ML в действии: строим улучшенный SOAR вместе с Security Vision

Security Vision

[Блог]
securityvision.ru/blog

[Telegram]
t.me/svplatform

[Хабр]
habr.com/ru/companies/securityvison

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

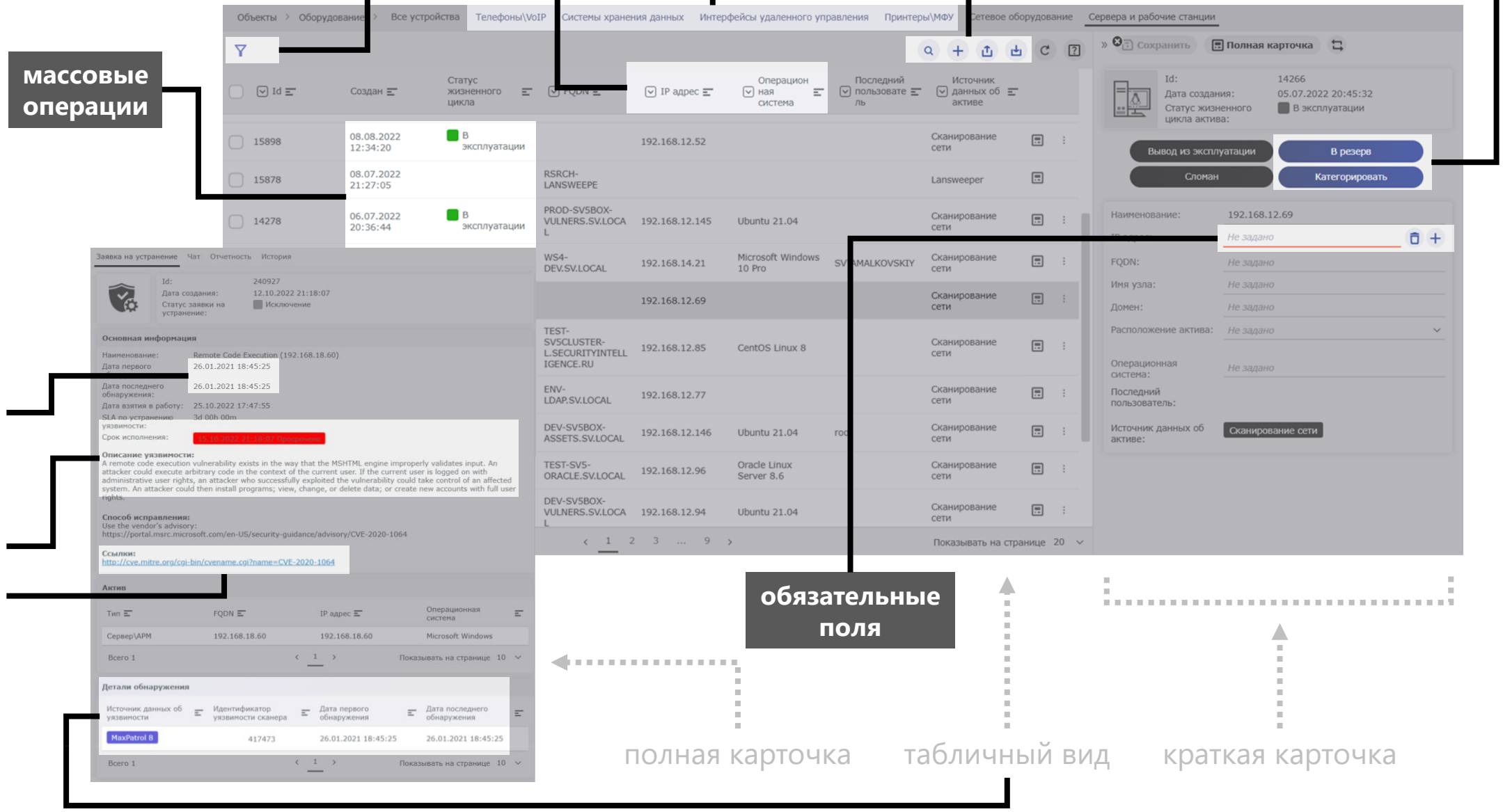
Security Vision

Аналитика, интерактивные виджеты и дашборды

Интеграции с внешними системами (коннекторы)

Отчёты, выгрузка файлов и логирование действий

Конструктор объектов



Конструктор рабочих процессов

управление глубиной отображаемых связей

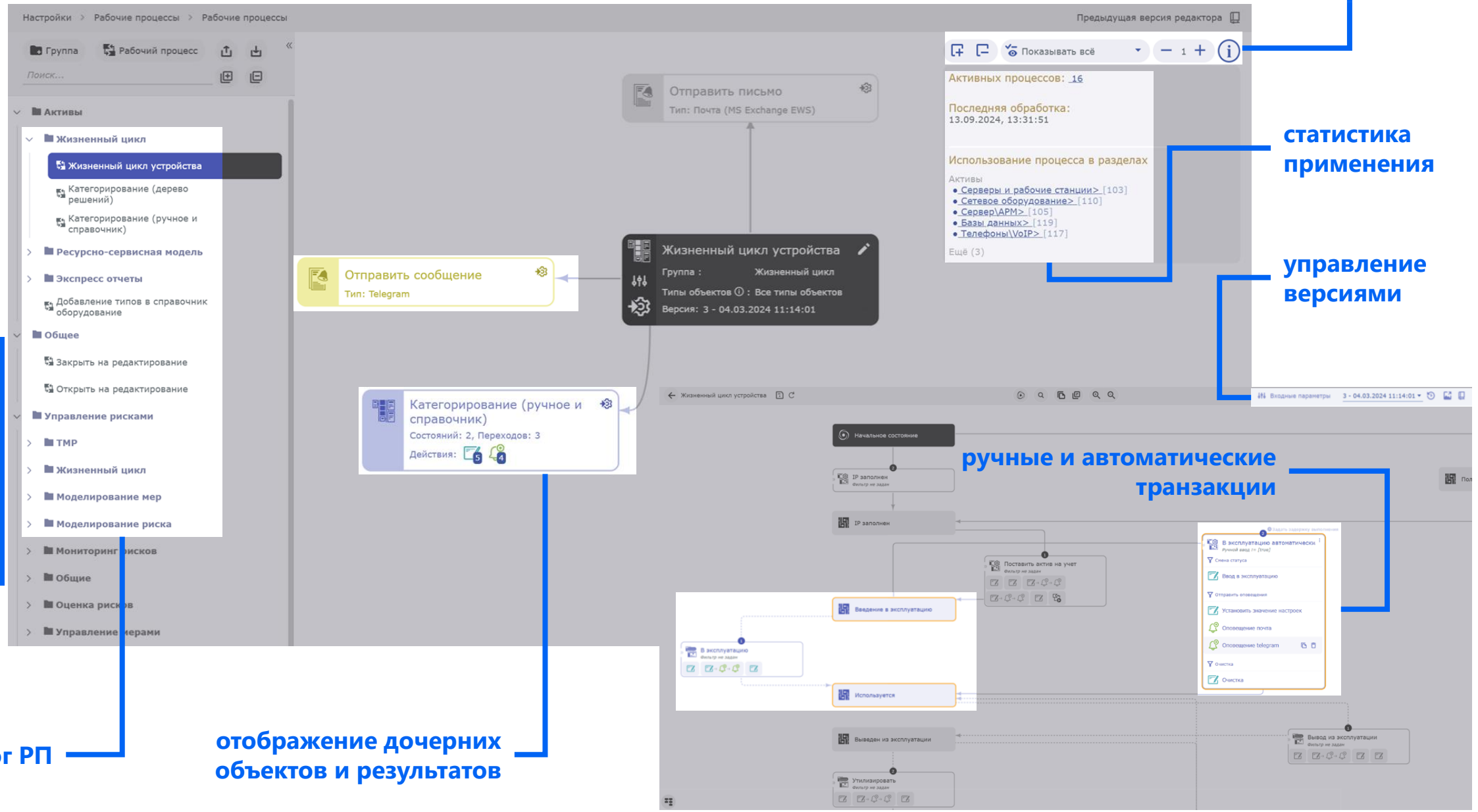
статистика применения

управление версиями

ручные и автоматические транзакции

каталог РП

отображение дочерних объектов и результатов



Конструктор интеграций

BI.ZONE RST CLOUD F.A.C.C.T. UserGate kaspersky positive technologies

VIRUSTOTAL urlscan.io A sandbox for the web WhoisXML API Unified Results! SHODAN GitHub ';--have i been pwned?

INFOWATCH SOLAR SEARCHINFORM Jira Software NAUMEN OTRS

ASTRA LINUX Microsoft Active Directory PowerShell SSH Lansweeper 1С ZABBIX

Exchange CISCO PostgreSQL ORACLE DATABASE Microsoft SQL kafka JSON XML CSV

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

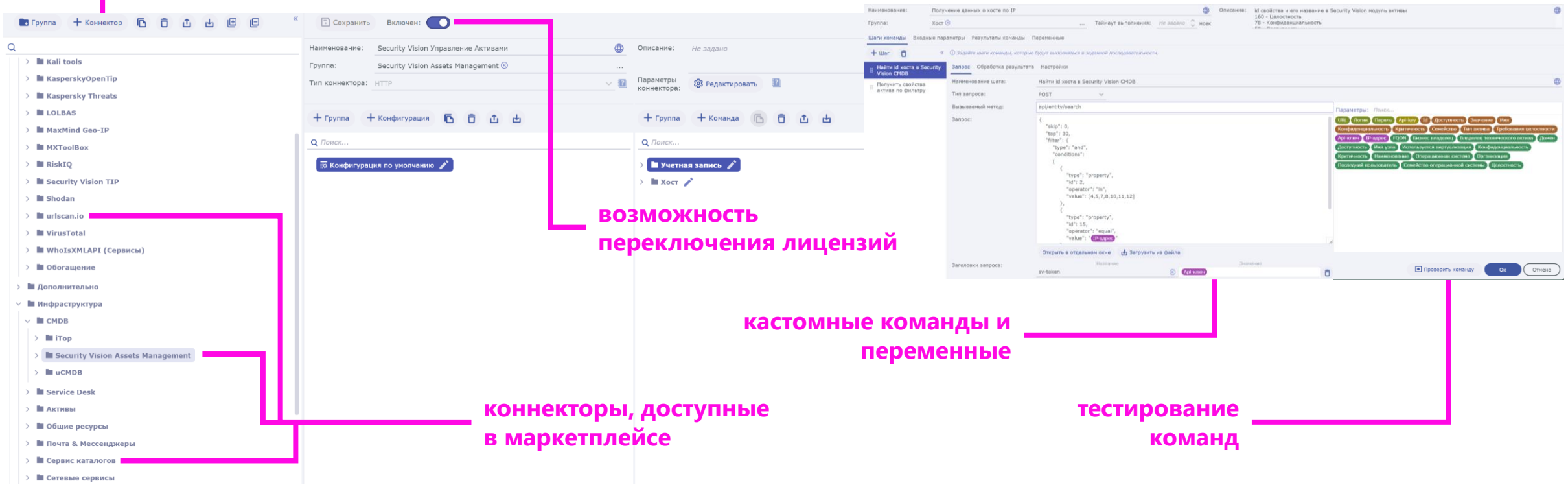
Сбор и обогащение

Реагирование на события

создание новых коннекторов **без участия вендоров**

Конструктор интеграций

создание интеграций через интерфейс



возможность переключения лицензий

кастомные команды и переменные

коннекторы, доступные в маркетплейсе

тестирование команд

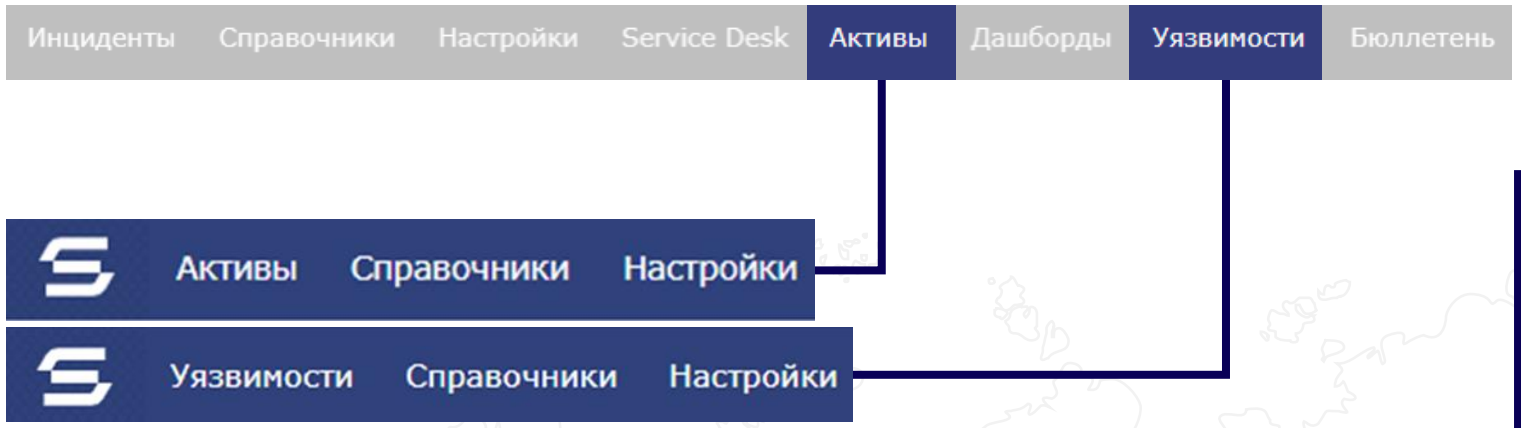
WMI | PS | SSH | файл | почта | БД | HTTP (API) | LDAP | EventLog | Syslog | DNS | скрипты и др.

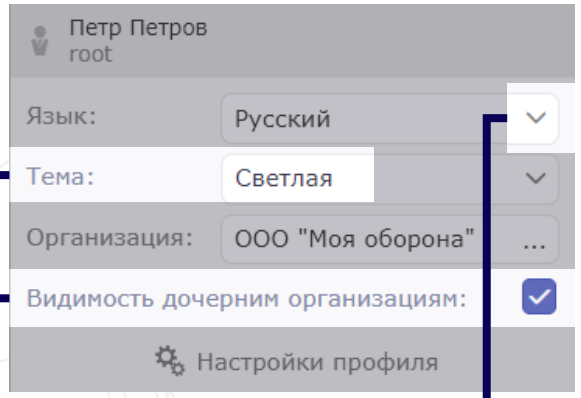
Сбор и обогащение

Реагирование на события

создание новых коннекторов **без участия вендоров**

Конструктор ролей и меню

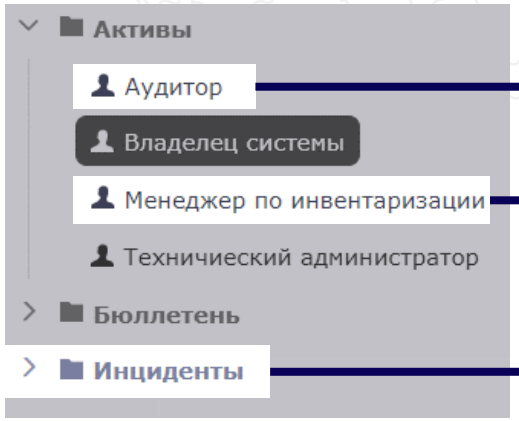




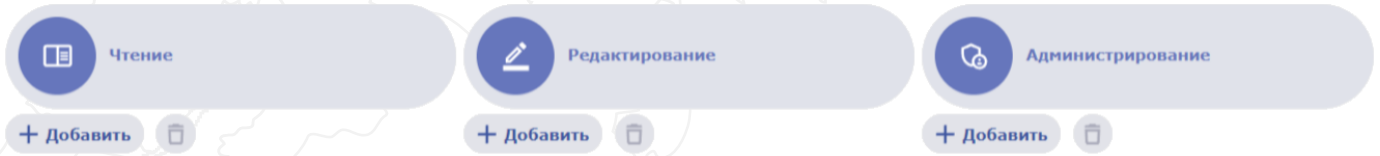
темы оформления

multitenancy

мультиязычность



персональная витрина

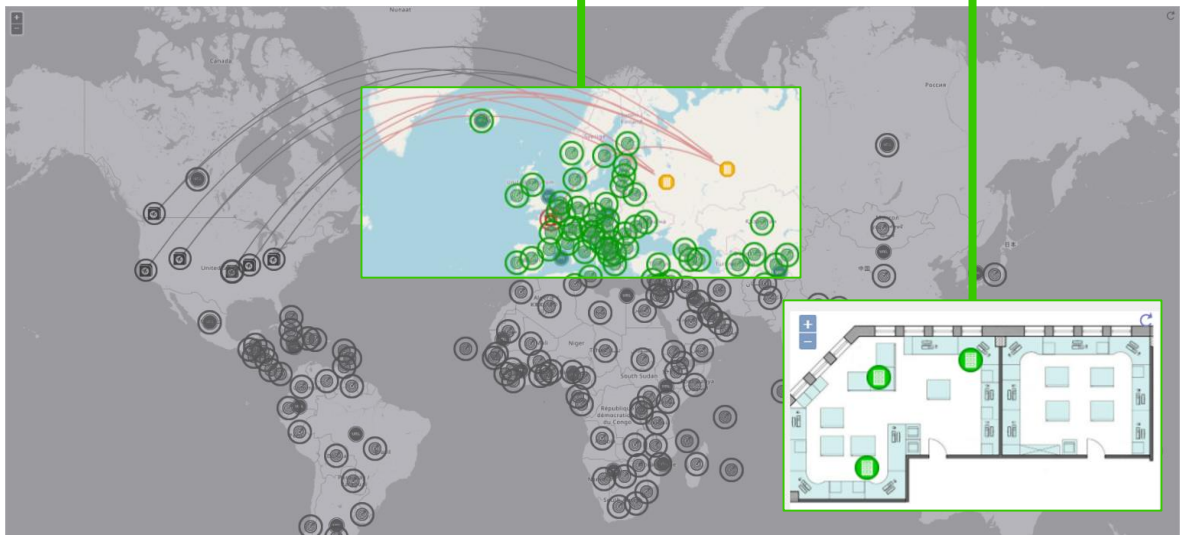


гранулярные настройки

Конструктор аналитики

карты и планы помещений

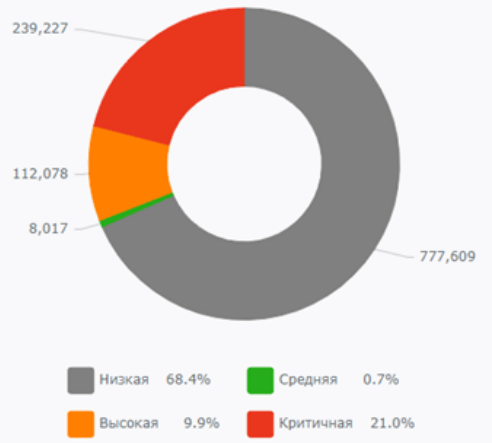
дашборды



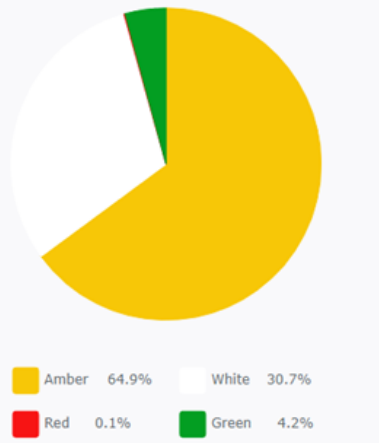
Топ-5 активных критичных инцидентов

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

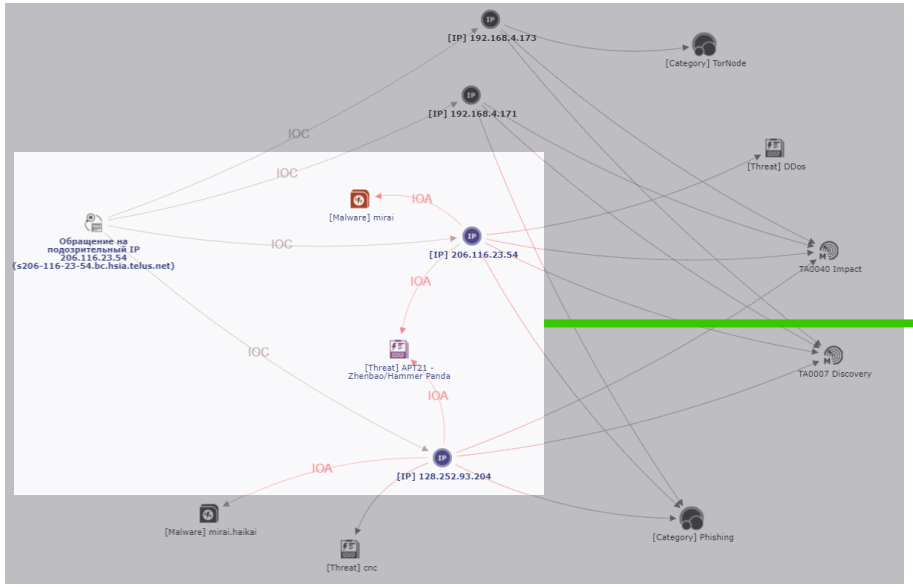
Критичность индикаторов



TLP для индикаторов



графы связей



интерактивная аналитика и связанные графики

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

Конструктор отчётов

Security Vision

Отчет по активам

Дата выгрузки: 04.06.2024 14:56:44

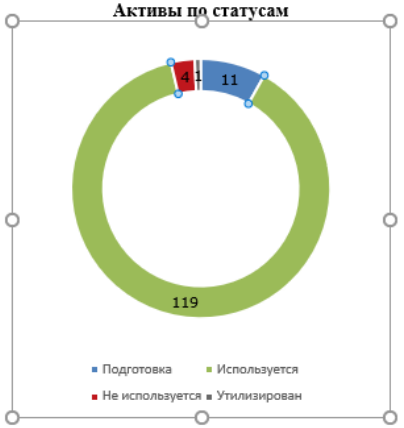
Период: 01.02.2023 - 27.06.2024

Статистика активов

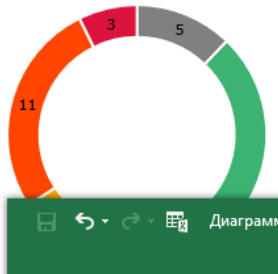
Новые активы	Новые критичные активы
135	14

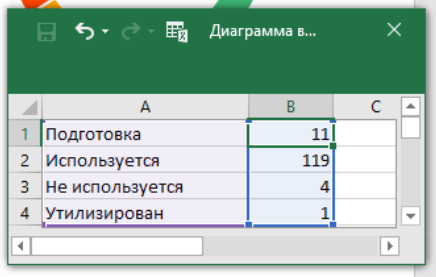
Инвентаризовано	Ошибка инвентаризации
9	45

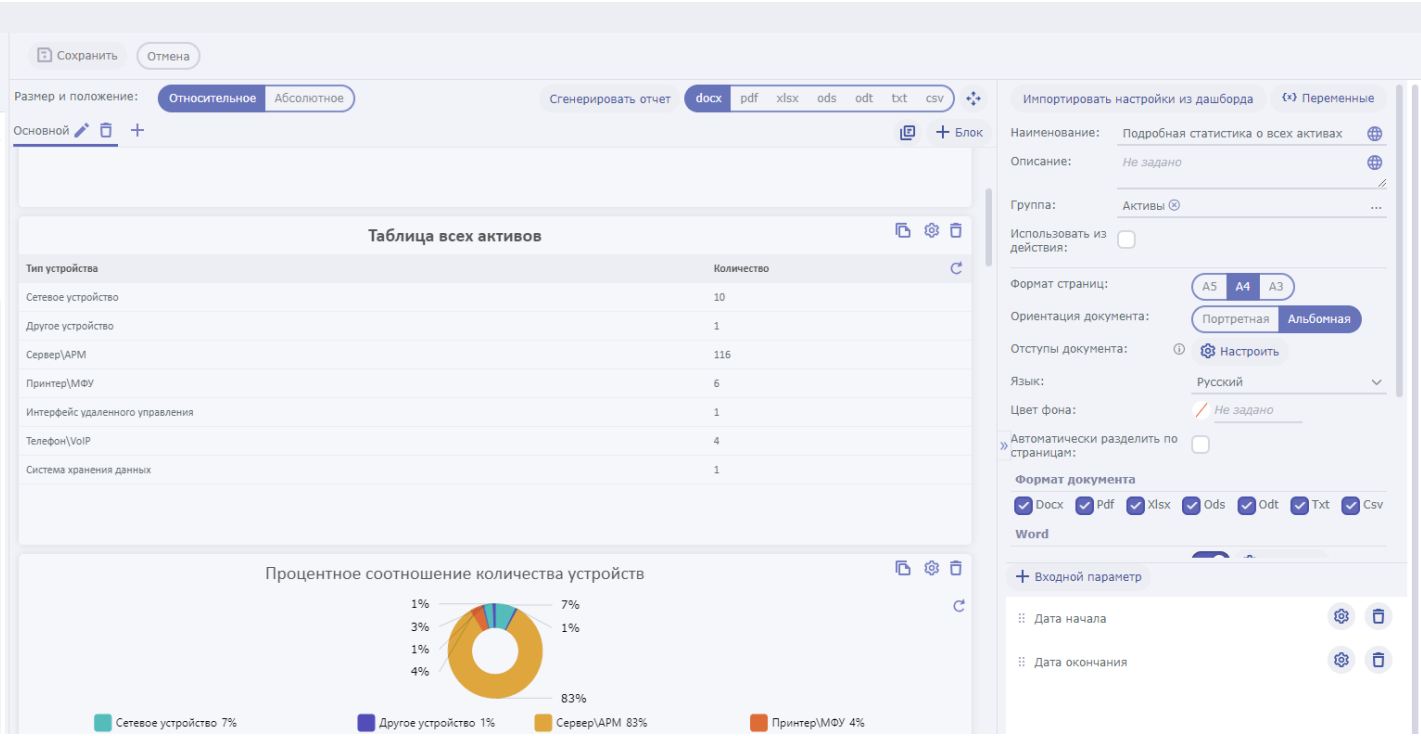
Активы по статусам



Активы по критичности







Прогресс устранения:

Исполнитель:
Петров Петр Петрович

Дата взятия в работу:
15.06.2022 21:21:29

SLA по устранению уязвимости:
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.

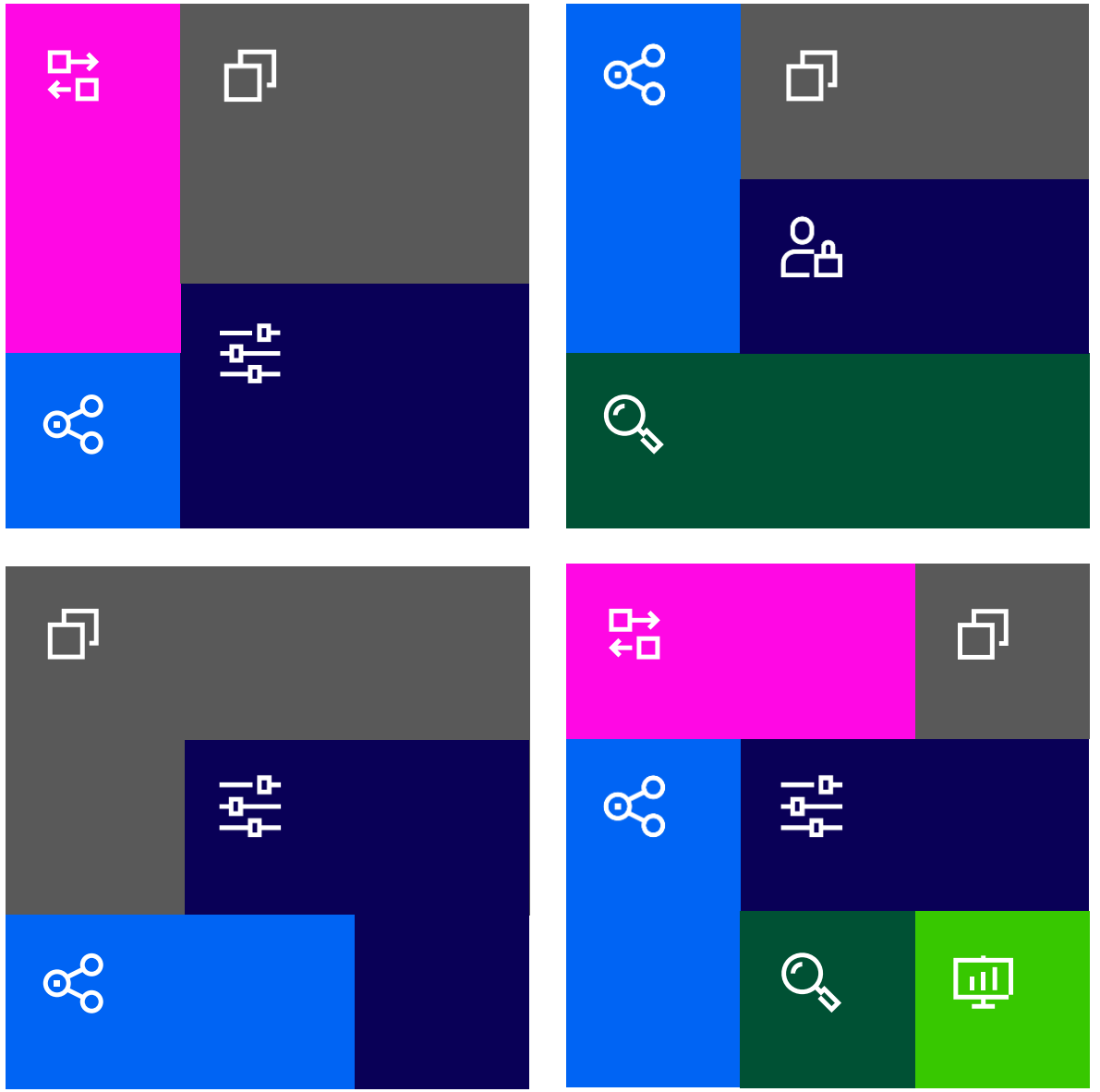
Способ исправления:
Use the vendor's advisory:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1055

Прогресс устранения:

Исполнитель:
Петров Петр Петрович

Дата взятия 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

AM
управление активами и инвентаризацией

КИИ
управление соответствием ФЗ-187

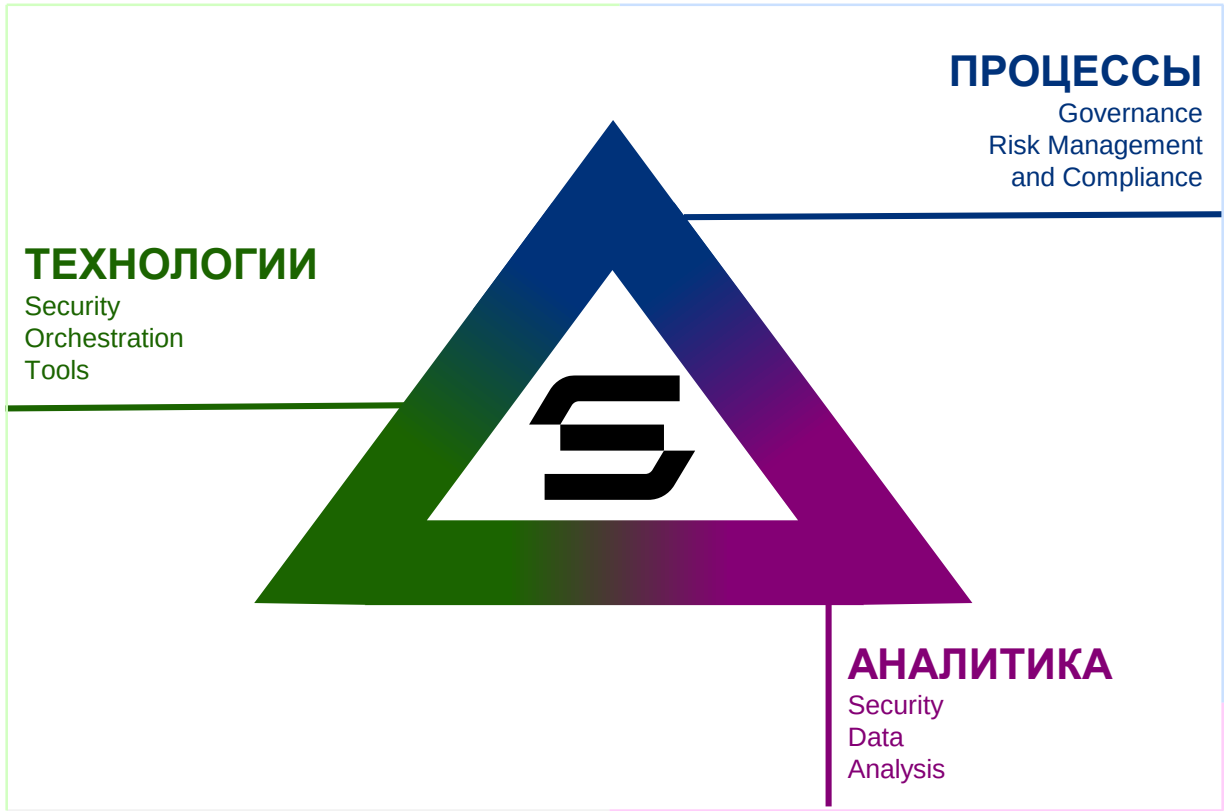
СМ
управление соответствием НМД

FinCERT
взаимодействие с ЦБ

ГосСОПКА
взаимодействие с НКЦКИ

VM
управление уязвимостями

VS
сканер уязвимостей



RM
управление рисками кибербезопасности

ORM
управление операционными рисками

BCM
управление непрерывностью бизнеса

SA
управление состоянием ИБ

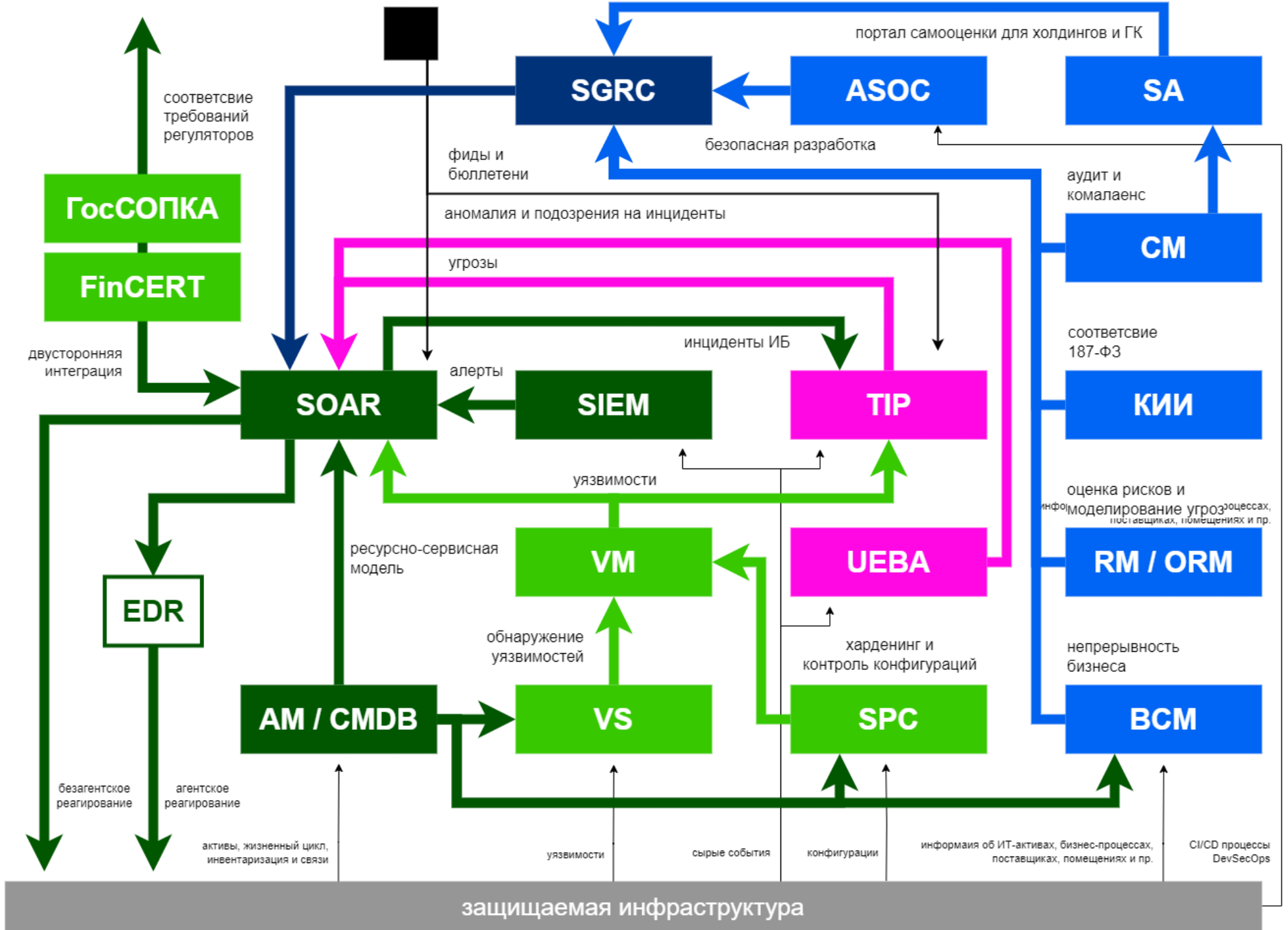
SPC
управление конфигурациями безопасности

BASIC
линейка для SMB

NGX
комплекты

TIP
анализ угроз кибербезопасности

UEBA
поведенческий анализ и поиск аномалий


портал самооценки для холдингов и ГК
SGRC
ASOC
SA
соответсвие требований регуляторов
безопасная разработка
фиды и бюллетени
аудит и комалаенс
ГосСОПКА
аномалия и подозрения на инциденты
CM
FinCERT
угрозы
соответсвие 187-ФЗ
двусторонняя интеграция
инциденты ИБ
алерты
SOAR
SIEM
TIP
КИИ
уязвимости
оценка рисков и моделирование угроз
ресурсно-сервисная модель
VM
UEBA
RM / ORM
EDR
обнаружение уязвимостей
харденинг и контроль конфигураций
непрерывность бизнеса
AM / CMDB
VS
SPC
BCM
безагентское реагирование
агентское реагирование
активы, жизненный цикл, инвентаризация и связи
уязвимости
сырые события
конфигурации
информаия об ИТ-активах, бизнес-процессах, поставщиках, помещениях и пр.
CI/CD процессы DevSecOps
защищаемая инфраструктура

Управление активами и инвентаризацией

1 поиск объектов

сканирование по расписанию, формирование каталогов активов и построение карты сети

2 ресурсно-сервисная модель

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

3 обогащение

сбор дополнительной информации из разных систем, БД и файлов

4 категорирование

фильтрация активов, поиск данных и связей между любыми объектами

5 жизненный цикл

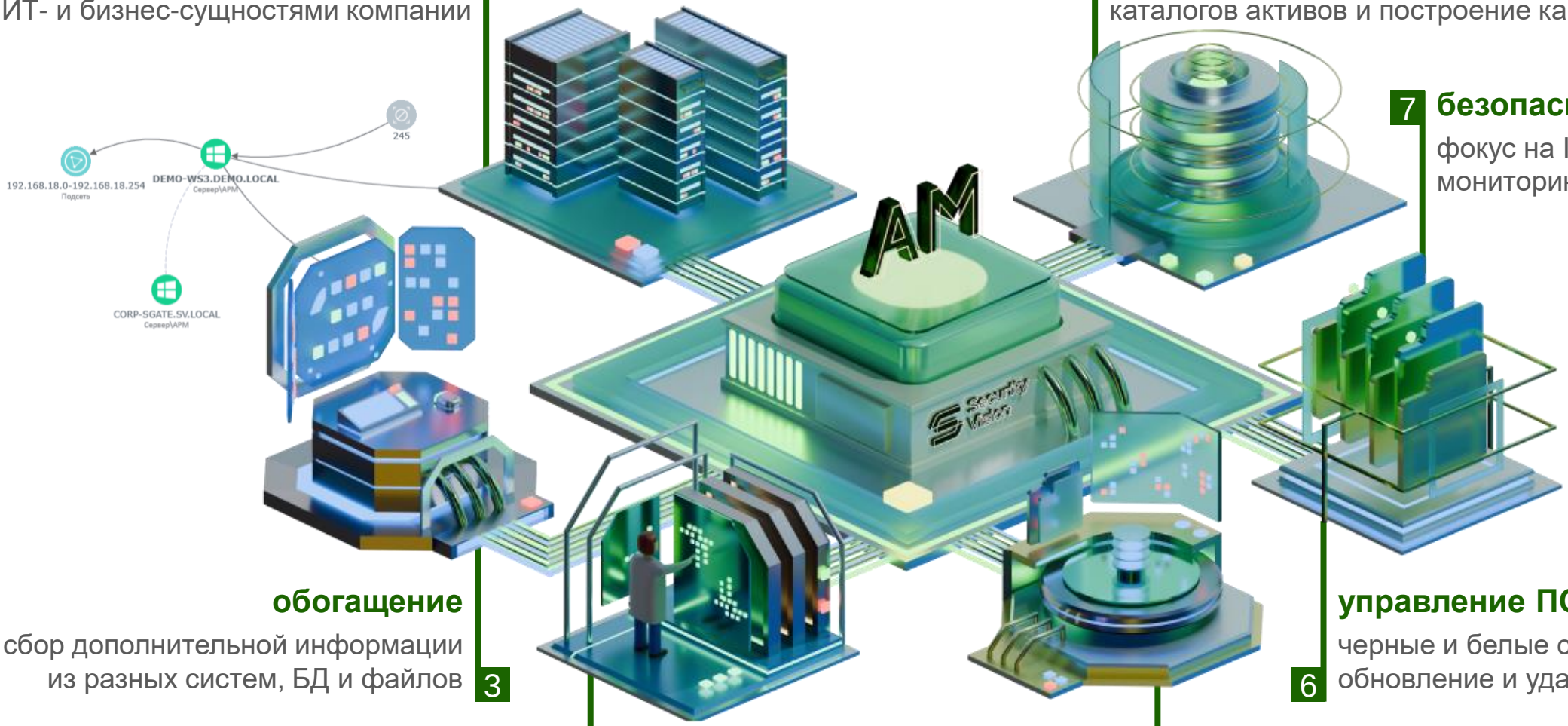
фиксация изменений атрибутов объектов от их появления до вывода эксплуатации

6 управление ПО

черные и белые списки, обновление и удаление

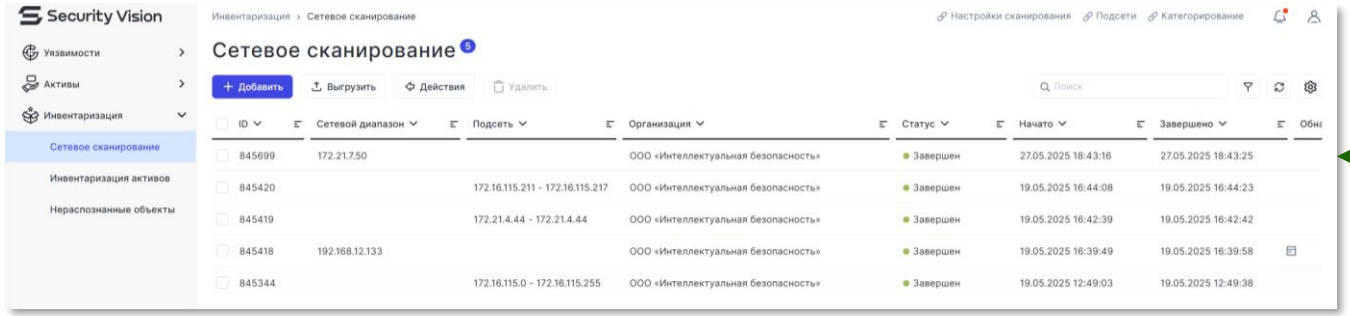
7 безопасность

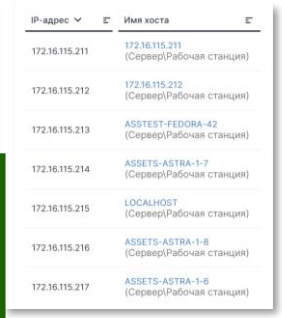
фокус на IT-задачах и мониторинге защищенности

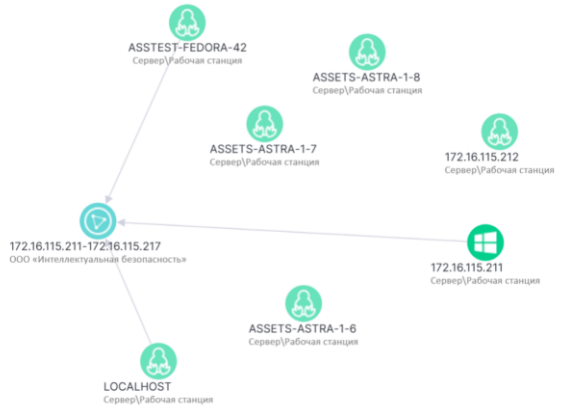


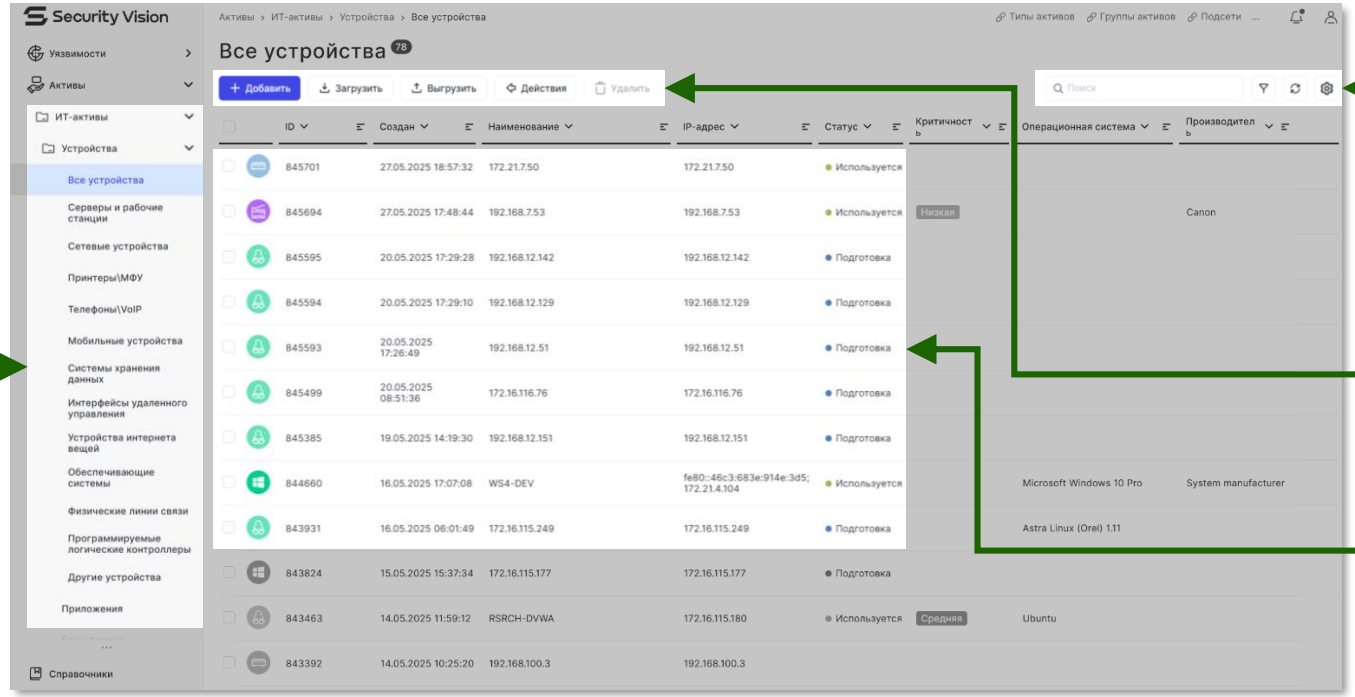
AM

Поиск объектов с построением карты сети









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**

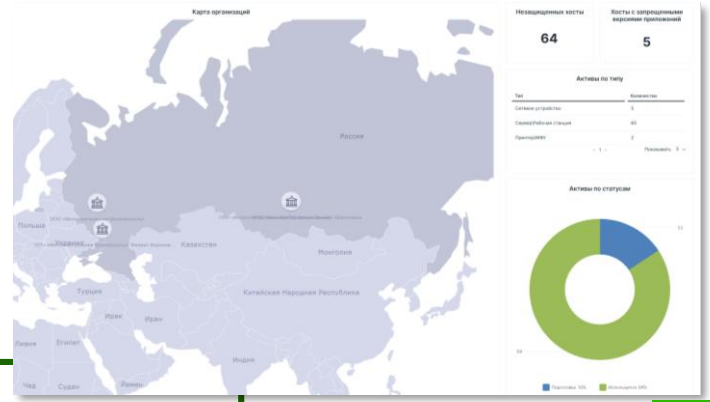
Ресурсно-сервисная модель

ИТ- и бизнес-активы, документы и схемы

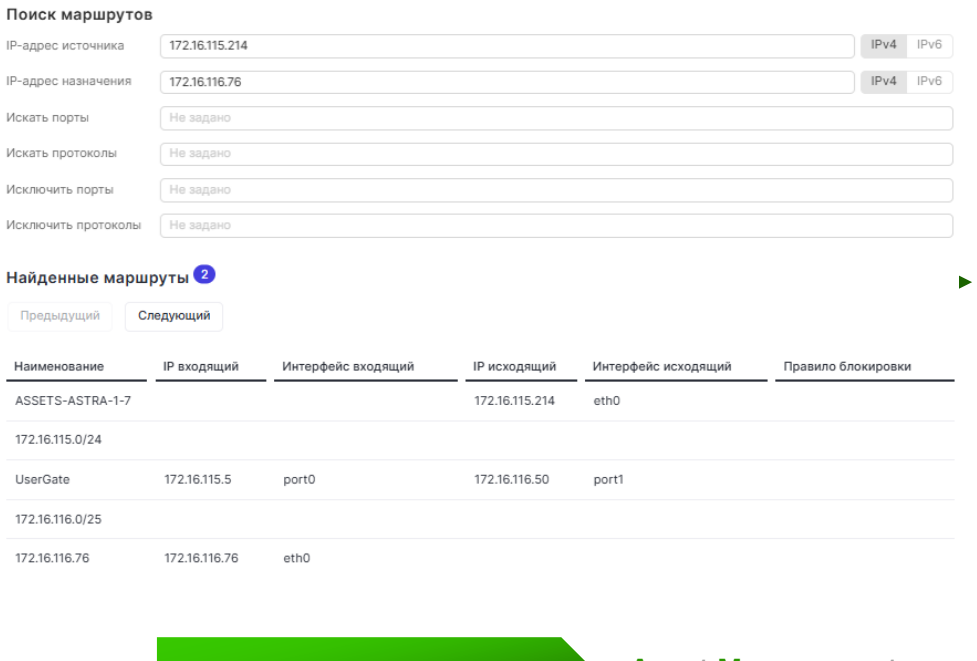
глобус, планы **помещений** и **карта сети**

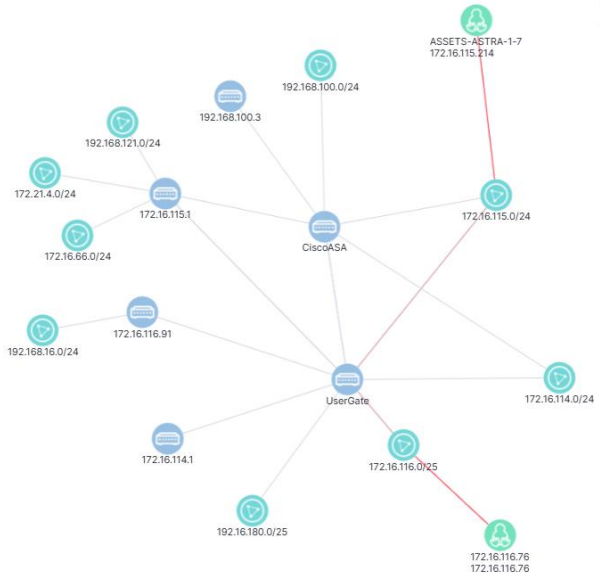
ИИ-инструмент для поиска сетевых **маршрутов**

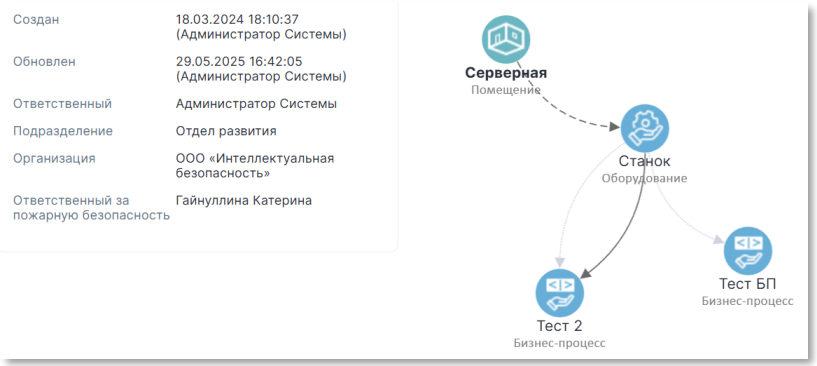
ИТ-активы и бизнес-сущности



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







AM

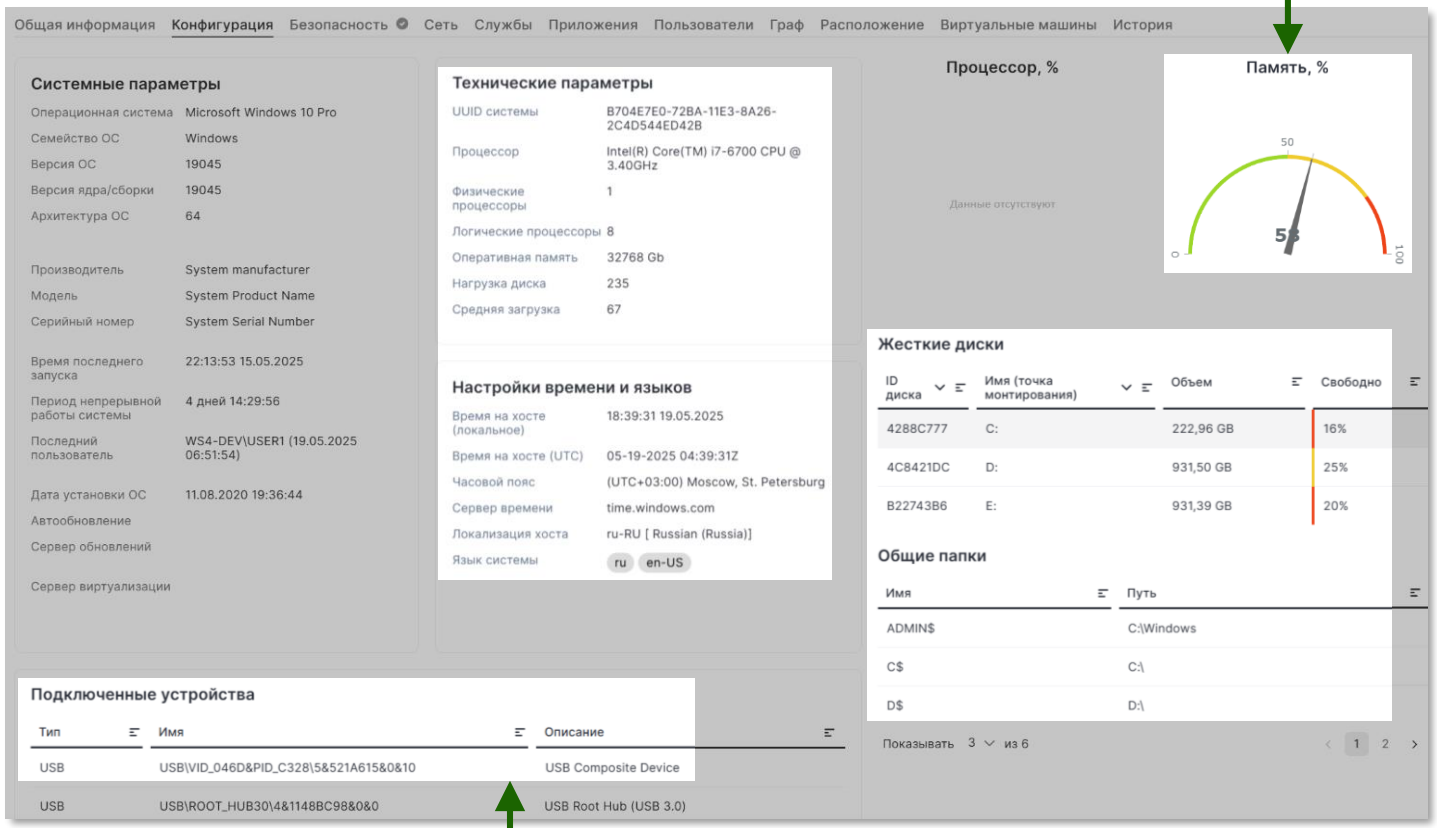
Asset Management

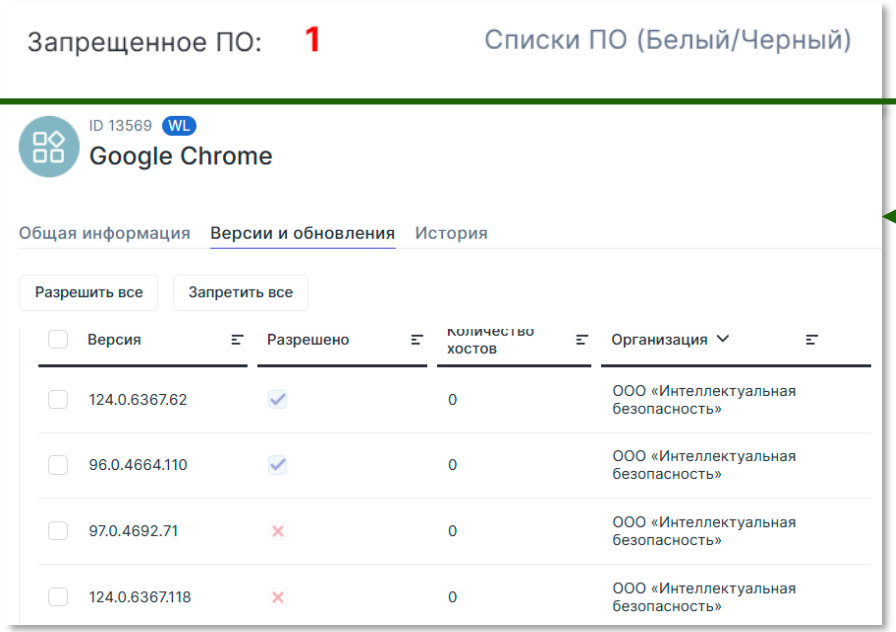
управление активами и инвентаризацией

Мониторинг состояния и управление ПО и оборудованием

управление **установкой, обновлением** и **удалением**

черные и **белые** списки для ПО на хостах и серверах





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

Управление инцидентами

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

3 управление СЗИ

интеграция ИБ и ИТ систем, управление статусами и SLA

4 цепочки атак

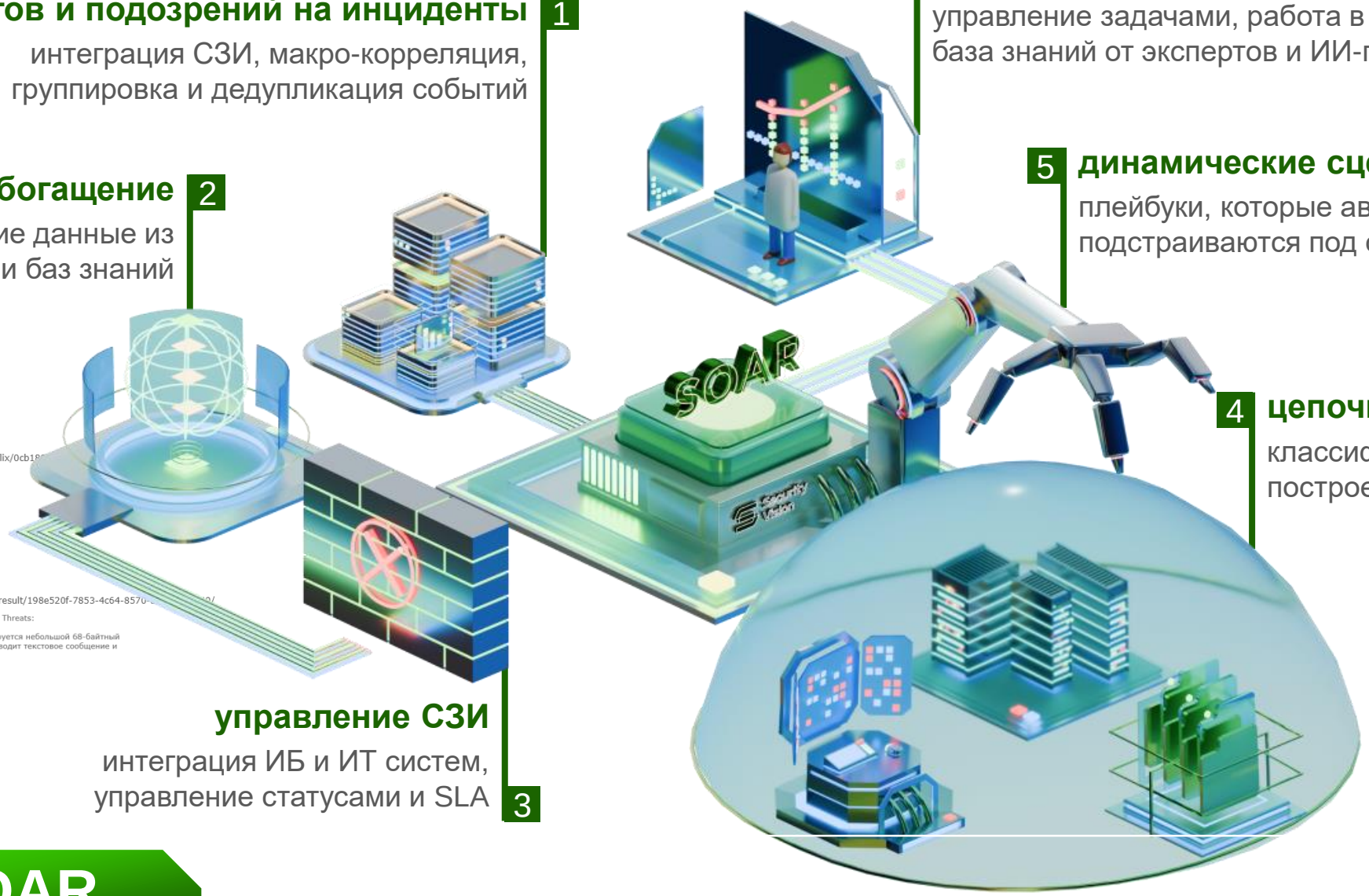
классификация и построение kill-chain

5 динамические сценарии

плейбуки, которые автоматически подстраиваются под окружение

6 рекомендации для аналитиков

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

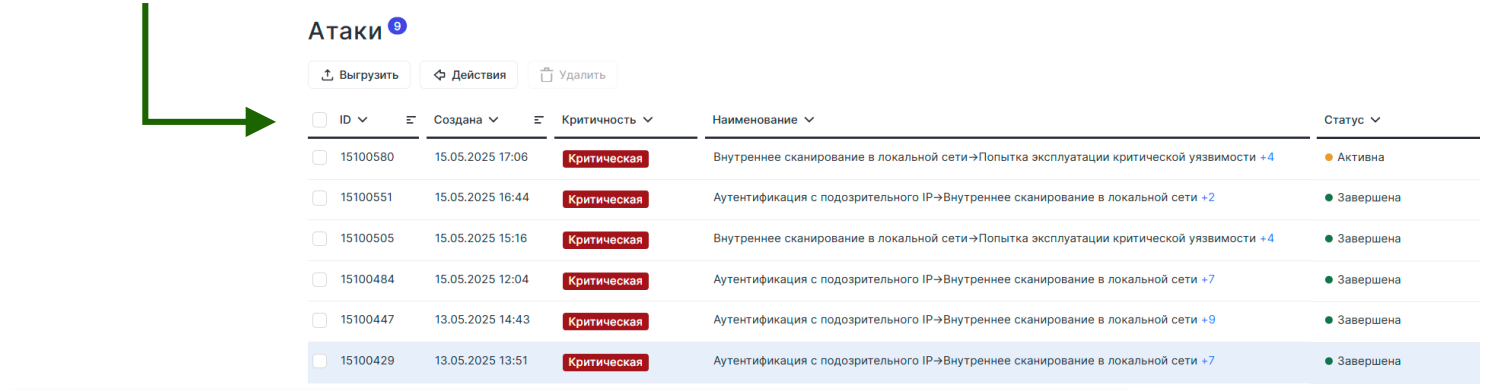


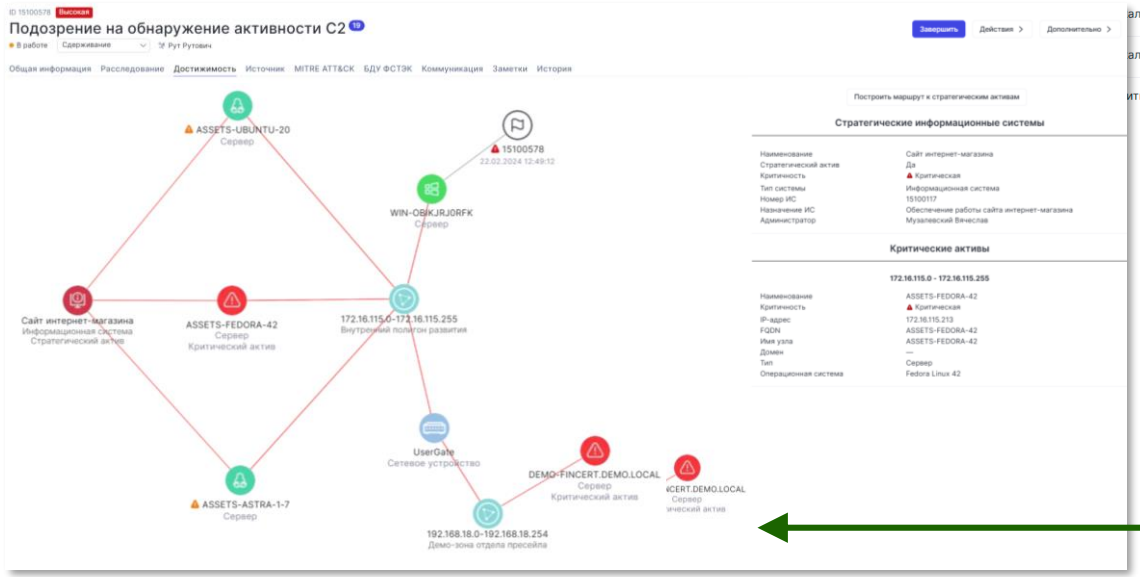
SOAR

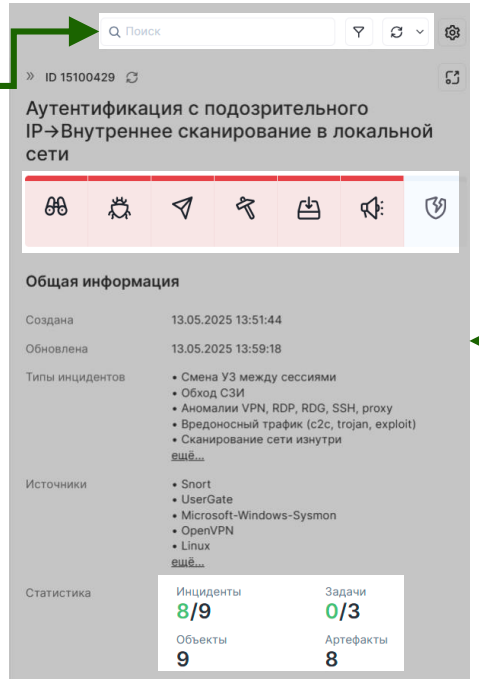
Сбор алертов, инцидентов и сырых данных с обогащением

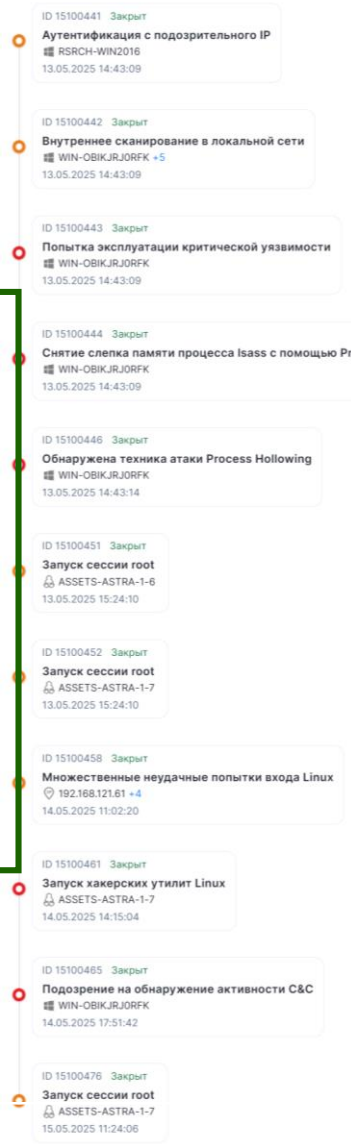
цепочки атак по NIST, группировка и **действия**

быстрый поиск по любым **параметрам** и **таблицам**









конструктор **коннекторов** и интеграция с **любым СЗИ**

поиск **деталей** и автоматическое **обогащение**

граф **достижимости** **маршруты** нарушителей

SOAR

Security **O**rchestration, **A**utomation and **R**esponse

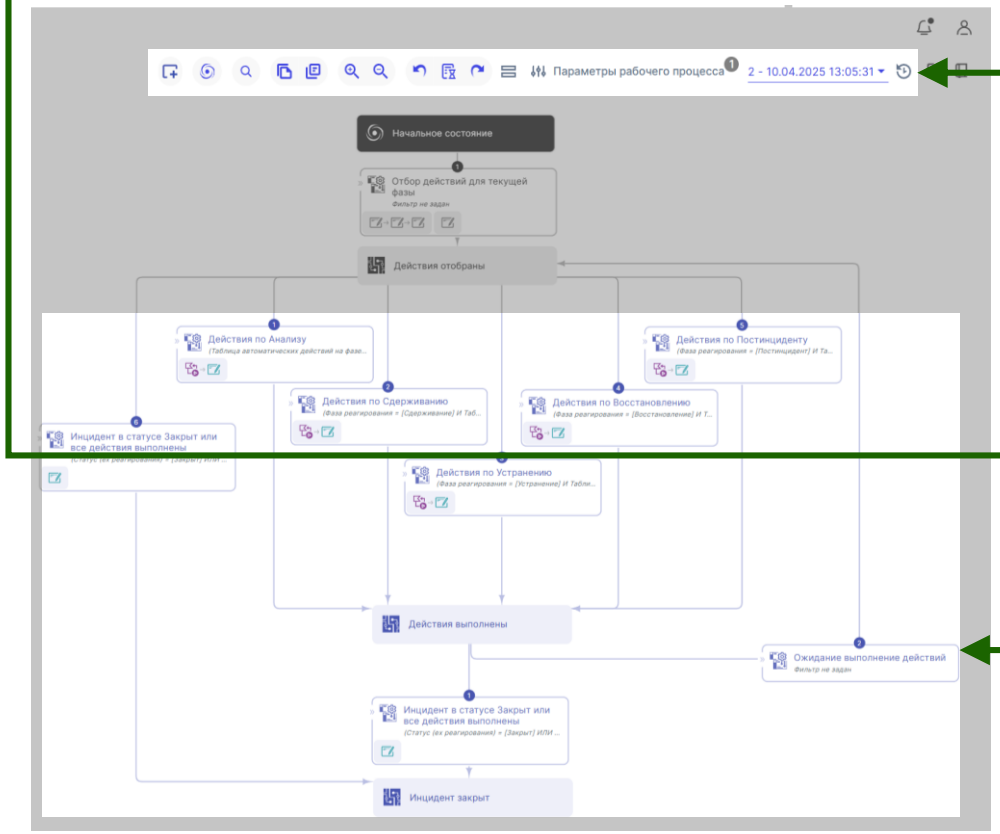
управление инцидентами

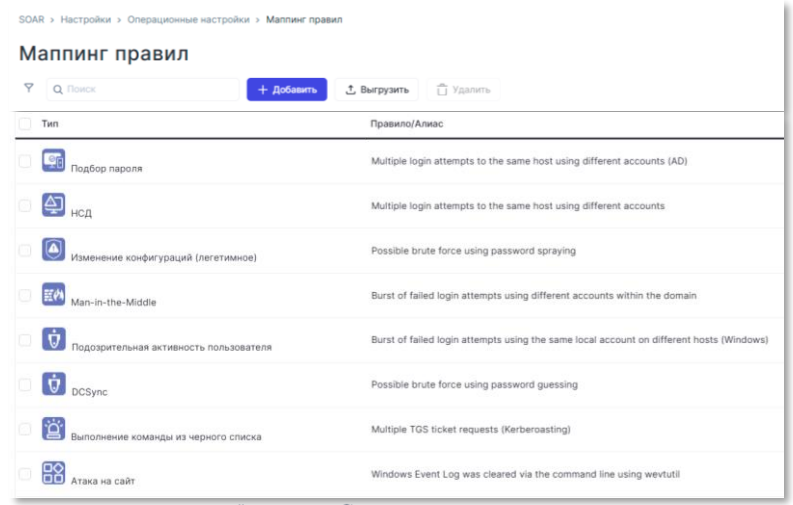
Динамические плейбуки и ориентирование на объекты

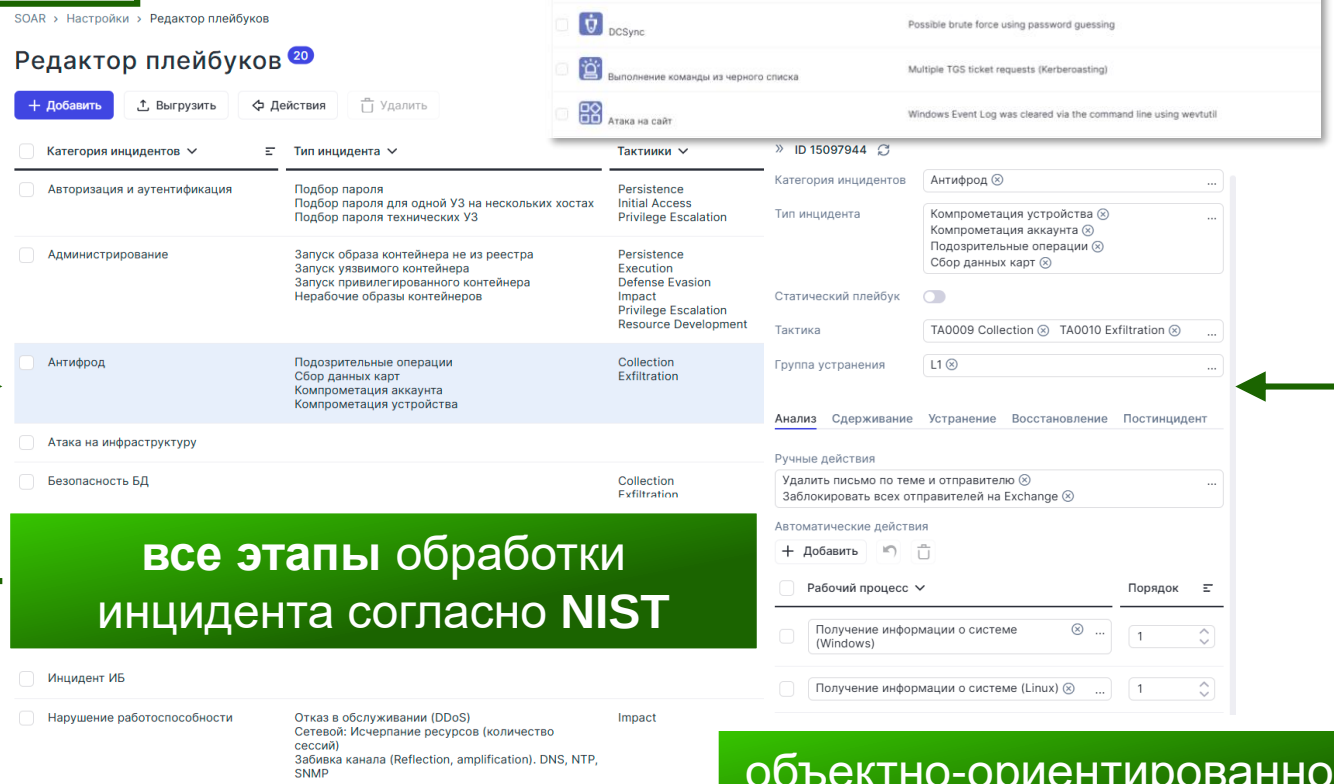
сценарии реагирования, **автоматические подстраивающиеся** под **окружение** инцидента и затронутые **объекты**

редактор в виде **таблиц** и **рабочих процессов**

конструктор и управление **версионностью** для отладки







все этапы обработки инцидента согласно **NIST**

объектно-ориентированное реагирование

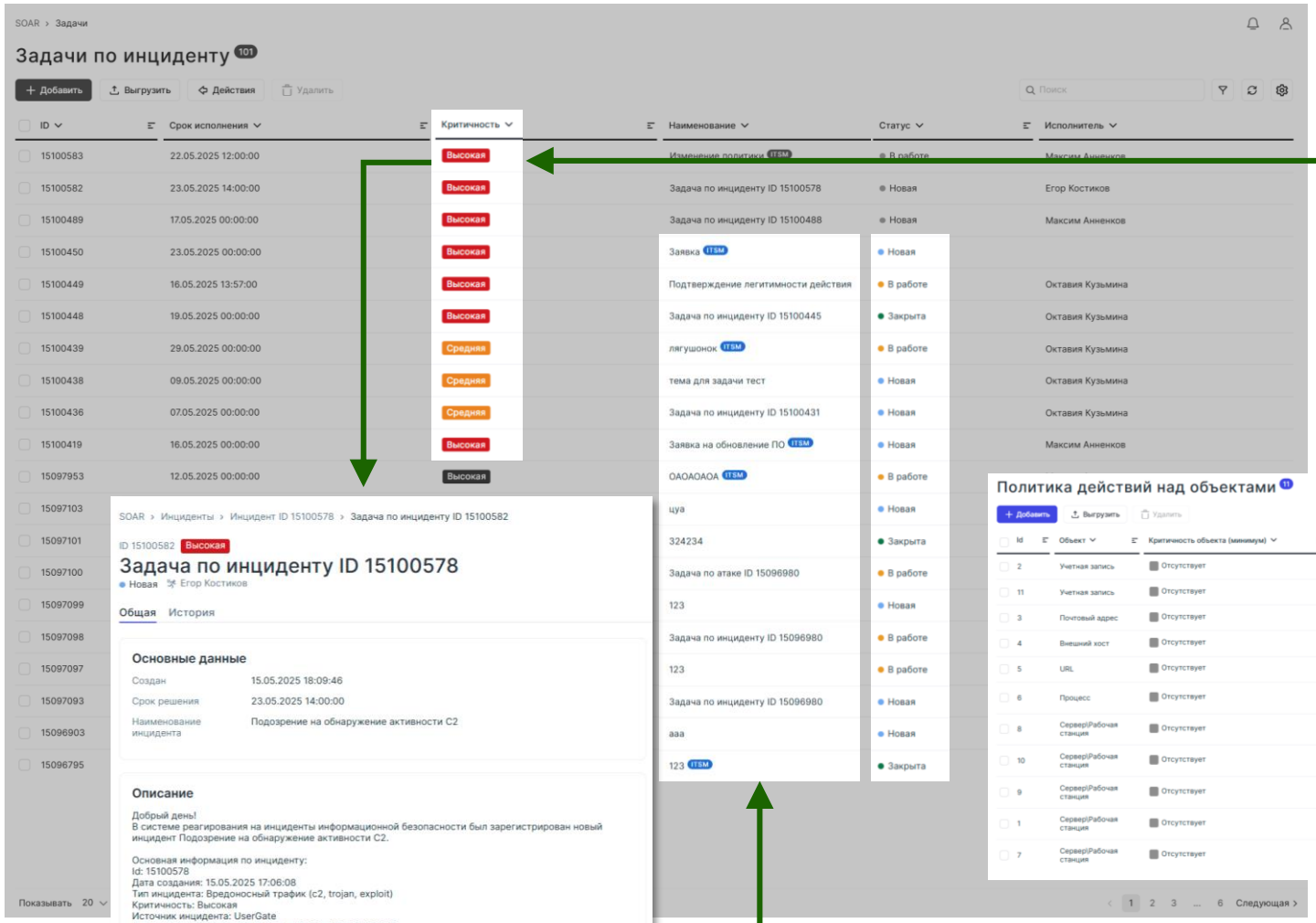
SOAR

Security **O**rchestration, **A**utomation and **R**esponse

управление инцидентами

Управление задачами и работа в команде

статусы и настройка видимости для совместной работы



встроенная система **тикетинга** и **интеграция с SD / ITSM**

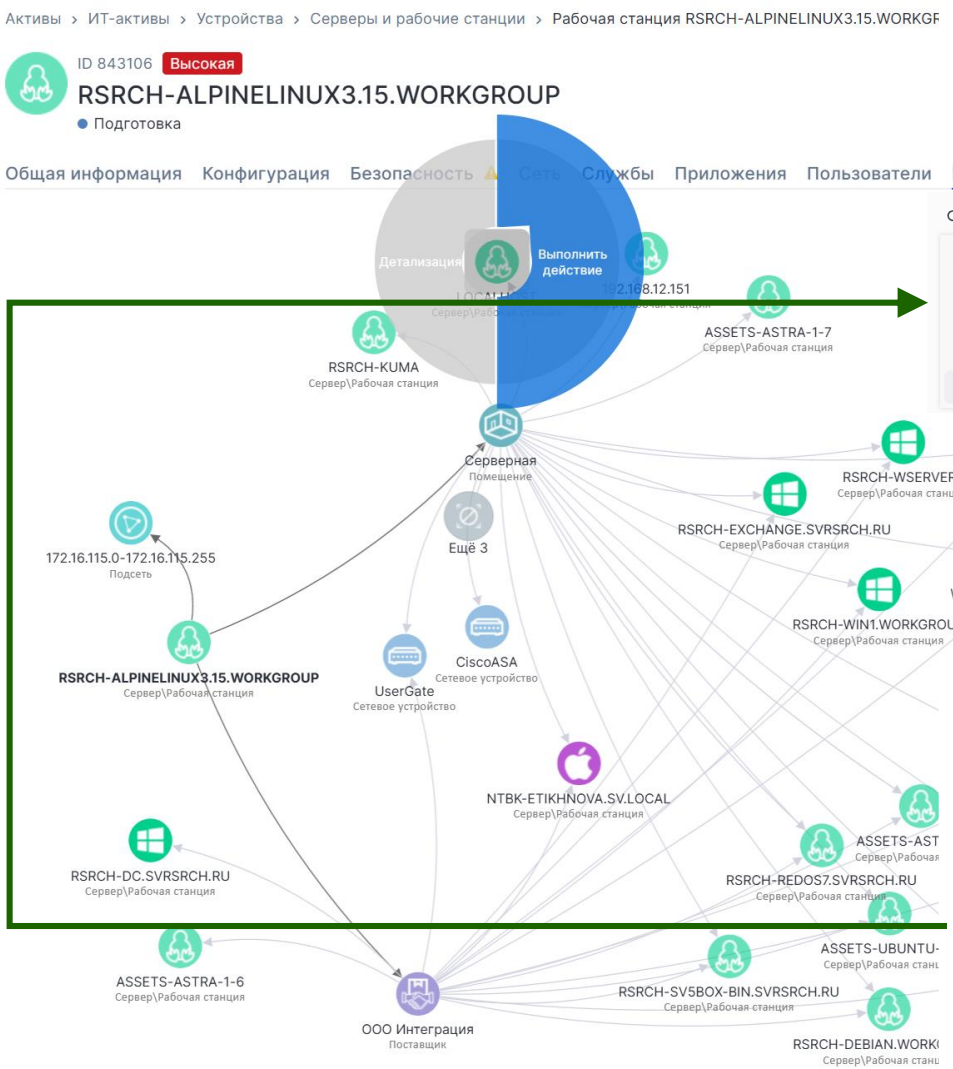
автоматический расчёт **SLA** с учетом **графиков** и **расписаний**

SOAR

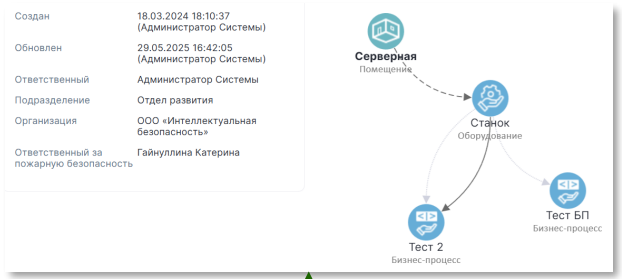
Security Orchestration, Automation and Response

управление инцидентами

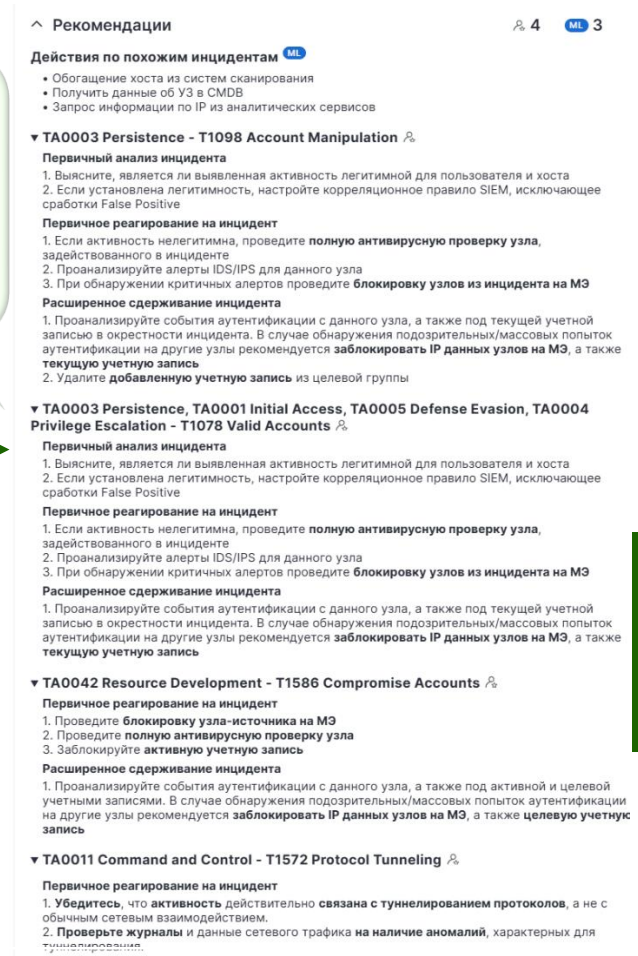
Умная система рекомендаций и база знаний



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



AI



рекомендации с применением **ML-моделей**

дополнительные **действия** по реагированию **в графе**

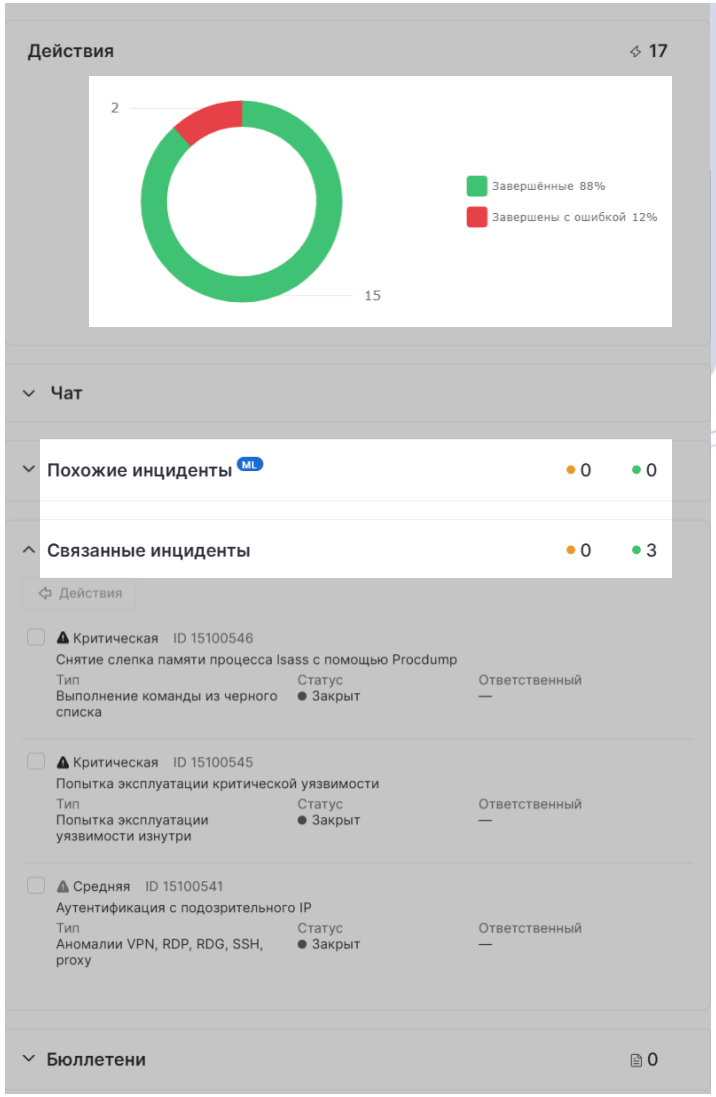
база знаний со всеми **действиями аналитиков**

SOAR

Security **O**rchestration, **A**utomation and **R**esponse

управление инцидентами

Применение ИИ-инструментов и аналитика



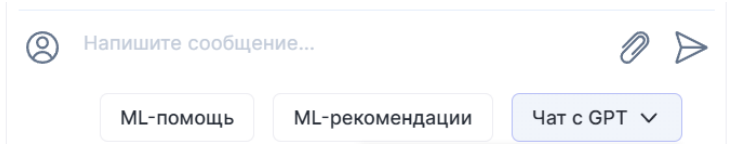
любые срезы данных и различные **способы визуализации** для анализа

MITRE ATT&CK
БДУ ФСТЭК

ML-модели для анализа **больших данных**

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

встроенные **интеграции** с внешними **LLM-моделями**

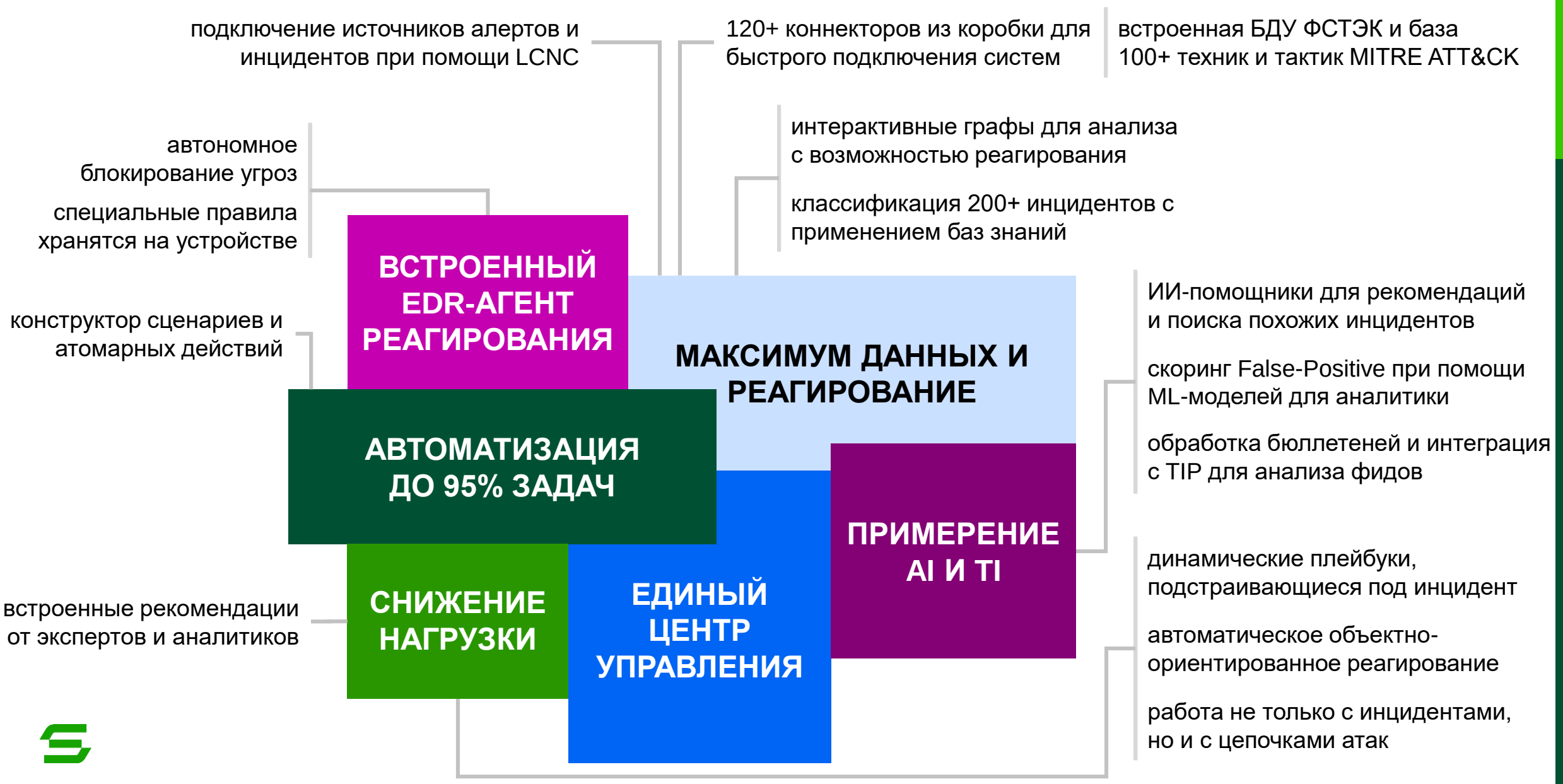


SOAR

Security **O**rchestration, **A**utomation and **R**esponse

управление инцидентами

SOAR, управление инцидентами



Спасибо за внимание

sales@securityvision.ru

Интеллектуальная платформа информационной безопасности и ИТ

Security Vision

securityvision.ru