

INNOSTAGE ORCHESTRATOR

1

Наличие рутинных повторяющихся задач, требующие большие временные трудозатраты на реагирование по инциденту ИБ

2

Отсутствие у руководителя отдела ИБ централизованного инструментария для отслеживания выполнения задач

3

Отсутствия интеграции с имеющимся средствами защиты и ИТ сервисами

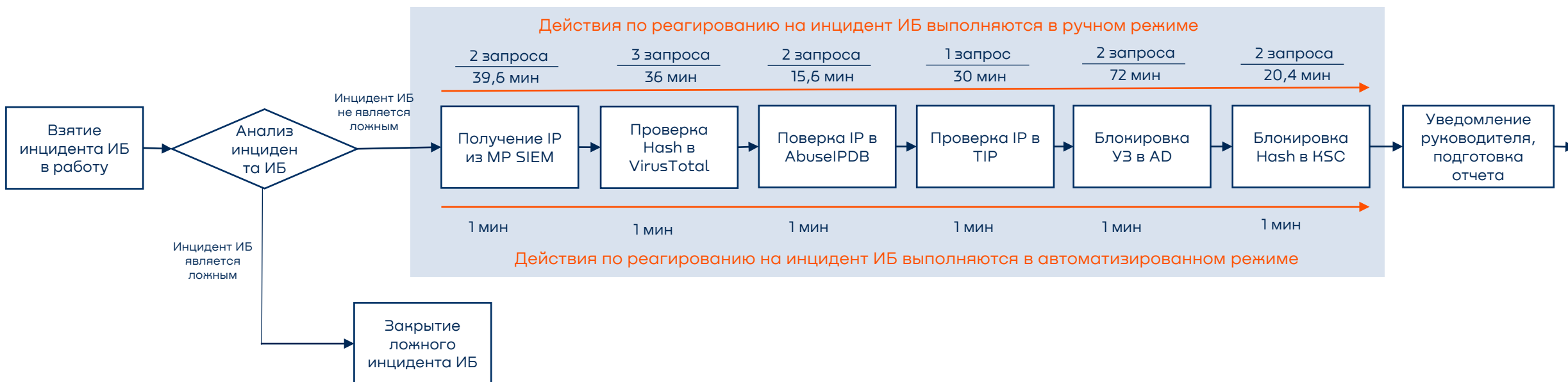
4

Необходимость круглосуточного реагирования на инденты ИБ

5

Нехватка квалифицированных специалистов ИБ и ИТ

Обработка инцидента



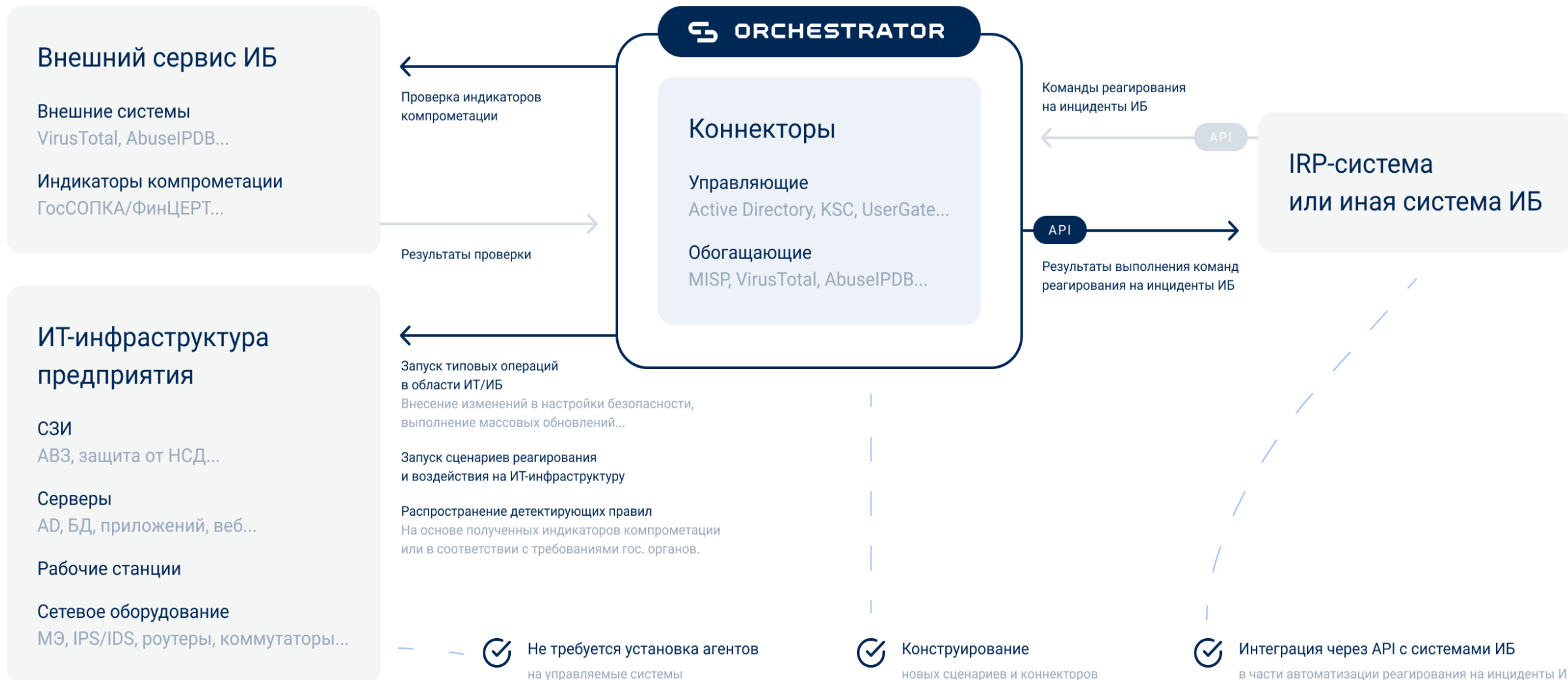
✓ ≈ **6 МИН.** Среднее время реагирования на инциденты ИБ в день **с автоматизацией**

✗ ≈ **213 МИН.** Среднее время реагирования на инциденты ИБ в день **без автоматизации**

Позволяет автоматизировать типовые операции в части реагирования на инциденты ИБ и воздействия на ИТ-инфраструктуру посредством заранее подготовленных и согласованных с профильными отделами сценариев реагирования.

- Автоматизированное выполнение блокирующих операций, внесение изменений в настройки безопасности средств защиты, компоненты ИТ-инфраструктуры, прикладные и автоматизированные системы, выполнение обновлений элементов ИТ-инфраструктуры
- Возможность межсистемной интеграции между СЗИ, в том числе для проверки и передачи индикаторов компрометации (IoC)
- Конструктор скриптов реагирования и/или воздействия на ИТ-инфраструктуру
- Наличие шаблонов и встроенного редактора кода для разработки новых коннекторов к целевым системам

Архитектура Innostage Orchestrator



Основные интеграции



ABUSEIPDB

Проверки доменного имени, IP-адреса

VIRUSTOTAL

Проверки доменного имени, хеш-суммы файла, IP-адреса, URL-адреса

PT APPLICATION FIREWALL

Получение списка IP-адресов и доменных имен для последующей блокировки на МЭ

ТИ ПЛАТФОРМА CYBERART

Получение индикаторов компрометации: IP адресов, доменных имен, для последующей блокировки на МЭ

МАХРАТРОЛ СИЕМ

Получение IP адресов, доменных имен для запуска антивирусных проверок на хостах, получение доменных учетных записей для последующей блокировки на AD

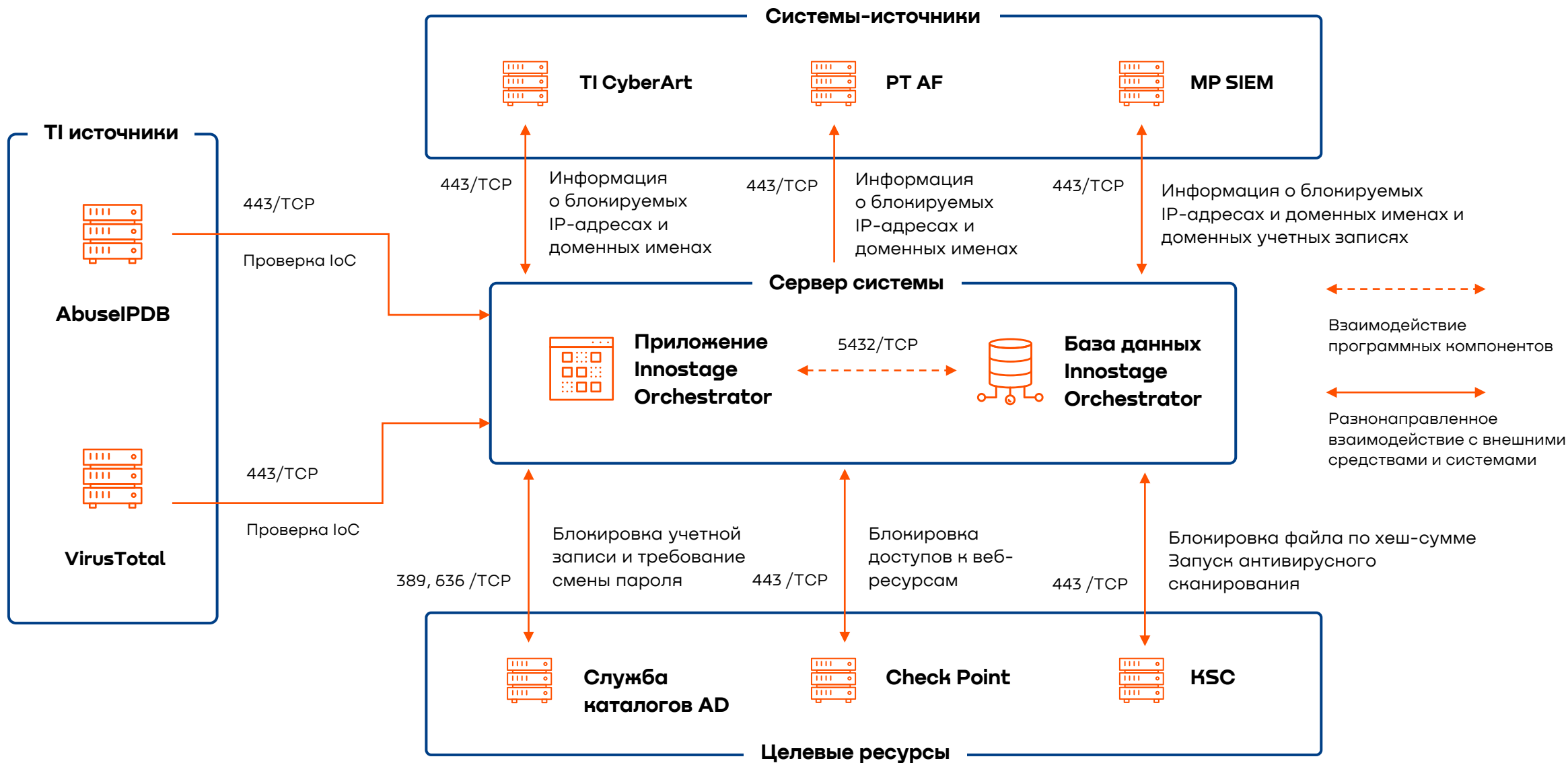
СРЕДСТВО АНТИВИРУСНОЙ ЗАЩИТЫ KSC

Блокировки запуска файлов по хеш-сумме и принудительного запуска антивирусного сканирования устройства

СЛУЖБА КАТАЛОГОВ AD

- Блокировка учетной записи
- Разблокировка учетной записи
- Исключение учетной записи из группы
- Требование смены пароля учетной записи
- Получение информации о пользователе
- Получение информации о группе
- Получение информации о компьютере
- Изменение расположения компьютера или пользователя

Схема установки



Статистика автоматизации реагирования на инциденты ИБ



ORCHESTRATOR

<

МОДУЛИ

Статистика

Сценарии

Очередь запусков

История запусков

Справочники

ПАНЕЛЬ УПРАВЛЕНИЯ

Пользователи

Настройки

О системе

Иванов И.
Администратор



25

Сценарии



20

Коннекторы



15

Целевые ресурсы



9

Учетные записи



6

Пользователи

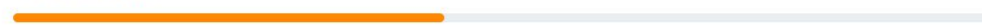


Сценарии

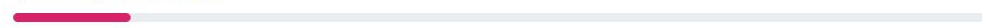
Статистика по сценариям

Неделя Месяц

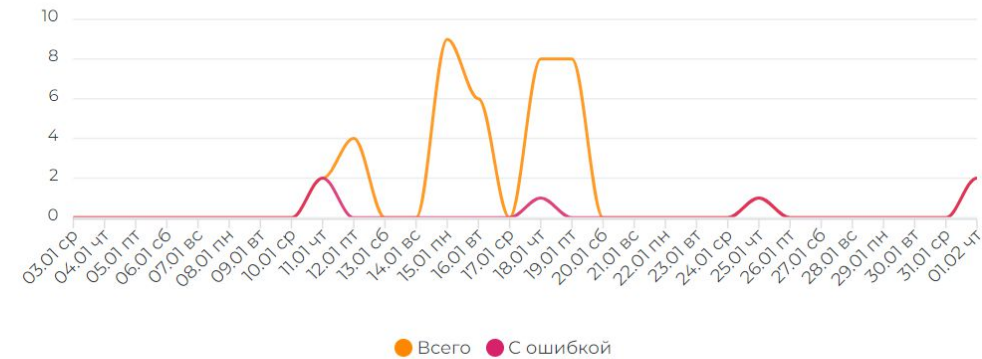
11/25 запущено



3/25 всегда с ошибкой

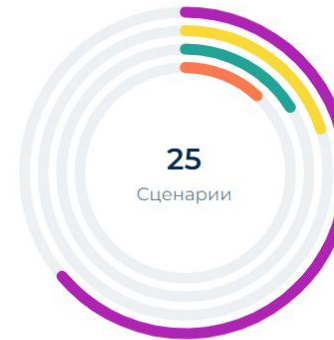


Статистика запусков сценариев



Коннекторы

0/20 установлены с ошибкой



Использование в сценариях

Innostage Security Platform	64%
VirusTotal	20%
Exchange	16%
Kaspersky Security Center	12%

Загруженность

Показатели системы



ТОП-5 сценариев

Часто используемые

Неделя Месяц

Запуск антивирусного сканирования (test_scan_1)

запусков: 2

Ошибки подключения к ресурсам



КОННЕКТОРЫ (20)

ВЕРСИЯ

ПАКЕТ УСТАНОВКИ

УСТАНОВКА

AbuseIPDB

Операции (2)

1.0.3

abuseip

20-09-2022 17:36



Active Directory

Скрыть

ОПЕРАЦИИ

- Блокировка учетной записи
- Установка требования смены пароля учетной записи
- Получение информации о пользователе
- Разблокировка учетной записи
- Получение информации о группе
- Получение информации о рабочей станции
- Изменение расположения компьютера или пользователя
- Исключение учетной записи из группы

1.1.1

ad

18-01-2024 11:37



Exchange

Скрыть

ОПЕРАЦИИ

- Блокировка писем от определенного отправителя
- Блокировка почтового ящика пользователя
- Поиск и удаление писем от определенного отправителя с определенной темой

1.0.2

exchange

07-08-2023 14:33



FortiGate

Скрыть

ОПЕРАЦИИ

- Блокировка доменного имени
- Блокировка IP-адреса

1.0.0

fortigate

09-12-2022 15:01



Innostage Security Platform

Операции (1)

2.0.0

isp

26-10-2023 15:45



Kaspersky Security Center

Операции (2)

1.0.3

kaspersky

20-09-2022 17:32



МОДУЛИ

Статистика

Сценарии

Очередь запусков

История запусков

Справочники

Коннекторы

Учетные записи

Целевые ресурсы

ПАНЕЛЬ УПРАВЛЕНИЯ

Пользователи

Настройки

О системе



СПАСИБО ЗА ВНИМАНИЕ

INNOSTAGE

Казань, ул. Подлужная, 60

+7 (843) 567-42-90

info@innostage-group.ru