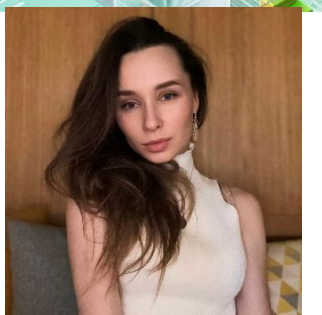
Систематизация и автоматизация процесса управления уязвимостями

Security Vision



Екатерина Урбах

Менеджер по работе
с партнерами
Security Vision

Максим Репко

Пресейл-менеджер
Security Vision

Security Vision в цифрах

100%

российская компания, специализирующаяся на автоматизации процессов обеспечения ИБ

сертифицирован ФСТЭК по 4 уровню доверия

включён в Единый реестр российского ПО

сертифицирован ОАЦ в республике Беларусь

государственные структуры

промышленность и энергетика

финансовые и страховые организации

ритейл и другие компании

телеком-операторы и коммерческие SOC

14/20

ТОП банков РФ

25

профессиональных наград в области ИБ

30/100

ТОП компаний РФ

100+

клиентов*

5+

MSSP** провайдеров ИБ-услуг

3

ТОП прогноза*** развития рынка на 2024-2028 годы

Security Vision

*securityvision.ru/projects/
**securityvision.ru/about/partners
***csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2024-2028-gody

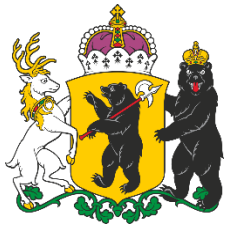
АО
«ГОЗНАК»

ФГБУ НИИ
«ИНТЕГРАЛ»

ФЕДЕРАЛЬНАЯ
СЛУЖБА ОХРАНЫ РФ

ПРАВИТЕЛЬСТВО
КРАСНОЯРСКОГО КРАЯ

ПРАВИТЕЛЬСТВО
ТЮМЕНСКОЙ ОБЛАСТИ



ПРАВИТЕЛЬСТВО
ЯРОСЛАВСКОЙ ОБЛАСТИ

СОВЕТ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОГО СОБРАНИЯ РФ

АО
«ДОМ.РФ»

АО НПП
«ИСТОК ИМ. ШОКИНА»

ПАО
«СЕВЕРСТАЛЬ»

ООО
«ЕВРАЗ»

АО КОНЦЕРН
«РОСЭНЕРГОАТОМ»

АО ОХК
«УРАЛХИМ»

ПАО ГМК
«НОРИЛЬСКИЙ НИКЕЛЬ»

ПАО
«ИНТЕР РАО»

ПАО
«РУСГИДРО»

ПАО
«СБЕРБАНК»

АО
«АЛЬФА-БАНК»

ПАО
«РОСБАНК»

АО
«Т-БАНК»

АО
«БАНК ГПБ»

ПАО БАНК
«ФК ОТКРЫТИЕ»

АО
«СМП БАНК»

ПАО
«СДМ-БАНК»

АО
«АБ РОССИЯ»

ООО
«X5 GROUP»

ПАО
«МАГНИТ»

ГРУППА
«ЧЕРКИЗОВО»

ООО ГК
«РУСАГРО».

АО
«ПЕРВЫЙ КАНАЛ»

АО
«ПОЧТА РОССИИ»

ГОСКОРПОРАЦИЯ
«РОСТЕХ»

ХОЛДИНГ
«CAPITAL GROUP»

ПАО
«МЕГАФОН»

ПАО
«ВЫМПЕЛКОМ»

ООО
«СОЛАР СЕКЬЮРИТИ»

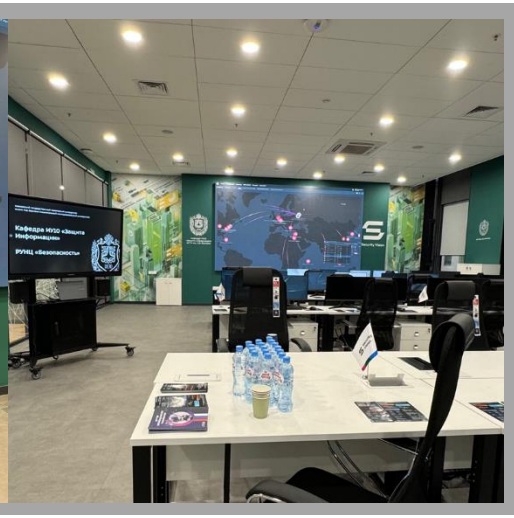
ООО
«АТ ГРУП»

ООО «ТТК-СВЯЗЬ»
(ТРАНСТЕЛЕКОМ)

ООО
«ИНФОСЕКЬЮРИТИ СЕРВИС»

КОММЕРЧЕСКИЙ SOC
«РОСТЕХ»

ВУЗы



МГТУ им. Баумана

Иннополис

НГТУ

НИЯУ МИФИ

СибГУ им. Решетнёва

УГНТУ

Сириус

УУНиТ

Московский политех

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

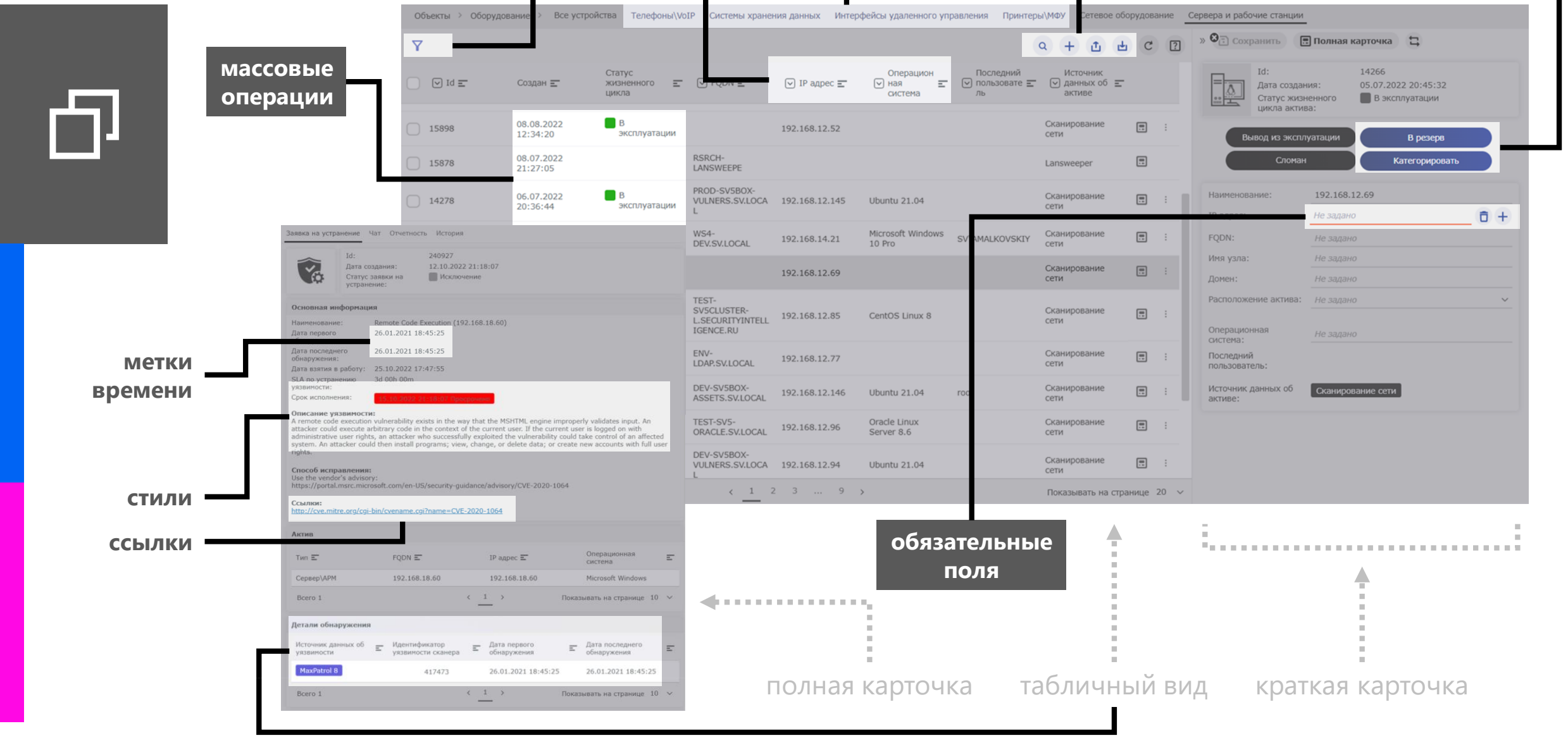
Security Vision

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

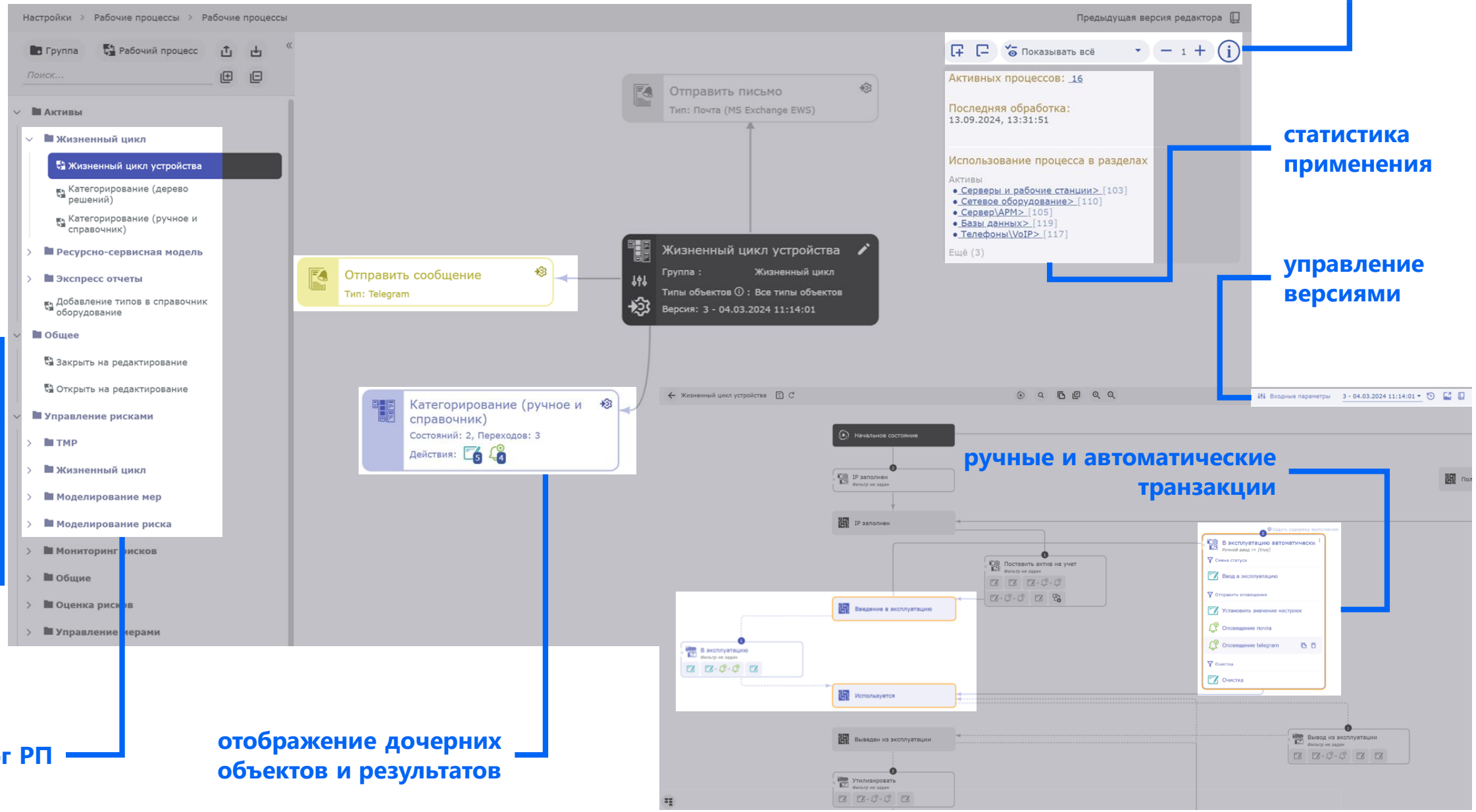
статистика применения

управление версиями

ручные и автоматические транзакции

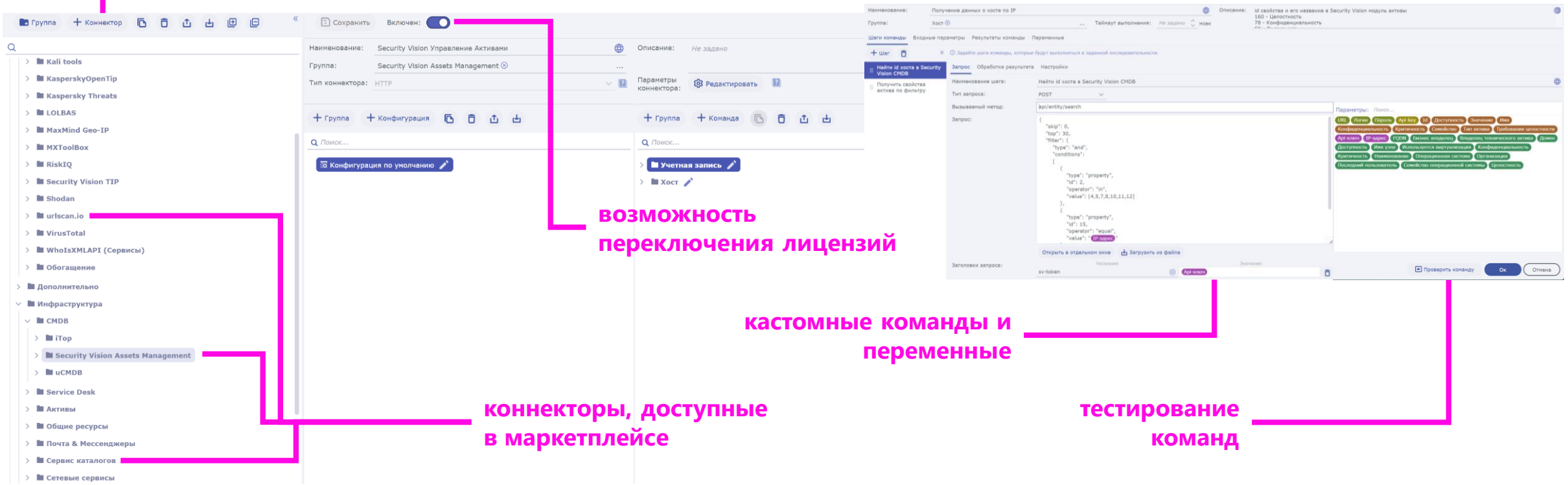
каталог РП

отображение дочерних объектов и результатов



Конструктор интеграций

создание интеграций через интерфейс



возможность переключения лицензий

кастомные команды и переменные

коннекторы, доступные в маркетплейсе

тестирование команд

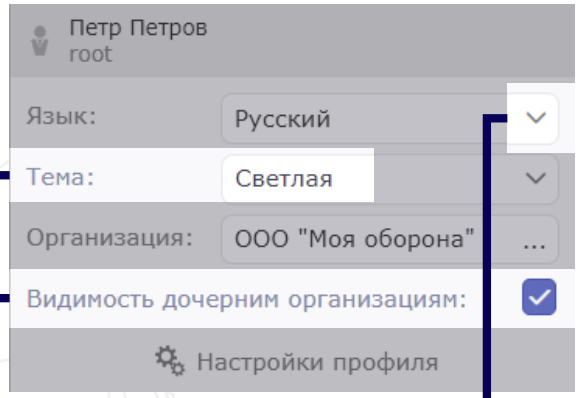
WMI | PS | SSH | файл | почта | БД | HTTP (API) | LDAP | EventLog | Syslog | DNS | скрипты и др.

Сбор и обогащение

Реагирование на события

создание новых коннекторов **без участия вендоров**

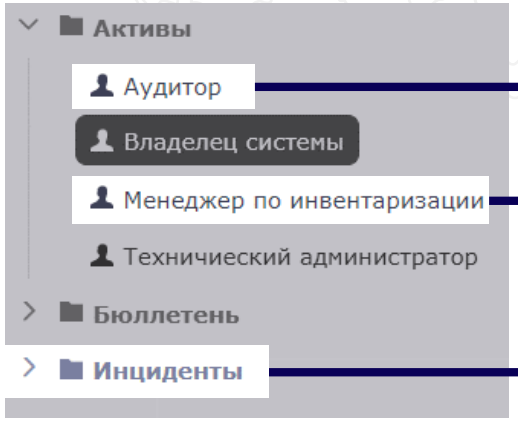
Конструктор ролей и меню



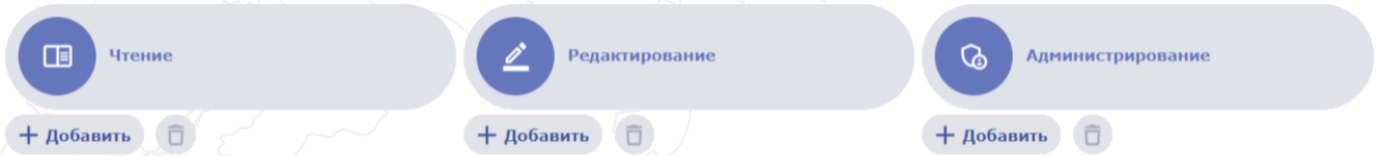
темы оформления

multitenancy

мультиязычность



персональная витрина

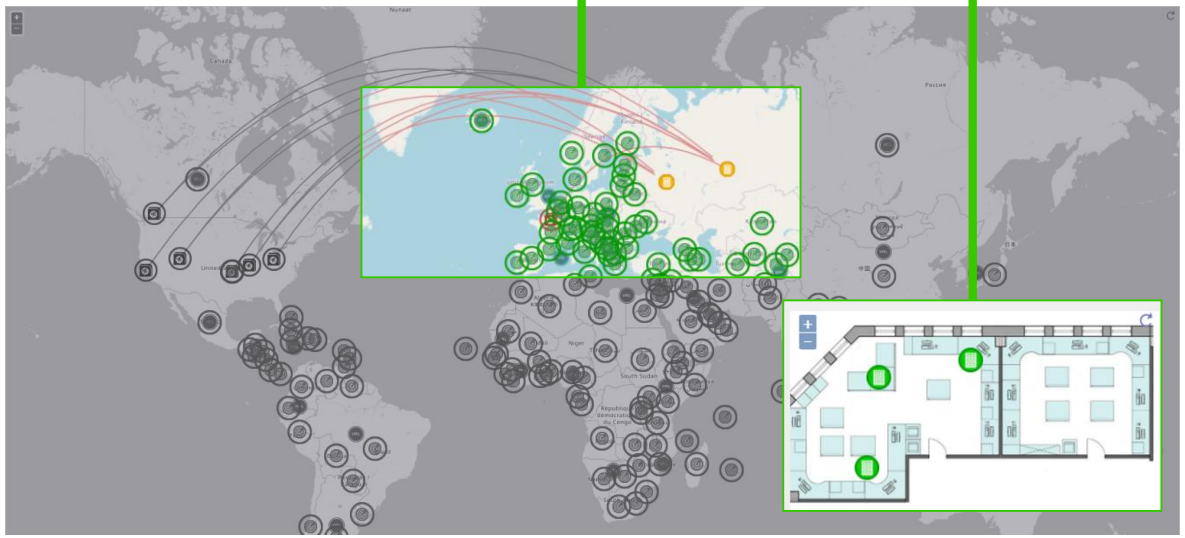


гранулярные настройки

Конструктор аналитики

карты и планы помещений

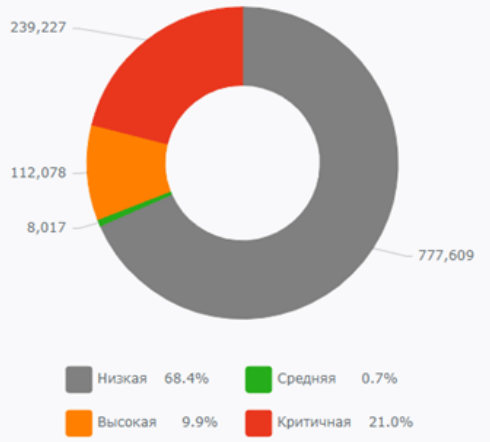
дашборды



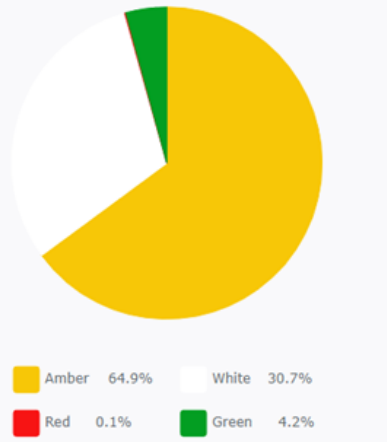
Топ-5 активных критичных инцидентов

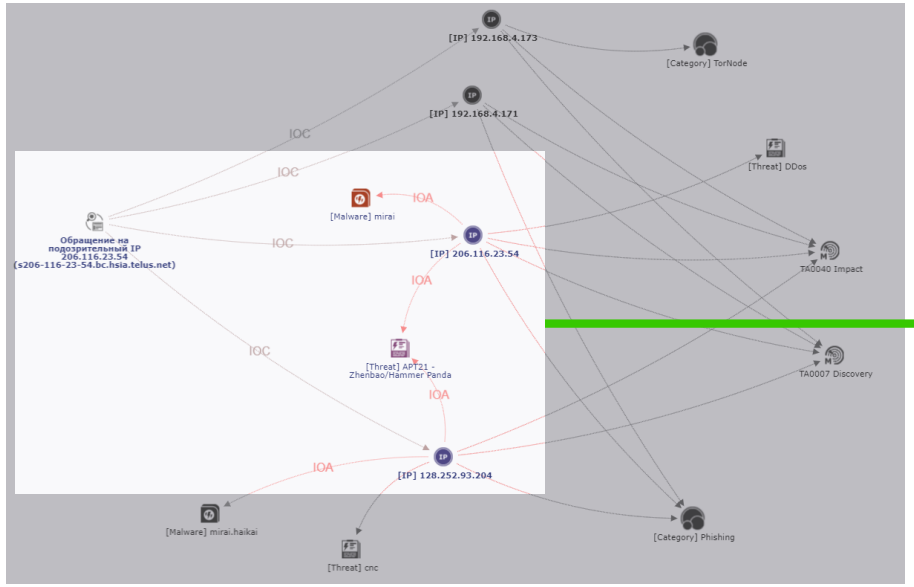
Наименование	Критичность	Статус
Отправка письма с подозрительного домена: acmetek.com	Критичная	Новый
Обращение на подозрительный домен cutt.ly	Высокая	Новый
Обращение на подозрительный домен conect-app.com	Высокая	Новый
Обращение с подозрительного IP 192.168.4.173 (ws4-dev.sv.local)	Высокая	Новый

Критичность индикаторов



TLP для индикаторов





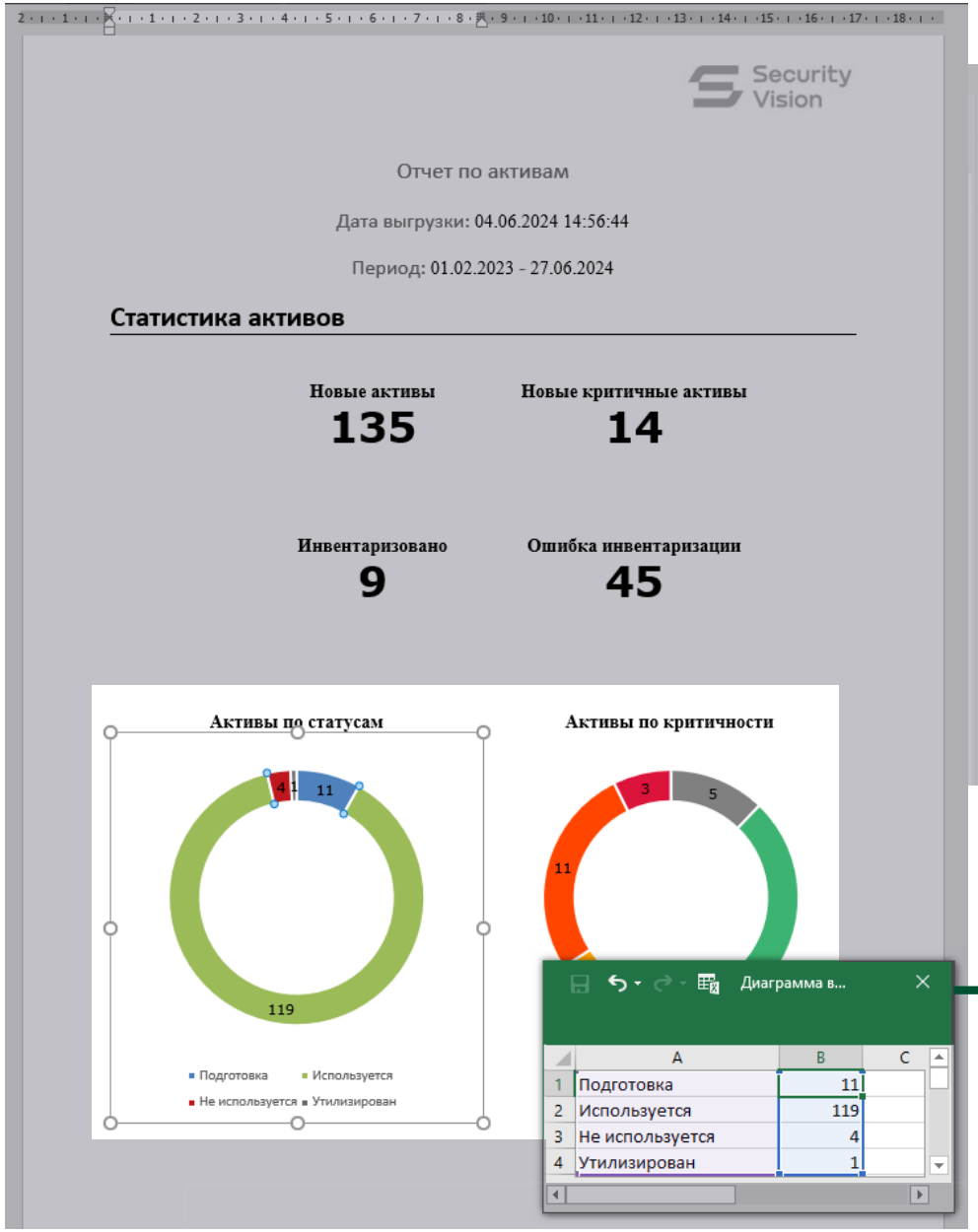
графы связей

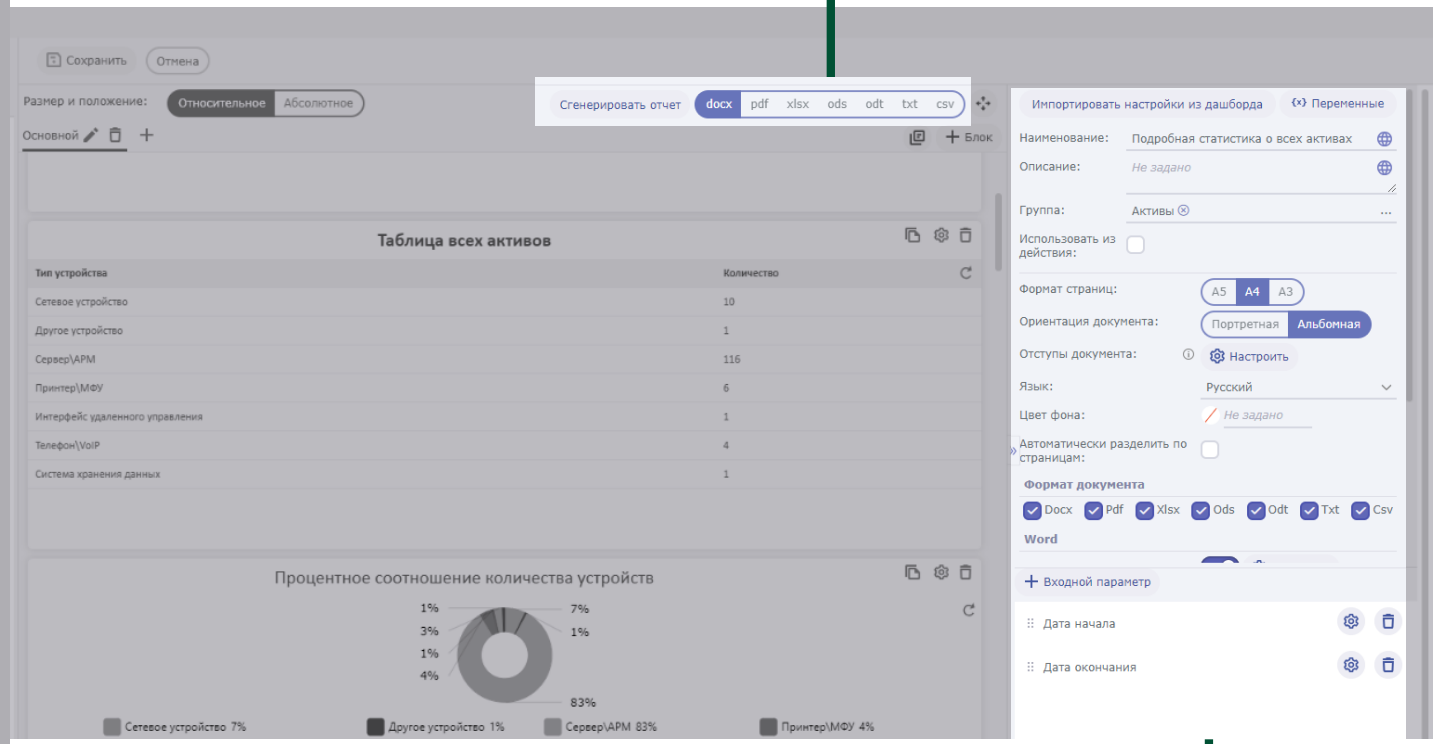
интерактивная аналитика и связанные графики

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

Конструктор отчётов

различные форматы

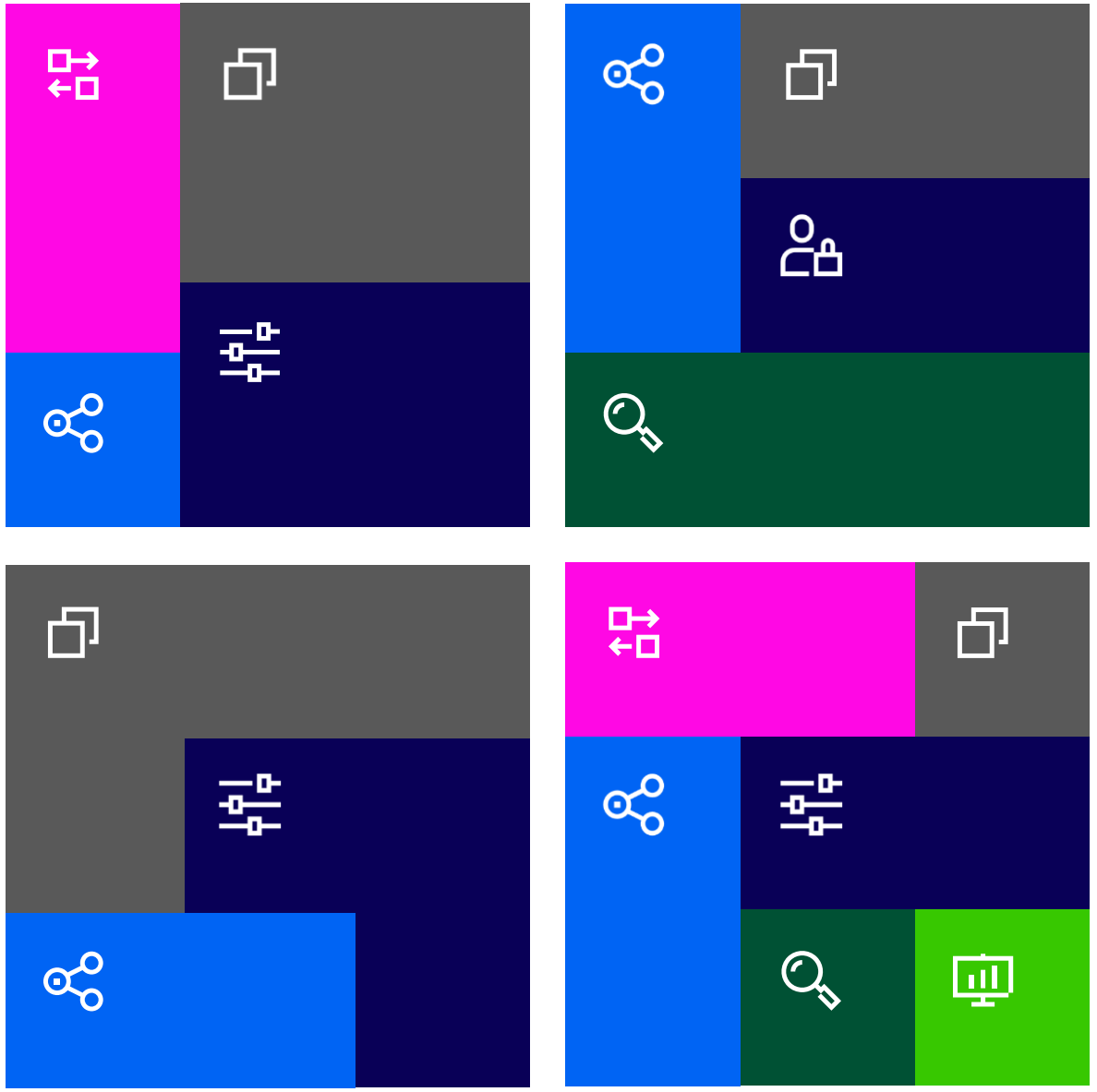




редактор шаблонов

хранение исходных данных

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



Единая платформа развивается в трех направлениях: технологии + процессы + аналитика

NG SOAR
Расширенное управление инцидентами

SOAR
Управление инцидентами

ГосСОПКА
Взаимодействие с НКЦКИ

FinCERT
Взаимодействие с ЦБ РФ

AM
Управление активами и инвентаризацией

VM + VS*
Управление уязвимостями *со сканером

SPC
Управление конфигурациями безопасности

КИИ
Управление соответствием ФЗ-187

RM
Управление рисками кибербезопасности

ORM
Управление операционными рисками

CM
Управление соответствием НМД

BCM
Управление непрерывностью бизнеса

SA
Портал самооценки ДЗО

TIP
Анализ угроз кибербезопасности

UEBA
Поведенческий анализ и поиск аномалий

[Блог]
securityvision.ru/blog

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

[Telegram]
t.me/svplatform

[YouTube]
youtube.com/@securityvision2421

ПРОЦЕССЫ
Governance, Risk Management and Compliance

ТЕХНОЛОГИИ
Security Orchestration Tools

АНАЛИТИКА
Security Data Analysis

Цикл управления уязвимостями