Автоматизация процессов ИТ и ИБ

Security Vision

[Блог]
securityvision.ru/blog

[Telegram]
t.me/svplatform

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

Security Vision в цифрах

lowcode.sk.ru

Топ 3 low-code платформ 2024

csr.ru/ru/research

Топ 3 прогноза развития 2024-2028

securityvision.ru

25+ профессиональных наград в области ИБ и ИТ

30 / 100
ТОП компаний РФ [1]

14 / 20
ТОП-банков [1]

10+ MSSP
провайдеров ИБ-услуг [2]

100+ клиентов из всех отраслей экономики

- социальная сфера и государственный сектор
- информационные технологии и связь
- финансы, страхование и недвижимость
- торговля, логистика и услуги
- промышленность, ТЭК и производство

1 securityvision.ru/about/work_with
2 securityvision.ru/about/partners

Security Vision

включён в **Единый реестр** российского ПО

сертифицирован **ФСБ России** ИТКС спец. назначения

сертифицирован **ФСТЭК России** по 4 уровню доверия

сертифицирован **ОАЦ Беларуси** технический регламент

социальная сфера и государственный сектор

ФЕДЕРАЛЬНАЯ СЛУЖБА ОХРАНЫ РФ

ПРАВИТЕЛЬСТВО КРАСНОЯРСКОГО КРАЯ

ПРАВИТЕЛЬСТВО ТЮМЕНСКОЙ ОБЛАСТИ

ПРАВИТЕЛЬСТВО ЯРОСЛАВСКОЙ ОБЛАСТИ

СОВЕТ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОГО СОБРАНИЯ РФ

СФ

информационные технологии и связь

СОЛАР

ANGARA SECURITY

ТТК

INFOSECURITY a Softline company

РТ Информационная безопасность

МегаФон

Почта России

Акционерное общество ГОЗНАК

финансы, страхование и недвижимость

Т БАНК

СБЕР

Газпромбанк

Ренессанс Банк

СМП

Банк России

Альфа Банк

CG CAPITAL GROUP

ДОМ РФ

торговля, логистика и услуги

черноголовка

X5Group

МАГНИТ

ЧЕРКИЗОВО С 1974

промышленность, ТЭК и производство

ИНТЕГРАЛ

УРАЛХИМ ГРУППА КОМПАНИЙ

РОСЭНЕРГОАТОМ РОСАТОМ

Северсталь

Ростех

ЕВРАЗ

ИНТЕР РАО

НОРНИКЕЛЬ

РУСАГРО

РусГидро

Security Vision

Злоумышленники знают, что специалисты перегружены

$4.88 млн

максимальная за 19 лет аналитики и отчётов **средняя стоимость утечки данных**

56%
специалистов ИБ не знают, что делать

+97%
организаций отмечают рост киберугроз за 2 года

33%
доля массовых атак из числа известных

194 days
среднее время обнаружения

3 billion
фишинговых писем ежедневно

68-88%
инцидентов - результат человеческой ошибки

https://www.varonis.com/blog/cybersecurity-statistics
https://www.ibm.com/reports/data-breach
https://www.cisco.com/c/dam/m/en_hk/ciscolive/2020-ciso-benchmark-cybersecurity-series.pdf
https://www.scworld.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023
https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity
https://www.securitymentor.com/security-awareness-training-statistics-and-trends

Преимущества предложения

Повышение эффективности коммуникаций – взаимодействие структурных подразделений и организаций группы компаний по единым согласованным правилам

Понятные и сопоставимые результаты оценки рисков для заинтересованных лиц благодаря применению стандартизованных методик и критериев оценки рисков

Уменьшение трудоемкости рабочих процессов, повышение оперативности сбора и актуализации статуса запланированных мероприятий по обработке рисков

Заинтересованные лица обеспечены информацией о рисках с необходимой детализацией для **принятия качественных управленческих решений**

Уменьшение затрат на поддержание актуальности информации, оперативный анализ влияния происходящих изменений на бизнес

Единая платформа развивается в трех направлениях

SOAR
управление инцидентами

AM
управление активами и инвентаризацией

КИИ
управление соответствием ФЗ-187

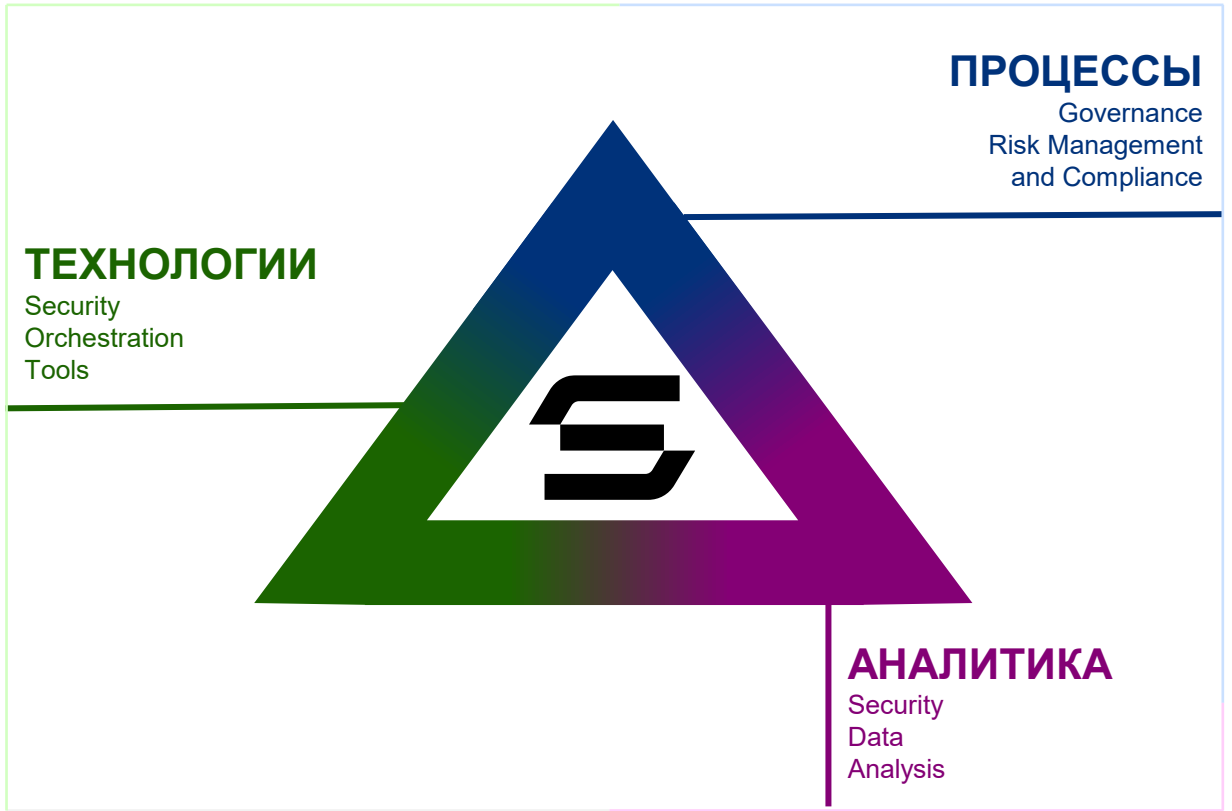
CM
управление соответствием НМД

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

Единая платформа развивается в трех направлениях

AM
Asset Management

описание ИТ-ландшафта, обнаружение новых объектов в сети, категорирование активов, инвентаризации и управления жизненным циклом оборудования и ПО на АРМ и серверах организаций, например процессами обновления/удаление программ

VM
Vulnerability Management

выстраивание процесса обнаружения и устранения технических уязвимостей, сбор информации с имеющихся сканеров защищённости, платформ управления обновлениями, экспертных внешних сервисов и других решений

SOAR
Security Orchestration, Automation and Response

автоматизация реагирования на инциденты информационной безопасности при помощи динамических плейбуков с применением СЗИ, выстраиванием цепочки атаки и объектно-ориентированным подходом к ликвидации инцидентов и устранению последствий

VS
Vulnerability Scanner

сканирование информационных активов с обогащением из внешних сервисов (дополнительных сканеров, БДУ и других аналитических баз данных) для анализа защищённости инфраструктуры, использования как самостоятельный сканер или для комплексного управления уязвимостями

FinCERT
Financial Computer Emergency Response Team

двустороннее взаимодействие с центрами Центрального банка: управление задачами, передача информации об инцидентах и получение оперативных уведомлений/бюллетеней по установленным регламентам регулятора

SPC
Security Profile Compliance

оценка конфигураций информационных активов в соответствии с принятыми в организации стандартами безопасности для выстраивает взаимосвязей с профилями технологических платформ и приведения параметров к эталонным значениям

ГосСОПКА
Государственная Система Обнаружения, Предупреждения и ликвидации последствий Компьютерных Атак

двустороннее взаимодействие с центрами реагирования НКЦКИ: управление задачами, передача информации об инцидентах и получение оперативных уведомлений/бюллетеней по установленным регламентам регулятора

встроенные **ИИ-помощники** и **коннекторы** позволяет интегрировать любую систему и расширить аналитические возможности

ТЕХНОЛОГИИ

КИИ

СМ

RM

ORM

BCM

SA

ПРОЦЕССЫ

TIP

UEBA

АНАЛИТИКА

Сертификат **ФСТЭК** 4574 (02.09.2022) | Заключение 8 Центра **ФСБ** России 149/3/6/908 (01.10.2024) | Реестр **отечественного ПО** №364 (08.04.2016)

Единая платформа развивается в трех направлениях

ТЕХНОЛОГИИ

- **AM**
- **SOAR**
- **FinCERT**
- **ГосСОПКА**
- **VM**
- **VS**
- **SPC**

КИИ

Критическая Информационная Инфраструктура

аудит и исполнение требований ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации» и других нормативных документов, включая процессы категорирования и управления задачами для соответствия

BCM

Business Continuity Management

автоматизация процесса обеспечения непрерывности и восстановления деятельности (ОНиВД) после наступления чрезвычайных ситуаций, включающий в себя BIA (Business Impact Analysis) и BCP (Business Continuity Planning) для обеспечения полного цикла

CM

Compliance Management

аудит соответствия и комплаенса различным методологиям и стандартам, как включённым в модуль экспертами (Приказы ФСТЭК 17, 21, 31, 239, ГОСТ 57580, PCI DSS, NIST, CIS, ФЗ №152 и №63 и др.), так и других документов заказчиков

SA

Self Assessment

специальный портал для оценки зрелости процессов кибербезопасности дочерних зависимых обществ (ДЗО) с контролем соответствия законодательным требованиям, отраслевым стандартам, визуализацией в реальном времени и выгрузкой всевозможных отчётов

RM

Risks Management

формирование реестра рисков, угроз, мер защиты, КИР и других параметров контроля, качественная и количественная методики оценок (FAIR, Монте-Карло и др.) с формированием перечня мер для изменения уровня риска, контроль исполнения

ORM

Operational Risks Management

формирование реестра, учёт событий операционного риска (СОР) и других параметров контроля, оценка для соответствия требованиям №716-П ЦБ РФ для формирования перечня мер для изменения уровня риска с контролем исполнения задач

все модули используют
единую ресурсно-сервисную модель
управления активами и инвентаризацией

десятки типов активов и конструктор новых:
технические узлы, СЗИ и бизнес-сущности
(процессы, продукты, помещения и т.д.)

ПРОЦЕССЫ

АНАЛИТИКА

- **TIP**
- **UEBA**

Единая платформа развивается в трех направлениях

ТЕХНОЛОГИИ

- AM
- SOAR
- FinCERT
- ГосСОПКА
- VM
- VS
- SPC

ПРОЦЕССЫ

- КИИ
- СМ
- RM
- ORM
- BCM
- SA

TIP

Threat Intelligence Platform

сбор и анализ данных об угрозах кибербезопасности, их обогащение, обнаружение в инфраструктуре, Threat Hunting и самостоятельный цикл расследования со встроенными функциями реагирования через интерактивные кнопки, таблицы и графы связей

UEBA

User and Entity Behavior Analytics

выстраивание моделей поведения и обнаружение отклонений от них при помощи нескольких десятков встроенных правил статического анализа, специально разработанных правил корреляции и предобученных моделей ИИ с возможностью обучения и на «живом» трафике

модули направления используют продвинутые способы обработки BIG DATA

правила корреляции и конструктор для их создания

бесшовная интеграция внутри экосистемы Security Vision

обработка «сырых» событий от **всех возможных источников**

специальный конструктор для интеграций **любых систем**

АНАЛИТИКА

Принятие качественных стратегических и тактических решений

Актуальная информация в режиме реального времени

Создания интеграций с любыми ИС при помощи веб-интерфейса

Сокращение трудовых ресурсов и исключение человеческого фактора

Автоматизация сбора информации и реагирования

Единый инсталлятор и платформенное решение

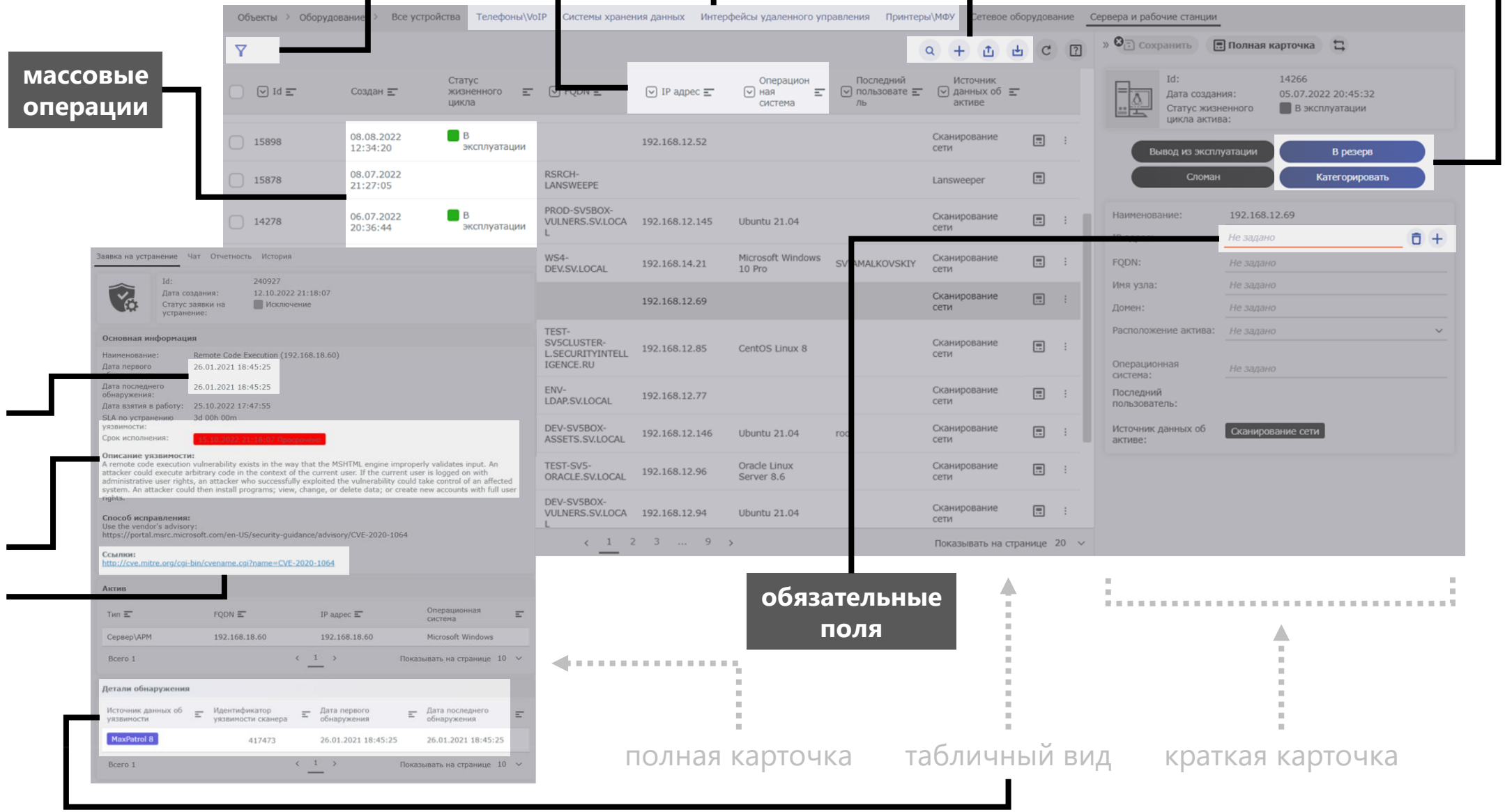
Снижение ущерба и времени воздействия инцидентов ИБ

Сокращение времени в среднем в 10 раз за счёт автоматизации

Любая сложность сценария и логика бизнес-процесса

ПЛАТФОРМА

Конструктор объектов



Конструктор рабочих процессов

управление глубиной отображаемых связей

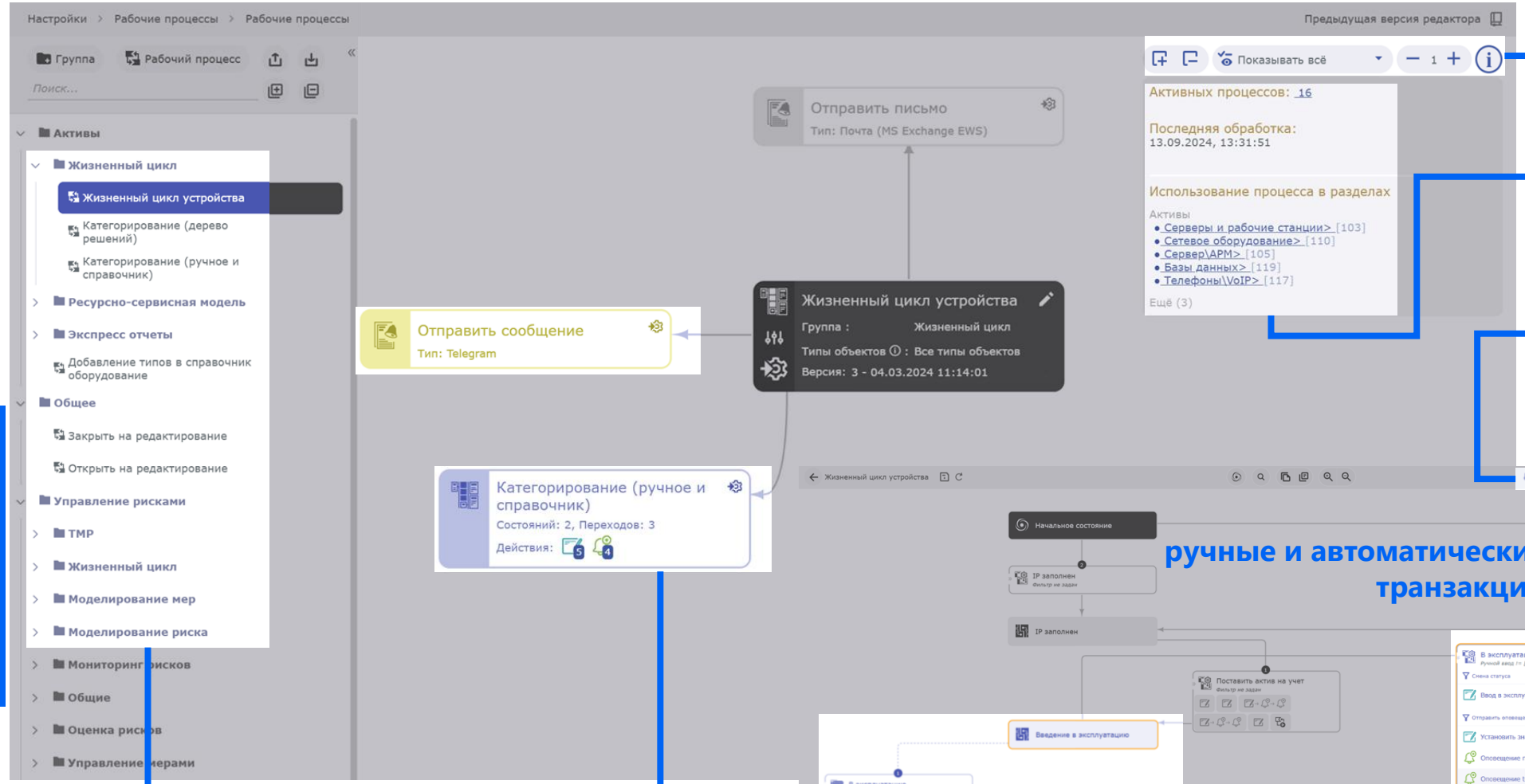
статистика применения

управление версиями

ручные и автоматические транзакции

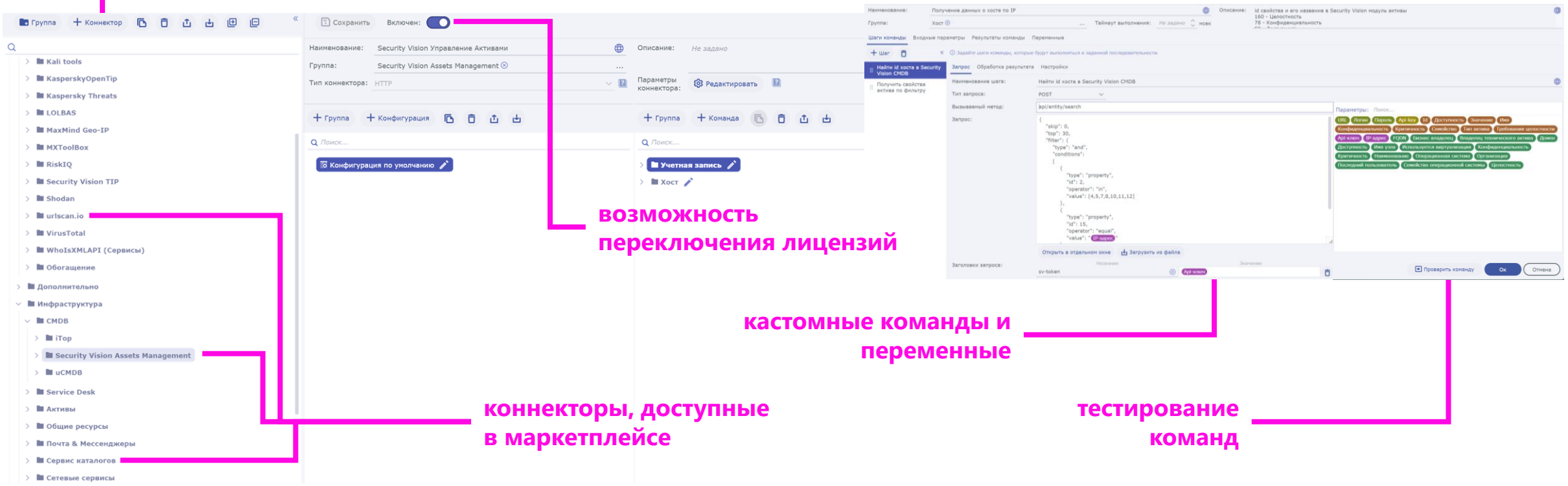
каталог РП

отображение дочерних объектов и результатов



Конструктор интеграций

создание интеграций через интерфейс



возможность переключения лицензий

кастомные команды и переменные

коннекторы, доступные в маркетплейсе

тестирование команд

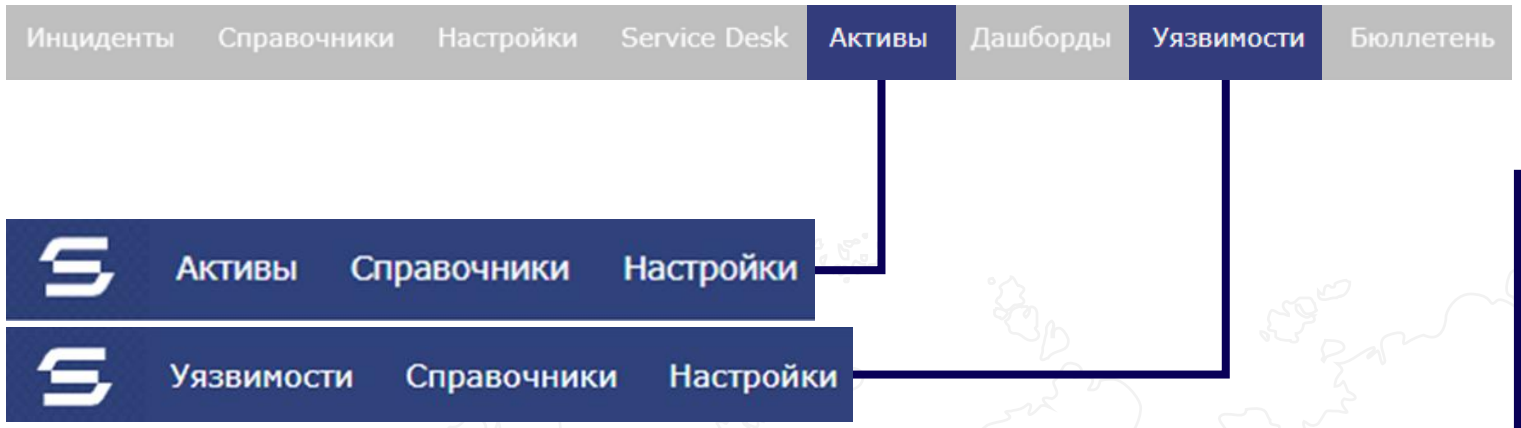
WMI | PS | SSH | файл | почта | БД | HTTP (API) | LDAP | EventLog | Syslog | DNS | скрипты и др.

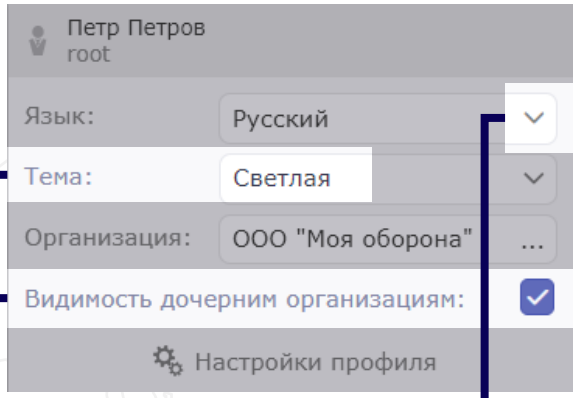
Сбор и обогащение

Реагирование на события

создание новых коннекторов **без участия вендоров**

Конструктор ролей и меню

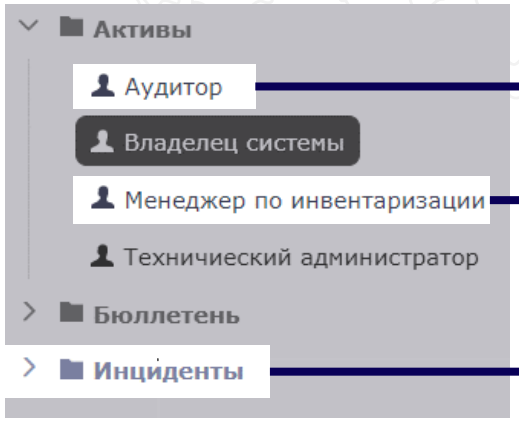




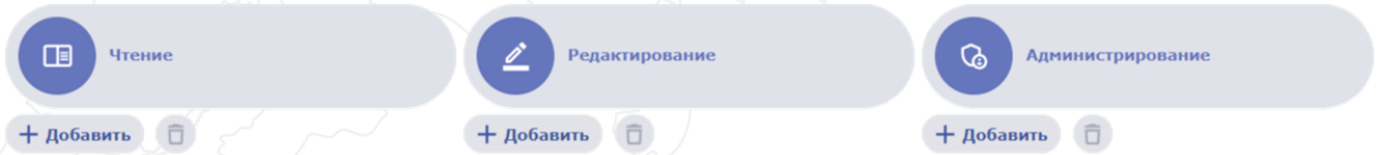
темы оформления

multitenancy

мультиязычность



персональная витрина

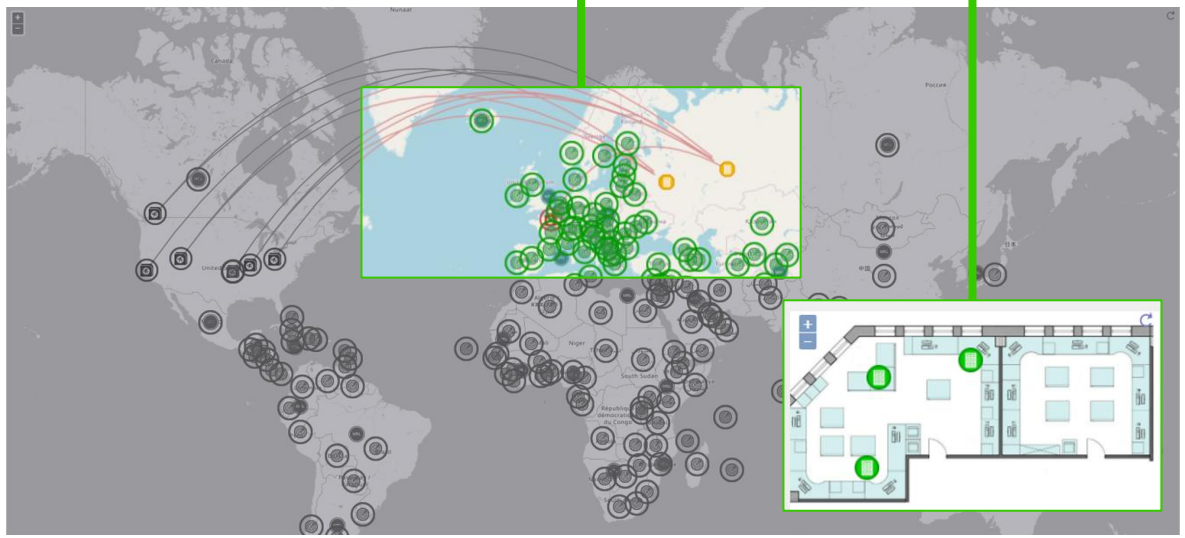


гранулярные настройки

Конструктор аналитики

карты и планы помещений

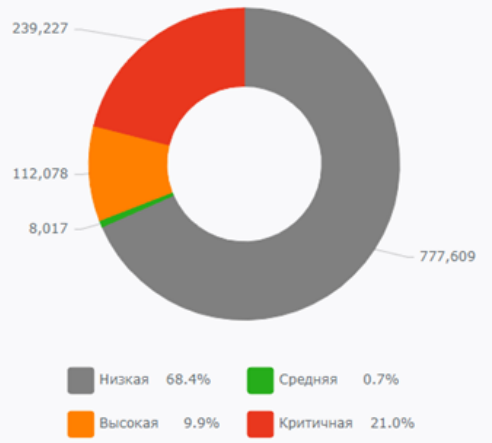
дашборды



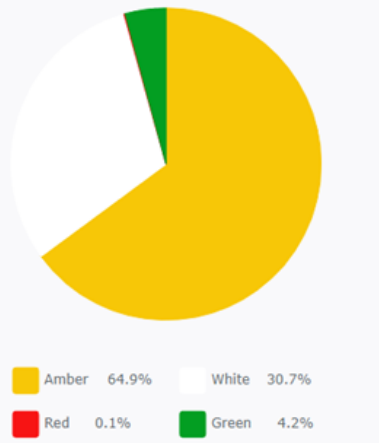
Топ-5 активных критичных инцидентов

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

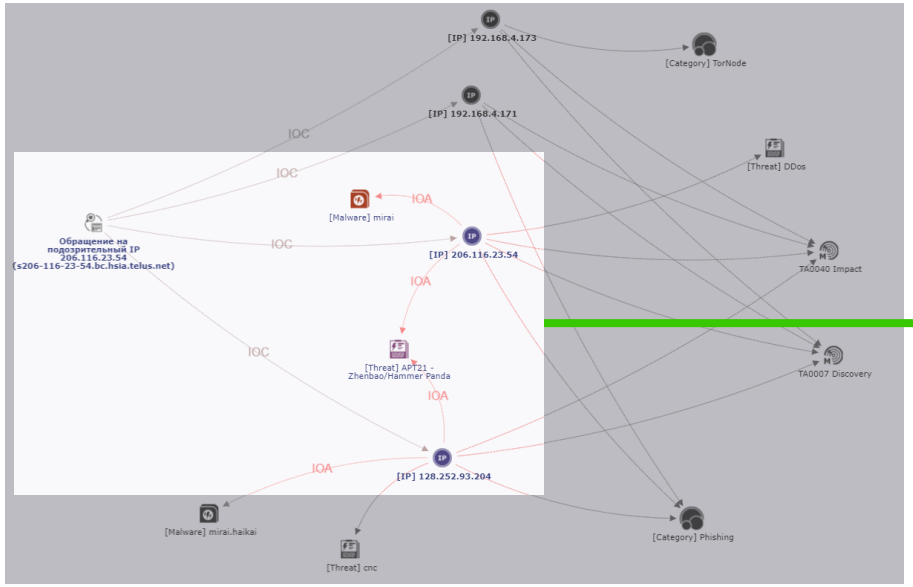
Критичность индикаторов



TLP для индикаторов



графы связей

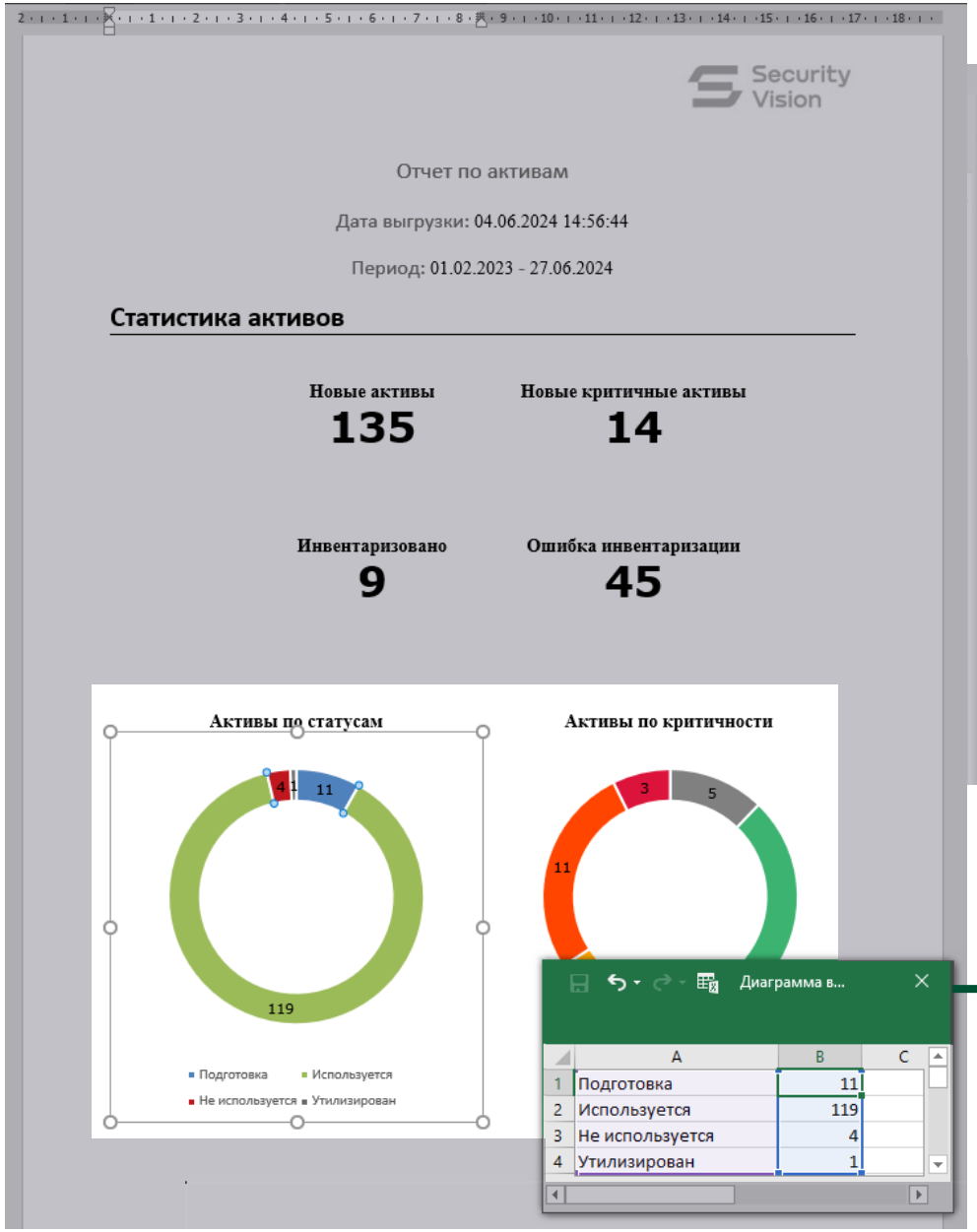


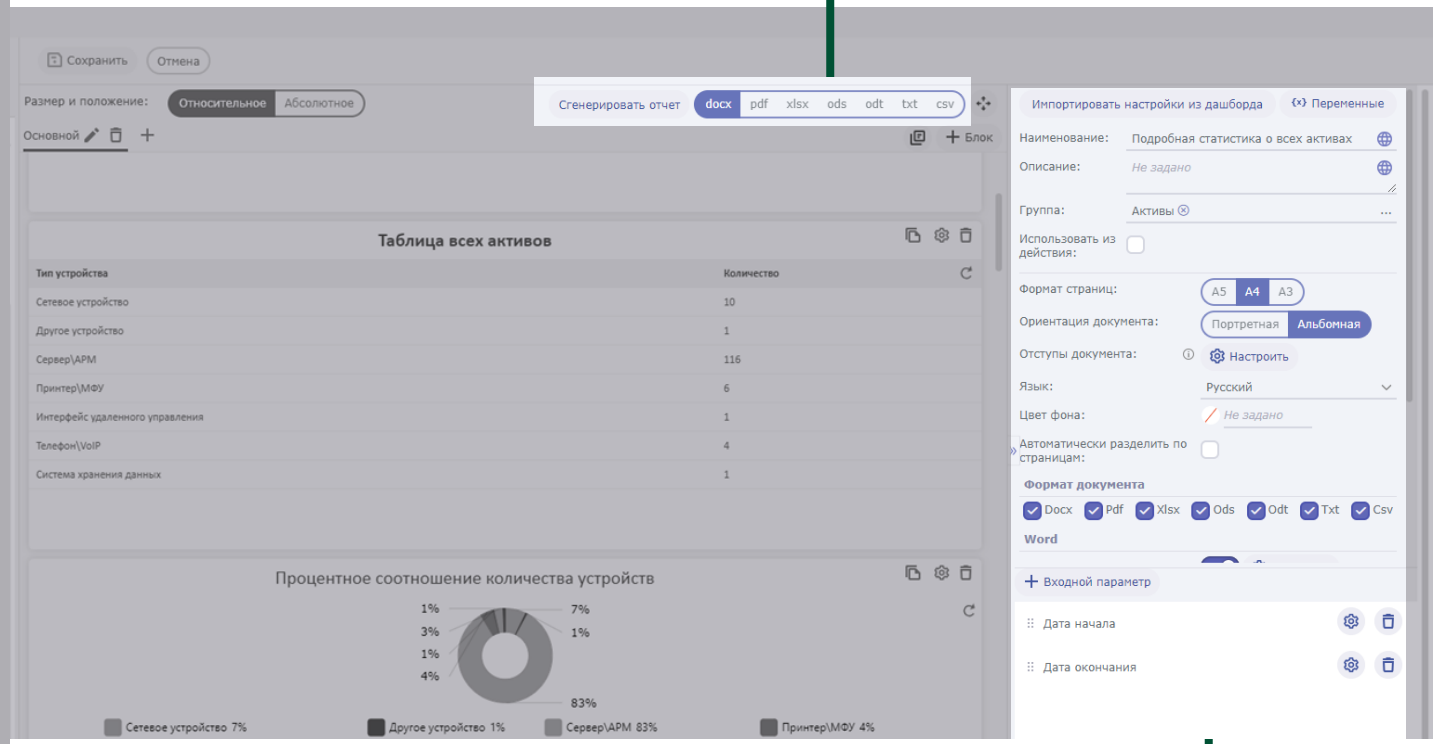
интерактивная аналитика и связанные графики

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

Конструктор отчётов

различные форматы





редактор шаблонов

хранение исходных данных

Единая гибкая платформа

с кастомизацией

Объекты, карточки и табличные представления

Роли и меню, доступ к данным и внешний вид

Рабочие процессы и автоматизация действий

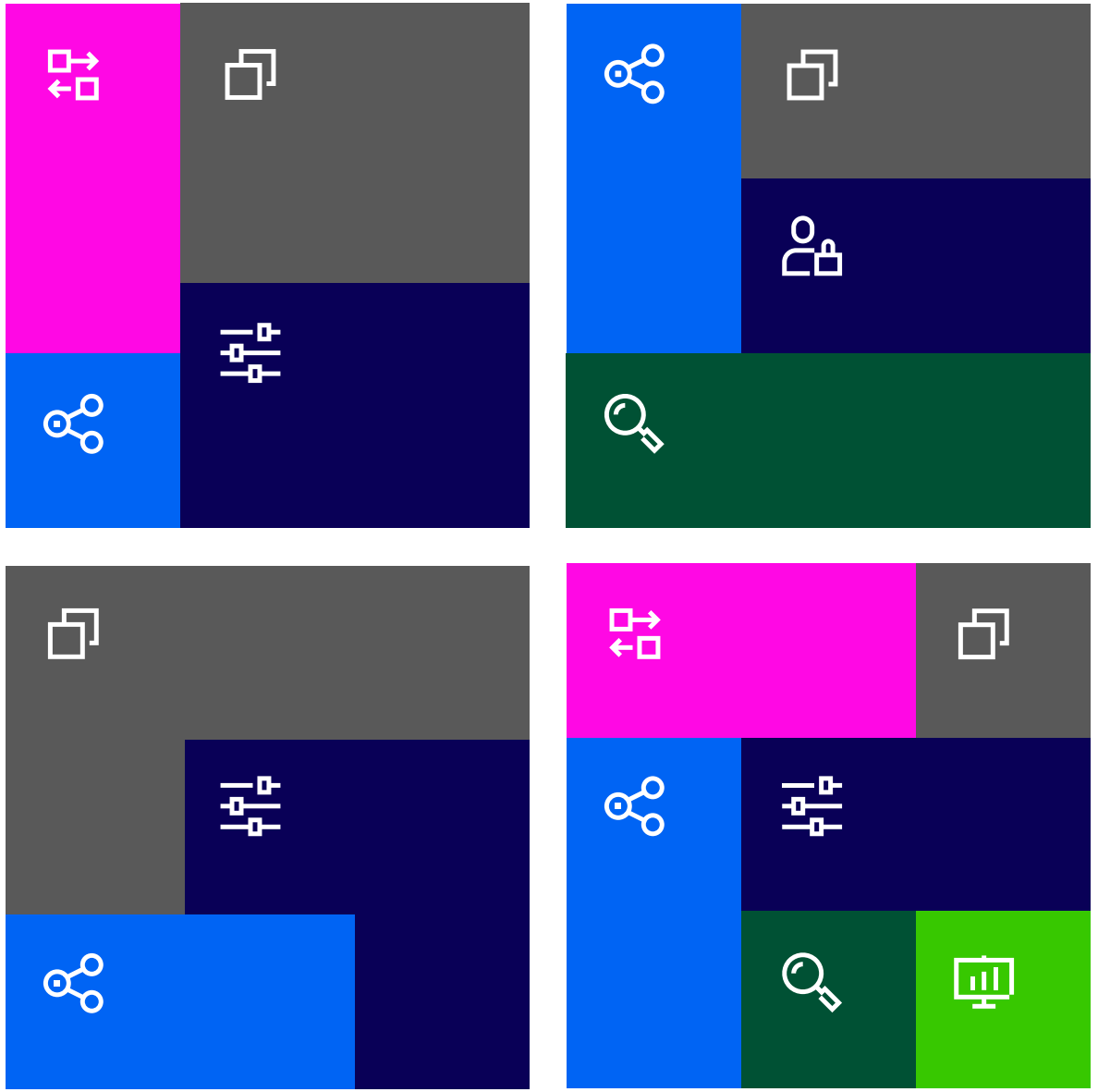
Security Vision

Аналитика, интерактивные виджеты и дашборды

Интеграции с внешними системами (коннекторы)

Отчёты, выгрузка файлов и логирование действий

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



Спасибо за внимание

sales@securityvision.ru

Интеллектуальная платформа информационной безопасности и ИТ

Security Vision

securityvision.ru