Управление ИБ и анализ угроз на стыке технологий и разных продуктов

Security Vision

ДиалогНаука

Роман Душков

Пресейл-менеджер

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

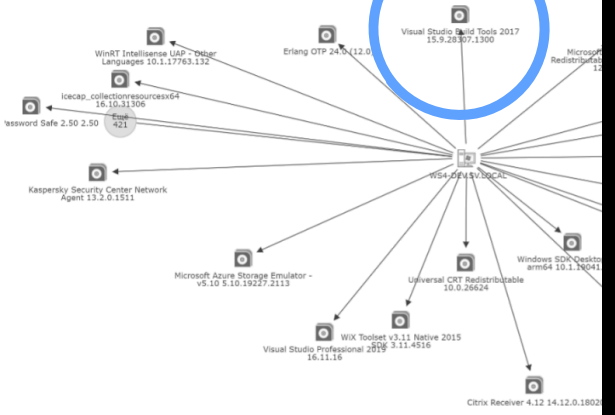
Управление разрозненными ИТ-системами

Управление активами

в Security Vision 5

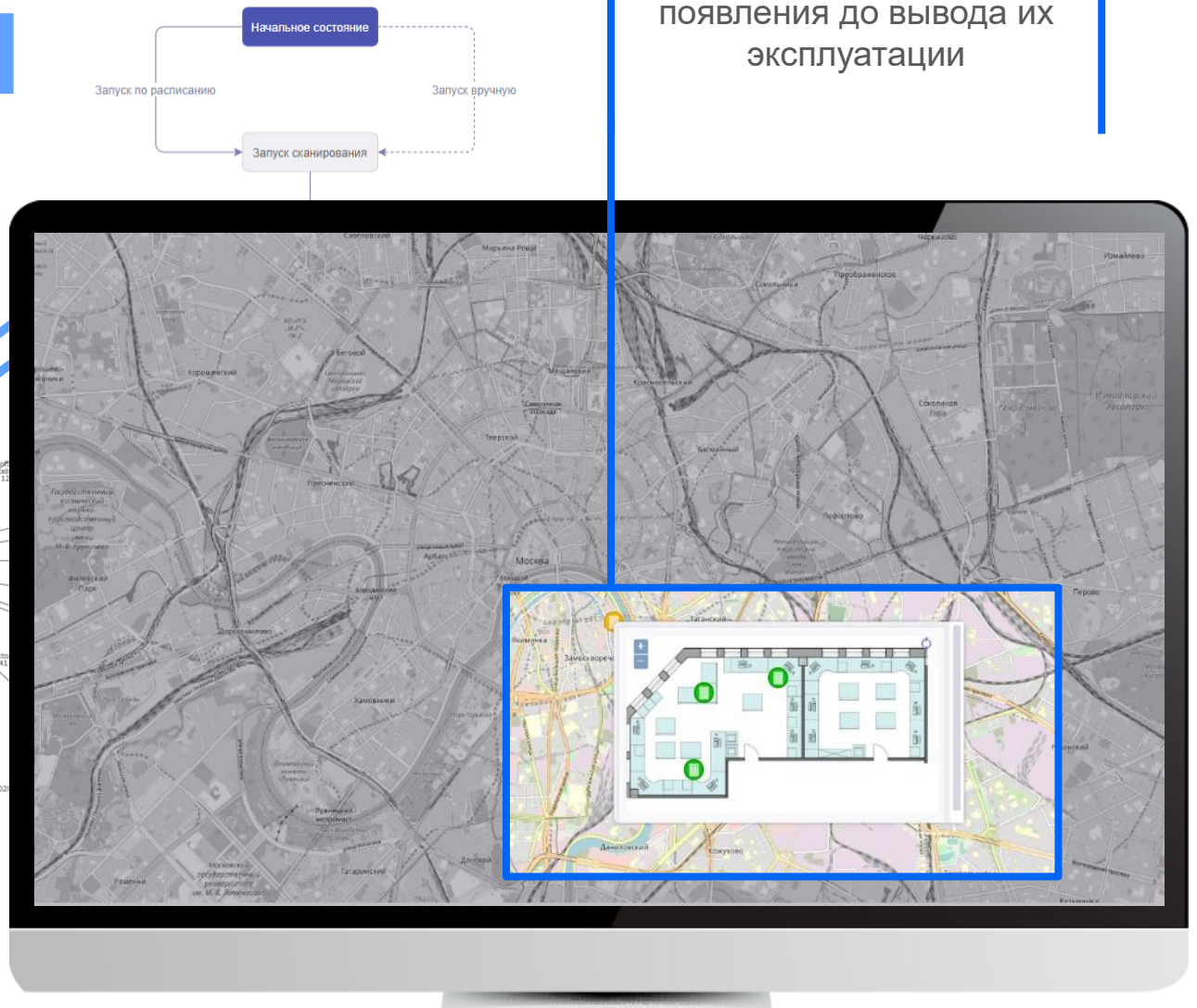
1 Поиск объектов

сканирование сети по расписанию, поиск нераспознанных объектов, фильтрация и drill-down



2 Жизненный цикл

фиксация изменений атрибутов ИТ-активов и организация процессов от появления до вывода их эксплуатации



3 Обогащение

сбор информации о ПО, УЗП, состоянии СЗИ, обновлениях и т.д. из разных систем, БД и файлов

Статус жизненного цикла актива	Операционная система	Источник данных об активе
В эксплуатации	Linux Kernel 2.6	MaxPatrol SIEM; KUMA SIEM
В эксплуатации	CentOS Linux 7	KUMA SIEM
В эксплуатации	CISCO IOSCisco	MaxPatrol SIEM; KUMA SIEM
В эксплуатации	<Microsoft Windows>	KUMA SIEM; MaxPatrol SIEM; Kaspersky Security Center
На категорировании	Windows 10 Pro	KUMA SIEM; MaxPatrol SIEM; IBM QRadar; Active Directory; Kaspersky Security Center; MS WSUS
На категорировании	Windows 10 Pro	IBM QRadar; KUMA SIEM; MaxPatrol SIEM; Active Directory; Kaspersky Security Center; MS WSUS

Управление активами

в Security Vision 5

1 **Обнаружение объектов**
активный безагентский поиск
по расписанию

2 **Жизненный цикл**
актуализация состояния
оборудования и состава ИС

3 **Обогащение данными**
единые интерфейс, СУБД и
ретроспективный поиск

СКАНИРОВАНИЕ СЕТИ

ОБНОВЛЕНИЕ ПО

БЕЛЫЙ СПИСОК ПО

СОФТ

ИНВЕНТАРИЗАЦИЯ

ЖЕЛЕЗО

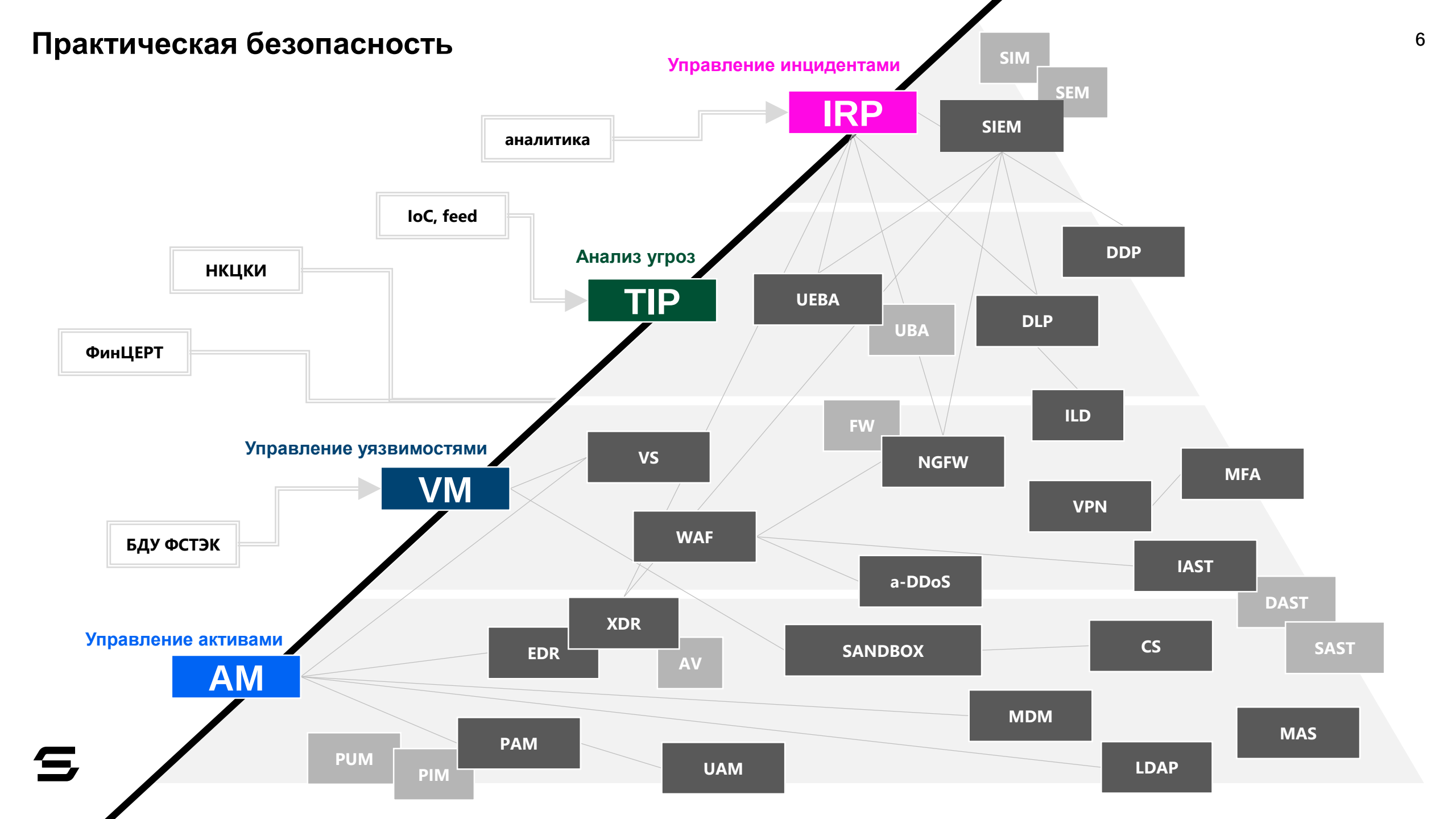
ПОЛЬЗОВАТЕЛИ

ОТЧЕТЫ

ВНЕШНИЕ СИСТЕМЫ

ТАБЛИЦЫ

Практическая безопасность



Управление инцидентами

1 Анализ письма

выделение темы, содержимого, текста и ссылок

15 мин

2 Поиск деталей

проверка отправителя, домена, вложений и ссылок

25 мин

3 Поиск похожих

поиск других получателей

10 мин

4 Блокировка

добавление отправителя и домена в чёрный список

10 мин

5 Очистка сервера

от опасных писем или вложений

10 мин

6 Оповещение пользователя

запуск проверки на рабочих станциях пользователей

5 мин

75 минут без SOAR

Управление инцидентами с автоматизацией

HYBRID ANALYSIS · urlscan.io · WhoisXML API · ThreatCrowd · MaxPatrol SIEM · kaspersky · Exchange

1

- **Анализ письма** — выделение темы, содержимого, текста и ссылок
- **Поиск деталей** — проверка отправителя, домена, вложений и ссылок
- **Поиск похожих** — поиск других получателей
- **Блокировка** — добавление отправителя и домена в чёрный список
- **Очистка сервера** — от опасных писем или вложений

4 мин

2

- **Оповещение пользователя** — запуск проверки на рабочих станциях пользователей

1 мин

5 минут с SOAR

Управление инцидентами

интернет, DMZ | периметр компании

сервисы обогащения

IP

URL

Email адрес

Хэш файлов

Best-practices

обнаружение

ЛЮБЫЕ СЗИ

FW, NGFW, Proxy, Email, DLP,

AV, EDR, XDR, Sandbox и др.

корреляция

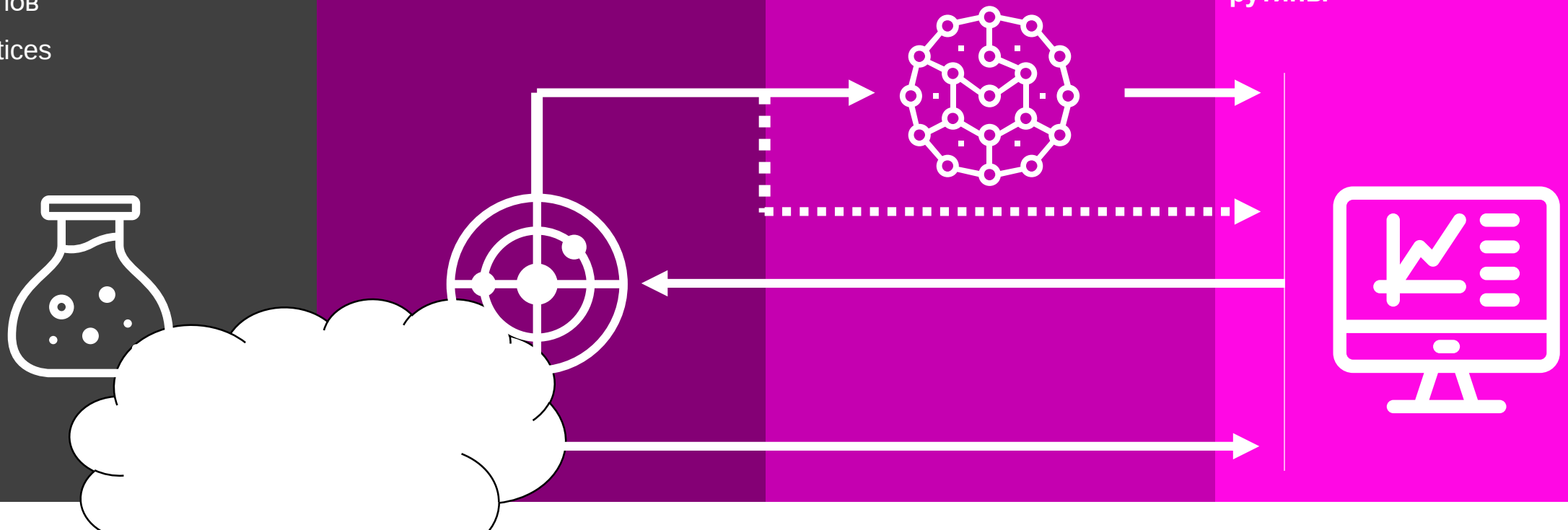
SV TIP

и/или SIEM, UBA/UEBA, ILD

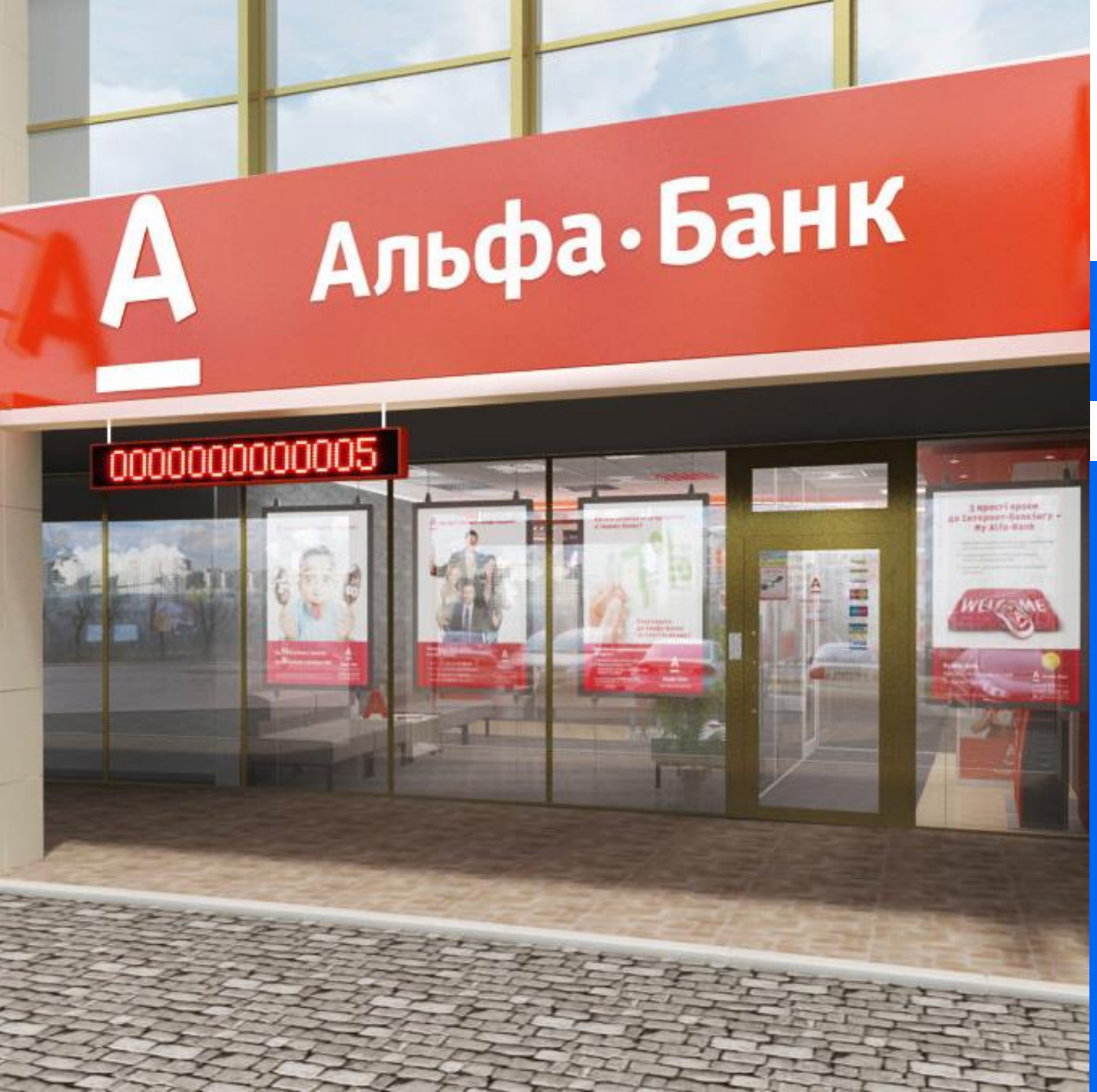
SV IRP

РЕАГИРОВАНИЕ

Жизненный цикл инцидентов, SLA и распределение задач, аналитика и автоматизация рутины



Создание экосистемы ИБ и ИТ



ИНТЕГРАЦИЯ И РОБОТИЗАЦИЯ

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

Управление инцидентами

в Security Vision 5

1

Сбор данных

Интеграция с СЗИ, группировка событий и дедупликация

2

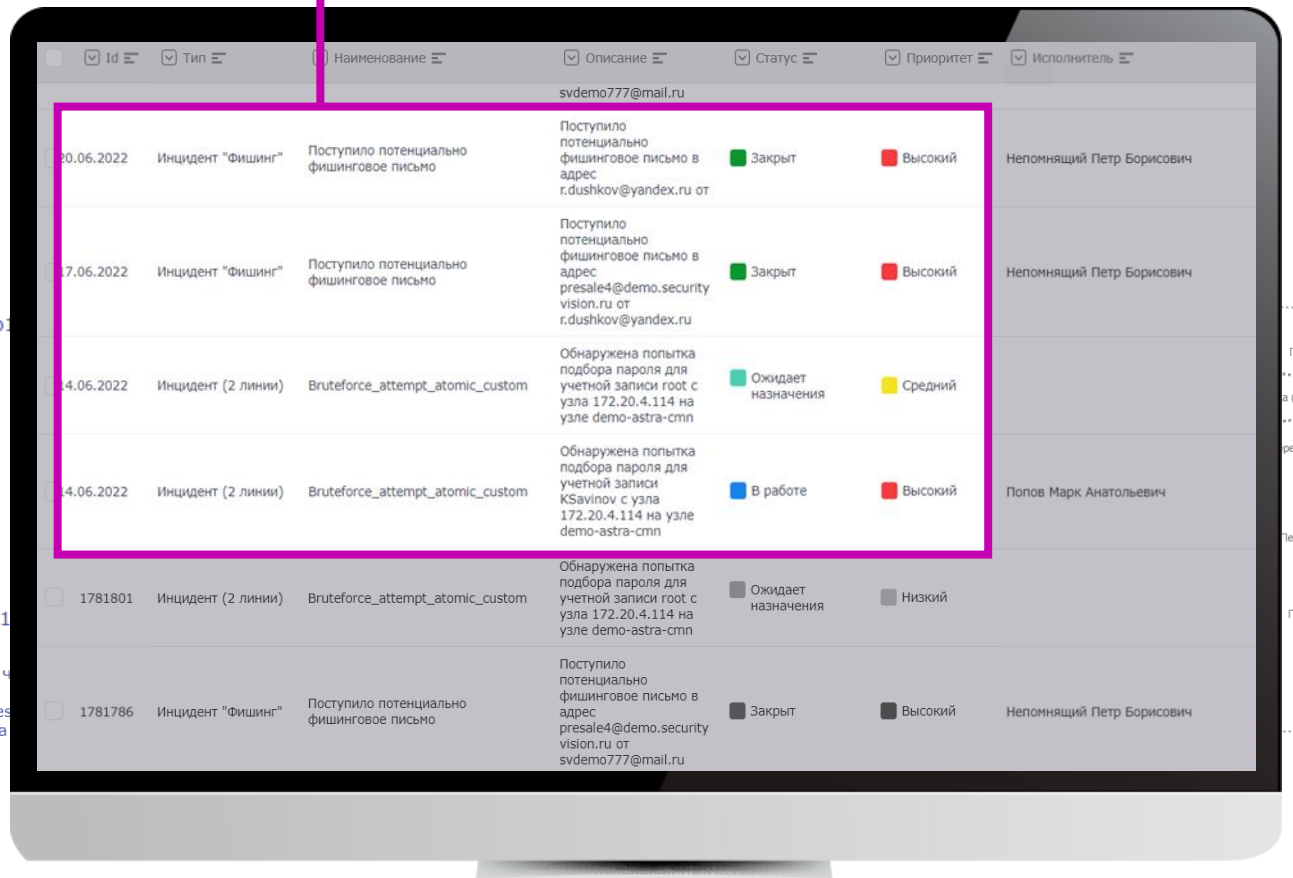
Тикетинг

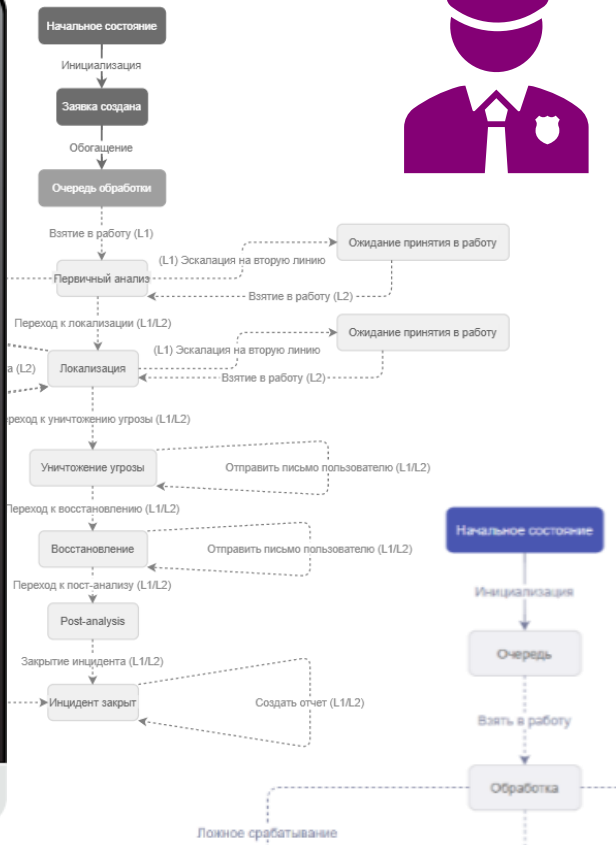
Передача в группу реагирования, обогащение данными из других систем

3

Реагирование

Управление СЗИ из единого окна,
SLA, формирование процессов





Управление инцидентами

в Security Vision 5

1 **Сбор инцидентов**
Подключение к различным СЗИ и ИТ-системам, шине данных

2 **Ведение задач**
Тикетинг с приоритезацией и чёткими процессами

3 **Реагирование**
Автоматизация и совместная работа всех уровней реагирования

ЗАДАЧИ

ОТВЕТСТВЕННЫЕ

SLA

СБОР

РЕАГИРОВАНИЕ

ИНЦИДЕНТЫ

ПРИОРИТЕТ

ОРКЕСТРАЦИЯ

АВТОМАТИЗАЦИЯ

УПРАВЛЕНИЕ

ЕДИНАЯ КОНСОЛЬ

ЧЕРКИЗОВО
С 1974

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- Территориально распределённая ГК
- Интеграция с коммерческим SOC – «Solar JSOC»

ЕВРАЗ

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

- Управление заявками ИБ как в инцидентах IT
- Реализация процесса управления уязвимостями

Управление уязвимостями

в Security Vision 5

1

Анализ отчёта

запуск по расписанию и организация полного жизненного цикла

2

Обогащение

дополнение информацией из БД по CVE (ФСТЭК, NVD NIST, Microsoft)

(Vulners)

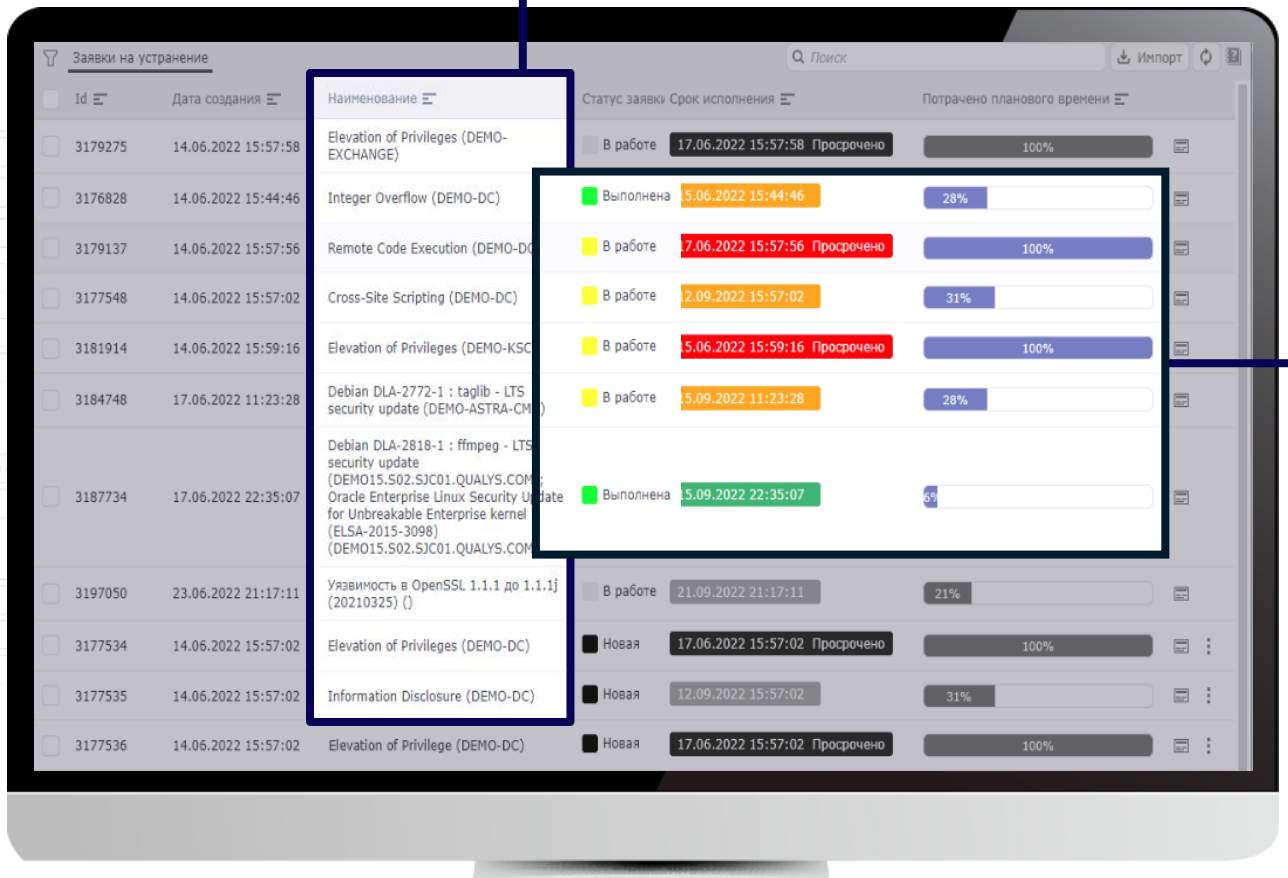
(OpenCVE)

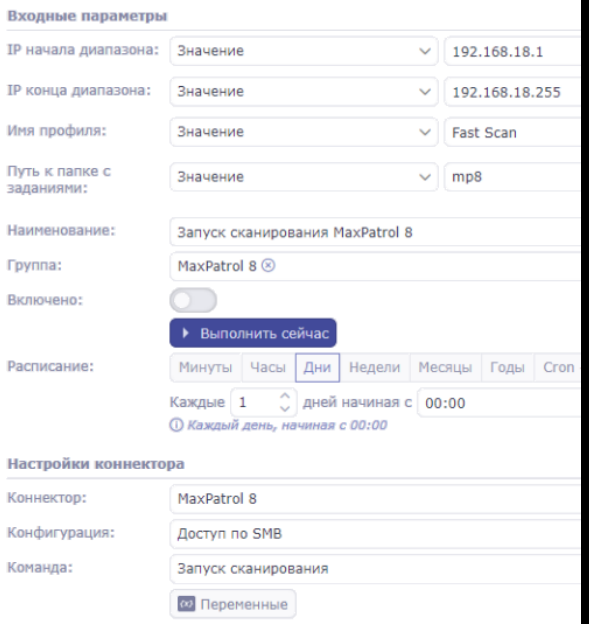
(NVD by NIST)

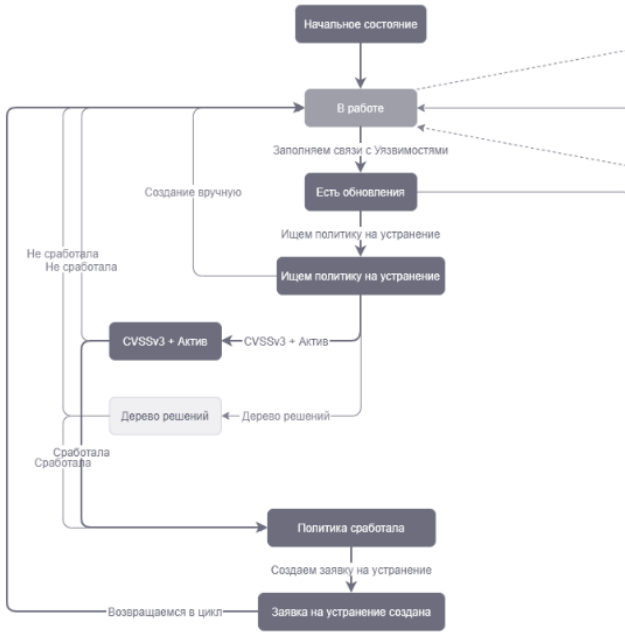
(AttackerKB)

Данные

Наименование:	CVE-2019-10072
Дата публикации:	21.06.2019 18:15:00
Дата проверки:	24.07.2020 00:12:06







3

Устранение

создание заявок с учетом критичности даже, связь с существующими активами и синхронизация между различными системами тикетинга (ITSM)

Управление уязвимостями

в Security Vision 5

1 **Анализ уязвимостей**
автоматический запуск сканеров и анализ отчётов любых объёмов

2 **Обогащение экспертизой**
внешние источники и рекомендации по повышению уровня защищенности

3 **Устранение уязвимостей**
выстраивание общего процесса для специалистов ИТ и ИБ

УСТРАНЕНИЕ

ЗАДАЧИ

ОТЧЕТЫ

SLA

ЗАПУСК СКАНЕРОВ

РАСПИСАНИЕ

БДУ ФСТЭК

VulDB.com

ОБОГАЩЕНИЕ

Vulners.com

OpenCVE.io

AttackersKB.com

NVD NIST

Северсталь

АНАЛИЗ УГРОЗ, КИБЕРРАЗВЕДКА

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

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)

3

Обнаружение

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

- SIEM
- NGFW
- Proxy
- Servers
- Users

и др.

злоумышленники

ВПО

угрозы

уязвимости

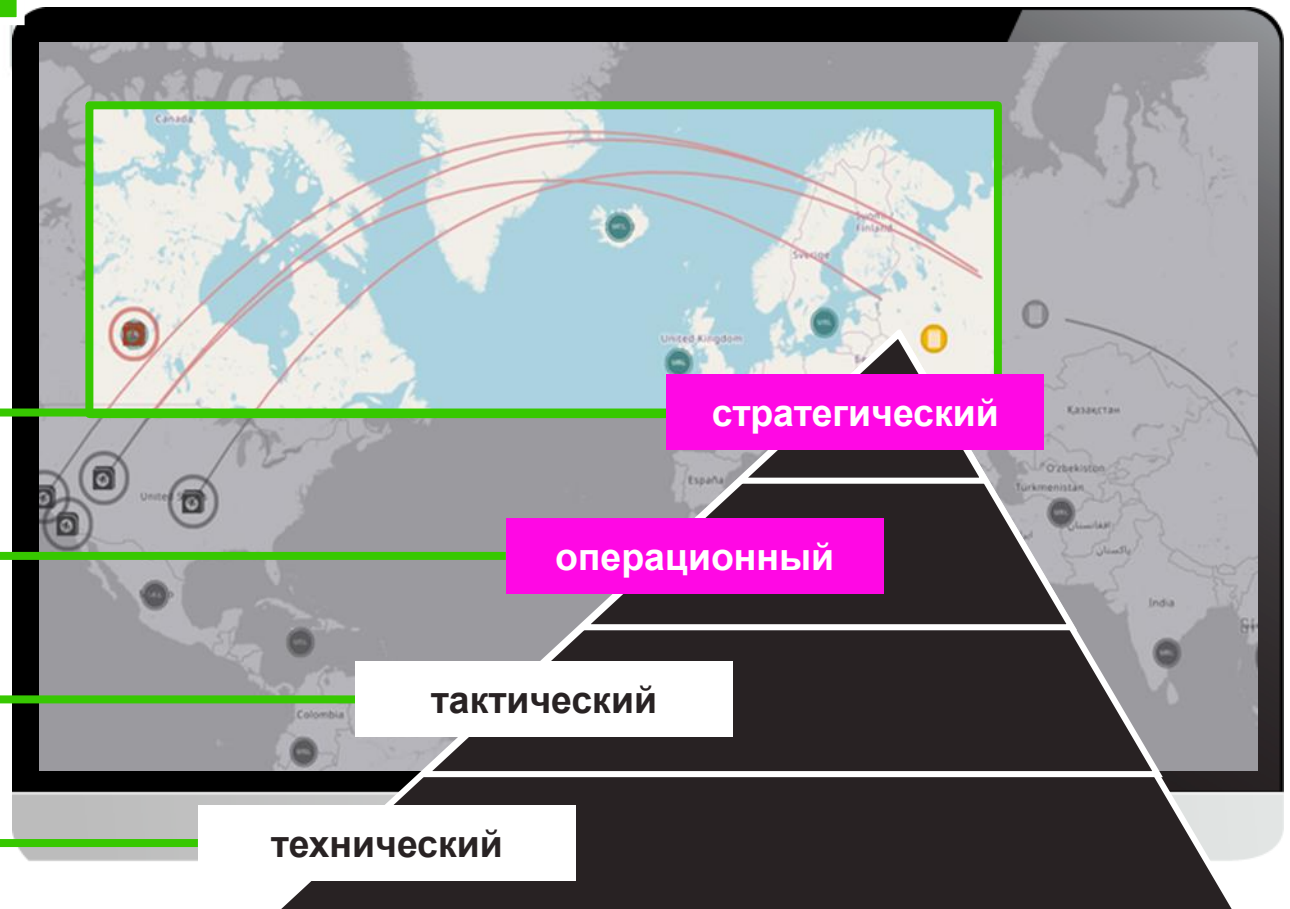
IoA

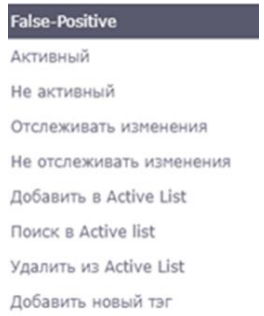
домены

URL

хэши

IP



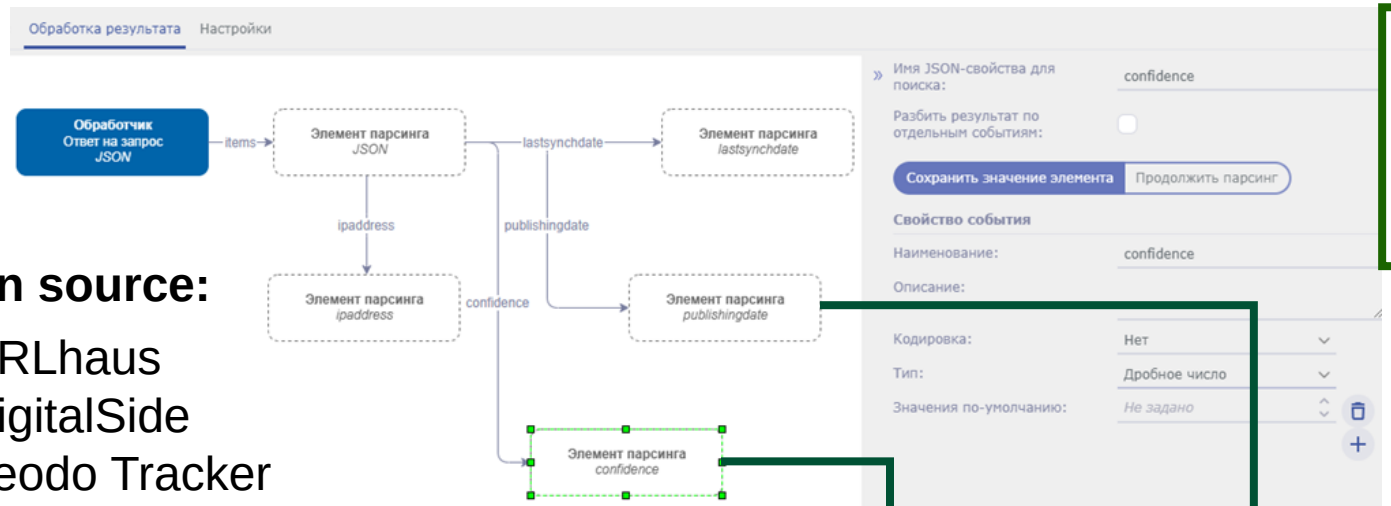


4

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

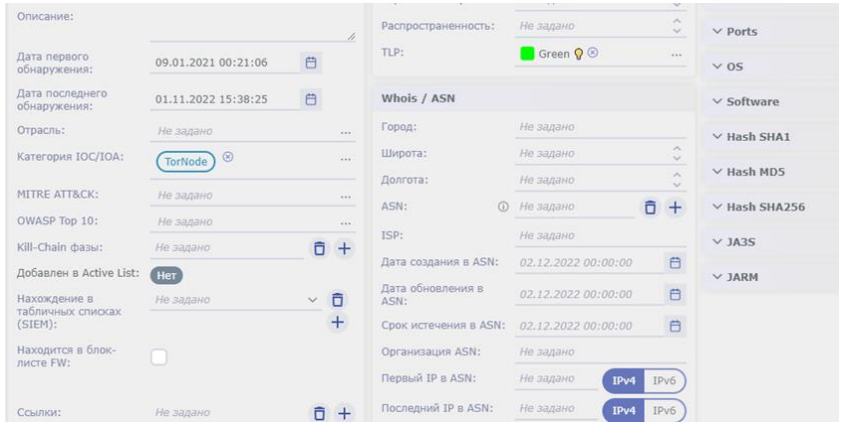
Настройки > Дополнительные > Время жизни IOC

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

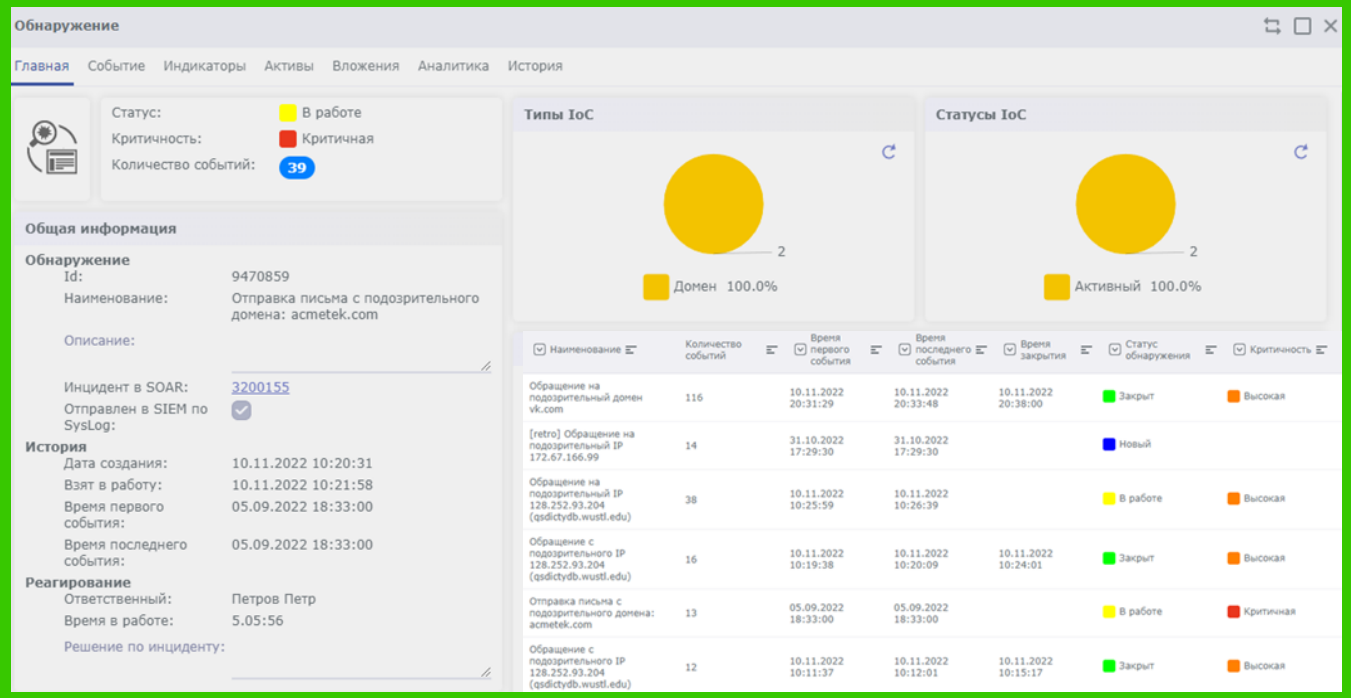
Группировка данных от всех поставщиков

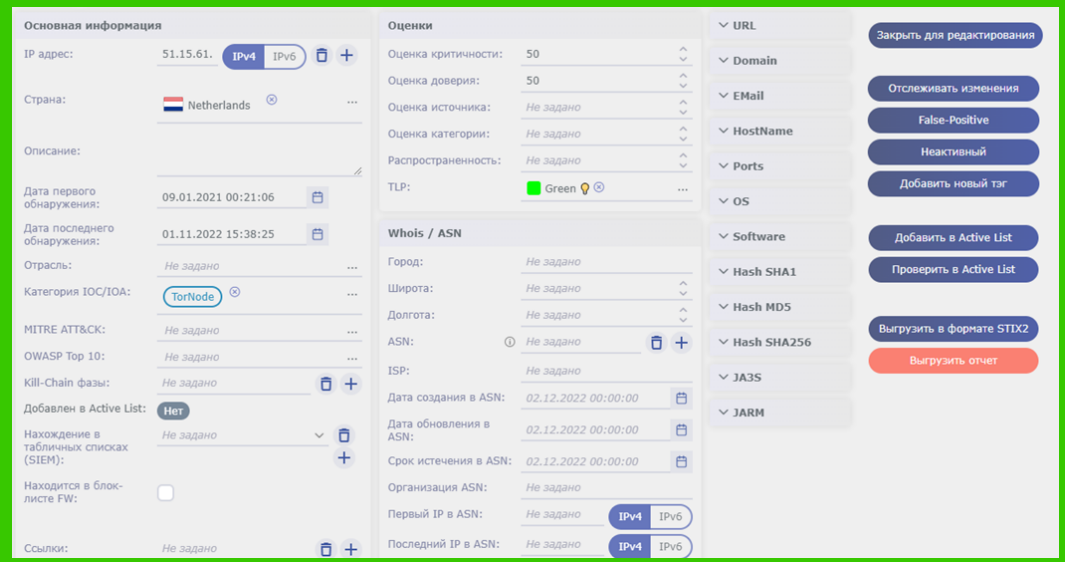
- False-Positive
- Активный
- Не активный
- Отслеживать изменения
- Не отслеживать изменения
- Добавить в Active List
- Поиск в Active list
- Удалить из Active List
- Добавить новый тэг

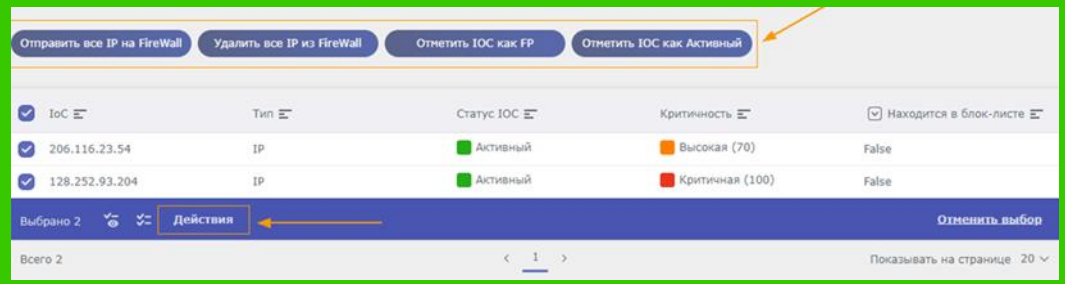


Только актуальные данные, меньше False Positive

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

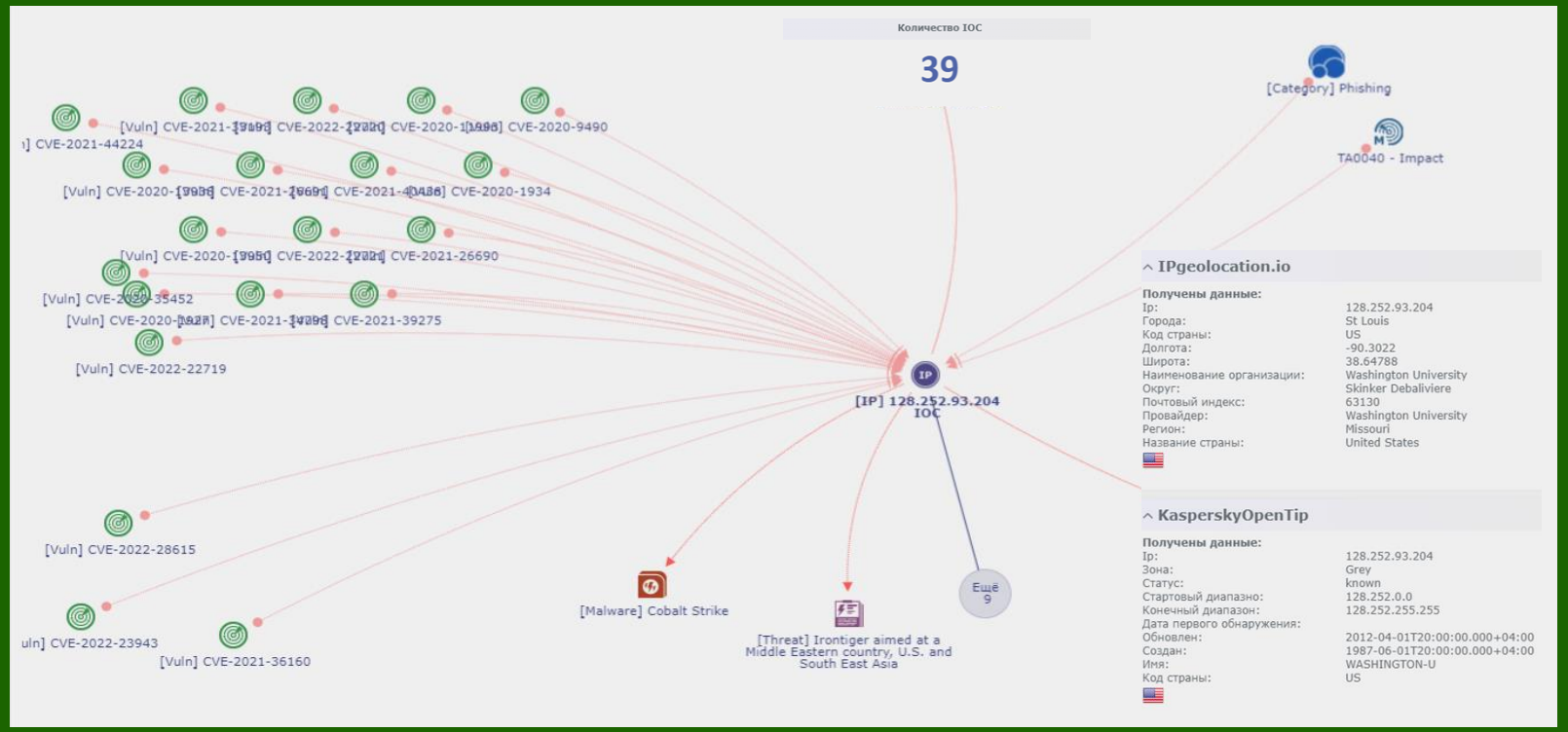
Машинное обучение
и пополняемая база

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

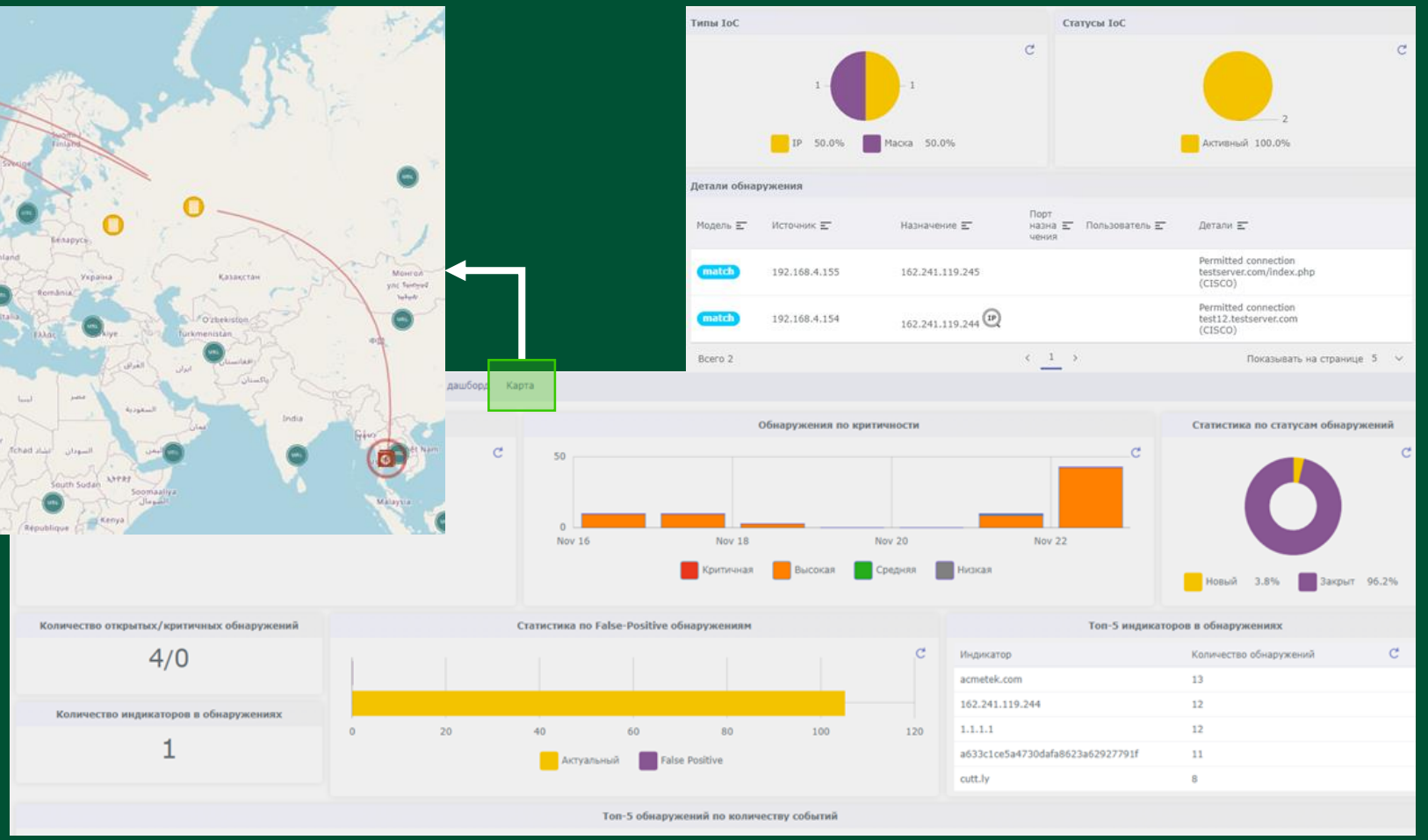
Стратегический уровень анализа

ВРЕДОНОСНОЕ ПО	ЗЛОУМЫШЛЕННИКИ

УЯЗВИМОСТИ	УГРОЗЫ	БЮЛЛЕТЕНИ

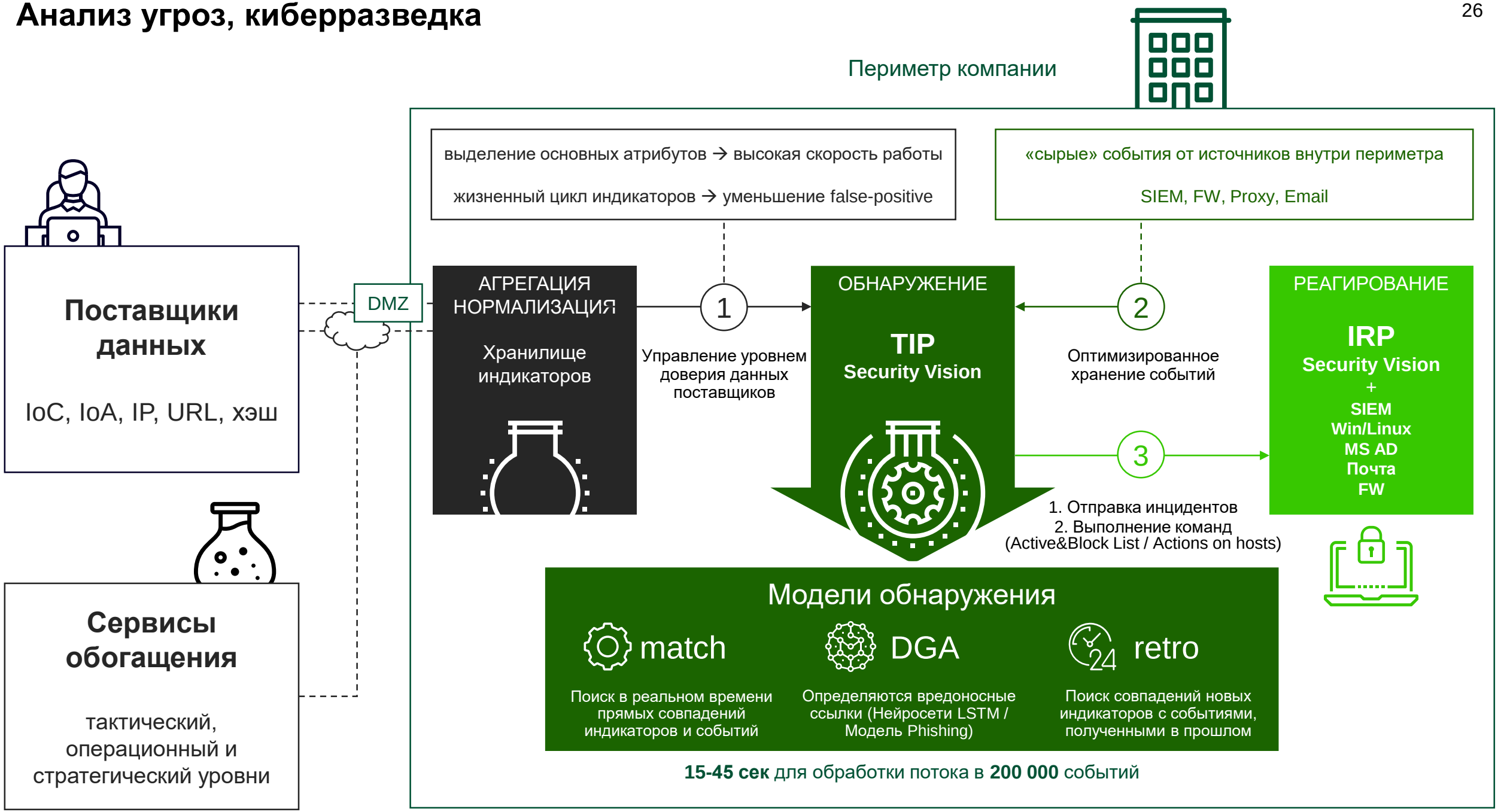


Анализ угроз, киберразведка



Полная картина для реагирования

Анализ угроз, киберразведка



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

Создание своего контента

ПОЧТА РОССИИ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 15+ плейбуков и процесс управления уязвимостями
- Управление внутренними проектами подразделения ИБ

СБЕР

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 100+ сотрудников команды SOC+IRP
- Разработка плейбуков, управление проблемами и др.
- 50+ интеграций с ИТ и ИБ системами

открытие

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- 30+ автоматизированных плейбуков и 50+ интеграций
- Проектная реализация процесса управление ИТ-активами
- Интеграция с Data Lake и использование ML модели

Единая гибкая платформа

~ CRM

~ BPM

Объекты, карточки и внешний вид

Ролевая модель и настройка меню

~ BI

Рабочие процессы и структура

Security Vision

Визуализация и аналитика

~ Word

~ RPA

Интеграции с внешними системами

Отчёты и логирование действий

Единая гибкая платформа

~ CRM

Объекты, карточки и внешний вид

Ролевая модель и настройка меню

~ BI

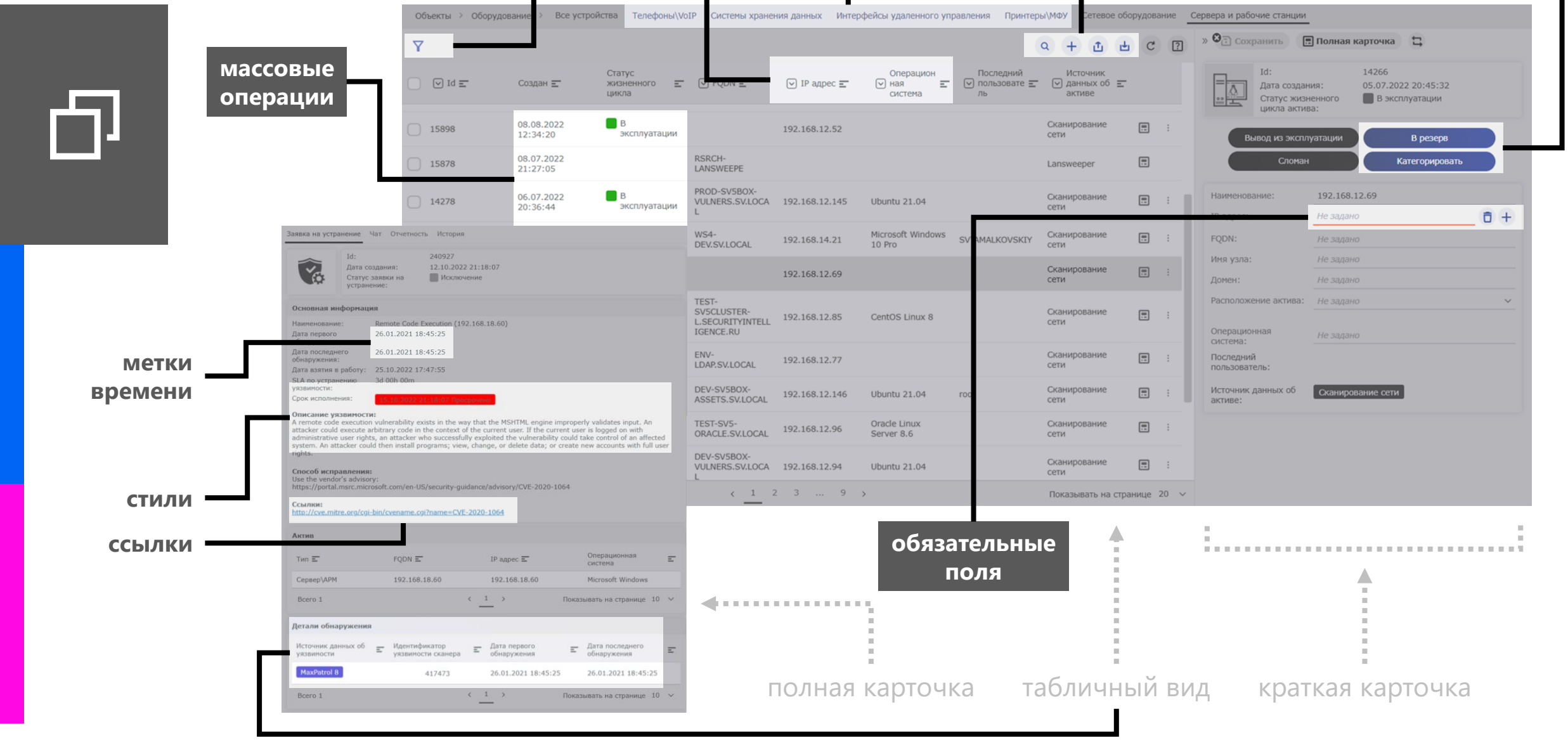
Security Vision

Визуализация и аналитика

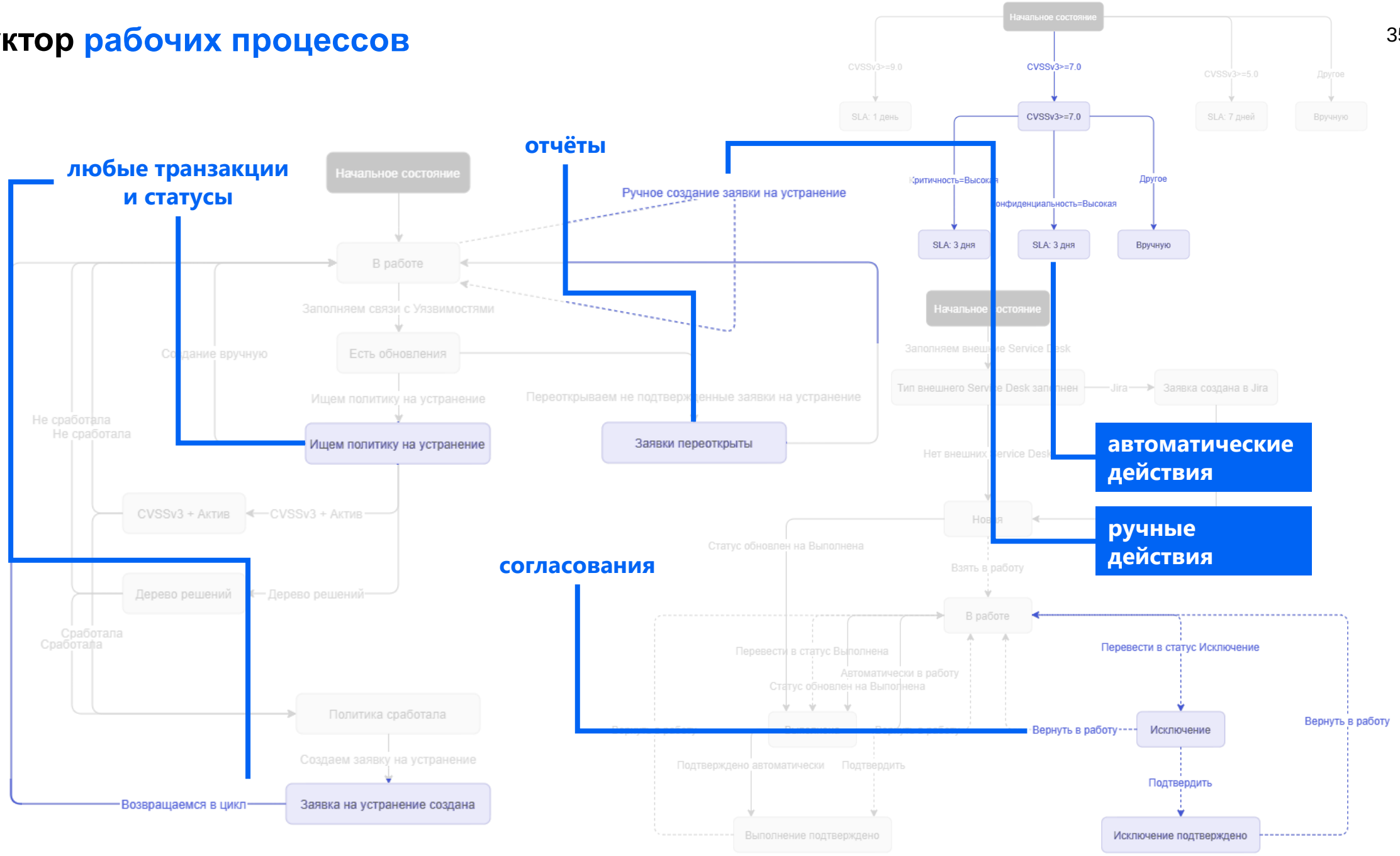
Отчёты и логирование действий

~ Word

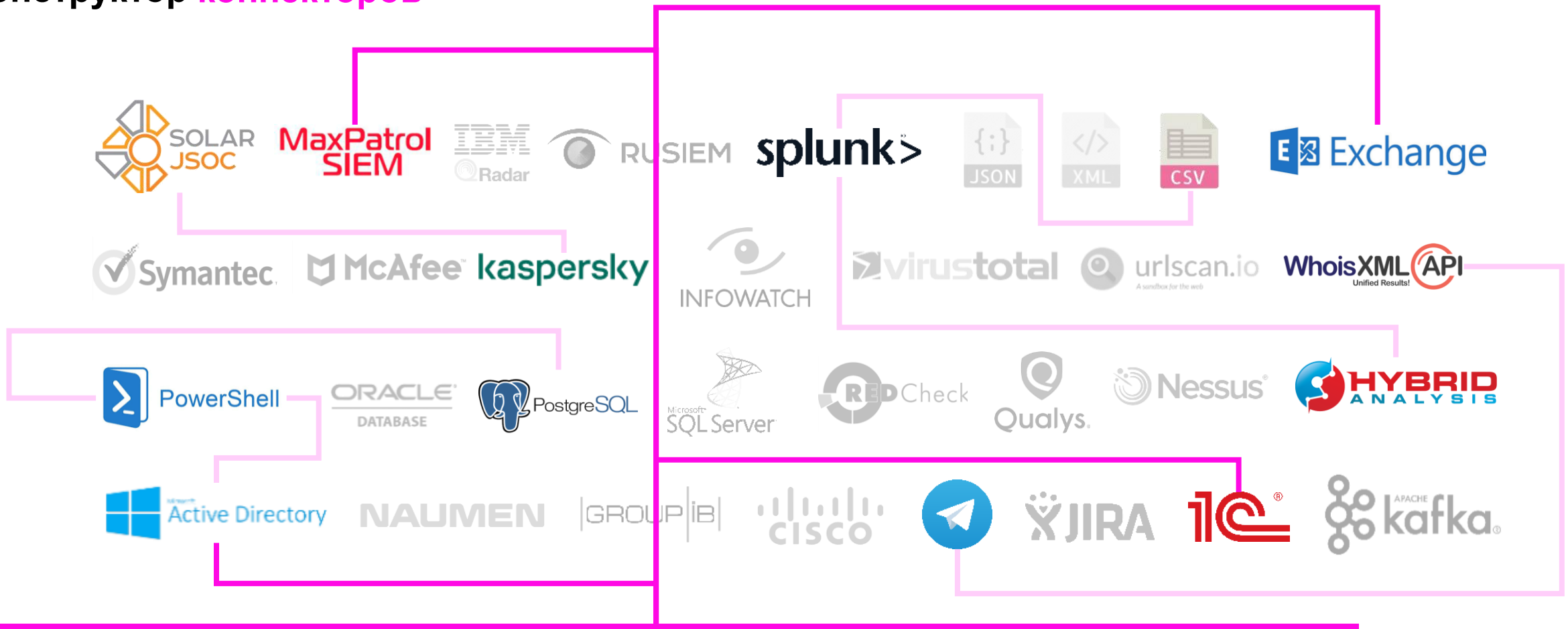
Конструктор объектов



Конструктор рабочих процессов



Конструктор коннекторов



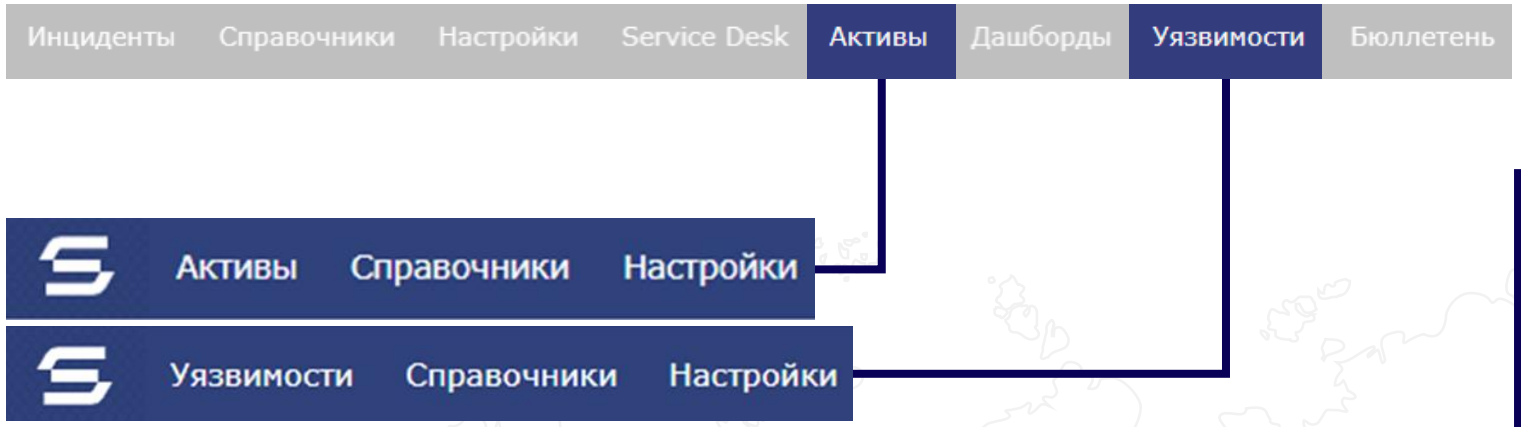
email | Syslog | файлы | БД | API | DNS | SNMP | LDAP | SOAP | скрипты

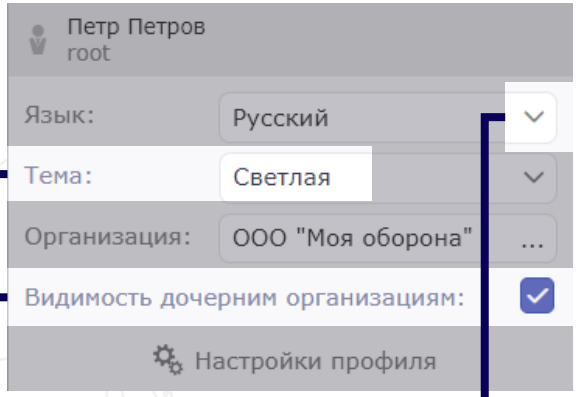
создание новых коннекторов **без участия вендоров**

Сбор и обогащение

Реагирование на события

Конструктор ролей и меню

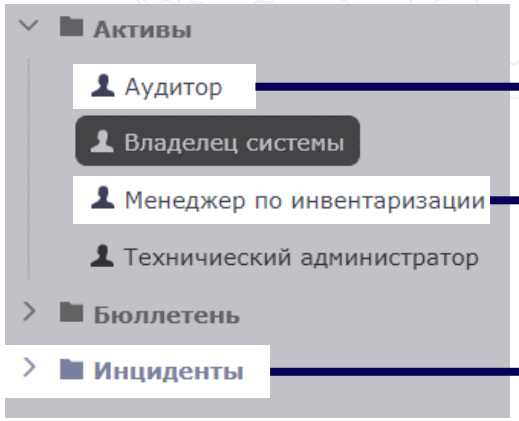




темы оформления

multitenancy

мультиязычность



персональная витрина

гранулярные настройки

ЧТЕНИЕ

ВКЛАДКИ МЕНЮ

РЕДАКТИРОВАНИЕ

АДМИНИСТРИРОВАНИЕ

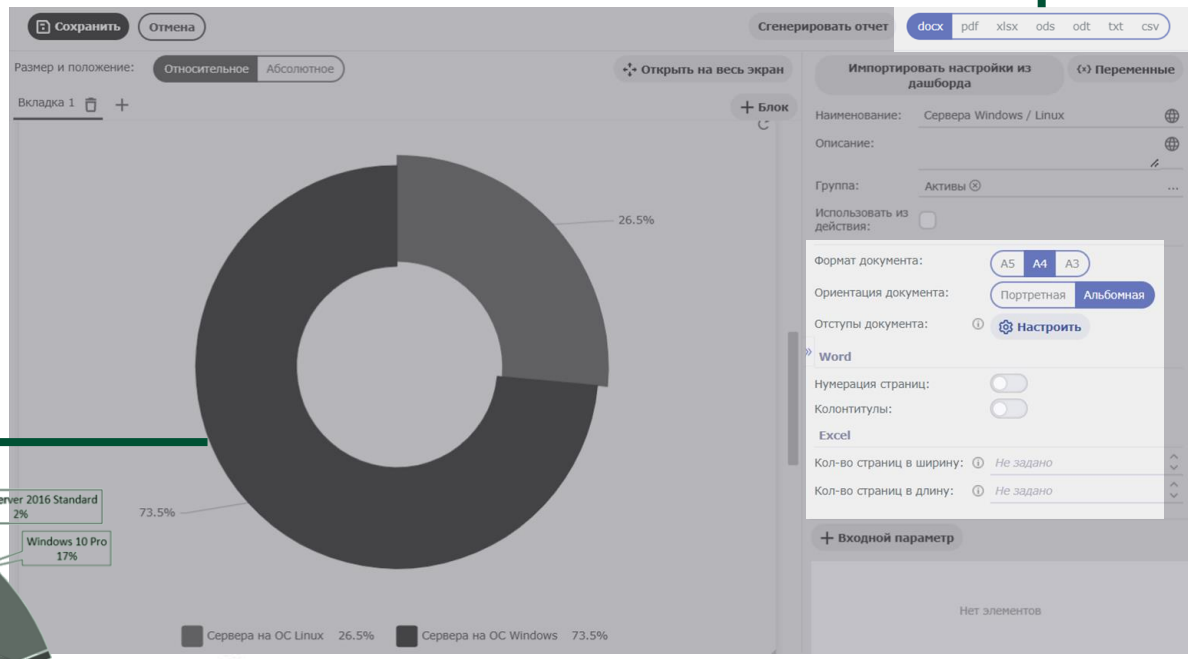
Конструктор виджетов и отчётов

графы связей

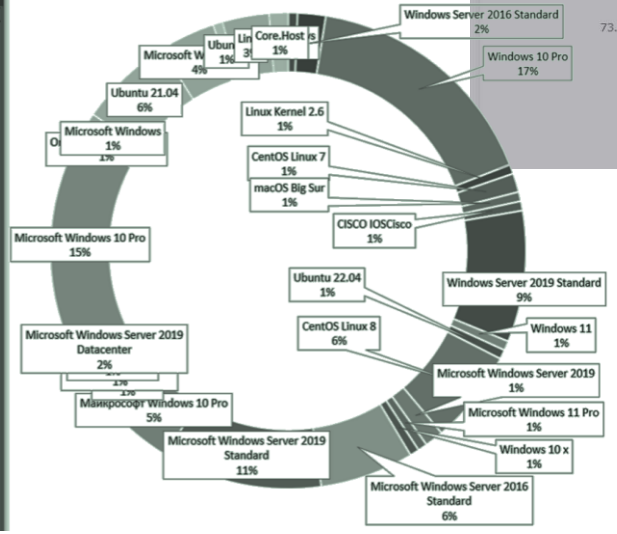
карты и планы помещений

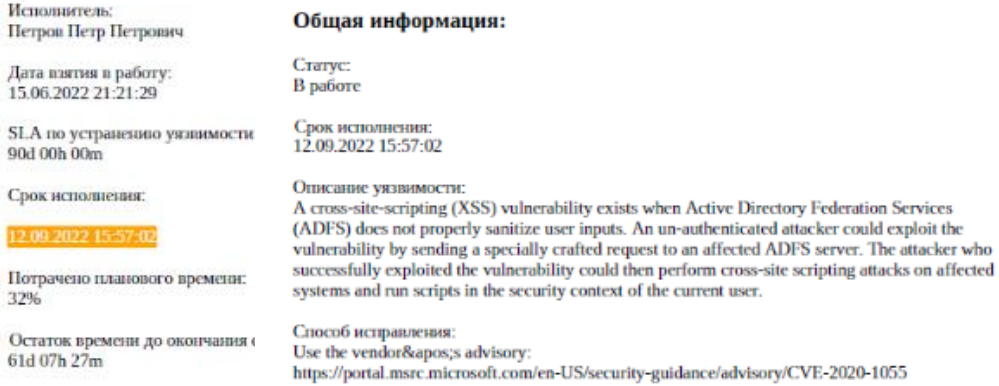
различные форматы

интерактивная аналитика и отчёты по расписанию

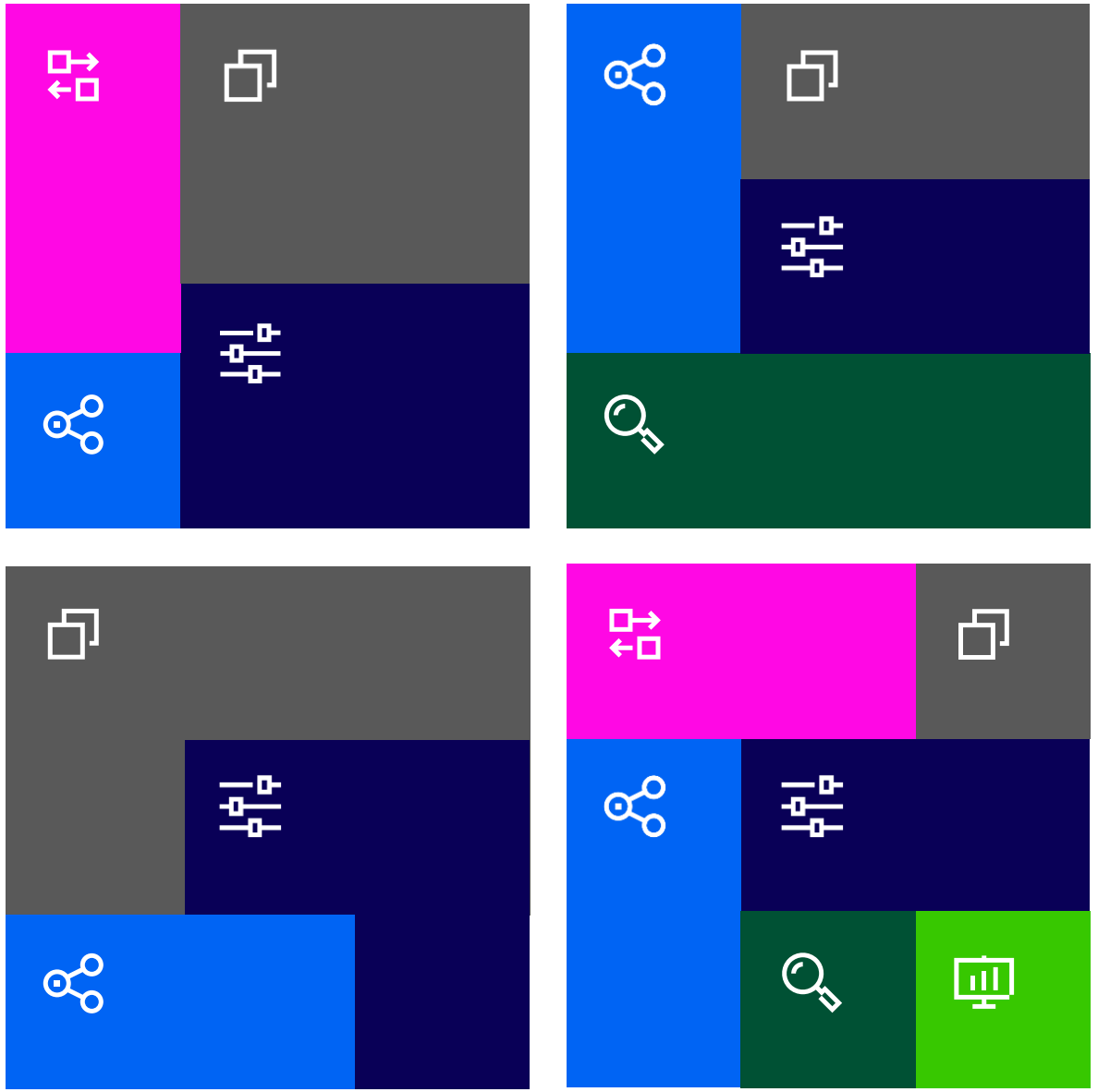


	A	B
1	Windows	1
2	Windows Server 2016 Standard	3
3	Windows 10 Pro	26
4	Linux Kernel 2.6	1
5	CentOS Linux 7	2
6	macOS Big Sur	1
7	CISCO IOSCisco	1
8	Windows Server 2019 Standard	14
9	Windows 11	1
10	Ubuntu 22.04	1
11	CentOS Linux 8	10
12	Microsoft Windows Server 2019	2
13	Microsoft Windows 11 Pro	1
14	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

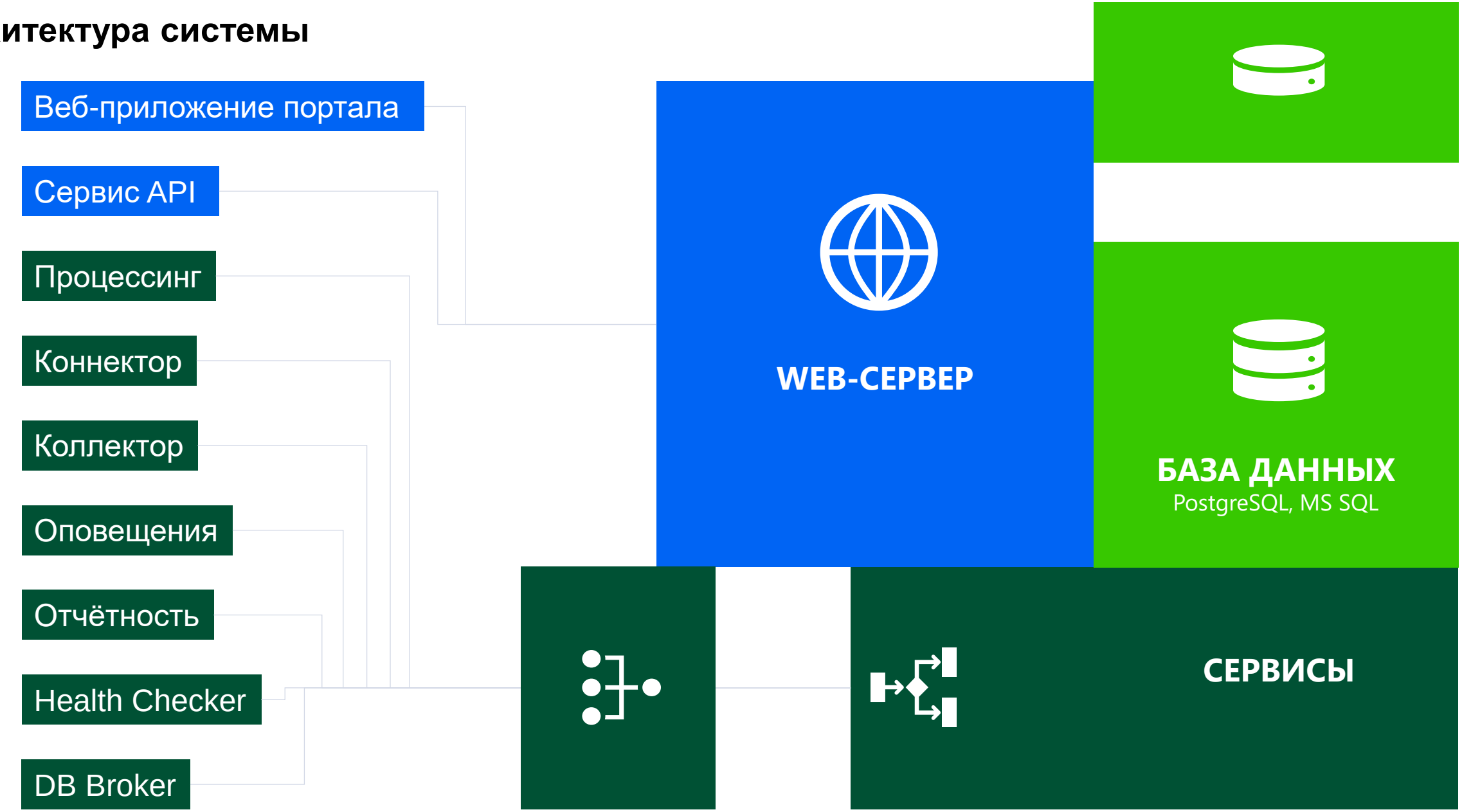




Собирайте модули под ваши задачи без навыков программирования с помощью гибких конструкторов



Архитектура системы



Задачи, решаемые Security Vision

Практическая безопасность

SOAR

Orchestration, Automation and Response

- Управление инцидентами
- Анализ угроз
- Управление уязвимостями
- Управление активами
- НКЦКИ
- ФинЦЕРТ

Стратегическая безопасность

SGRC

Governance, Risk Management and Compliance

- Оценка рисков
  - риски кибербезопасности
  - операционные риски, 716-П
- Аудит
  - 187-ФЗ, КИИ
  - ГОСТ 57580
  - ISO 27001
  - PCI-DSS

и др.

Спасибо за внимание

Роман
Душков

пресейл менеджер

+7 995 880 40 63
rdushkov@securityvision.ru

sales@securityvision.ru

Интеллектуальная платформа информационной безопасности и ИТ

Security Vision

securityvision.ru