Управление безопасностью и анализ угроз

на стыке технологий и решений ИБ/ИТ

Security Vision

1 ДОВЕРИЕ

100+ клиентов из банковской сферы, индустрии, государственных структур, частного бизнеса

и других сфер

2 ЭКСПЕРТИЗА

~100 экспертов, собственная разработка, тестирование, внедрение

развитая партнёрская сеть

3 КАЧЕСТВО

ИБ-решение 2022, лучший партнёр банков 2021, лучшая платформа автоматизации 2020

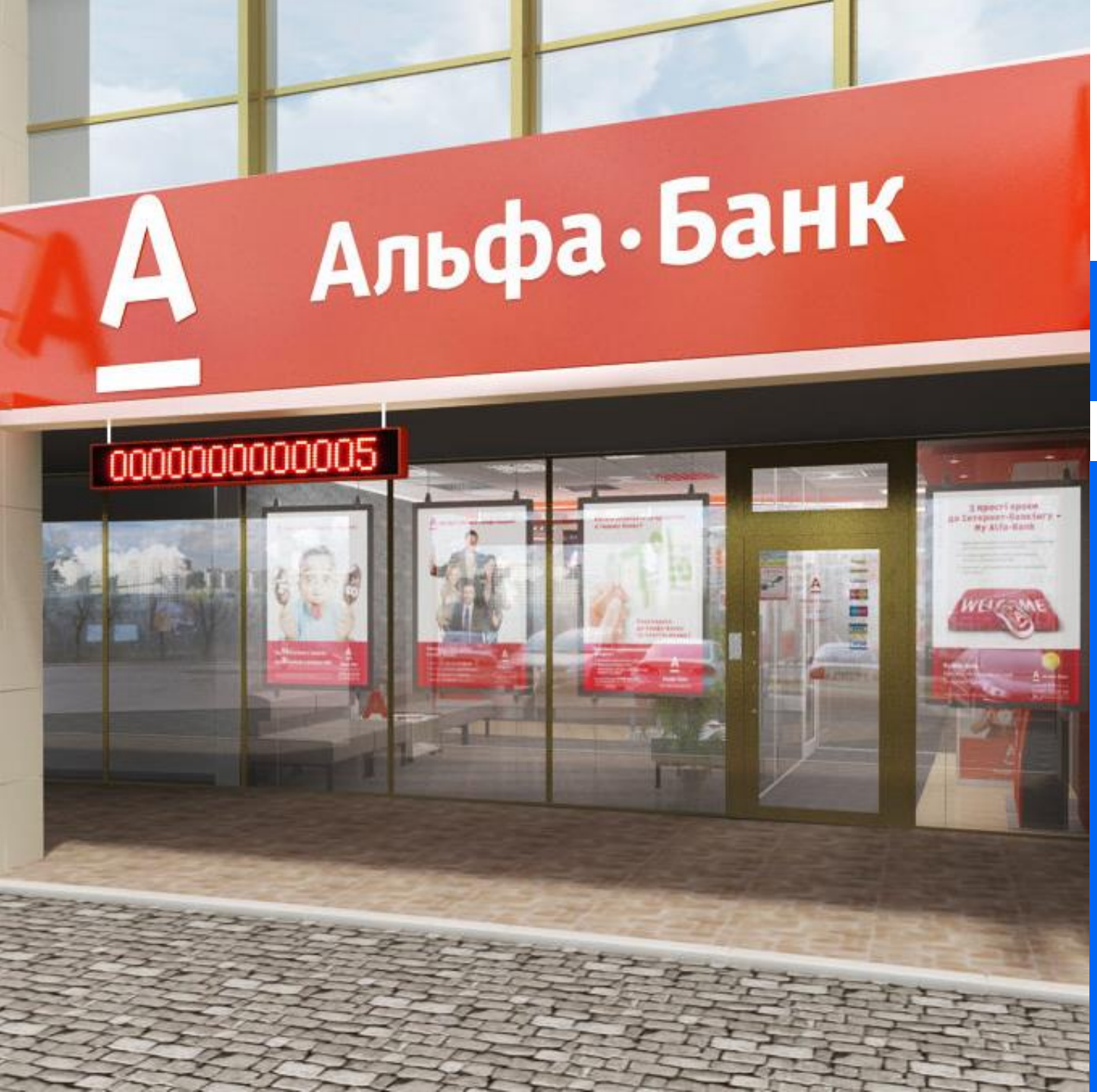
20+ профессиональных наград

КЛИЕНТЫ и коммерческие центры реагирования

Security Vision

← Click here

НАЦИОНАЛЬНАЯ БАНКОВСКАЯ ПРЕМИЯ



УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 20+ автоматизированных плейбуков реагирования
- Реализация процесса управление уязвимостями
- 30+ интеграций, включая взаимодействие с ФинЦЕРТ

Северсталь

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 20+ автоматизированных плейбуков реагирования
- Реализация процесса анализа угроз кибербезопасности
- 40+ интеграций с ИТ-системами и СЗИ

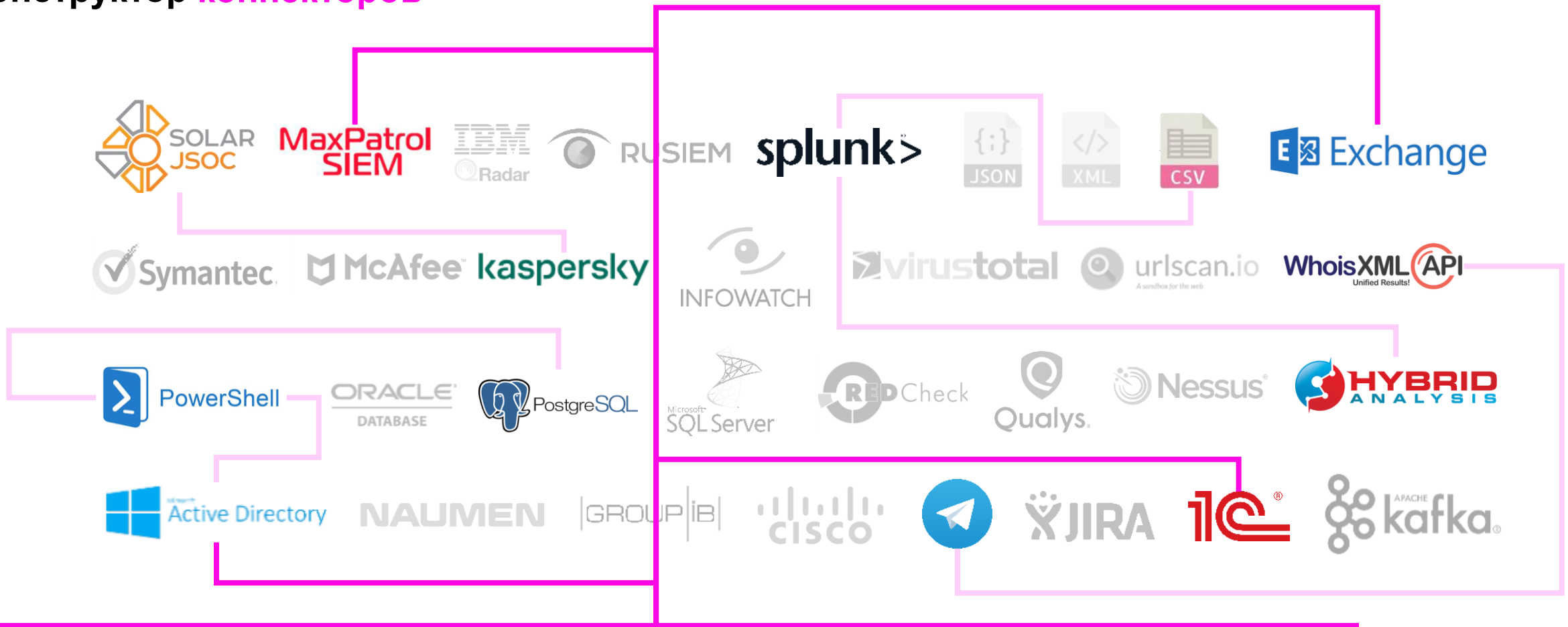
X5 Group

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 15+ автоматизированных плейбуков реагирования
- Глубокие процессы обработки инцидентов
- 20+ интеграций с ИТ-системами и СЗИ

на стыке технологий

Конструктор коннекторов



email | Syslog | файлы | БД | API | DNS | SNMP | LDAP | SOAP | скрипты

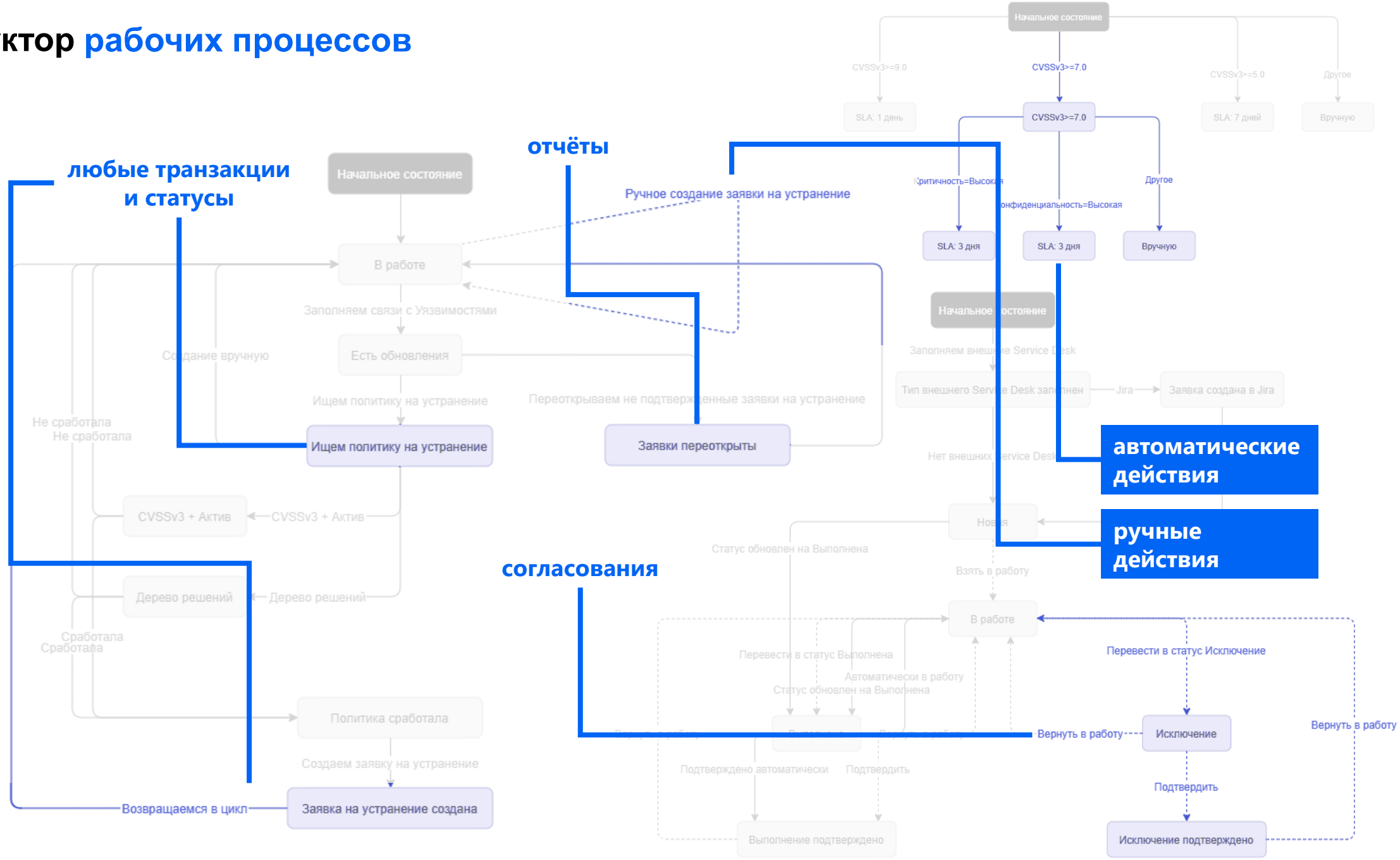
создание новых коннекторов **без участия вендоров**

Сбор и обогащение

Реагирование на события

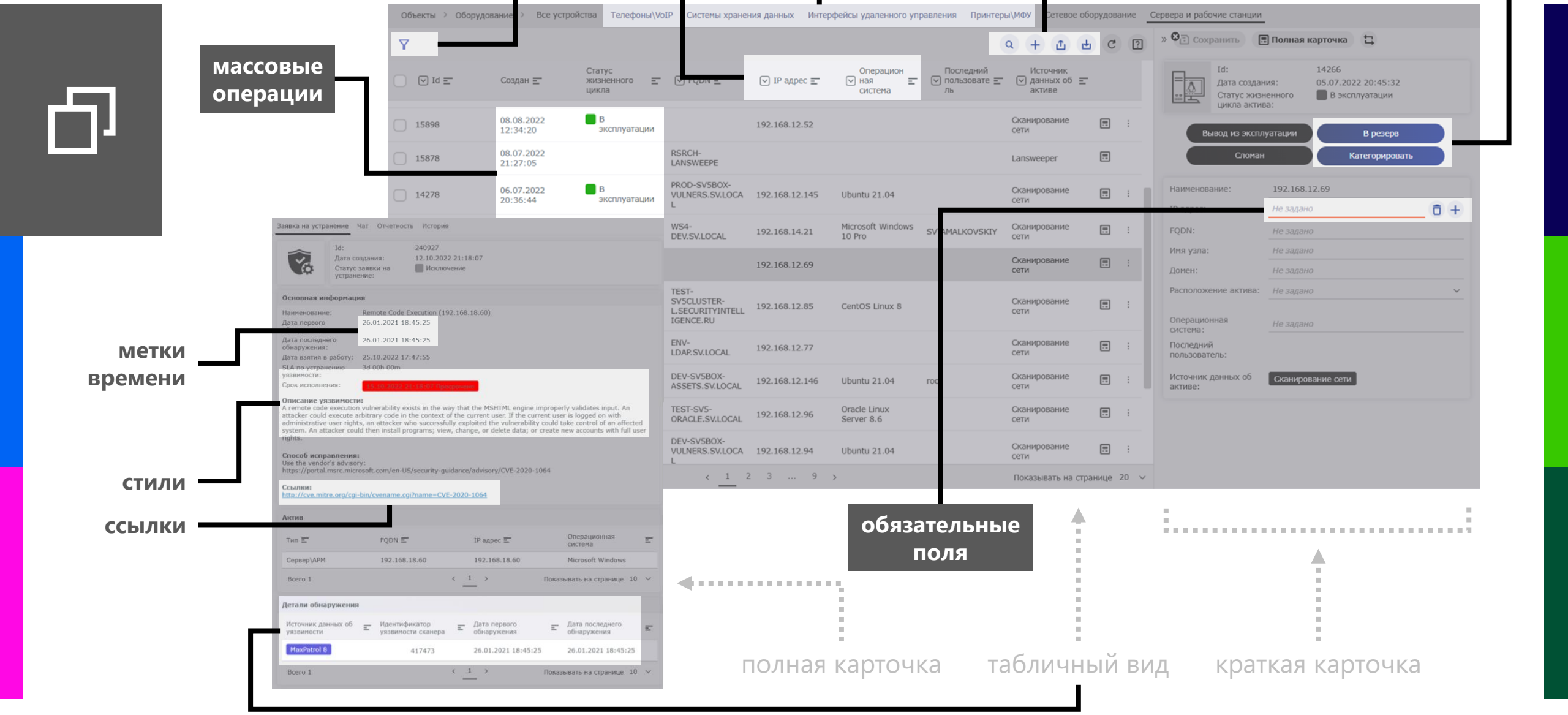
настоящие задачи

Конструктор рабочих процессов



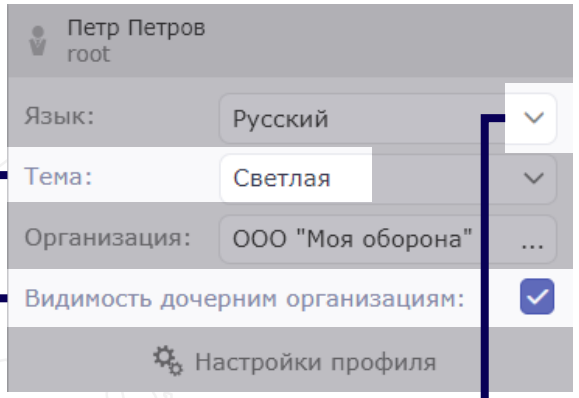
интерфейсы и язык

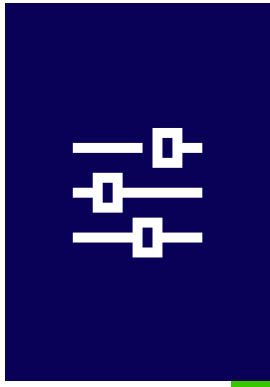
Конструктор объектов



распределённые команды

Конструктор ролей

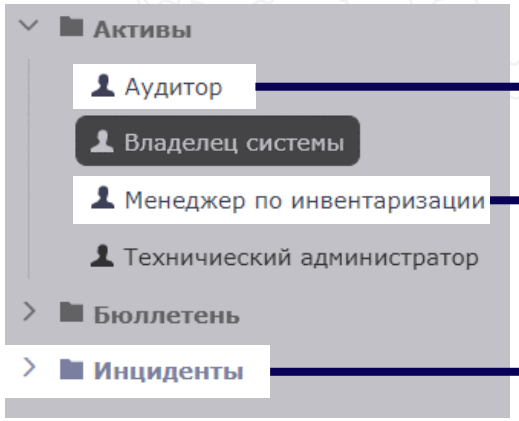




темы оформления

multitenancy

мультиязычность



персональная витрина

гранулярные настройки

ЧТЕНИЕ

ВКЛАДКИ МЕНЮ

РЕДАКТИРОВАНИЕ

АДМИНИСТРИРОВАНИЕ

аналитика и документация

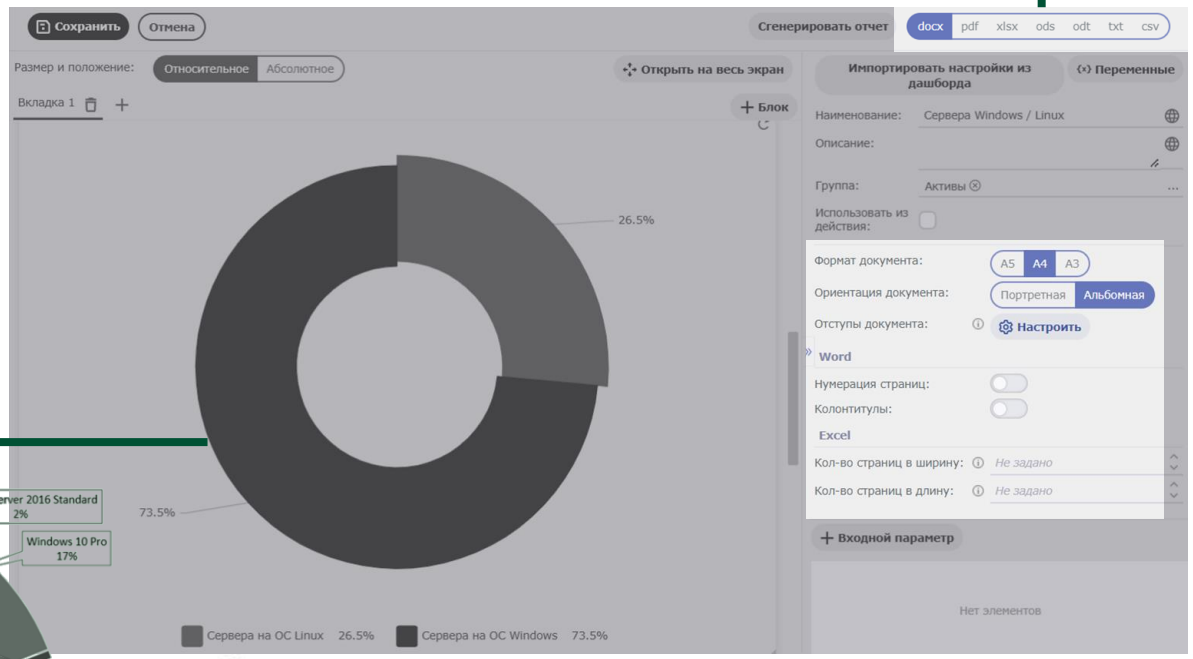
Конструктор виджетов и отчётов

графы связей

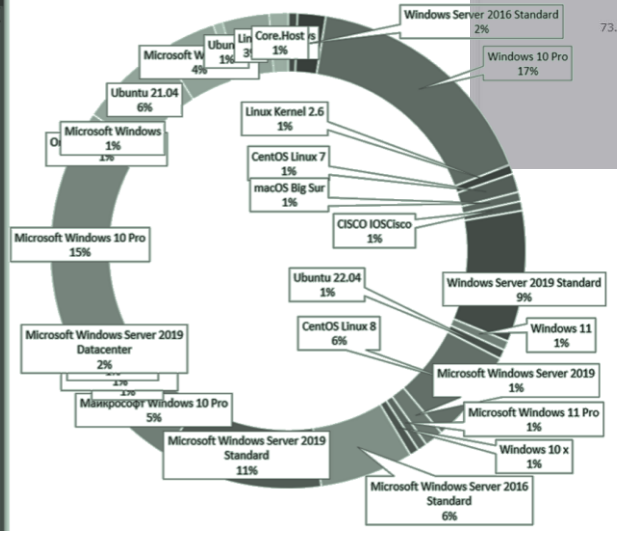
карты и планы помещений

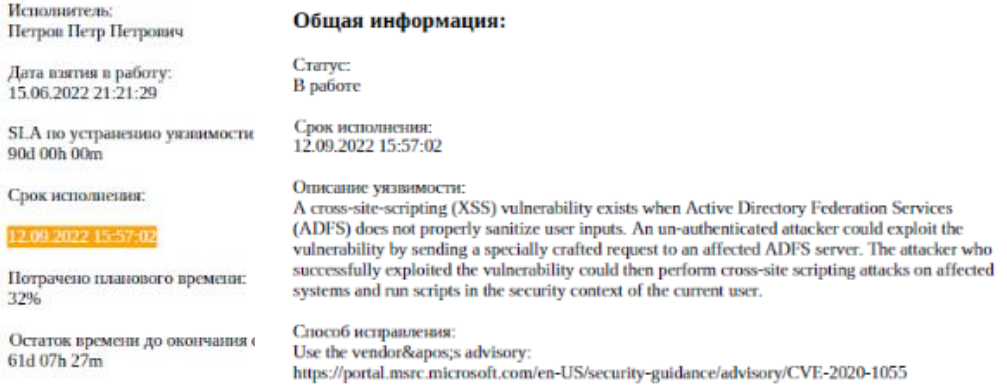
различные форматы

интерактивная аналитика и отчёты по расписанию



	A	B
1	Windows	1
2	Windows Server 2016 Standard	3
3	Windows 10 Pro	26
4	Linux Kernel 2.6	1
5	CentOS Linux 7	2
6	macOS Big Sur	1
7	CISCO IOSCisco	1
8	Windows Server 2019 Standard	14
9	Windows 11	1
10	Ubuntu 22.04	1
11	CentOS Linux 8	10
12	Microsoft Windows Server 2019	2
13	Microsoft Windows 11 Pro	1
14	Windows 10 x	1
15	Microsoft Windows Server 2016	10
16	Microsoft Windows Server 2019	17
17	Майкрософт Windows 10 Pro	8
18	Windows 10	1
19	<Microsoft Windows>	2
20	CentOS Stream 8	1
21	Microsoft Windows Server 2019	3
22	Microsoft Windows 10 Pro	23
23	Oracle Linux Server 8.6	1
24	Microsoft Windows	2
26	Ubuntu 21.04	10
27	Microsoft Windows 10	6
28	Ubuntu	1
29	Linux	5
30	Core.Host	2





Единая гибкая платформа

~ CRM

~ BPM

Объекты, карточки и внешний вид

Ролевая модуль и настройка меню

~ BI

Рабочие процессы и структура

Security Vision

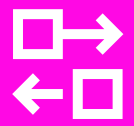
Визуализация и аналитика

~ RPA

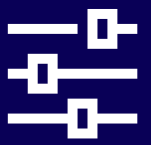
Интеграции с внешними системами

Отчёты и логирование действий

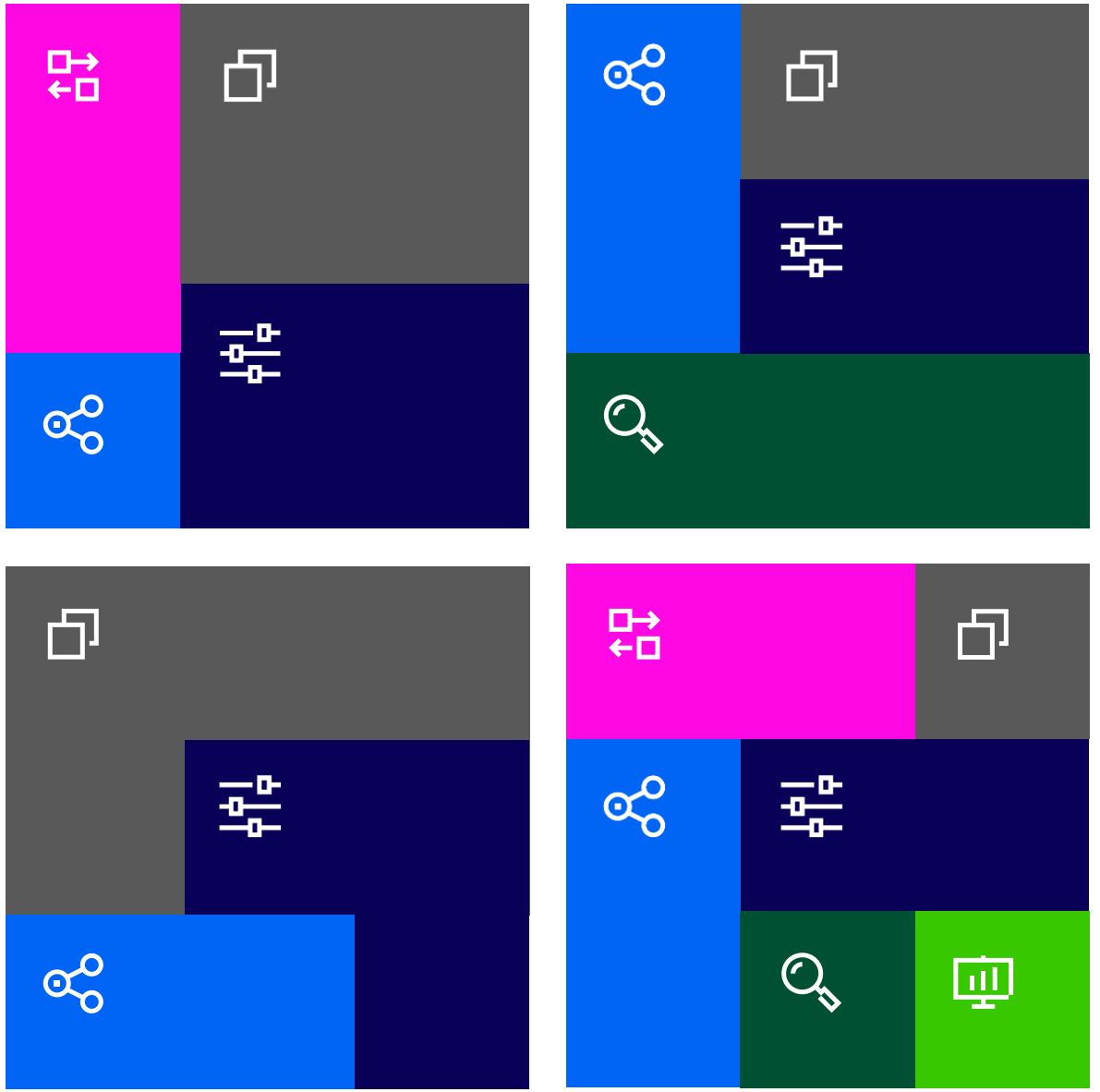
~ Word



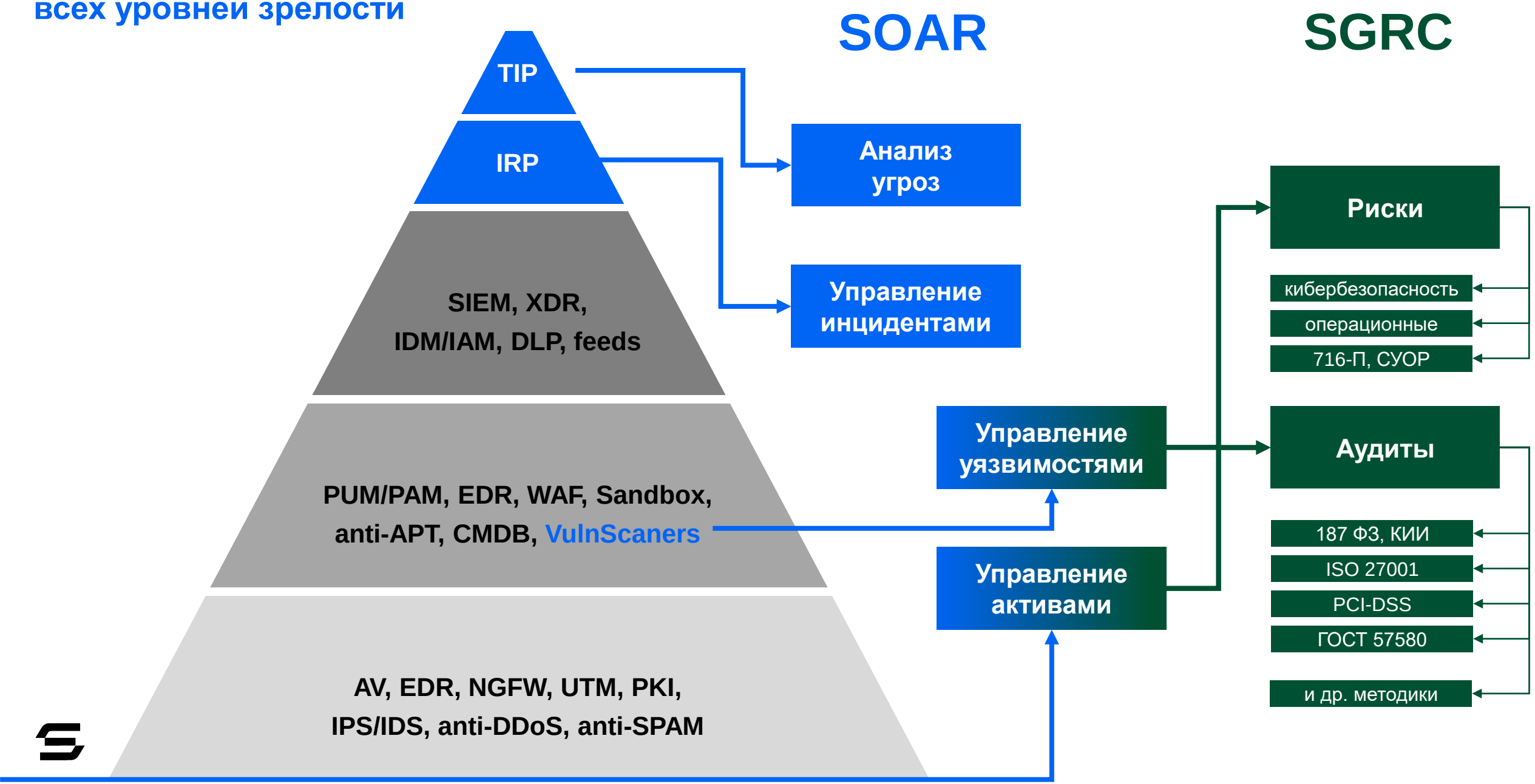
МОДУЛИ



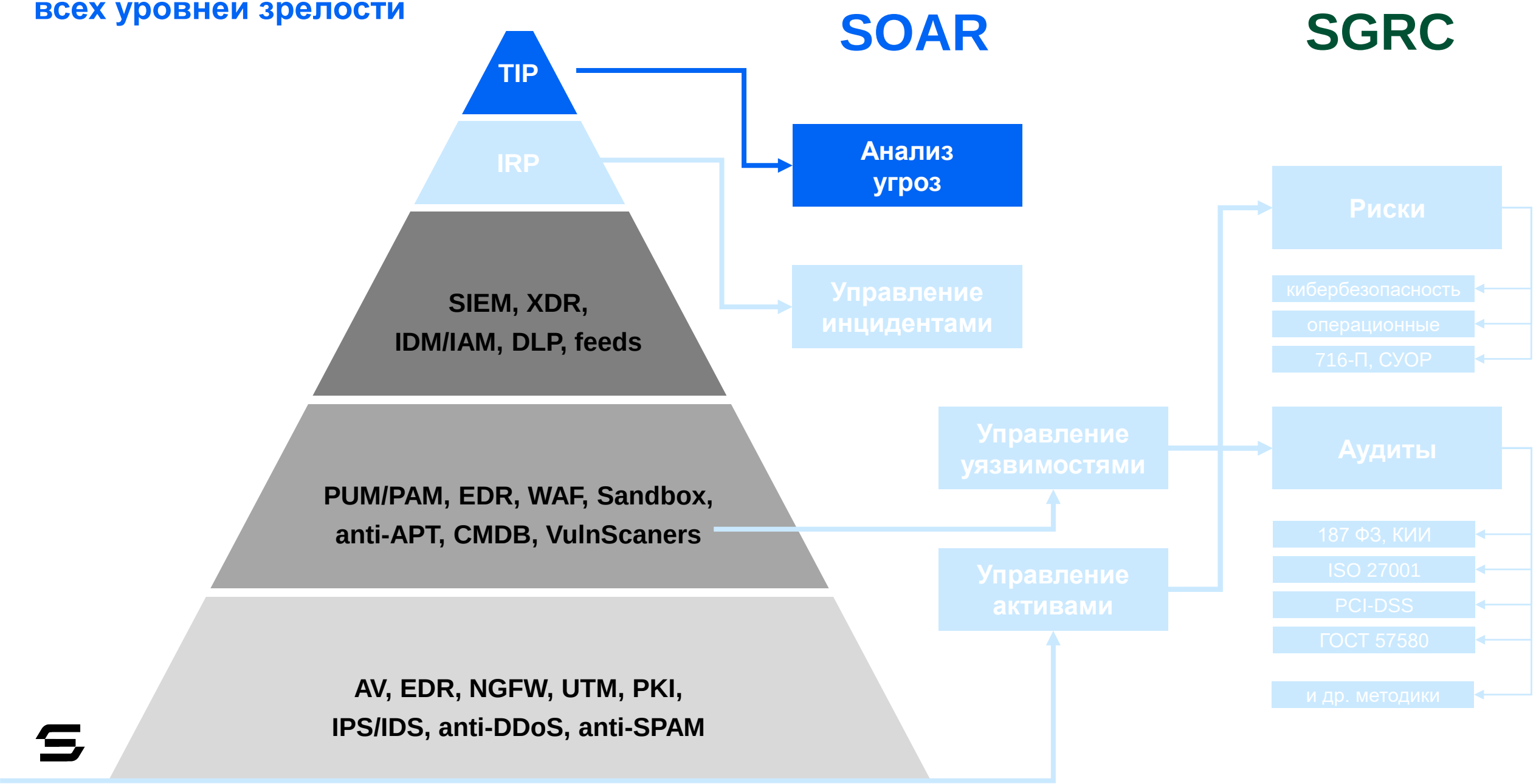
Собирайте модули под ваши задачи без навыков программирования с помощью гибких конструкторов



Решения SV для процессов всех уровней зрелости



Решения SV для процессов всех уровней зрелости



Анализ угроз, киберразведка

в Security Vision 5

1. Сбор событий
2. Обогащение
3. Обнаружение

Анализ угроз, киберразведка

в Security Vision 5

1

Загрузка данных

события, фиды, IoC, бюллетени, источники угроз

2

Работа с IoC

MITRE ATT&CK, OWASP, оптимизация параметров (IP, URL, Домен, Маска, Хэш)

Обнаружение

Ретроспективный поиск,Match, DGA: random, wordlist, фишинговые домены

3

- SIEM
- NGFW
- Proxy
- Servers
- Users

и др.

злоумышленники

ВПО

угрозы

уязвимости

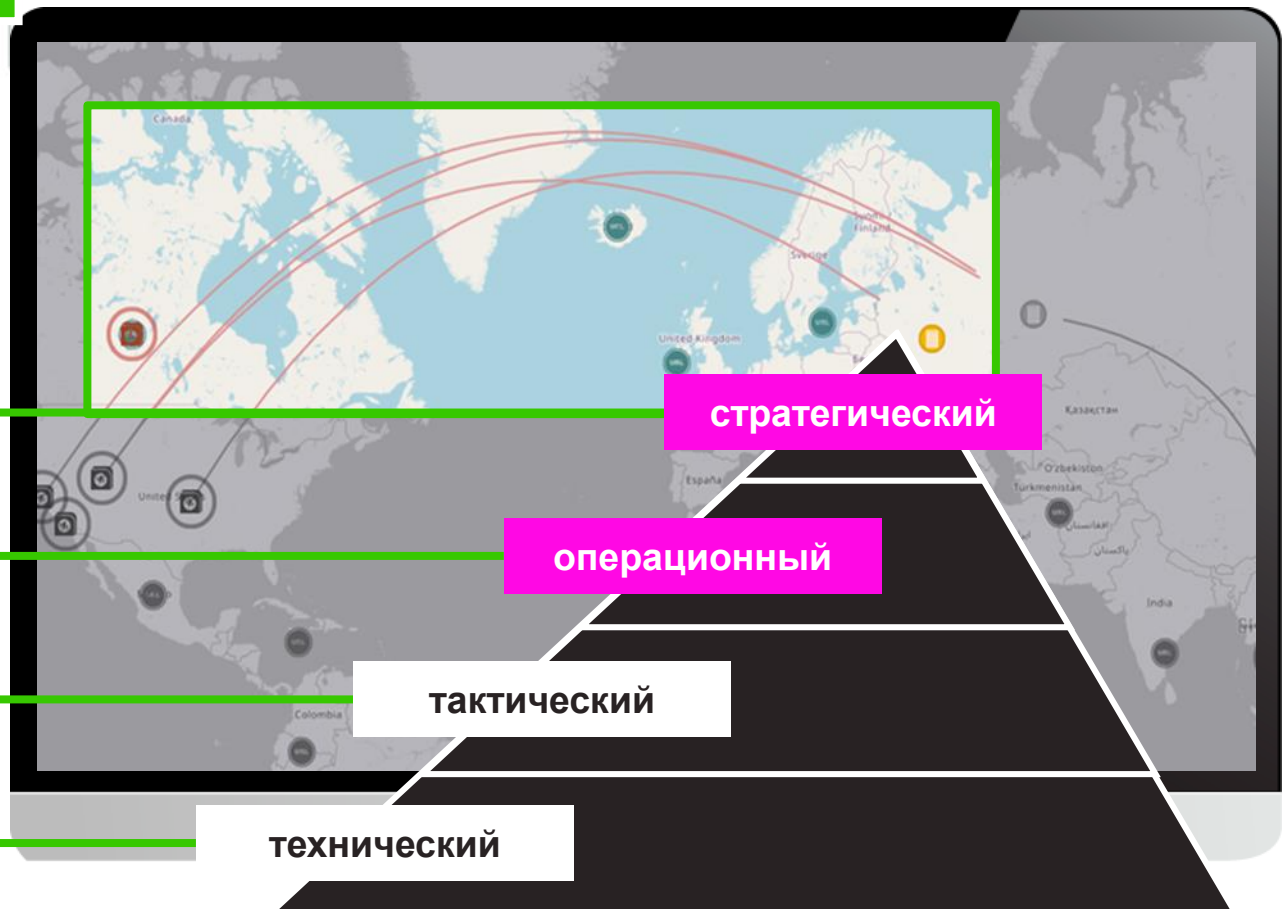
IoA

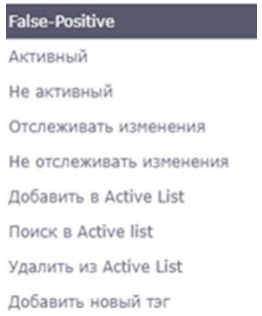
домены

URL

хэши

IP



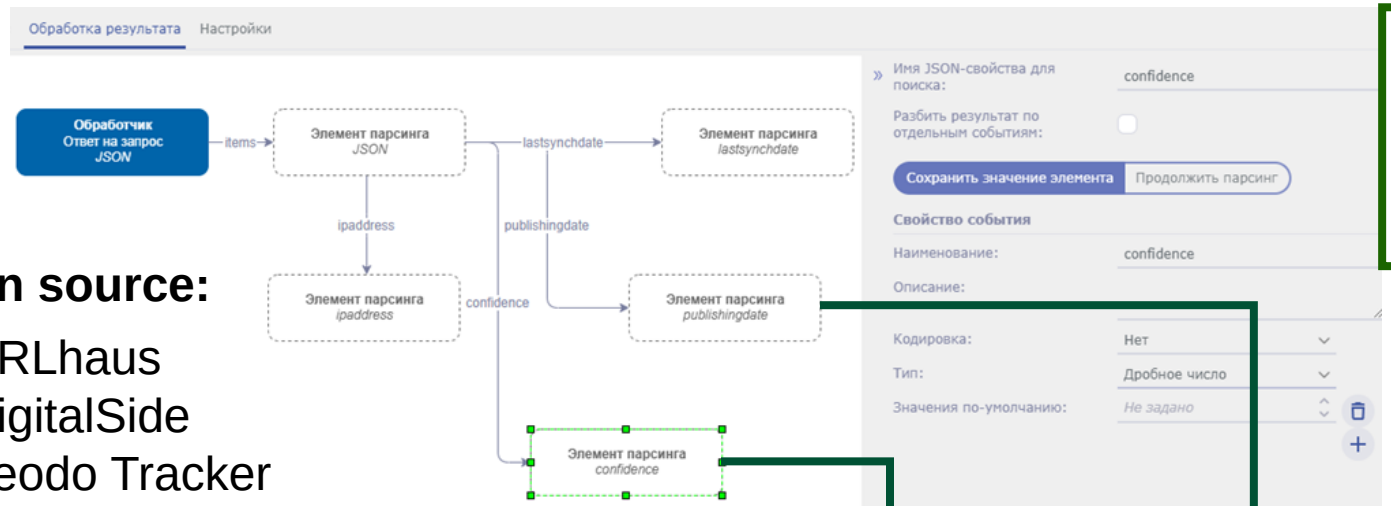


4

Реагирование

управление политиками в едином продукте

Анализ угроз, киберразведка



CSV, CEF, LEEF, STIX2, MISP

УНИВЕРСАЛЬНЫЕ ИНСТРУМЕНТЫ

Open source:

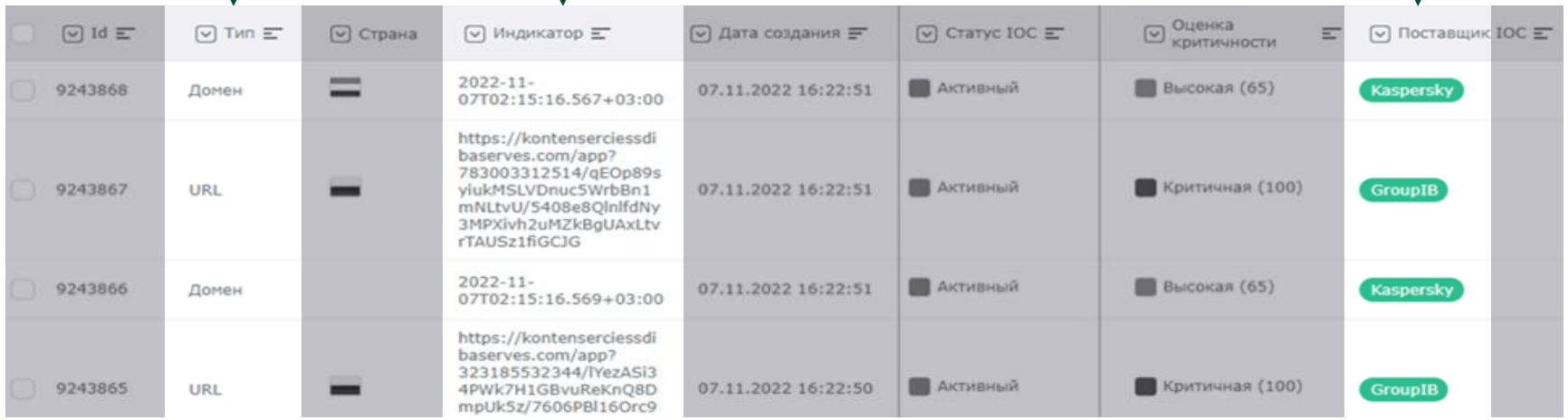
- URLhaus
- DigitalSide
- Feodo Tracker

Публичные поставщики:

- AlienVault
- MISP

Отечественные поставщики:

- RST Cloud
- BI.ZONE
- Group-IB
- Kaspersky



Id	Тип	Страна	Индикатор	Дата создания	Статус IOC	Оценка критичности	Поставщик IOC
9243868	Домен		2022-11-07T02:15:16.567+03:00	07.11.2022 16:22:51	Активный	Высокая (65)	Kaspersky
9243867	URL		https://kontenserciessdibaserves.com/app?783003312514/qEOp89syiukMSLVDnuc5WrbBn1mNLtvU/5408e8QlnIfdNy3MPXivh2uMZkBgUAxLtvrTAUSz1fiGCJG	07.11.2022 16:22:51	Активный	Критичная (100)	GroupIB
9243866	Домен		2022-11-07T02:15:16.569+03:00	07.11.2022 16:22:51	Активный	Высокая (65)	Kaspersky
9243865	URL		https://kontenserciessdibaserves.com/app?323185532344/lYezASi34PWk7H1GBvuReKnQ8DmpUk5z/7606PBl16Orc9	07.11.2022 16:22:50	Активный	Критичная (100)	GroupIB

Сбор индикаторов от поставщиков

Анализ угроз, киберразведка

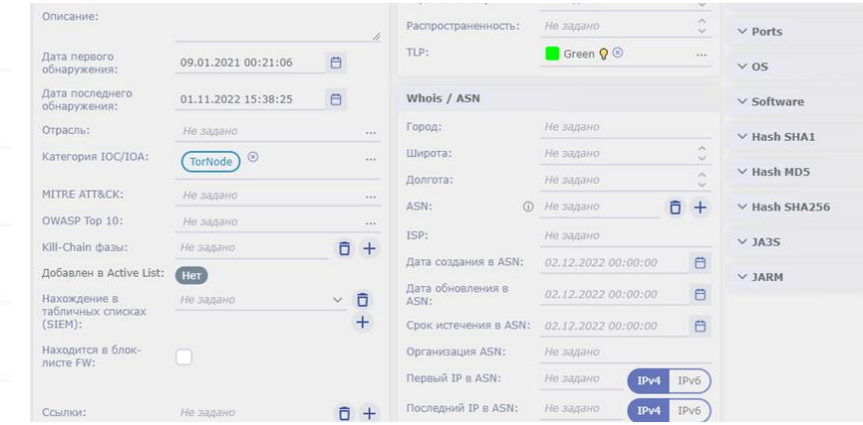
Настройки > Дополнительные > Время жизни IOC

Время участия в обнаружении и жизни внутри системы

Id	Тип IOC	Время активности IOC, дни	Время жизни IOC в системе, дни
1	IP	30	90
2	Домен	30	90
3	URL	30	90
4	Хэш		
5	Маска	30	90
6	Вредоносное ПО	180	180
7	Угроза	180	180
8	Злоумышленники	365	365

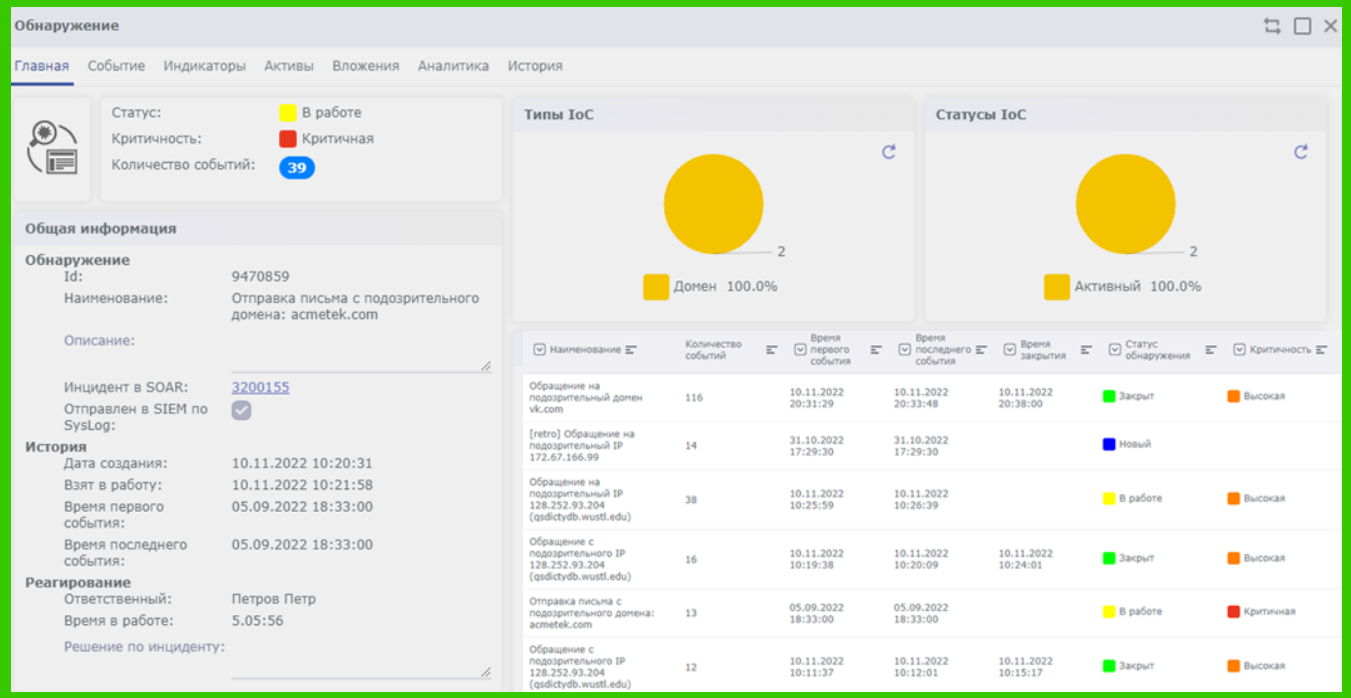
Группировка данных от всех поставщиков

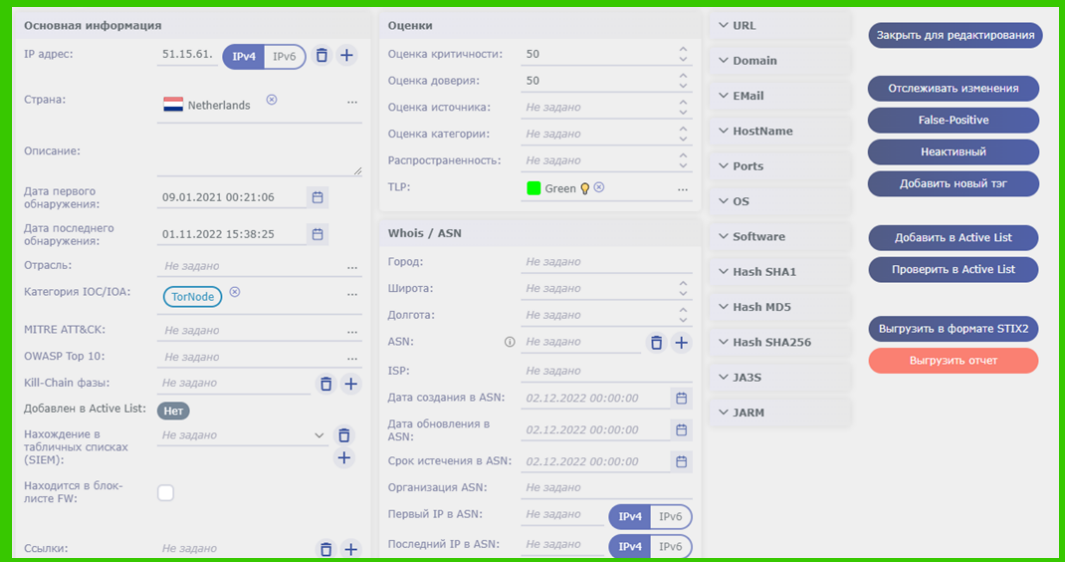
- False-Positive
- Активный
- Не активный
- Отслеживать изменения
- Не отслеживать изменения
- Добавить в Active List
- Поиск в Active list
- Удалить из Active List
- Добавить новый тэг

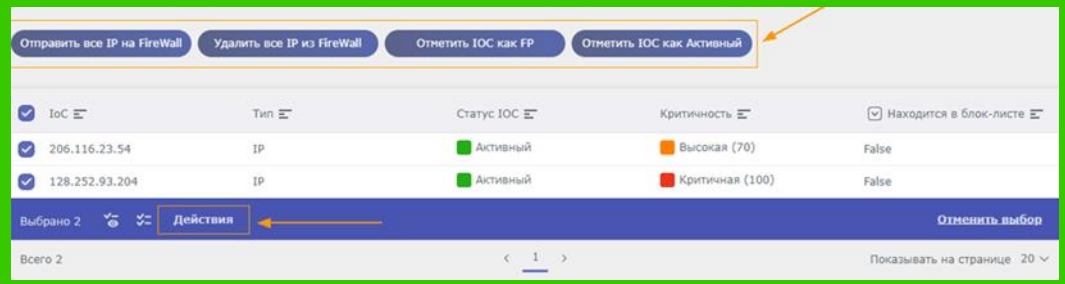


Только актуальные данные, меньше False Positive

Анализ угроз, киберразведка







Обнаружение внутри периметра

комбинирование обнаружения

RETRO
поиск по базе

MATCH
обработка на лету

время на обработку **200 000 событий**

45 сек	**45 сек**	**15 сек**
DGA – random	DGA – wordlist	phishing
случайные домены из набора букв	случайный набор слов и фразы	поиск доменов, схожих с известными
jnouayonvoquria.ru	crackquote-assistance.com	payplticket.info

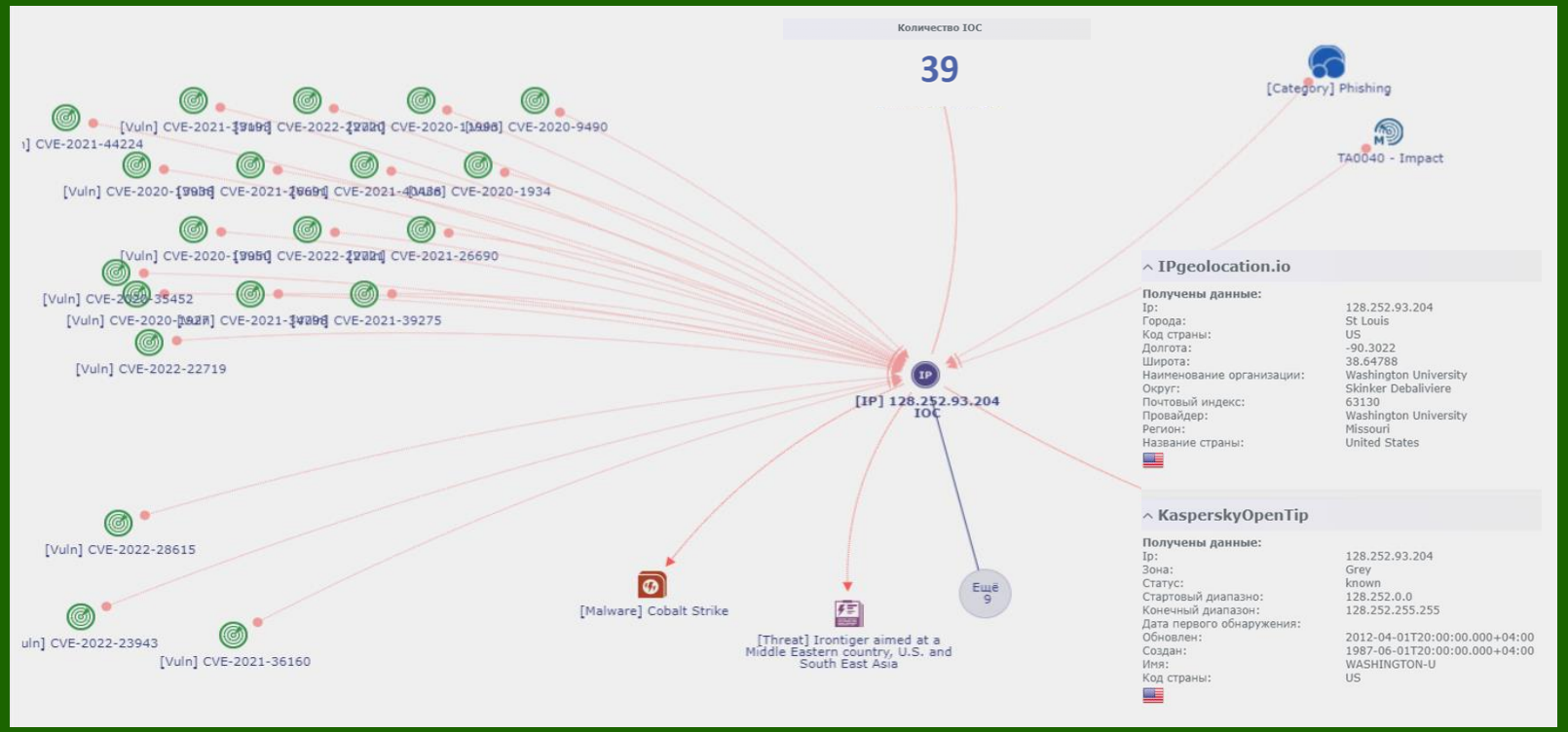
Машинное обучение
и пополняемая база

- IPgeolocation.io
- KasperskyOpenTip
- IPInfo.io
- MaxMind Geo-IP
- IPGeolocation (Whoisxmlapi)
- IPNet-blocks (Whoisxmlapi)
- VirusTotal
- Shodan

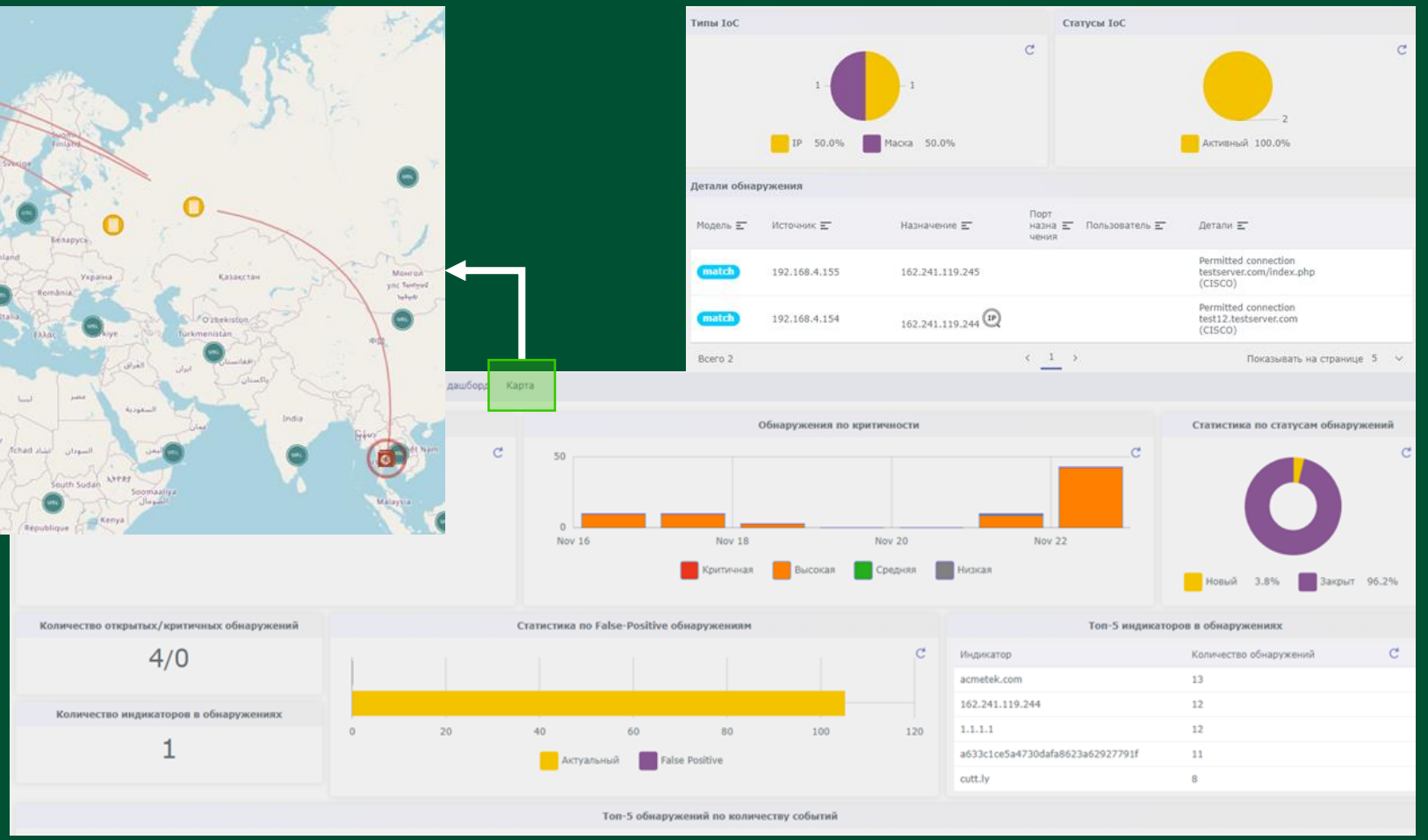
Стратегический уровень анализа

ВРЕДОНОСНОЕ ПО	ЗЛОУМЫШЛЕННИКИ

УЯЗВИМОСТИ	УГРОЗЫ	БЮЛЛЕТЕНИ



Анализ угроз, киберразведка



Полная картина для реагирования

Анализ угроз, киберразведка

в Security Vision 5

1 Сбор событий
Подключение к внутренним и внешним источникам данных

2 Обогащение
Коммерческие и open-source аналитические центры

3 Обнаружение
Поиск в реальном времени и базе событий с машинным обучением

Управление безопасностью и анализ угроз

на стыке технологий и решений ИБ/ИТ

Роман
Душков

пресейл менеджер

+7 995 880 40 63
rdushkov@securityvision.ru

sales@securityvision.ru

Security Vision

Интеллектуальная платформа информационной безопасности и ИТ

securityvision.ru