

# ML в действии: строим улучшенный SOAR вместе с Security Vision



[ Блог ]  
[securityvision.ru/blog](https://securityvision.ru/blog)



[ Telegram ]  
[t.me/svplatform](https://t.me/svplatform)



[ Хабр ]  
[habr.com/ru/companies/securityvision](https://habr.com/ru/companies/securityvision)

# ПЛАТФОРМА



# Единая гибкая платформа

с кастомизацией



Объекты, карточки и  
табличные представления



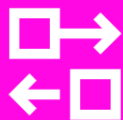
Роли и меню, доступ к  
данным и внешний вид



Рабочие процессы и  
автоматизация действий



Аналитика, интерактивные  
виджеты и дашборды



Интеграции с внешними  
системами (коннекторы)



Отчёты, выгрузка файлов  
и логирование действий

# Конструктор объектов



массовые операции

фильтрация

сортировка

быстрые ссылки

полнотекстовый поиск

кнопки управления

The screenshot displays a web application interface for object management. At the top, there is a breadcrumb navigation: "Объекты > Оборудование > Все устройства". Below this is a search bar and a toolbar with icons for search, add, and refresh. The main area contains a table of objects with columns for selection, ID, creation date, status, FQDN, IP address, operation system, last user, and data source. A detailed view of a vulnerability is shown in the foreground, including fields for ID, creation date, status, and a description of the vulnerability. The interface also features a right-hand sidebar with a "Full card" view and a "Short card" view.

метки времени

стили

ссылки

обязательные поля

полная карточка

табличный вид

краткая карточка

The screenshot displays the 'Конструктор рабочих процессов' (Process Builder) interface. On the left is a sidebar with a search bar and a tree view of process categories: 'Активы', 'Жизненный цикл', 'Ресурсно-сервисная модель', 'Экспресс отчеты', 'Общее', 'Управление рисками', 'Мониторинг дисков', 'Общие', 'Оценка рисков', and 'Управление мерами'. The main workspace shows a workflow with steps: 'Отправить сообщение' (Telegram), 'Жизненный цикл устройства', and 'Отправить письмо' (MS Exchange EWS). A 'Жизненный цикл устройства' step is expanded to show its configuration: 'Группа: Жизненный цикл', 'Типы объектов: Все типы объектов', and 'Версия: 3 - 04.03.2024 11:14:01'. Below this, a flowchart shows states: 'Начальное состояние', 'IP заполнен', 'Введение в эксплуатацию', 'Используется', and 'Выведен из эксплуатации'. A 'Введение в эксплуатацию' step is expanded to show its configuration: 'В эксплуатацию автоматически', 'Ввод в эксплуатацию', 'Отправить оповещения', 'Очистка', and 'Оповещение telegram'. On the right, a 'Статистика применения' (Usage Statistics) panel shows 'Активных процессов: 16', 'Последняя обработка: 13.09.2024, 13:31:51', and a list of active processes: 'Серверы и рабочие станции', 'Сетевое оборудование', 'Сервер АРМ', 'Базы данных', and 'Телефоны/VoIP'. A blue icon on the left represents a catalog of RPs.

статистика применения

управление версиями

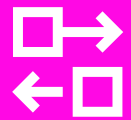
ручные и автоматические транзакции

каталог РП

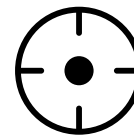
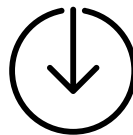
отображение дочерних объектов и результатов



WMI | PS | SSH | файл | почта | БД | HTTP (API) | LDAP | EventLog | Syslog | DNS | скрипты и др.



Сбор и обогащение



Реагирование на события

создание новых коннекторов **без участия вендоров**

создание интеграций  
через интерфейс

The screenshot displays the 'Security Vision' connector configuration in the interface. The connector is named 'Security Vision Управление Активами' and is of type 'HTTP'. Below the configuration, there is a search bar and a list of available connectors, including 'Kali tools', 'KasperskyOpenTip', 'Kaspersky Threats', 'LOLBAS', 'MaxMind Geo-IP', 'MXToolBox', 'RiskIQ', 'Security Vision TIP', 'Shodan', 'urlscan.io', 'VirusTotal', 'WhoIsXMLAPI (Сервисы)', 'Обогащение', 'Дополнительно', 'Инфраструктура', 'CMDDB', 'ITop', 'Security Vision Assets Management', 'uCMDB', 'Service Desk', 'Активы', 'Общие ресурсы', 'Почта & Мессенджеры', 'Сервис каталогов', and 'Сетевые сервисы'. The 'Security Vision Assets Management' connector is highlighted. To the right, a custom command configuration is shown for the step 'Найти ID хоста в Security Vision CMDB'. The command is a POST request to 'ip/entity/search' with a JSON body containing search criteria for host IDs. The interface also shows a 'Включен' (Enabled) toggle and a 'Получение данных о хосте по IP' (Get host data by IP) description.

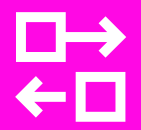
возможность  
переключения лицензий

кастомные команды и  
переменные

коннекторы, доступные  
в маркетплейсе

тестирование  
команд

WMI | PS | SSH | файл | почта | БД | HTTP (API) | LDAP | EventLog | Syslog | DNS | скрипты и др.

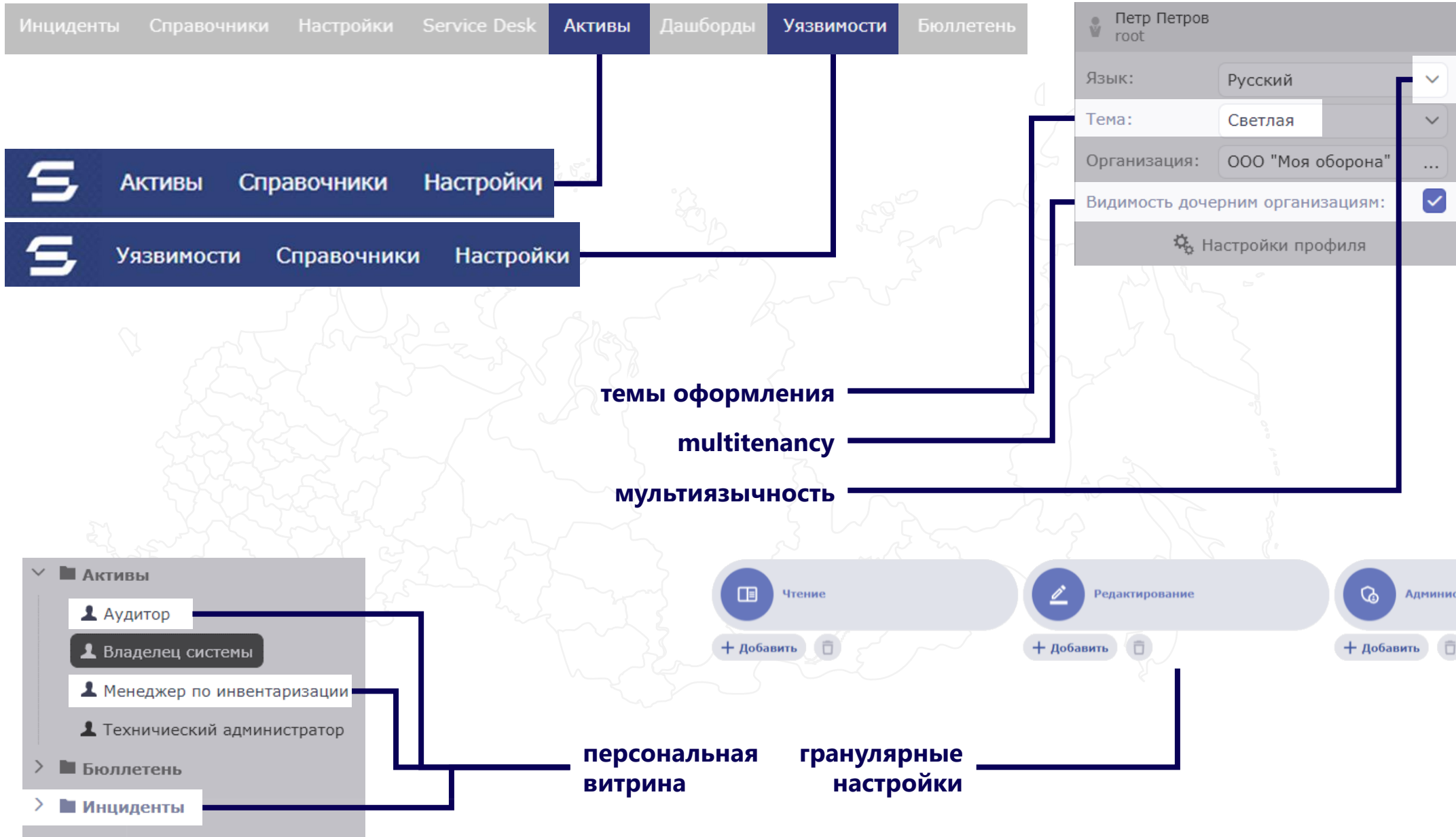


Сбор и обогащение

Реагирование на события

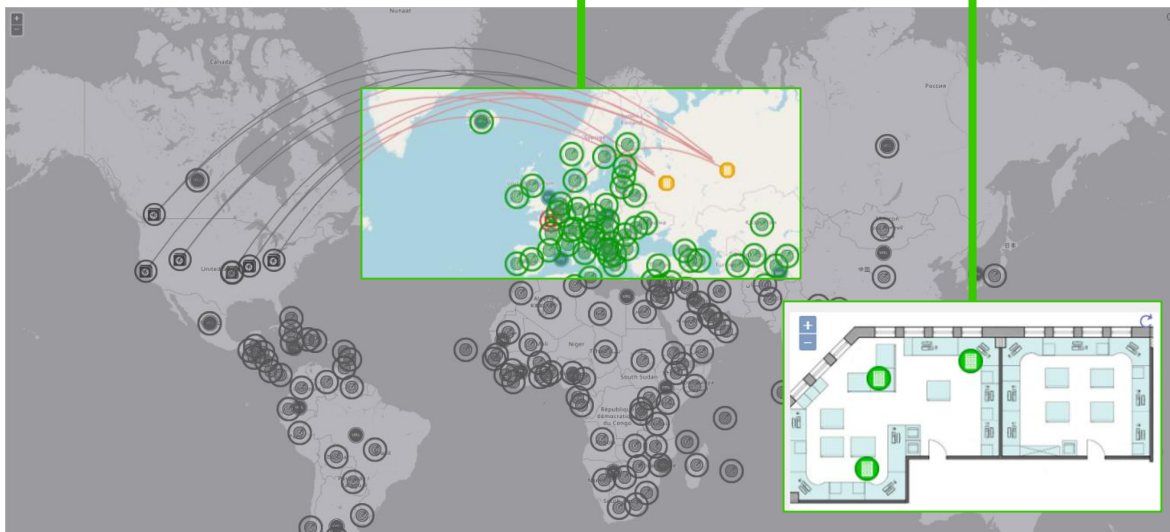
создание новых коннекторов **без участия вендоров**

# Конструктор ролей и меню



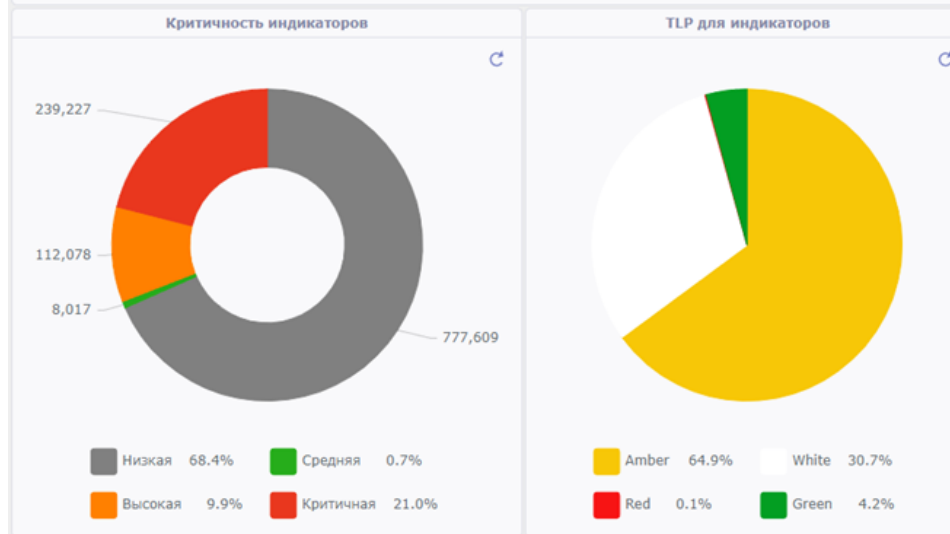
карты и планы помещений

дашборды

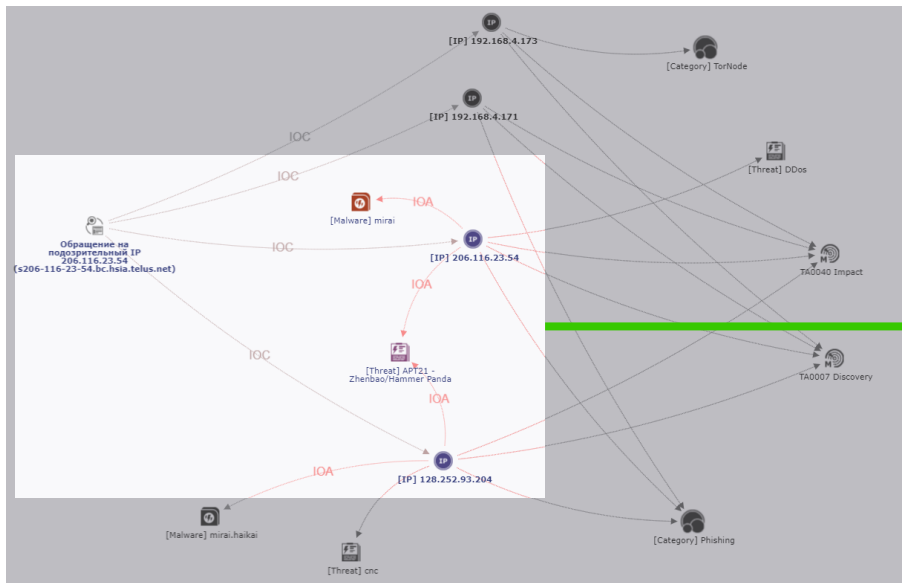


Топ-5 активных критичных инцидентов

Наименование	Критичность	Статус
Отправка письма с подозрительного домена: acmetek.com	Критичная	Новый
Обращение на подозрительный домен cutt.ly	Высокая	Новый
Обращение на подозрительный домен conect-app.com	Высокая	Новый
Обращение с подозрительного IP 192.168.4.173 (ws4-dev.sv.local)	Высокая	Новый




графы связей



интерактивная аналитика и связанные графики

Количество активных индикаторов за период	Количество активных инцидентов за период
934676	7





Отчет по активам

Дата выгрузки: 04.06.2024 14:56:44

Период: 01.02.2023 - 27.06.2024

### Статистика активов

Новые активы

**135**

Новые критичные активы

**14**


Инвентаризовано

**9**

Ошибка инвентаризации

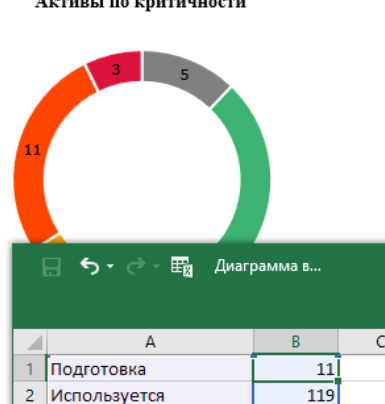
**45**

#### Активы по статусам



Статус	Количество
Подготовка	4
Используется	119
Не используется	11
Утилизирован	0

#### Активы по критичности



Критичность	Количество
Высокая	11
Средняя	3
Низкая	5

Сохранить Отмена

Размер и положение: Относительное Абсолютное

Сгенерировать отчет: docx pdf xlsx ods odt txt csv

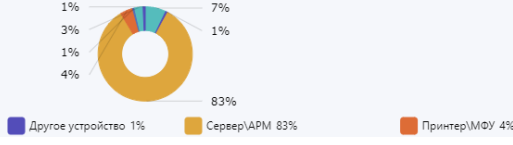
Импортировать настройки из дашборда ↔ Переменные

Основной +

#### Таблица всех активов

Тип устройства	Количество
Сетевое устройство	10
Другое устройство	1
Сервер\АРМ	116
Принтер\МФУ	6
Интерфейс удаленного управления	1
Телефон\VoIP	4
Система хранения данных	1

#### Процентное соотношение количества устройств



Тип устройства	Процент
Сервер\АРМ	83%
Сетевое устройство	7%
Принтер\МФУ	4%
Другое устройство	1%

#### Прогресс устранения:

Исполнитель: Петров Петр Петрович

Дата визита в работу: 15.06.2022 21:21:29

SLA по устранению узвимости: 90d 00h 00m

Срок исполнения: **12.09.2022 15:57:02**

Потрачено планового времени: 32%

Остаток времени до окончания срока исполнения: 61d 07h 27m

#### Данные по хосту:

Тип	FQDN	IP адрес	Операционная система
Сервер\АРМ	DEMO-DC	192.168.18.50	Microsoft Windows Server 2019 Standard

#### Общая информация:

Статус: В работе

Срок исполнения: 12.09.2022 15:57:02

Описание уязвимости: A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs. An un-authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected ADFS server. The attacker who successfully exploited the vulnerability could then perform cross-site scripting attacks on affected systems and run scripts in the security context of the current user.

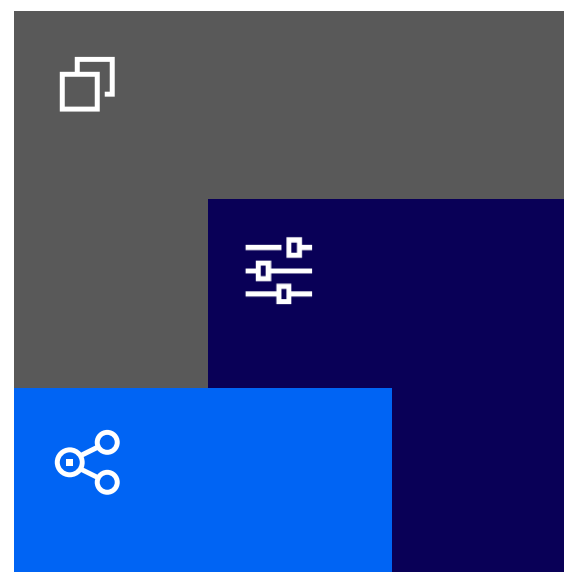
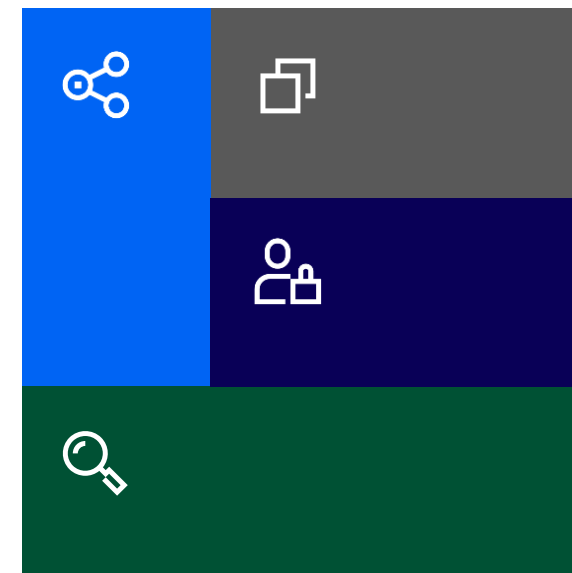
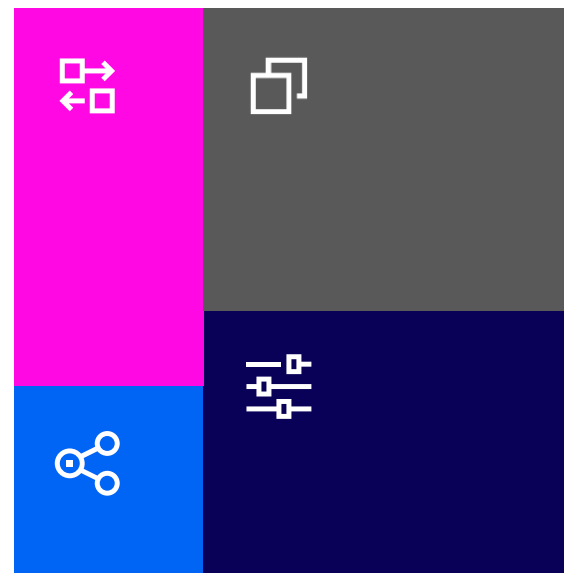
Способ исправления: Use the vendor's advisory: <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1055>

#### Прогресс устранения:

Исполнитель: Петров Петр Петрович

Дата визита в работу: 15.06.2022 21:21:29

Собирайте модули  
под ваши задачи  
без навыков  
программирования  
с помощью гибких  
конструкторов



# Единая платформа развивается в **трех** направлениях

**SOAR**  
управление инцидентами

**FinCERT**  
взаимодействие с ЦБ

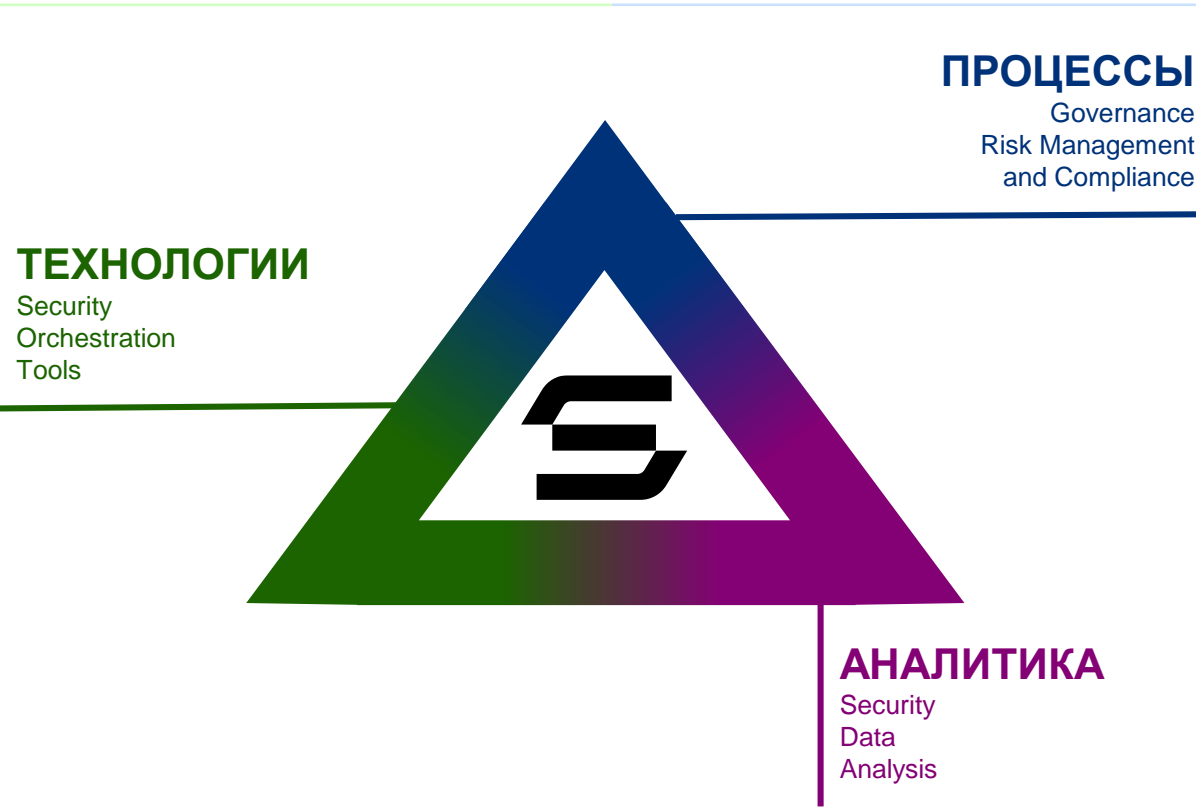
**ГосСОПКА**  
взаимодействие с НКЦКИ

**VM**  
управление уязвимостями

**VS**  
сканер уязвимостей

**SPC**  
управление конфигурациями безопасности

**AM**  
управление активами и инвентаризацией



**КИИ**  
управление соответствием ФЗ-187

**СМ**  
управление соответствием НМД

**RM**  
управление рисками кибербезопасности

**ORM**  
управление операционными рисками

**BCM**  
управление непрерывностью бизнеса

**SA**  
управление состоянием ИБ

**BASIC**  
линейка для SMB

**NGX**  
комплекты

**TIP**  
анализ угроз кибербезопасности

**UEBA**  
поведенческий анализ и поиск аномалий

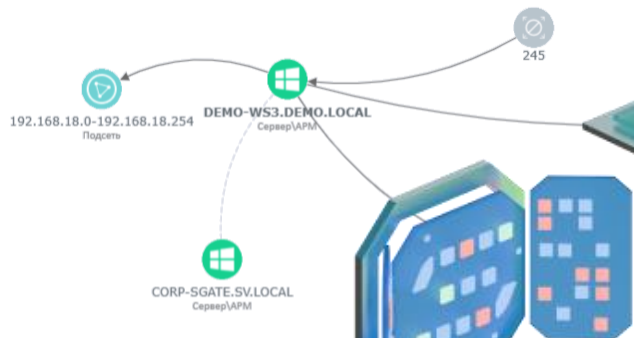


# Управление активами и инвентаризацией

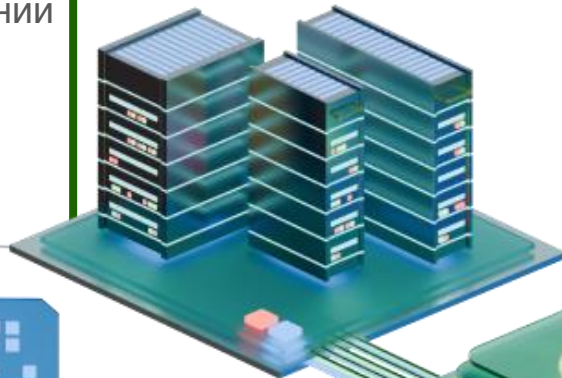


## ресурсно-сервисная модель

единая модель данных для связей с ИТ- и бизнес-сущностями компании

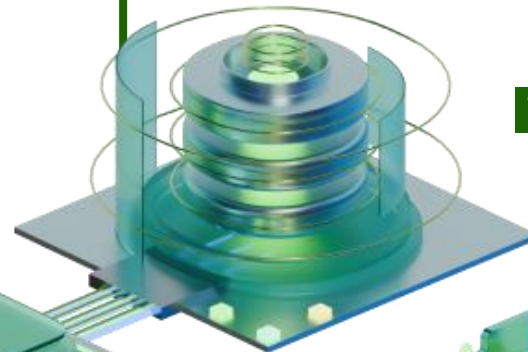


2



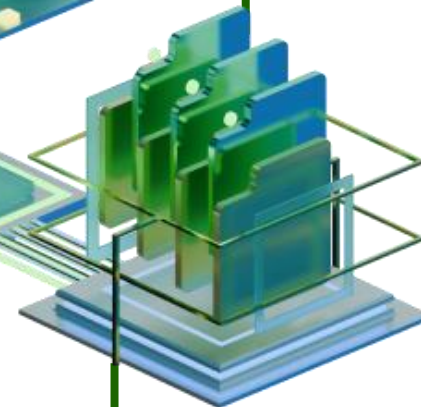
## 1 поиск объектов

сканирование по расписанию, формирование каталогов активов и построение карты сети



## 7 безопасность

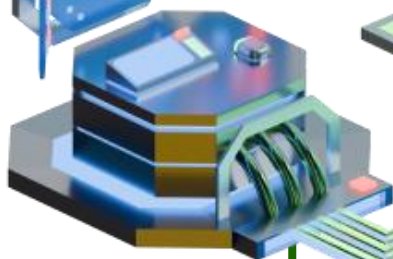
фокус на ИТ-задачах и мониторинге защищенности



## обогащение

сбор дополнительной информации из разных систем, БД и файлов

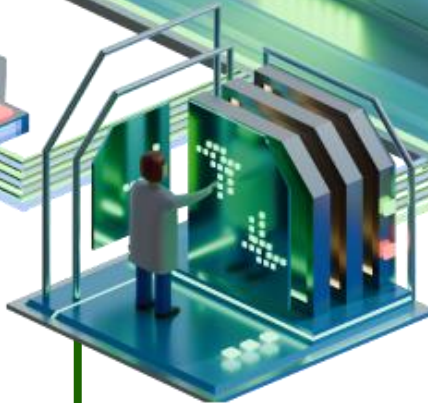
3



## 4 категорирование

фильтрация активов, поиск данных и связей между любыми объектами

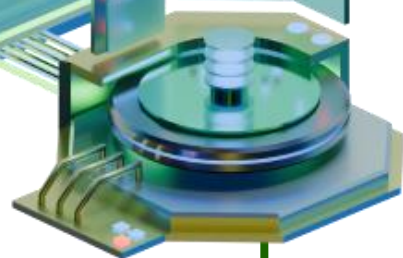
4



## жизненный цикл

фиксация изменений атрибутов объектов от их появления до вывода эксплуатации

5



## управление ПО

черные и белые списки, обновление и удаление

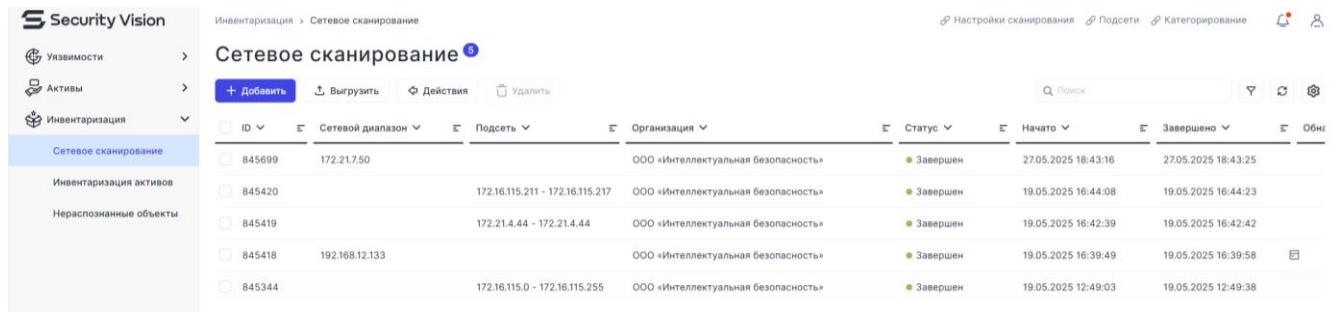
6



AM

3

# Поиск объектов с построением карты сети



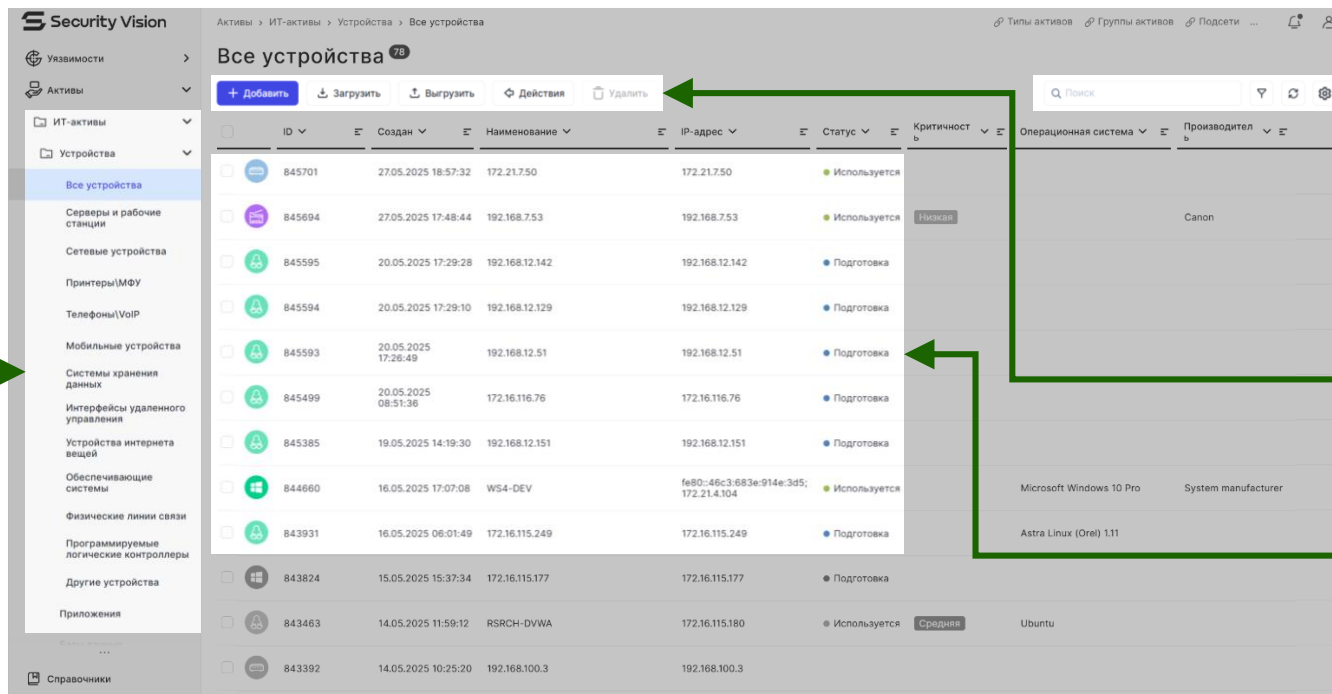
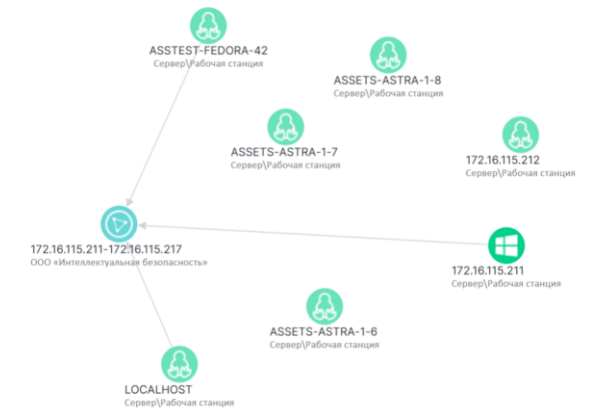
Security Vision - Сетевое сканирование

Сетевое сканирование

ID	Сетевой диапазон	Подсеть	Организация	Статус	Начато	Завершено	Обн
845699	172.217.50		ООО «Интеллектуальная безопасность»	Завершен	27.05.2025 18:43:16	27.05.2025 18:43:25	
845420	172.16.115.211 - 172.16.115.217		ООО «Интеллектуальная безопасность»	Завершен	19.05.2025 16:44:08	19.05.2025 16:44:23	
845419	172.21.4.44 - 172.21.4.44		ООО «Интеллектуальная безопасность»	Завершен	19.05.2025 16:42:39	19.05.2025 16:42:42	
845418	192.168.12.133		ООО «Интеллектуальная безопасность»	Завершен	19.05.2025 16:39:49	19.05.2025 16:39:58	
845344	172.16.115.0 - 172.16.115.255		ООО «Интеллектуальная безопасность»	Завершен	19.05.2025 12:49:03	19.05.2025 12:49:38	



IP-адрес	Имя хоста
172.16.115.211	172.16.115.211 (Сервер/Рабочая станция)
172.16.115.212	172.16.115.212 (Сервер/Рабочая станция)
172.16.115.213	ASSTEST-FEDORA-42 (Сервер/Рабочая станция)
172.16.115.214	ASSETS-ASTRA-1-7 (Сервер/Рабочая станция)
172.16.115.215	LOCALHOST (Сервер/Рабочая станция)
172.16.115.216	ASSETS-ASTRA-1-8 (Сервер/Рабочая станция)
172.16.115.217	ASSETS-ASTRA-1-6 (Сервер/Рабочая станция)



Security Vision - Все устройства

ID	Создан	Наименование	IP-адрес	Статус	Критичность	Операционная система	Производитель
845701	27.05.2025 18:57:32	172.217.50	172.217.50	Используется			
845694	27.05.2025 17:48:44	192.168.7.53	192.168.7.53	Используется	Низкая		Canon
845595	20.05.2025 17:29:28	192.168.12.142	192.168.12.142	Подготовка			
845594	20.05.2025 17:29:10	192.168.12.129	192.168.12.129	Подготовка			
845593	20.05.2025 17:26:49	192.168.12.51	192.168.12.51	Подготовка			
845499	20.05.2025 08:51:36	172.16.116.76	172.16.116.76	Подготовка			
845385	19.05.2025 14:19:30	192.168.12.151	192.168.12.151	Подготовка			
844660	16.05.2025 17:07:08	WS4-DEV	fe80::46c3:683e:914e:3d5; 172.21.4.104	Используется		Microsoft Windows 10 Pro	System manufacturer
843931	16.05.2025 06:01:49	172.16.115.249	172.16.115.249	Подготовка		Astra Linux (Oran) 1.11	
843824	15.05.2025 15:37:34	172.16.115.177	172.16.115.177	Подготовка			
843463	14.05.2025 11:59:12	RSRCH-DVWA	172.16.115.180	Используется	Средняя	Ubuntu	
843392	14.05.2025 10:25:20	192.168.100.3	192.168.100.3				

гранулярная настройка расписаний и окон сканирования

сквозной поиск по всем объектам, свойствам и фильтрам

автоматическое сканирование и загрузка активов из файлов

обогащение данными и каталог для нераспознанных активов

кастомизируемые группы и любые типы объектов



AM

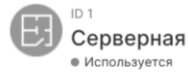
Asset Management

управление активами и инвентаризацией

# Ресурсно-сервисная модель

# ИТ-активы и бизнес-сущности

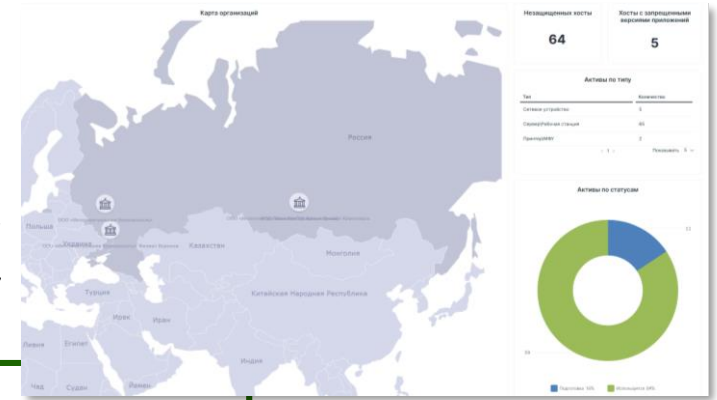
ИТ- и бизнес-активы, документы и схемы



Общая информация План **Документы** История

Наименование	Номер	Дата	Файл
Приказ №333	№333	06.03.2024	Бизнес-процесс_Тест 2 (10).pdf

глобус, планы помещений и карта сети



десятки технических и бизнес типов активов «из коробки» с возможностью расширения

ИИ-инструмент для поиска сетевых маршрутов

## Поиск маршрутов

IP-адрес источника: 172.16.115.214 [IPv4 IPv6]

IP-адрес назначения: 172.16.116.76 [IPv4 IPv6]

Искать порты:

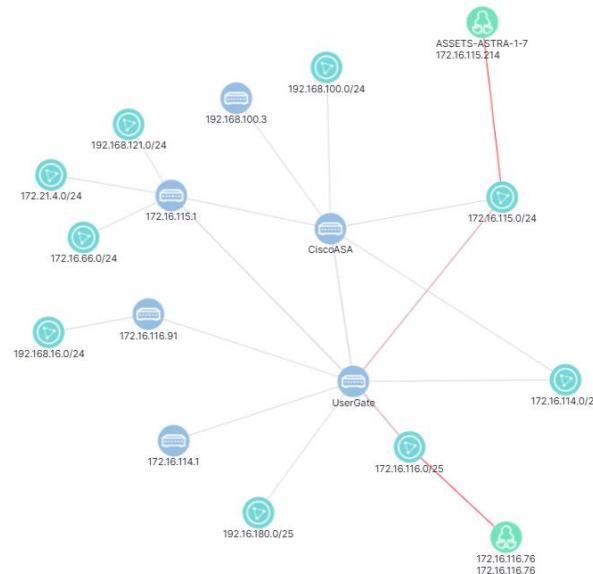
Искать протоколы:

Исключить порты:

Исключить протоколы:

## Найденные маршруты 2

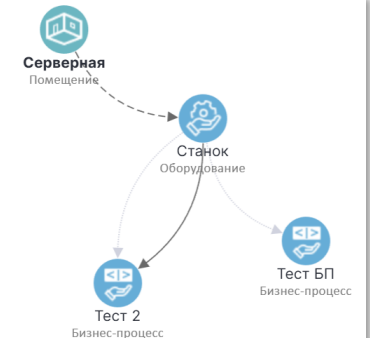
Наименование	IP входящий	Интерфейс входящий	IP исходящий	Интерфейс исходящий	Правило блокировки
ASSETS-ASTRA-1-7			172.16.115.214	eth0	
172.16.115.0/24					
UserGate	172.16.115.5	port0	172.16.116.50	port1	
172.16.116.0/25					
172.16.116.76	172.16.116.76	eth0			



План помещения photo\_2023-10-20-12-10-41.121.jpg



Создан: 18.03.2024 18:10:37 (Администратор Системы)  
 Обновлено: 29.05.2025 16:42:05 (Администратор Системы)  
 Ответственный: Администратор Системы  
 Подразделение: Отдел развития  
 Организация: ООО «Интеллектуальная безопасность»  
 Ответственный за пожарную безопасность: Гайнуллина Катерина



AM

Asset Management

управление активами и инвентаризацией

# Мониторинг состояния и управление ПО и оборудованием

управление установкой, обновлением и удалением

черные и белые списки для ПО на хостах и серверах

Запрещенное ПО: **1** Списки ПО (Белый/Черный)

ID 13569 **WL**  
Google Chrome

Общая информация **Версии и обновления** История

Разрешить все Запретить все

Версия	Разрешено	Количество хостов	Организация
<input type="checkbox"/> 124.0.6367.62	<input checked="" type="checkbox"/>	0	ООО «Интеллектуальная безопасность»
<input type="checkbox"/> 96.0.4664.110	<input checked="" type="checkbox"/>	0	ООО «Интеллектуальная безопасность»
<input type="checkbox"/> 97.0.4692.71	<input checked="" type="checkbox"/>	0	ООО «Интеллектуальная безопасность»
<input type="checkbox"/> 124.0.6367.118	<input checked="" type="checkbox"/>	0	ООО «Интеллектуальная безопасность»

Общая информация **Конфигурация** Безопасность Сеть Службы Приложения Пользователи Граф Расположение Виртуальные машины История

**Системные параметры**

Операционная система Microsoft Windows 10 Pro  
Семейство ОС Windows  
Версия ОС 19045  
Версия ядра/сборки 19045  
Архитектура ОС 64

Производитель System manufacturer  
Модель System Product Name  
Серийный номер System Serial Number

Время последнего запуска 22:13:53 15.05.2025

Период непрерывной работы системы 4 дней 14:29:56

Последний пользователь WS4-DEV\USER1 (19.05.2025 06:51:54)

Дата установки ОС 11.08.2020 19:36:44

Автообновление  
Сервер обновлений  
Сервер виртуализации

**Технические параметры**

UUID системы B704E7E0-72BA-11E3-8A26-2C4D544ED42B

Процессор Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz

Физические процессоры 1

Логические процессоры 8

Оперативная память 32768 Gb

Нагрузка диска 235

Средняя загрузка 67

**Настройки времени и языков**

Время на хосте (локальное) 18:39:31 19.05.2025

Время на хосте (UTC) 05-19-2025 04:39:31Z

Часовой пояс (UTC+03:00) Moscow, St. Petersburg

Сервер времени time.windows.com

Локализация хоста ru-RU [ Russian (Russia) ]

Язык системы ru en-US

**Процессор, %**  
Данные отсутствуют

**Память, %**  
50

**Жесткие диски**

ID Диска	Имя (точка монтирования)	Объем	Свободно
428BC777	C:	222,96 GB	16%
4C8421DC	D:	931,50 GB	25%
B22743B6	E:	931,39 GB	20%

**Общие папки**

Имя	Путь
ADMIN\$	C:\Windows
C\$	C:\
D\$	D:\

Подключенные устройства

Тип	Имя	Описание
USB	USB\VID_046D&PID_C328\5&521A615&0&10	USB Composite Device
USB	USB\ROOT_HUB30\4&1148BC98&0&0	USB Root Hub (USB 3.0)

контроль утилизации оборудования (использования ресурсов)

200+ метрик «из коробки» и комбинирование переменных

подключаемые носители данных и другие внешние устройства



AM

Asset Management  
управление активами и инвентаризацией

ПО и железо

Управление

Безопасность

Поиск объектов  
Модель данных



## 1 сбор алертов и подозрений на инциденты

интеграция СЗИ, макро-корреляция, группировка и дедупликация событий

## 2 обогащение

аналитические данные из внешних систем и баз знаний

Результат анализа <https://tuiaazul.com.br/www.netflix/0cb18...>

Домен: tuiaazul.com.br  
Страна: US  
Город:  
Сервер: Apache  
IP-адрес: 192.185.177.73  
ASN: AS26337  
Имя ASN: OIS1, US

UrlSCAN Score: 100  
True

Ссылка на результат проверки: <https://urlscan.io/result/198e520f-7853-4c64-8570-...>

Результат анализа сигнатуры EICAR-Test-File через Kaspersky Threats:

Описание сигнатуры: Под именем "EICAR-Test-File" детектируется небольшой 68-байтный COM-файл, который вирусом НЕ ЯВЛЯЕТСЯ, а всего лишь выводит текстовое сообщение и возвращает управление DOS.

Дата обнаружения:

Класс: DangerousObject  
Дата публикации в базе: 19/04/2016

## 3 управление СЗИ

интеграция ИБ и ИТ систем, управление статусами и SLA

## 6 рекомендации для аналитиков

управление задачами, работа в группе, база знаний от экспертов и ИИ-помощники

## 5 динамические сценарии

плейбуки, которые автоматически подстраиваются под окружение

## 4 цепочки атак

классификация и построение kill-chain



# SOAR

# Сбор алертов, инцидентов и сырых данных с обогащением

цепочки атак по NIST, группировка и действия

быстрый поиск по любым параметрам и таблицам

Атаки 9

Выгрузить Действия Удалить

ID	Создана	Критичность	Наименование	Статус
15100580	15.05.2025 17:06	Критическая	Внутреннее сканирование в локальной сети→Попытка эксплуатации критической уязвимости +4	Активна
15100551	15.05.2025 16:44	Критическая	Аутентификация с подозрительного IP→Внутреннее сканирование в локальной сети +2	Завершена
15100505	15.05.2025 15:16	Критическая	Внутреннее сканирование в локальной сети→Попытка эксплуатации критической уязвимости +4	Завершена
15100484	15.05.2025 12:04	Критическая	Аутентификация с подозрительного IP→Внутреннее сканирование в локальной сети +7	Завершена
15100447	13.05.2025 14:43	Критическая	Аутентификация с подозрительного IP→Внутреннее сканирование в локальной сети +9	Завершена
15100429	13.05.2025 13:51	Критическая	Аутентификация с подозрительного IP→Внутреннее сканирование в локальной сети +7	Завершена

Поиск

ID 15100429

Аутентификация с подозрительного IP→Внутреннее сканирование в локальной сети

Общая информация

Создана 13.05.2025 13:51:44

Обновлена 13.05.2025 13:59:18

Типы инцидентов

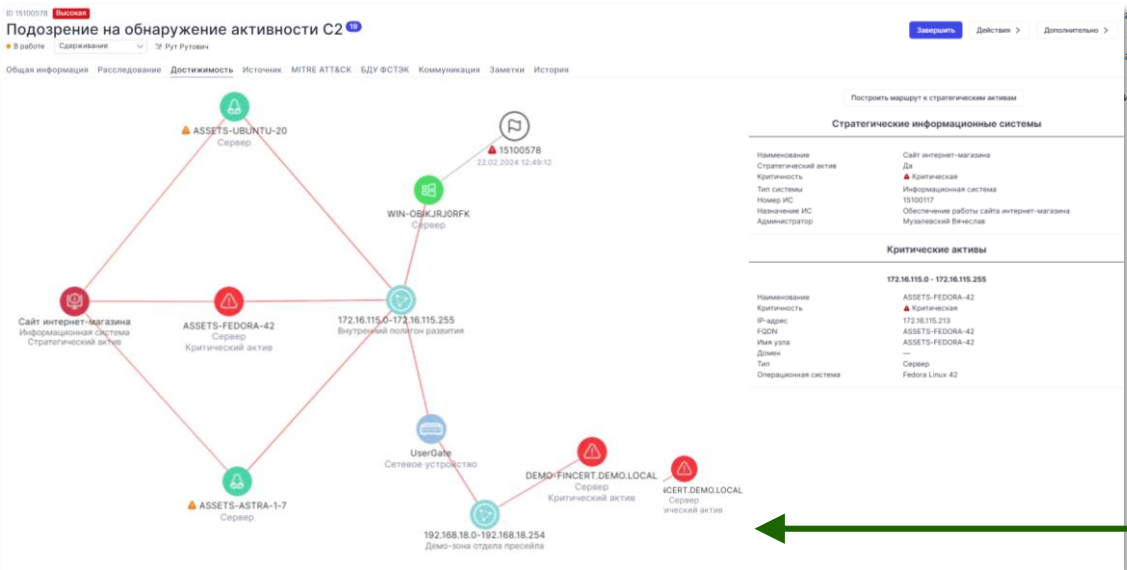
- Смена УЗ между сессиями
- Обход СЗИ
- Аномалии VPN, RDP, RDG, SSH, proxy
- Вредоносный трафик (c2c, trojan, exploit)
- Сканирование сети изнутри

Источники

- Snort
- UserGate
- Microsoft-Windows-Sysmon
- OpenVPN
- Linux

Статистика

Инциденты	Задачи
8/9	0/3
Объекты	Артефакты
9	8



конструктор коннекторов и интеграция с любым СЗИ

поиск деталей и автоматическое обогащение

граф достижимости маршруты нарушителей

- ID 15100441 Закрыт Аутентификация с подозрительного IP
- ID 15100442 Закрыт Внутреннее сканирование в локальной сети
- ID 15100443 Закрыт Попытка эксплуатации критической уязвимости
- ID 15100444 Закрыт Снятие снимка памяти процесса lsass с помощью Procdump
- ID 15100446 Закрыт Обнаружена техника атаки Process Hollowing
- ID 15100451 Закрыт Запуск сессии root
- ID 15100452 Закрыт Запуск сессии root
- ID 15100458 Закрыт Множественные неудачные попытки входа Linux
- ID 15100461 Закрыт Запуск хакерских утилит Linux
- ID 15100465 Закрыт Подозрение на обнаружение активности C&C
- ID 15100476 Закрыт Запуск сессии root



SOAR

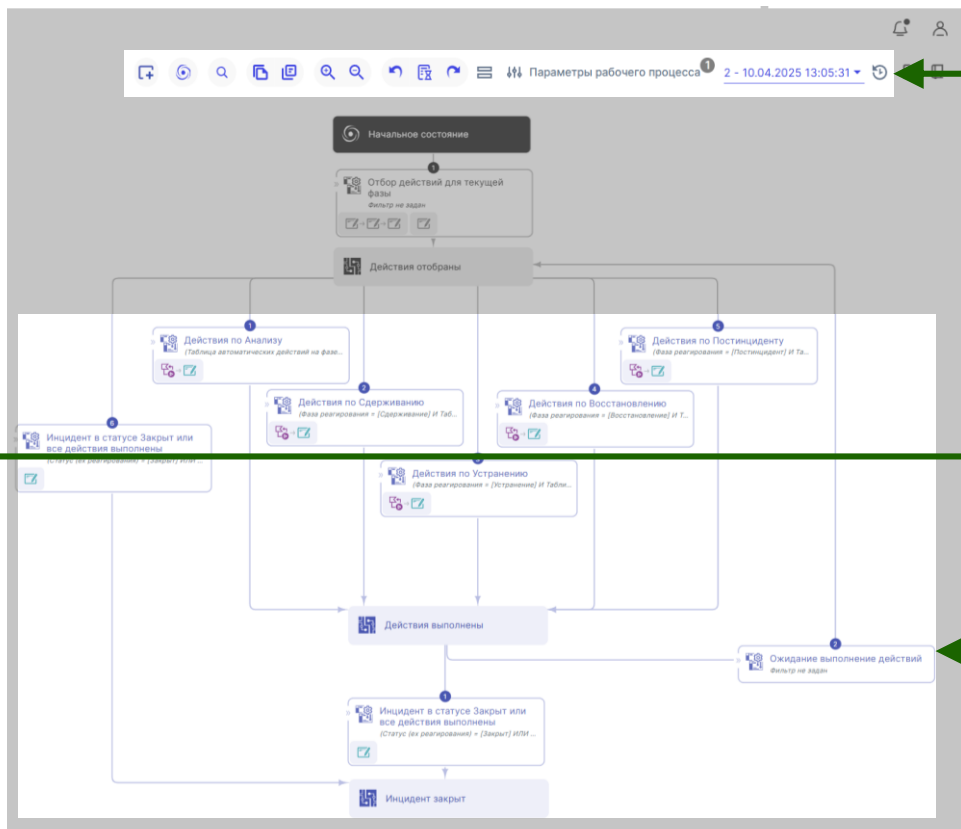
Security Orchestration, Automation and Response  
управление инцидентами

# Динамические плейбуки и ориентирование на объекты

сценарии реагирования, автоматически подстраивающиеся под окружение инцидента и затронутые объекты

редактор в виде таблиц и рабочих процессов

конструктор и управление версионностью для отладки



SOAR > Настройки > Редактор плейбуков

## Редактор плейбуков

+ Добавить Выгрузить Действия Удалить

Категория инцидентов	Тип инцидента	Тактики
Авторизация и аутентификация	Подбор пароля Подбор пароля для одной УЗ на нескольких хостах Подбор пароля технических УЗ	Persistence Initial Access Privilege Escalation
Администрирование	Запуск образа контейнера не из реестра Запуск уязвимого контейнера Запуск привилегированного контейнера Нерабочие образы контейнеров	Persistence Execution Defense Evasion Impact Privilege Escalation Resource Development
Антифрод	Подозрительные операции Сбор данных карт Компрометация аккаунта Компрометация устройства	Collection Exfiltration
Атака на инфраструктуру		
Безопасность БД		Collection Fvfiltration
Инцидент ИБ		
Нарушение работоспособности	Отказ в обслуживании (DDoS) Сетевых: Исчерпание ресурсов (количество сессий) Забивка канала (Reflection, amplification). DNS, NTP, SNMP	Impact

все этапы обработки инцидента согласно NIST

SOAR > Настройки > Операционные настройки > Мappings правил

## Мэппинг правил

Поиск + Добавить Выгрузить Удалить

Тип	Правило/Алиас
<input type="checkbox"/>	Подбор пароля Multiple login attempts to the same host using different accounts (AD)
<input type="checkbox"/>	НСД Multiple login attempts to the same host using different accounts
<input type="checkbox"/>	Изменение конфигураций (легитимное) Possible brute force using password spraying
<input type="checkbox"/>	Man-in-the-Middle Burst of failed login attempts using different accounts within the domain
<input type="checkbox"/>	Подозрительная активность пользователя Burst of failed login attempts using the same local account on different hosts (Windows)
<input type="checkbox"/>	DCSync Possible brute force using password guessing
<input type="checkbox"/>	Выполнение команды из черного списка Multiple TGS ticket requests (Kerberoasting)
<input type="checkbox"/>	Атака на сайт Windows Event Log was cleared via the command line using wevtutil

ID 15097944

Категория инцидентов: Антифрод

Тип инцидента: Компрометация устройства, Компрометация аккаунта, Подозрительные операции, Сбор данных карт

Статический плейбук:

Тактика: TA0009 Collection, TA0010 Exfiltration

Группа устранения: L1

Анализ: Сдерживание, Устранение, Восстановление, Постинцидент

Ручные действия: Удалить письмо по теме и отправителю, Заблокировать всех отправителей на Exchange

Автоматические действия:

Рабочий процесс	Порядок
Получение информации о системе (Windows)	1
Получение информации о системе (Linux)	1

объектно-ориентированное реагирование



SOAR

Security Orchestration, Automation and Response  
управление инцидентами

# Управление задачами и работа в команде

статусы и настройка видимости для совместной работы

The screenshot displays the SOAR interface for task management. At the top, there's a header 'Задачи по инциденту' with a count of 101. Below it are filters and a search bar. The main area shows a table of tasks with columns for ID, deadline, priority, name, status, and assignee. A dropdown menu for 'Критичность' (Priority) is open, showing options like 'Высокая', 'Средняя', and 'Низкая'. A detailed view of a task (ID 15100578) is shown on the right, including its description and details.

### Настройки SLA

Группа исполнения	Критичность	SLA взята в работу интервал времени	SLA завершения интервал времени
L1	Отсутствует	1:00:00:00	2:00:00:00
L2	Отсутствует	0:10:00:00	0:14:00:00
L3	Отсутствует	0:08:00:00	0:12:00:00
Общая	Отсутствует	1:00:00:00	2:00:00:00
L1	Низкая	0:08:00:00	1:00:00:00
L2	Низкая	0:08:00:00	0:12:00:00
L3	Низкая	0:06:00:00	0:04:00:00
Общая	Низкая	0:12:00:00	1:00:00:00
L1	Средняя	0:06:00:00	0:08:00:00
L2	Средняя	0:08:00:00	0:08:00:00

### Политика действий над объектами

ID	Объект	Критичность объекта (минимум)	Критичность объекта (максимум)	Критичность инцидента (минимум)	Критичность инцидента (максимум)	Действие по реагированию	Включено
2	Учетная запись	Отсутствует	Критическая	Средняя	Критическая	Заблокировать УЗ в сервисе каталогов	✓
11	Учетная запись	Отсутствует	Средняя	Средняя	Критическая	Сбросить пароль УЗ	✓
3	Почтовый адрес	Отсутствует	Отсутствует	Средняя	Критическая	Заблокировать отправителя по Email	✓
4	Внешний хост	Отсутствует	Отсутствует	Средняя	Критическая	Заблокировать хост на FW	✓
5	URL	Отсутствует	Отсутствует	Средняя	Критическая	Заблокировать URL на FW	✓
6	Процесс	Отсутствует	Отсутствует	Средняя	Критическая	Заблокировать процесс в Антивирусеном ПО (вост)	✓
8	Сервер/Рабочая станция	Отсутствует	Высокая	Средняя	Критическая	Запустить быстрое сканирование хоста Антивирусеном ПО	✓
10	Сервер/Рабочая станция	Отсутствует	Средняя	Высокая	Критическая	Завершить все RDP сессии	✓
9	Сервер/Рабочая станция	Отсутствует	Средняя	Высокая	Критическая	Запустить полное сканирование хоста Антивирусеном ПО	✓
1	Сервер/Рабочая станция	Отсутствует	Средняя	Низкая	Критическая	Заблокировать хост на FW	✓
7	Сервер/Рабочая станция	Отсутствует	Низкая	Низкая	Критическая	Выключить хост	✓

встроенная система тикетинга и интеграция с SD / ITSM

автоматический расчёт SLA с учетом графиков и расписаний



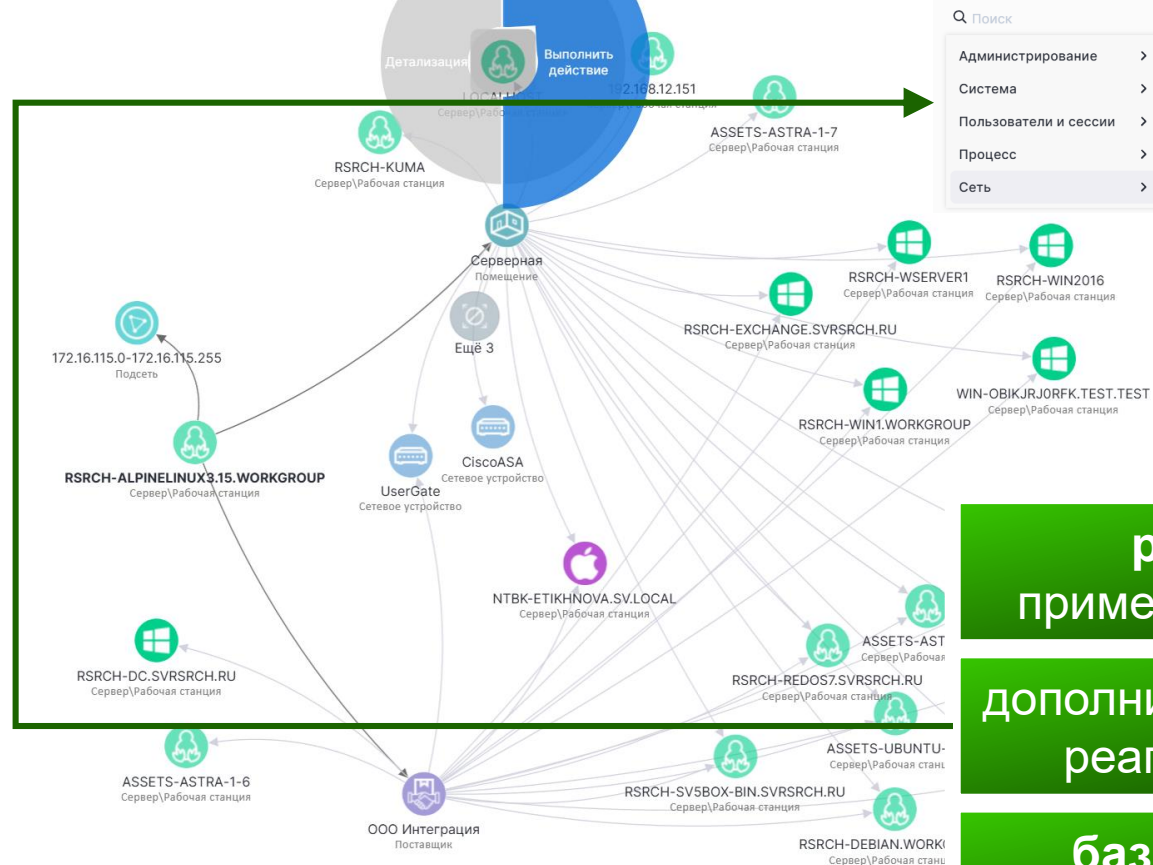
Security Orchestration, Automation and Response  
управление инцидентами

# Умная система рекомендаций и база знаний

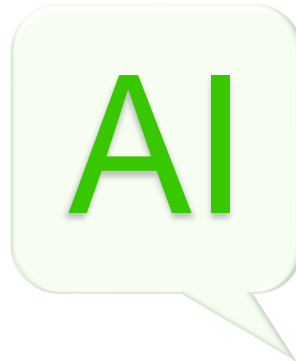
Активы > ИТ-активы > Устройства > Серверы и рабочие станции > Рабочая станция RSRCH-ALPINELINUX3.15.WORKGPF

ID 843106 **Высокая**  
**RSRCH-ALPINELINUX3.15.WORKGROUP**  
 ● Подготовка

Общая информация Конфигурация Безопасность **Сеть** Службы Приложения Пользователи **Граф** Расположение



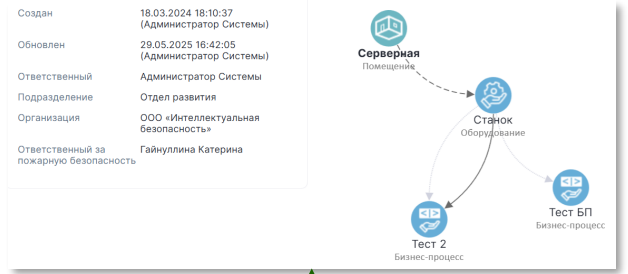
**ресурсно-сервисная модель с учетом бизнес-сущностей**



**рекомендации с применением ML-моделей**

**дополнительные действия по реагированию в графе**

**база знаний со всеми действиями аналитиков**



**Рекомендации** 4 ML 3

**Действия по похожим инцидентам**

- Обогащение хоста из систем сканирования
- Получить данные об УЗ в CMDB
- Запрос информации по IP из аналитических сервисов

**▼ TA0003 Persistence - T1098 Account Manipulation**

**Первичный анализ инцидента**

- Выясните, является ли выявленная активность легитимной для пользователя и хоста
- Если установлена легитимность, настройте корреляционное правило SIEM, исключающее сработки False Positive

**Первичное реагирование на инцидент**

- Если активность нелегитимна, проведите полную антивирусную проверку узла, задействованного в инциденте
- Проанализируйте алерты IDS/IPS для данного узла
- При обнаружении критичных алертов проведите **блокировку узлов из инцидента на МЭ**

**Расширенное сдерживание инцидента**

- Проанализируйте события аутентификации с данного узла, а также под текущей учетной записью в окрестности инцидента. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется **заблокировать IP данных узлов на МЭ, а также текущую учетную запись**
- Удалите **добавленную учетную запись** из целевой группы

**▼ TA0003 Persistence, TA0001 Initial Access, TA0005 Defense Evasion, TA0004 Privilege Escalation - T1078 Valid Accounts**

**Первичный анализ инцидента**

- Выясните, является ли выявленная активность легитимной для пользователя и хоста
- Если установлена легитимность, настройте корреляционное правило SIEM, исключающее сработки False Positive

**Первичное реагирование на инцидент**

- Если активность нелегитимна, проведите полную антивирусную проверку узла, задействованного в инциденте
- Проанализируйте алерты IDS/IPS для данного узла
- При обнаружении критичных алертов проведите **блокировку узлов из инцидента на МЭ**

**Расширенное сдерживание инцидента**

- Проанализируйте события аутентификации с данного узла, а также под текущей учетной записью в окрестности инцидента. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется **заблокировать IP данных узлов на МЭ, а также текущую учетную запись**

**▼ TA0042 Resource Development - T1586 Compromise Accounts**

**Первичное реагирование на инцидент**

- Проведите **блокировку узла-источника на МЭ**
- Проведите полную антивирусную проверку узла
- Заблокируйте активную учетную запись

**Расширенное сдерживание инцидента**

- Проанализируйте события аутентификации с данного узла, а также под активной и целевой учетными записями. В случае обнаружения подозрительных/массовых попыток аутентификации на другие узлы рекомендуется **заблокировать IP данных узлов на МЭ, а также целевую учетную запись**

**▼ TA0011 Command and Control - T1572 Protocol Tunneling**

**Первичное реагирование на инцидент**

- Убедитесь, что **активность действительно связана с туннелированием протоколов**, а не с обычным сетевым взаимодействием.
- Проверьте журналы и данные сетевого трафика на наличие аномалий, характерных для туннелирования.

**Расширенное реагирование на инцидент**

- Если обнаружены признаки туннелирования, **изолируйте затронутые системы или сетевые сегменты**, чтобы предотвратить дальнейшее распространение или доступ злоумышленников.
- Анализируйте журналы и заващенный трафик, чтобы определить, **какие протоколы используются для туннелирования и откуда происходят подключения.**



**Security Orchestration, Automation and Response**  
 управление инцидентами

# Применение ИИ-инструментов и аналитика

Действия 17

2

15

Завершённые 88%

Завершены с ошибкой 12%

Чат

Похожие инциденты ML 0 0

Связанные инциденты 0 3

Действия

- Критическая ID 15100546  
Снятие слепка памяти процесса lsass с помощью ProcDump  
Тип: Выполнение команды из черного списка  
Статус:  Закрыт  
Ответственный: —
- Критическая ID 15100545  
Попытка эксплуатации критической уязвимости  
Тип: Попытка эксплуатации уязвимости изнутри  
Статус:  Закрыт  
Ответственный: —
- Средняя ID 15100541  
Аутентификация с подозрительного IP  
Тип: Аномалии VPN, RDP, RDG, SSH, проху  
Статус:  Закрыт  
Ответственный: —

Бюллетени 0

любые срезы данных и различные способы визуализации для анализа



**ML-модели для анализа больших данных**

**поиск похожих инцидентов  
система рекомендаций  
скоринг false-positive  
справка продукта**

**встроенные интеграции с внешними LLM-моделями**

Напишите сообщение...

ML-помощь ML-рекомендации Чат с GPT

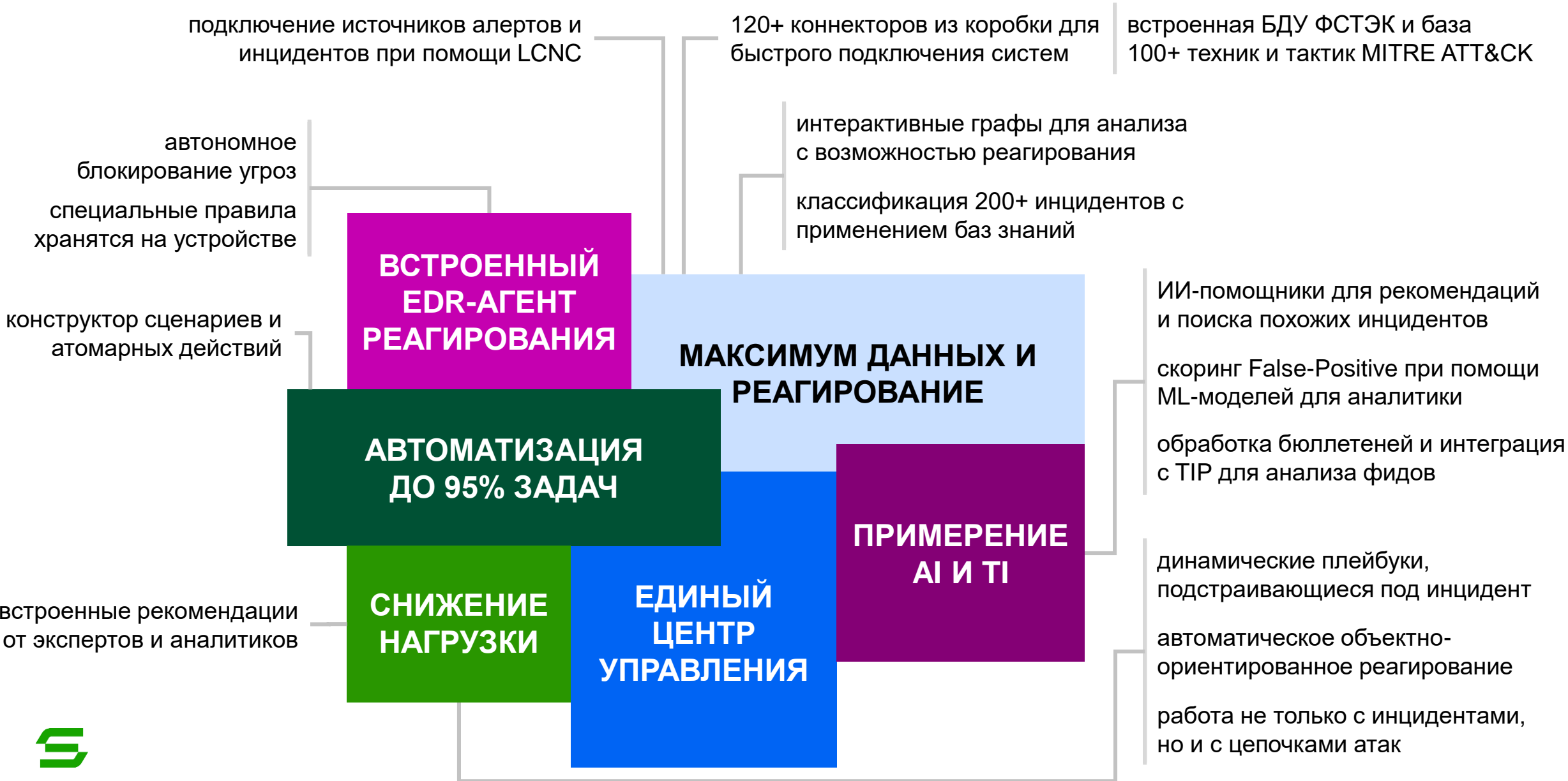
- Написать в ChatGPT
- Написать в YandexGPT
- Написать в DeepSeek



Security Orchestration, Automation and Response  
управление инцидентами

ИИ-ПОМОЩНИКИ

# SOAR, управление инцидентами



# Спасибо за внимание

[sales@securityvision.ru](mailto:sales@securityvision.ru)

Интеллектуальная  
платформа  
информационной  
безопасности и ИТ



[securityvision.ru](http://securityvision.ru)