



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

SecOps - это не только про события

Александр Падурин
apadurin@securityvision.ru

SecOps – это про

События

Состояние



АКТИВЫ

Фундамент процессов ИБ

Интеграции с внутренними системами

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

Категорирование

Адаптивность модели активов



Уязвимости



Диалог ИТ и ИБ

Обогащение

Приоритезация

Конвертация уязвимостей в патчи

Проверка SLA

Верификация

Emergency Patching

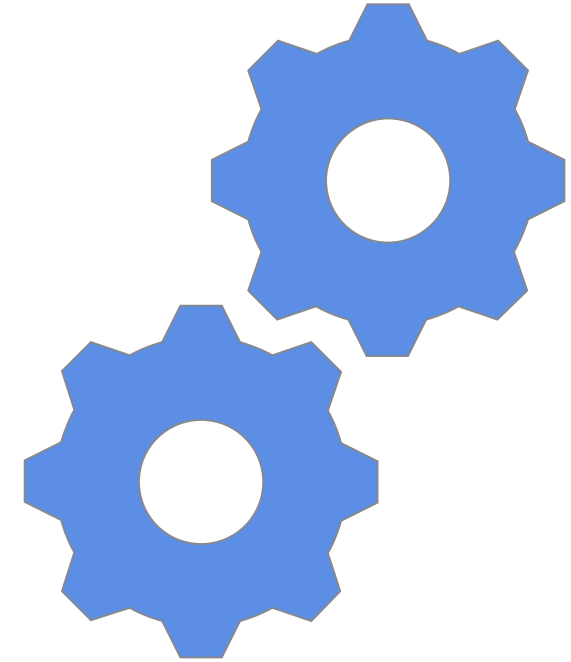
Регулярные контроли

Управление учетными записями

Управление сертификатами

Управление установленным ПО

Управление потоками данных



Log Management

Приоритезация при сборе логов

Управление доступностью логов

Управление глубиной хранения логов



Инциденты

SIEM ≠ Incident Management

Playbooks

Сокращение false positive

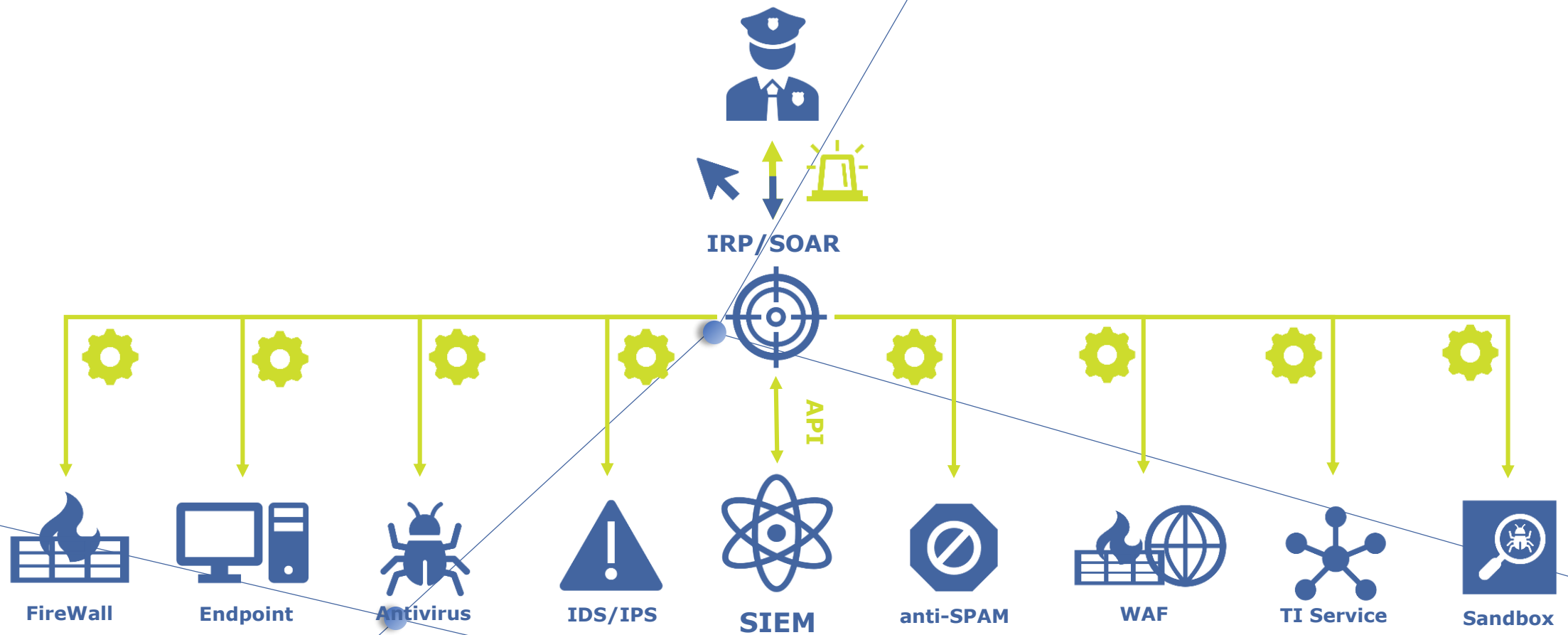
Обогащения

Единый инструмент

Оценка загруженности аналитиков

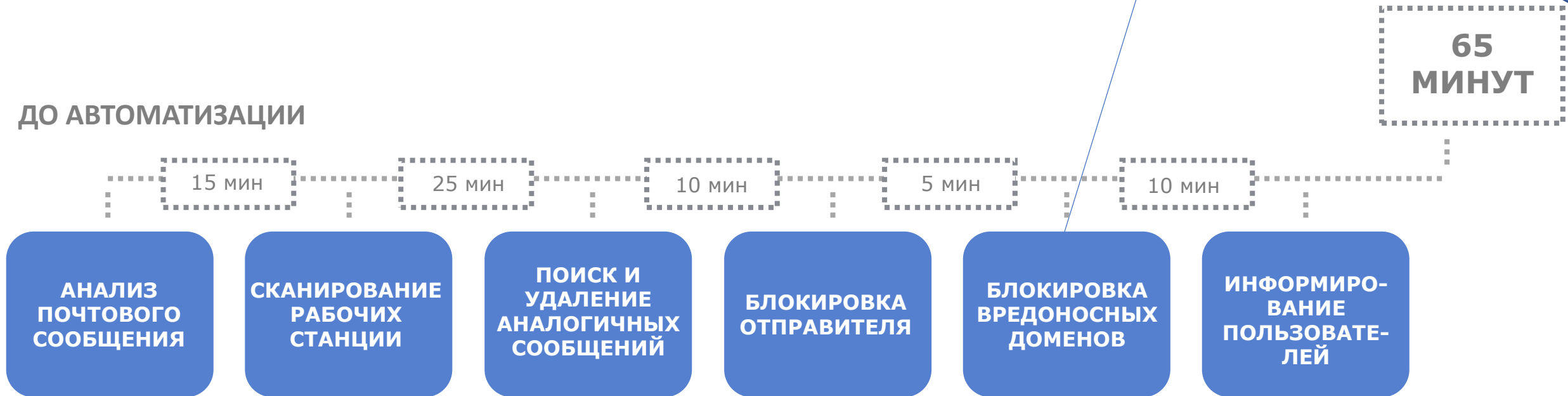


Автоматизация



ФИШИНГ

ДО АВТОМАТИЗАЦИИ



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

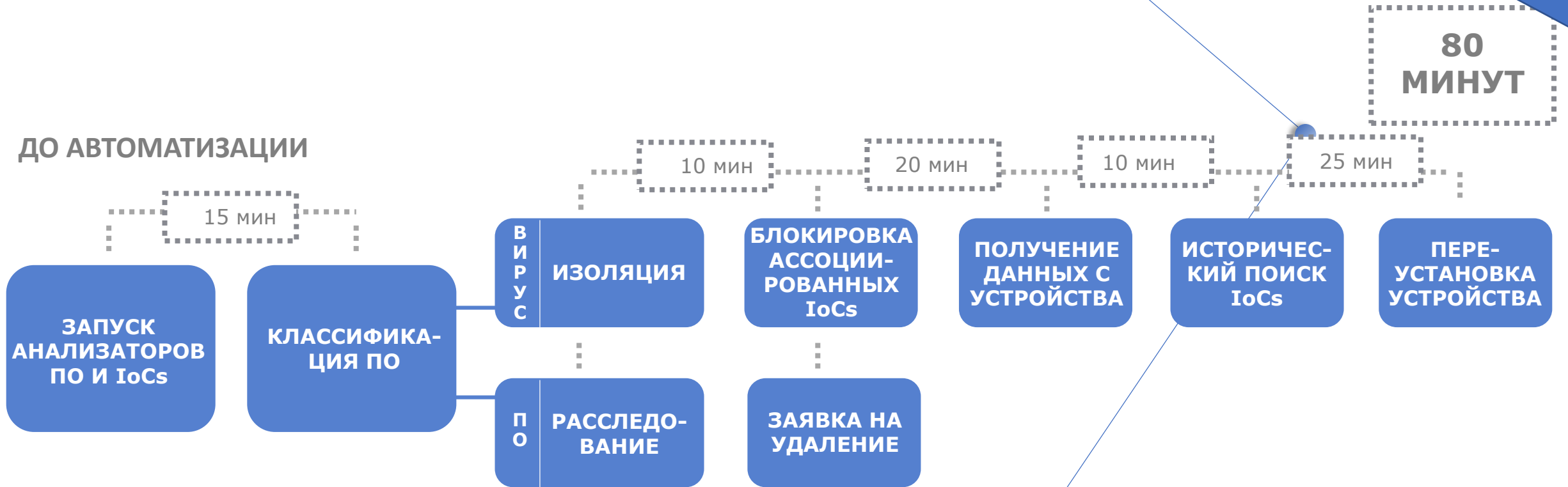
ИНФОРМИРОВАНИЕ
ПОЛЬЗОВАТЕЛЕЙ

ПОСЛЕ АВТОМАТИЗАЦИИ

5
МИНУТ

ЗАРАЖЕНИЕ

ДО АВТОМАТИЗАЦИИ



ЗАРАЖЕНИЕ

80 МИНУТ → 10 МИНУТ С SOAR

ДО АВТОМАТИЗАЦИИ



ПОСЛЕ АВТОМАТИЗАЦИИ

участие человека

10 МИНУТ

АТАКА НА ВНЕШНИЙ САЙТ

ДО АВТОМАТИЗАЦИИ

10 мин

ПОЛУЧЕНИЕ
ИНФОРМАЦИИ ОБ
АТАКУЕМОМ
РЕСУРСЕ

15 мин

ПОИСК
АССОЦИИРОВАННЫХ
ИНДИКАТОРОВ

25 мин

БЛОКИРОВКА
ИНДИКАТОРОВ И
СИГНАТУР АТАКИ

10 мин

ИСТОРИЧЕСКИЙ
ПОИСК
ВРЕДНОСНОЙ
АКТИВНОСТИ

70
МИНУТ

ПОДГОТОВКА
ОТЧЕТА ОБ АТАКЕ

АТАКА НА ВНЕШНИЙ САЙТ

70 МИНУТ → 5 МИНУТЫ С SOAR

ДО АВТОМАТИЗАЦИИ

10 мин

15 мин

25 мин

10 мин

70
МИНУТ

ПОЛУЧЕНИЕ
ИНФОРМАЦИИ ОБ
АТАКУЕМОМ
РЕСУРСЕ

ПОИСК
АССОЦИИРОВАННЫХ
ИНДИКАТОРОВ

БЛОКИРОВКА
ИНДИКАТОРОВ И
СИГНАТУР АТАКИ

ИСТОРИЧЕСКИЙ
ПОИСК
ВРЕДОНОСНОЙ
АКТИВНОСТИ

ПОДГОТОВКА
ОТЧЕТА ОБ АТАКЕ

ПОСЛЕ АВТОМАТИЗАЦИИ

5
МИНУТЫ



АНАЛИЗ

ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ

ДО АВТОМАТИЗАЦИИ

35 мин

ПОЛУЧЕНИЕ
ИНФОРМАЦИИ СО
СКАНЕРА
УЯЗВИМОСТИ

25 мин

АНАЛИЗ
КОНТЕКСТА
УЯЗВИМОСТИ

15 мин

УСТАНОВКА
SLA/OLA
НА УСТРАНЕНИЕ

10 мин

СОЗДАНИЕ ЗАЯВОК
НА УСТРАНЕНИЕ

КОНТРОЛЬ
УСТРАНЕНИЯ И
ПОДГОТОВКА
ОТЧЕТА

85
МИНУТ

АНАЛИЗ

ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ

85 МИНУТ

2 МИНУТЫ С SOAR

ДО АВТОМАТИЗАЦИИ

85
МИНУТ

35 мин

25 мин

15 мин

10 мин

ПОЛУЧЕНИЕ
ИНФОРМАЦИИ СО
СКАНЕРА
УЯЗВИМОСТИ

АНАЛИЗ
КОНТЕКСТА
УЯЗВИМОСТИ

УСТАНОВКА
SLA/OLA
НА УСТРАНЕНИЕ

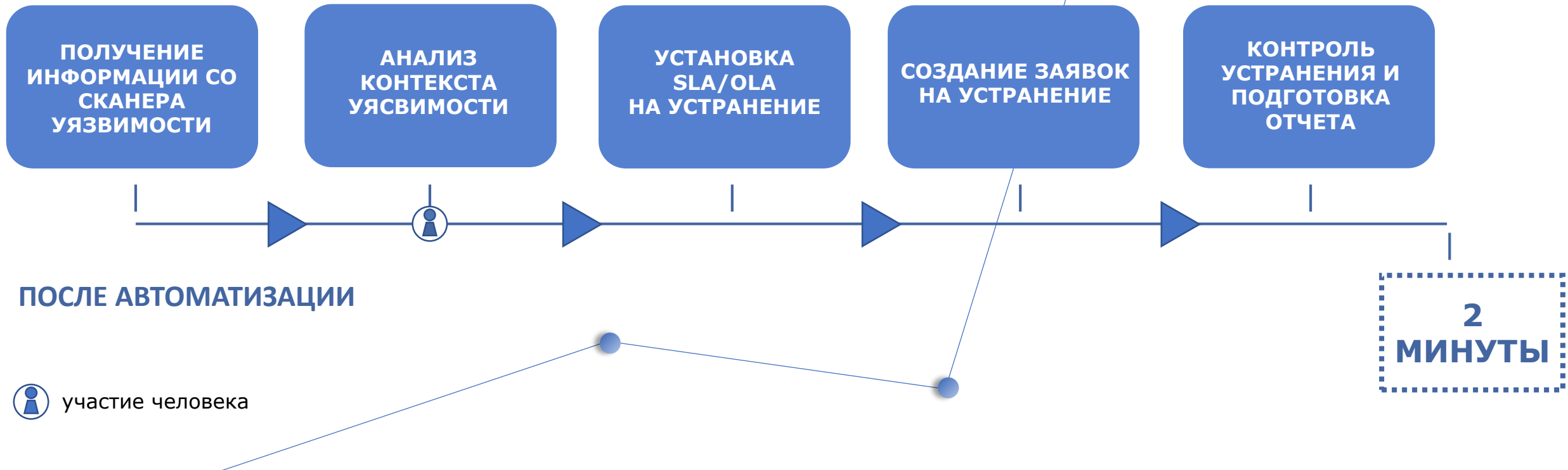
СОЗДАНИЕ ЗАЯВОК
НА УСТРАНЕНИЕ

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

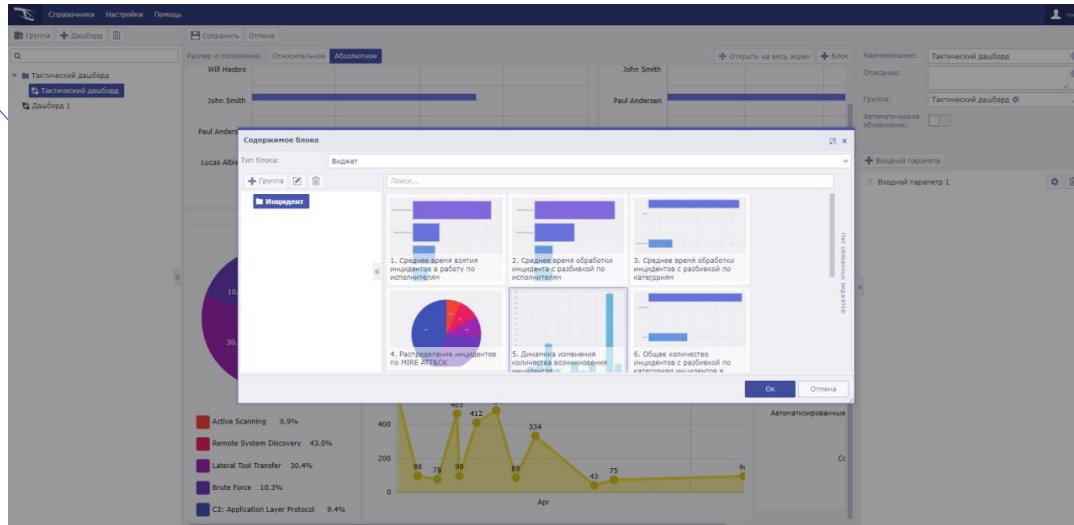
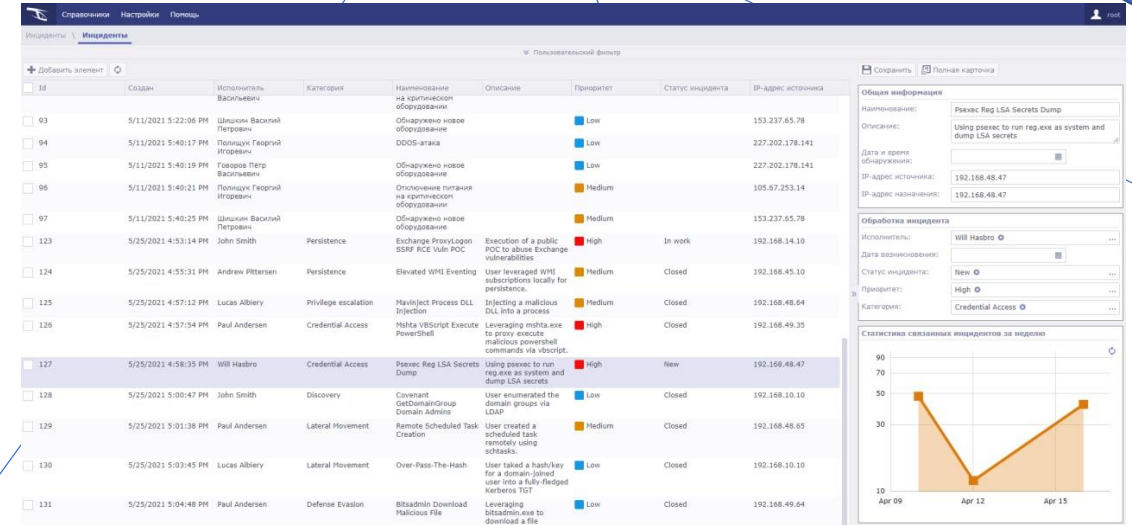
02 Дефицит кадров с соответствующей компетенцией

03 Кастомные решение требуют детального описания (технического писателя)

04 Разработка и актуализация интеграций ложится на внутреннюю команду

IRP (SOAR)

SECURITY VISION

Инциденты

Инцидент	Создан	Исполнитель	Категория	Наименование на критическом оборудовании	Описание	Приоритет	Статус инцидента	IP-адрес источника
93	5/11/2021 5:22:06 PM	Шимкин Василий Петрович		Обнаружено новое оборудование		Low		153.237.65.78
94	5/11/2021 5:40:17 PM	Полухин Георгий Игоревич		DDOS-атака		Low		227.202.178.141
95	5/11/2021 5:40:19 PM	Говоров Петр Васильевич		Обнаружено новое оборудование		Low		227.202.178.141
96	5/11/2021 5:40:21 PM	Полухин Георгий Игоревич		Отключение питания на критическом оборудовании		Medium		105.67.253.14
97	5/11/2021 5:40:25 PM	Шимкин Василий Петрович		Обнаружено новое оборудование		Medium		153.237.65.78
123	5/25/2021 4:53:14 PM	John Smith	Persistence	Exchange PrivyLogon	Execution of a public POW to abuse Exchange vulnerabilities	High	In work	192.168.14.10
124	5/25/2021 4:55:31 PM	Andrew Pittersen	Persistence	Elevated WMI Eventing	User leveraged WMI subscriptions locally for persistence.	Medium	Closed	192.168.45.10
125	5/25/2021 4:57:12 PM	Lucas Albiery	Privilege escalation	Manipulated Process DLL Injection	Injecting a malicious DLL into a process.	Medium	Closed	192.168.48.64
126	5/25/2021 4:57:54 PM	Paul Andersen	Credential Access	Malta VBScript Execute PowerShell	Leveraging malta.exe to proxy execute malicious powershell commands via vbscript.	High	Closed	192.168.49.35
127	5/25/2021 4:58:35 PM	Will Habro	Credential Access	Powercat LSA Secrets Dump	Using powercat to run reg.exe as system and dump LSA secrets.	High	New	192.168.48.47
128	5/25/2021 5:00:47 PM	John Smith	Discovery	Covenant GetDomainGroup Domain Admins	User enumerated the domain groups via LDAP.	Low	Closed	192.168.10.10
129	5/25/2021 5:01:38 PM	Paul Andersen	Lateral Movement	Remote Scheduled Task Creation	User created a scheduled task remotely using schtasks.	Medium	Closed	192.168.48.65
130	5/25/2021 5:03:45 PM	Lucas Albiery	Lateral Movement	Over-Pass-The-Hash	User talked a hash/key for a domain-based user into a fully-fledged malware TOT.	Low	Closed	192.168.10.10
131	5/25/2021 5:04:48 PM	Paul Andersen	Defense Evasion	Bitsadmin Download Malicious File	Leveraging bitsadmin.exe to download a file.	Low	Closed	192.168.49.64

Общая информация

Наименование: Powercat LSA Secrets Dump

Описание: Using powercat to run reg.exe as system and dump LSA secrets.

Дата и время обнаружения: 192.168.48.47

IP-адрес источника: 192.168.48.47

IP-адрес назначения: 192.168.48.47

Обработка инцидента

Исполнитель: Will Habro


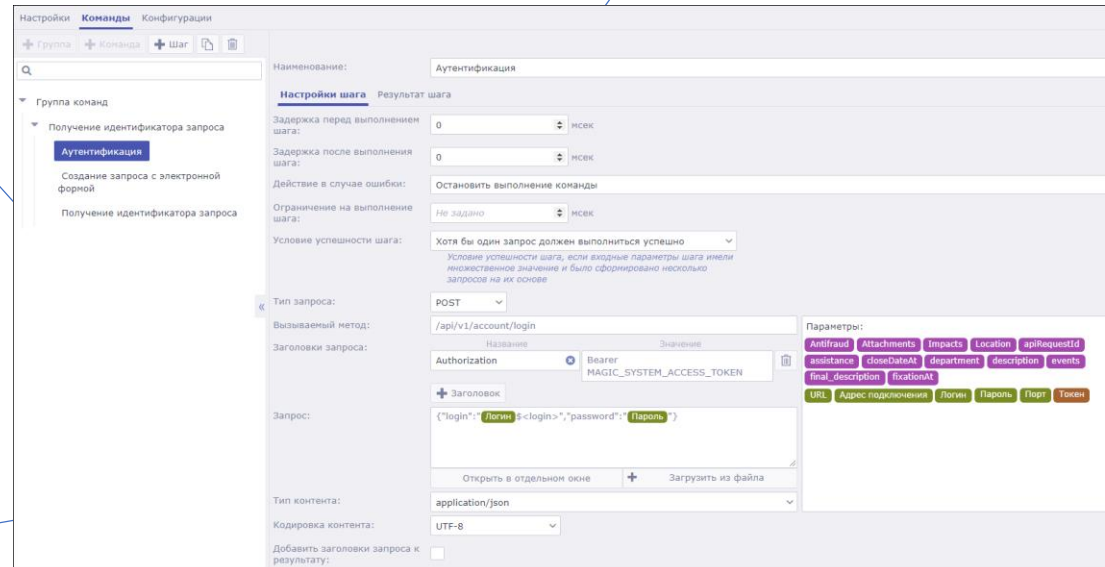
Дата возникновения: 192.168.48.47

Статус инцидента: New

Приоритет: High

Категория: Credential Access

Статистика связанных инцидентов за неделю

Настройки Команды Конфигурация

Группа Команда Шаг

Наименование: Аутентификация

Настройка шага Результат шага

Задержка перед выполнением шага: 0 мсек

Задержка после выполнения шага: 0 мсек

Действие в случае ошибки: Остановить выполнение команды

Ограничение на выполнение шага: Не задано мсек

Условие успешности шага: Хотя бы один запрос должен выполниться успешно

Условие успешности шага, если входные параметры шага имели множественное значение и было сформировано несколько запросов на их основе

Тип запроса: POST

Вызываемый метод: /api/v1/account/login

Заголовки запроса:

Название	Значение
Authorization	Bearer MAGIC_SYSTEM_ACCESS_TOKEN

Запрос: ("login" |<login> "password" |<password>)

Тип контента: application/json

Кодировка контента: UTF-8

Параметры:

- Antifraud
- Attachments
- Impacts
- Location
- apiRequestId
- assistance
- closeDateAt
- department
- description
- events
- final_description
- fixationAt
- URL
- Адрес подключения
- Логин
- Пароль
- Порт
- Токен



SECURITY VISION

УВИДЕТЬ БЕЗОПАСНОСТЬ

СПАСИБО

ЗА ВНИМАНИЕ