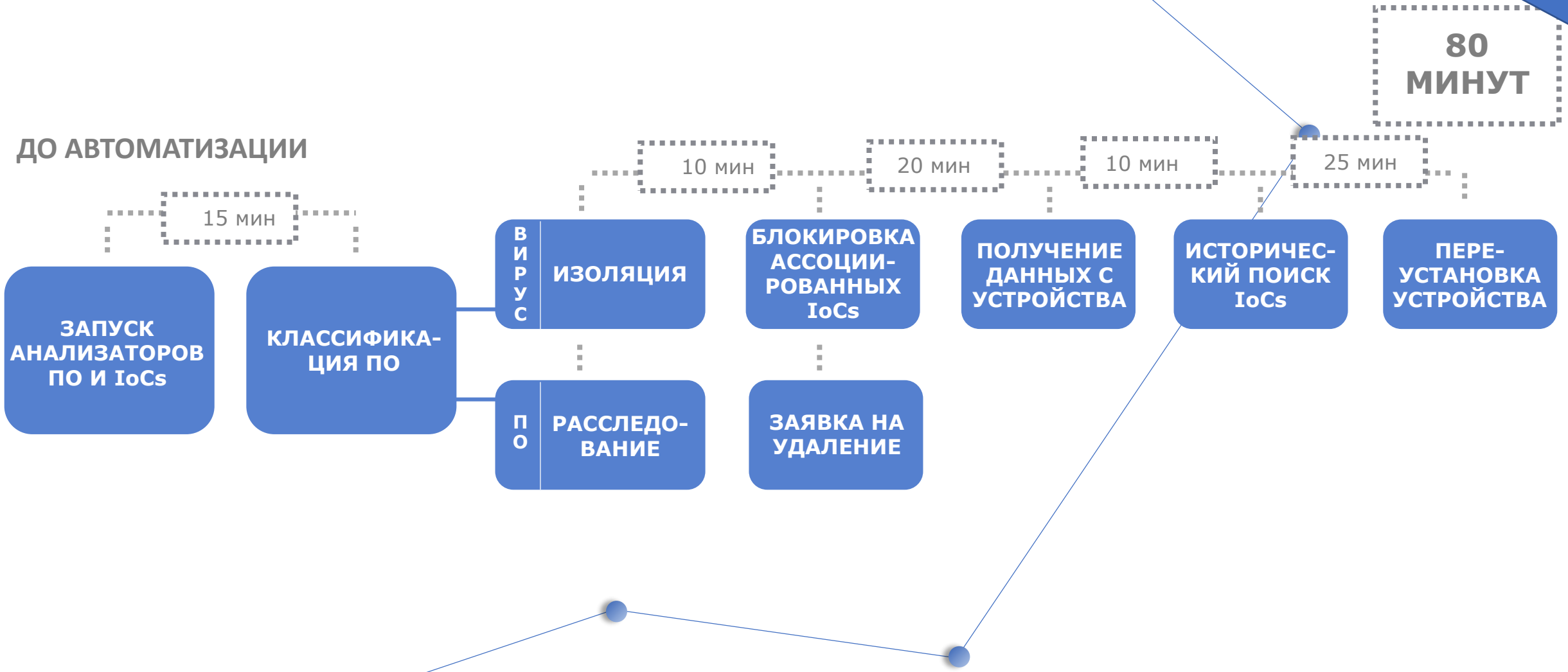


ПОСЛЕ АВТОМАТИЗАЦИИ

5 МИНУТ

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ЗАРАЖЕНИЕ



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ЗАРАЖЕНИЕ

80 МИНУТ → 10 МИНУТ С SOAR

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

АТАКА НА ВНЕШНИЙ САЙТ

70 МИНУТ

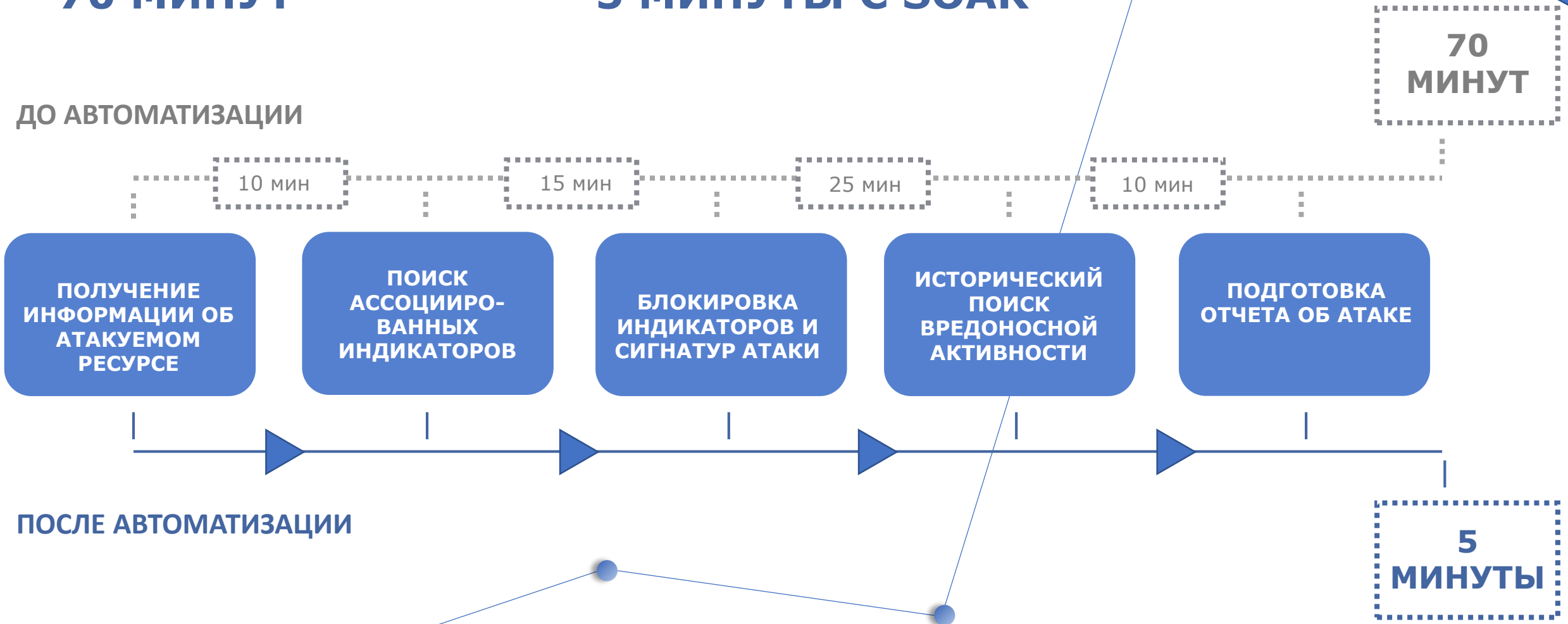
ДО АВТОМАТИЗАЦИИ

10 мин	15 мин	25 мин	10 мин
ПОЛУЧЕНИЕ ИНФОРМАЦИИ ОБ АТАКУЕМОМ РЕСУРСЕ	ПОИСК АССОЦИИРО-ВАННЫХ ИНДИКАТОРОВ	БЛОКИРОВКА ИНДИКАТОРОВ И СИГНАТУР АТАКИ	ИСТОРИЧЕСКИЙ ПОИСК ВРЕДОНОСНОЙ АКТИВНОСТИ	ПОДГОТОВКА ОТЧЕТА ОБ АТАКЕ

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

АТАКА НА ВНЕШНИЙ САЙТ

70 МИНУТ → 5 МИНУТЫ С SOAR



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

АНАЛИЗ ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ

85 МИНУТ

ДО АВТОМАТИЗАЦИИ

35 мин | 25 мин | 15 мин | 10 мин

- **ПОЛУЧЕНИЕ ИНФОРМАЦИИ СО СКАНЕРА УЯЗВИМОСТИ**
- **АНАЛИЗ КОНТЕКСТА УЯСВИМОСТИ**
- **УСТАНОВКА SLA/OLA НА УСТРАНЕНИЕ**
- **СОЗДАНИЕ ЗАЯВОК НА УСТРАНЕНИЕ**
- **КОНТРОЛЬ УСТРАНЕНИЯ И ПОДГОТОВКА ОТЧЕТА**

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:

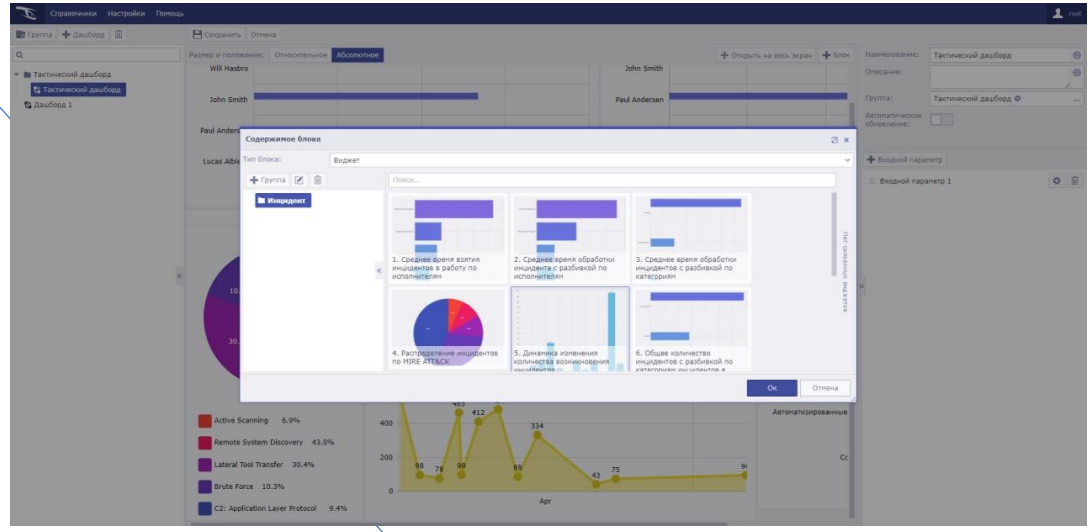
- Cortex, MISP, N8N
- Linux
- Docker\k8s
- Python\Rest API
- ElasticSearch
- Angular

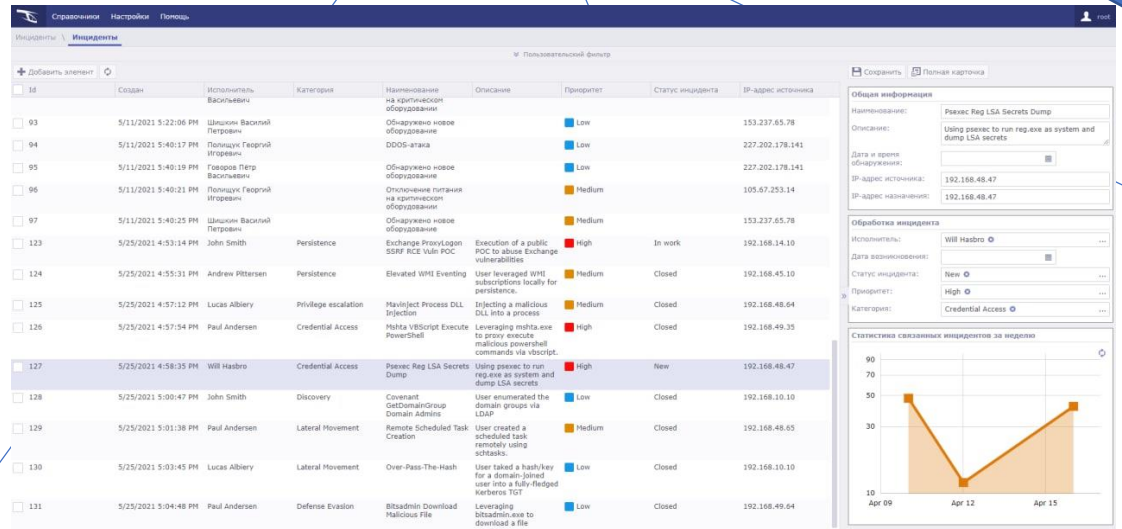
02 Дефицит кадров с соответствующей компетенцией

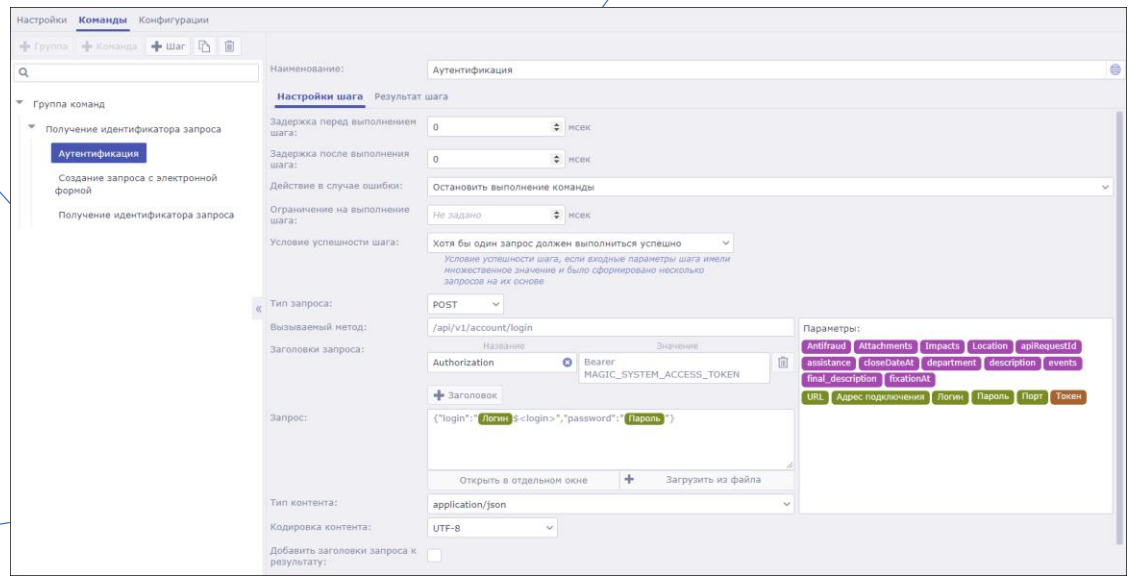
03 Кастомные решение требуют детального описания (технического писателя)

04 Разработка и актуализация интеграций ложится на внутреннюю команду

IRP (SOAR) SECURITY VISION







SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

СПАСИБО ЗА ВНИМАНИЕ