

Управление безопасностью и анализ угроз

на стыке технологий
и решений ИБ/ИТ

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

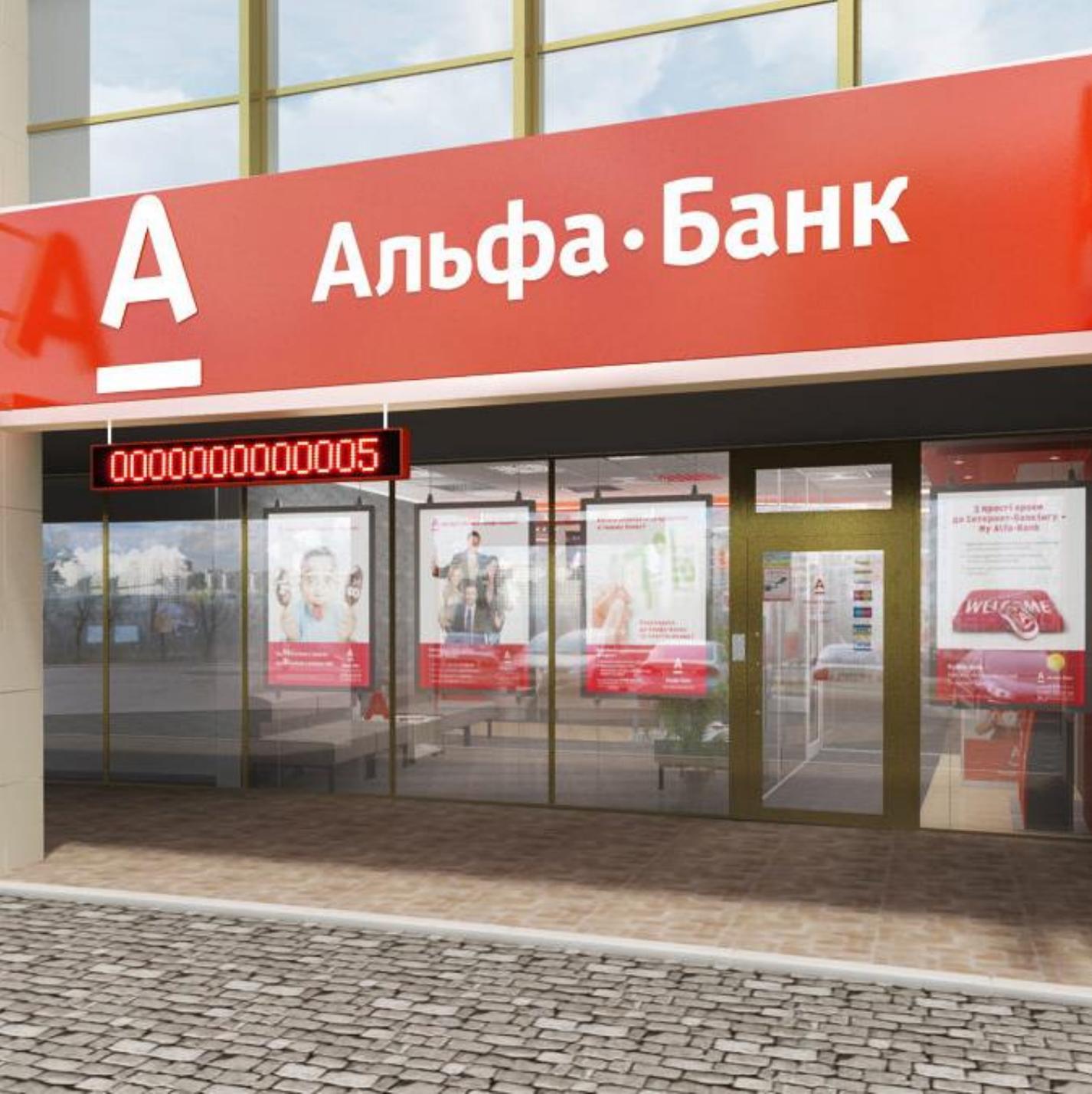
ИБ-решение 2022, лучший партнёр банков 2021, лучшая платформа автоматизации 2020

20+ профессиональных наград



← Click here





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



УПРАВЛЕНИЕ ИНЦИДЕНТАМИ



15+ автоматизированных
плейбуков реагирования



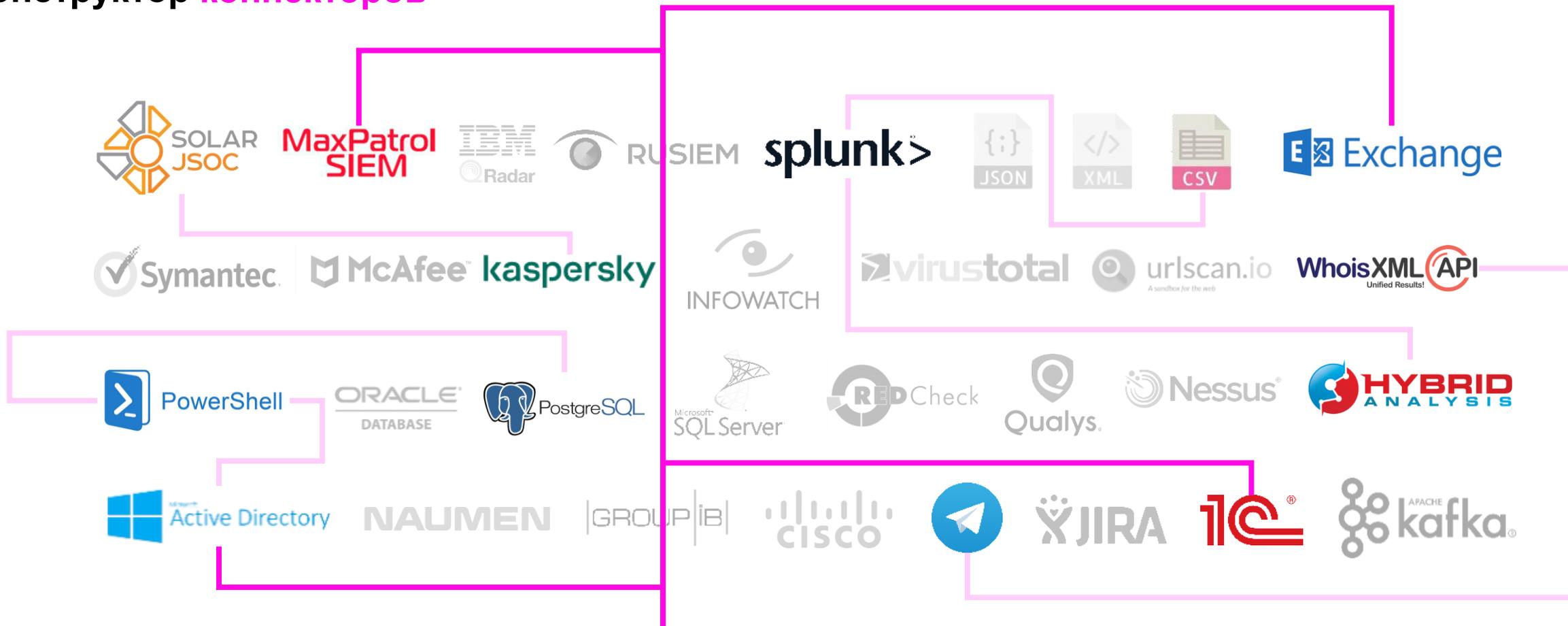
Глубокие процессы обработки
инцидентов



20+ интеграций с ИТ-системами
и СЗИ



на стыке технологий



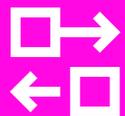
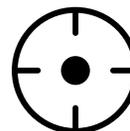
email | Syslog | файлы | БД | API | DNS | SNMP | LDAP | SOAP | скрипты

создание новых коннекторов **без участия вендоров**

Сбор и обогащение

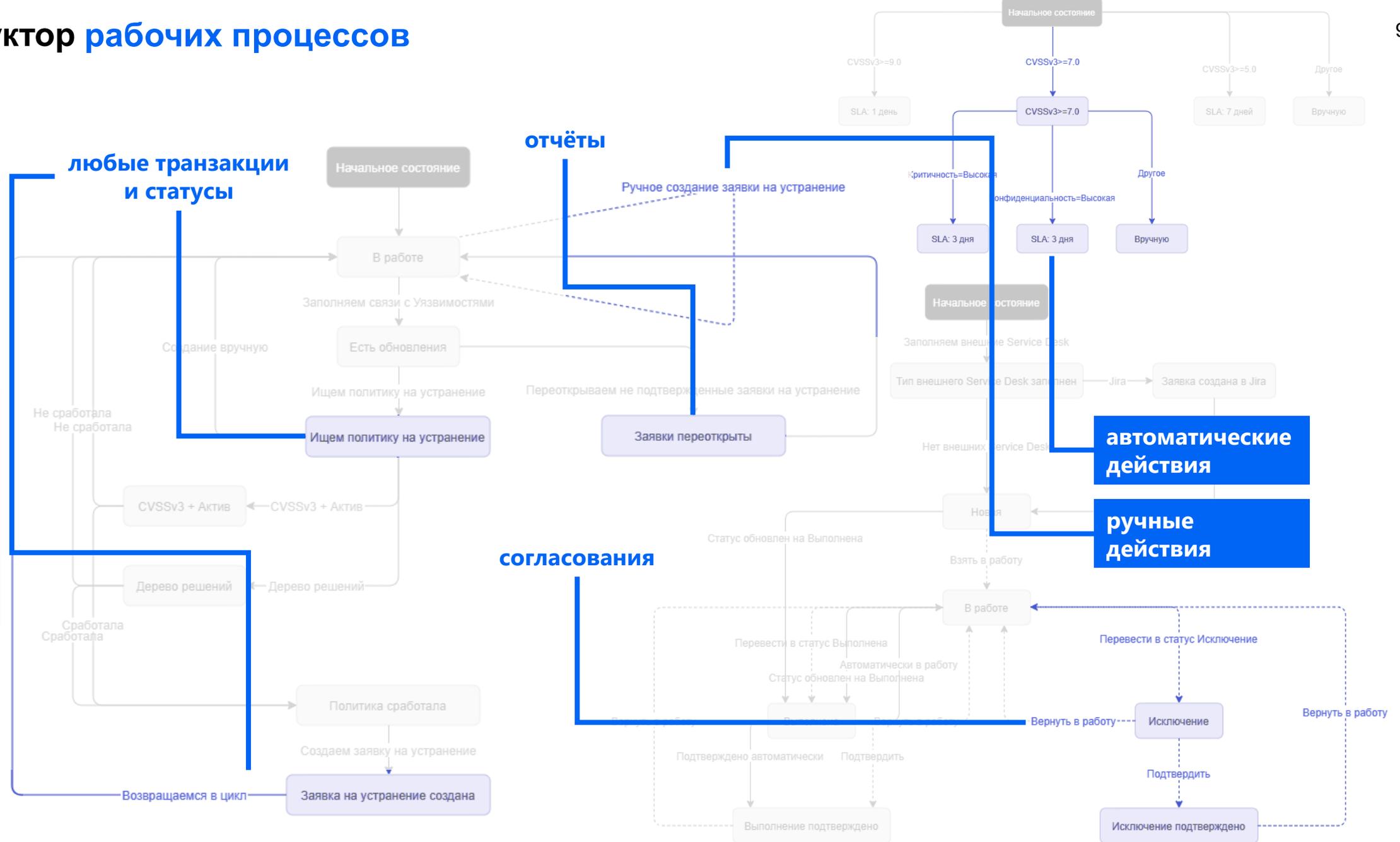


Реагирование на события



настоящие задачи

Конструктор рабочих процессов



интерфейсы и язык

Конструктор объектов



массовые операции

фильтрация

сортировка

быстрые ссылки

полнотекстовый поиск

кнопки управления

The screenshot displays a web application interface for managing objects. At the top, there is a breadcrumb navigation: "Объекты > Оборудование > Все устройства". Below this is a search bar and a toolbar with icons for search, add, and refresh. The main area is a table of objects with columns for selection, ID, creation date, status, FQDN, IP address, operation system, last user, and data source. A detailed view of a vulnerability report is shown in the foreground, including fields for ID, creation date, status, and a description of the vulnerability. The report also includes a list of active objects with columns for type, FQDN, IP address, and operation system.

метки времени

стили

ссылки

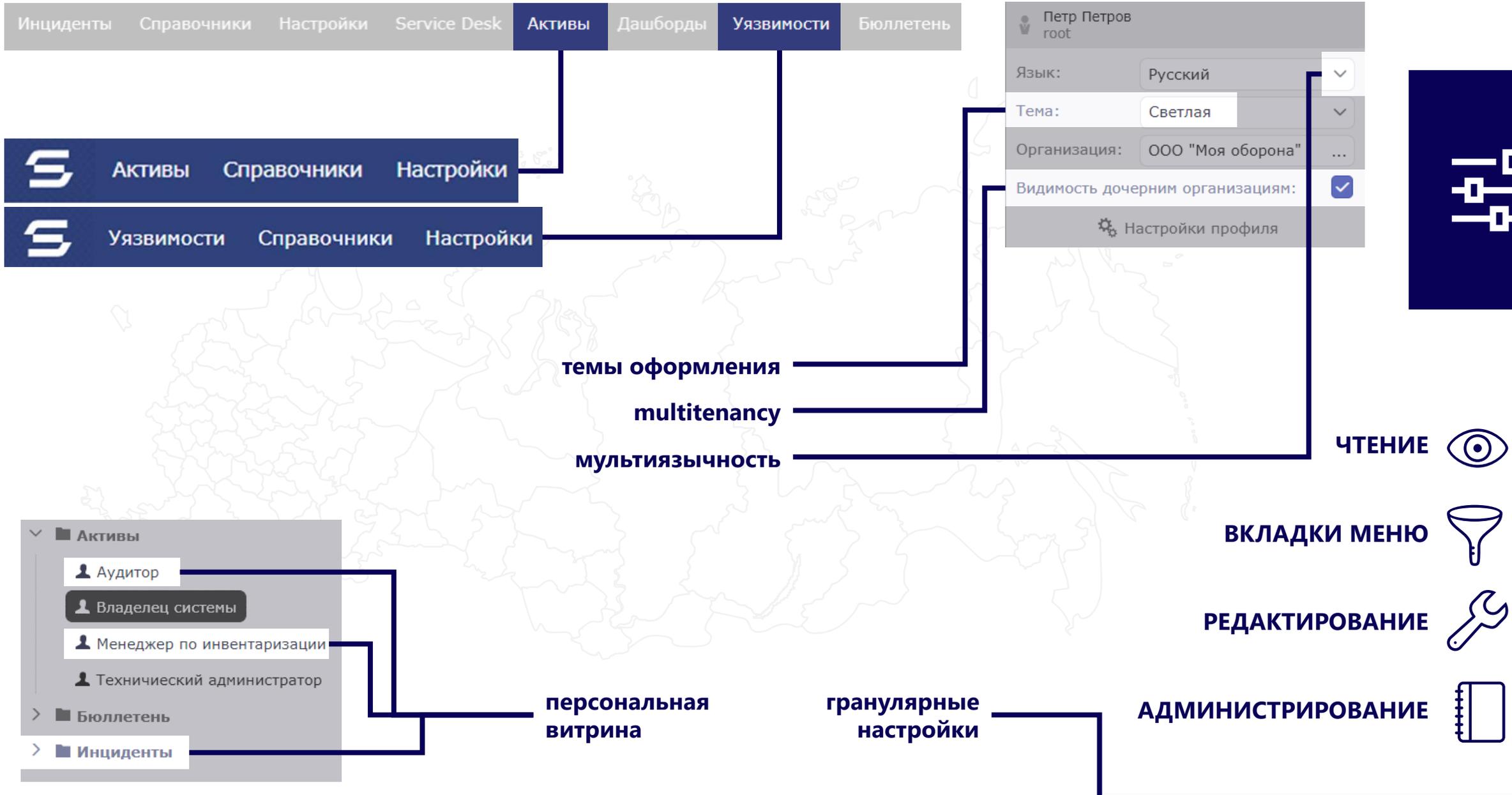
обязательные поля

полная карточка

табличный вид

краткая карточка

распределённые команды



аналитика и документация

графы связей

карты и планы помещений

различные форматы

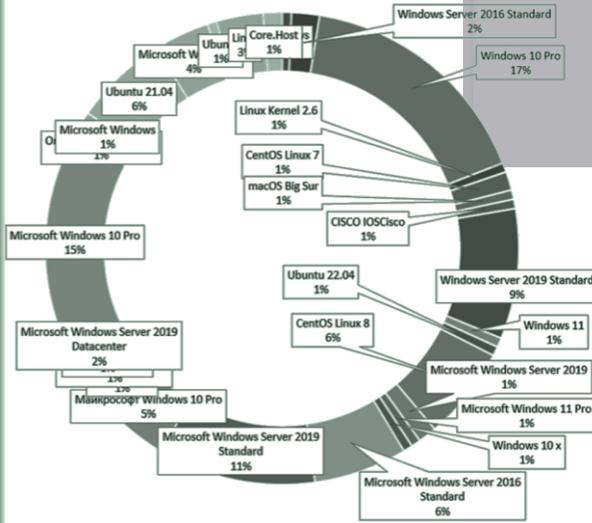


интерактивная аналитика и отчёты по расписанию



A screenshot of a dashboard interface. It features a large donut chart showing the distribution of servers by OS: Linux (26.5%) and Windows (73.5%). To the right, there is a settings panel for generating reports, including options for document format (docx, pdf, xlsx, ods, odt, txt, csv), orientation (Portrait, Landscape), and margins. Below the chart, there is a table with columns for 'Исполнитель', 'Дата взятия в работу', 'SLA по устранению узвимости', 'Срок исполнения', 'Потрачено планового времени', and 'Остаток времени до окончания'.

	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
25	Ubuntu 21.04	10
27	Microsoft Windows 10	6
28	Ubuntu	1
29	Linux	5
30	Core.Host	2



Исполнитель:
Петров Петр Петрович

Дата взятия в работу:
15.06.2022 21:21:29

SLA по устранению узвимости:
90d 00h 00m

Срок исполнения:
12.09.2022 15:57:02

Потрачено планового времени:
32%

Остаток времени до окончания:
61d 07h 27m

Общая информация:

Статус:
В работе

Срок исполнения:
12.09.2022 15:57:02

Описание узвимости:
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.

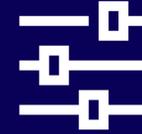
Способ исправления:
Use the vendor's advisory:
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1055>



~ CRM



Объекты, карточки и
внешний вид



Ролевая модуль и
настройка меню

~ BPM

~ BI



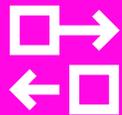
Рабочие процессы и
структура



Security
Vision



Визуализация и
аналитика



Интеграции с внешними
системами

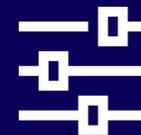
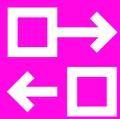


Отчёты и логирование
действий

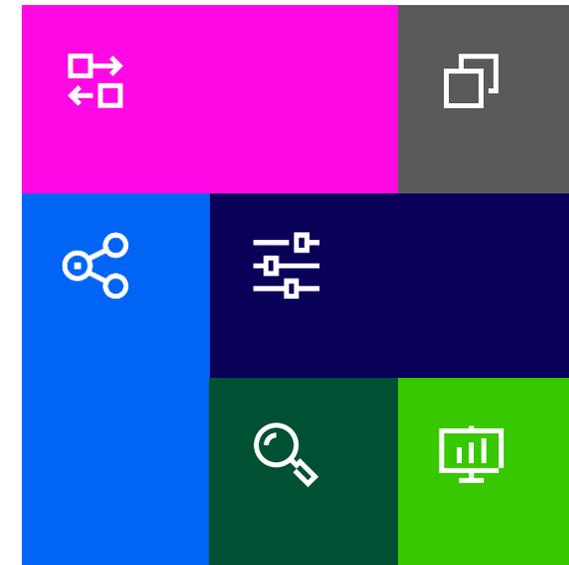
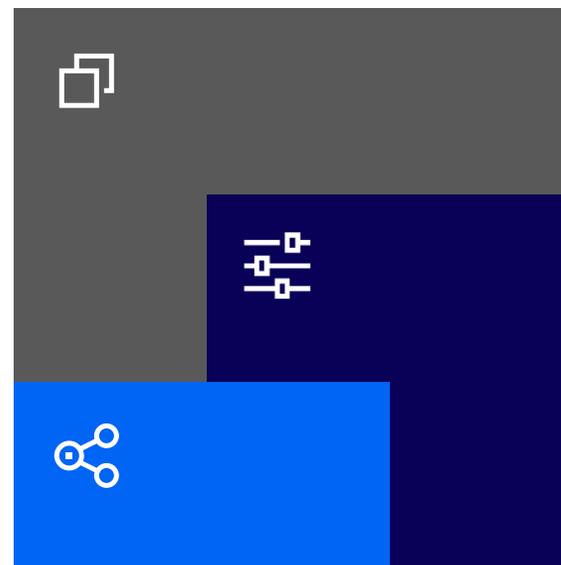
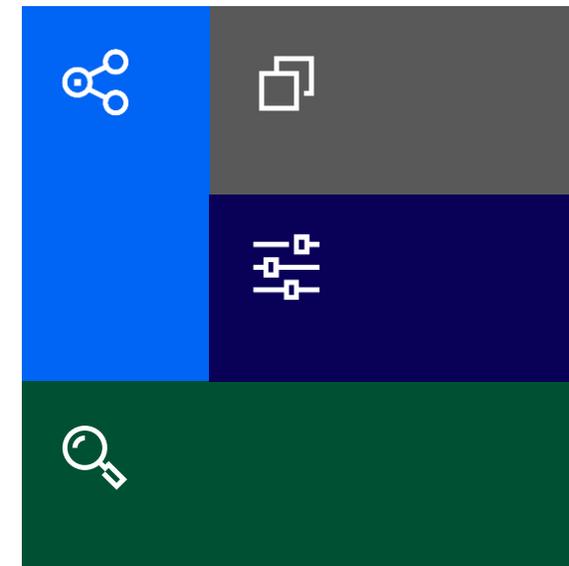
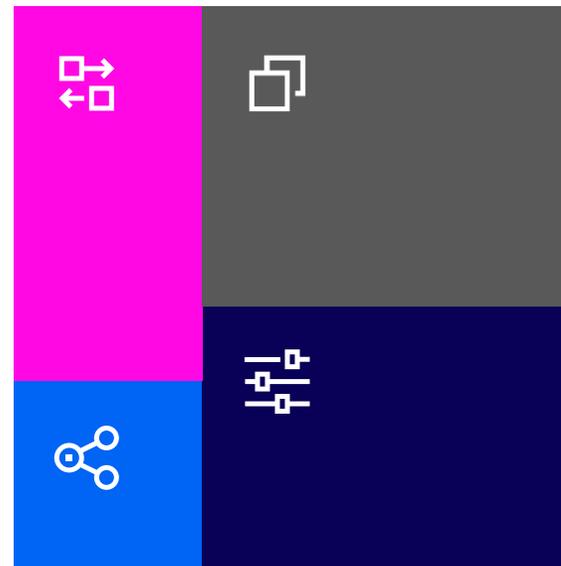
~ RPA

~ Word

МОДУЛИ



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



Решения SV для процессов всех уровней зрелости

SOAR

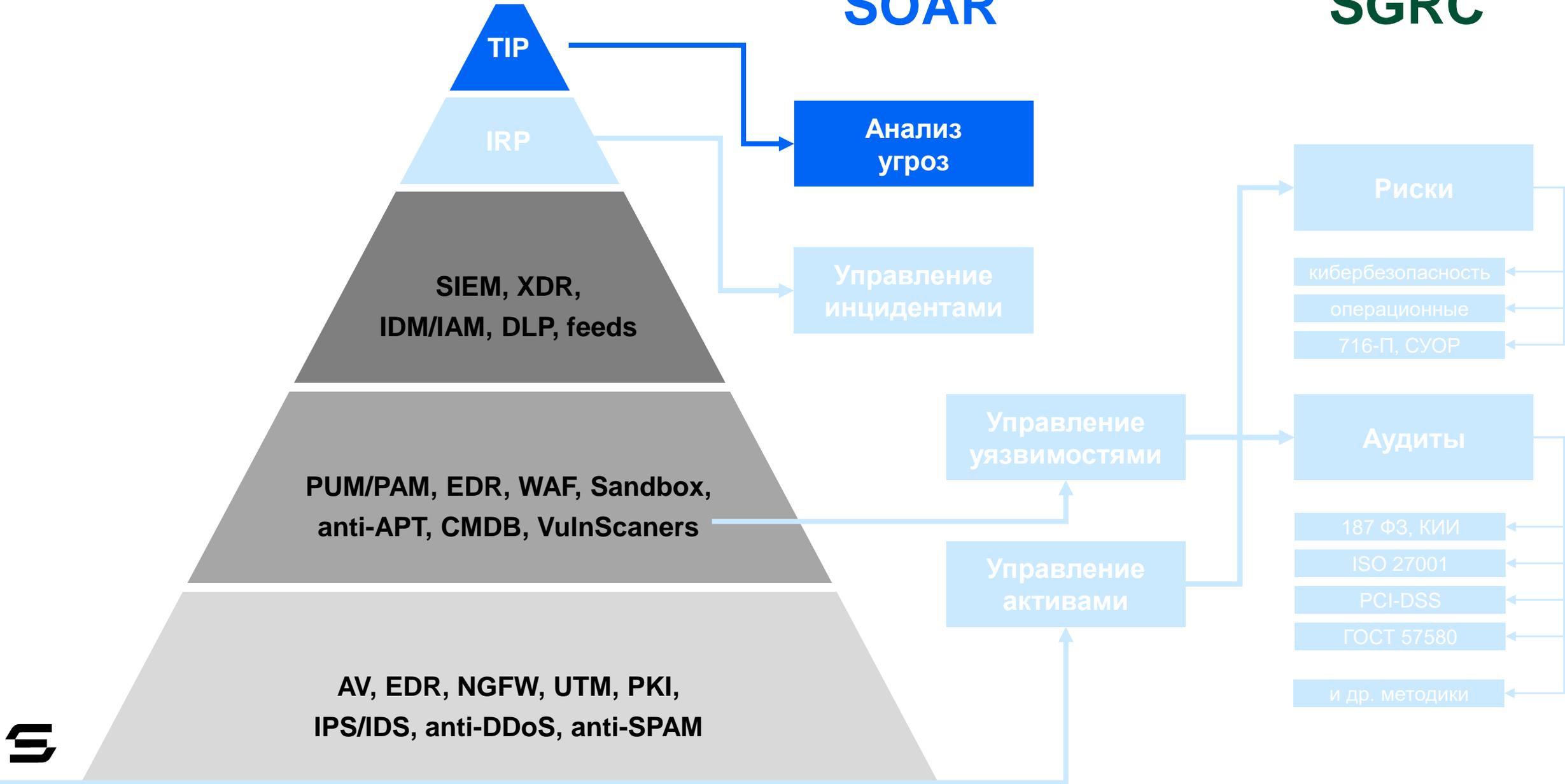
SGRC



Решения SV для процессов всех уровней зрелости

SOAR

SGRC



Анализ угроз, киберразведка в Security Vision 5

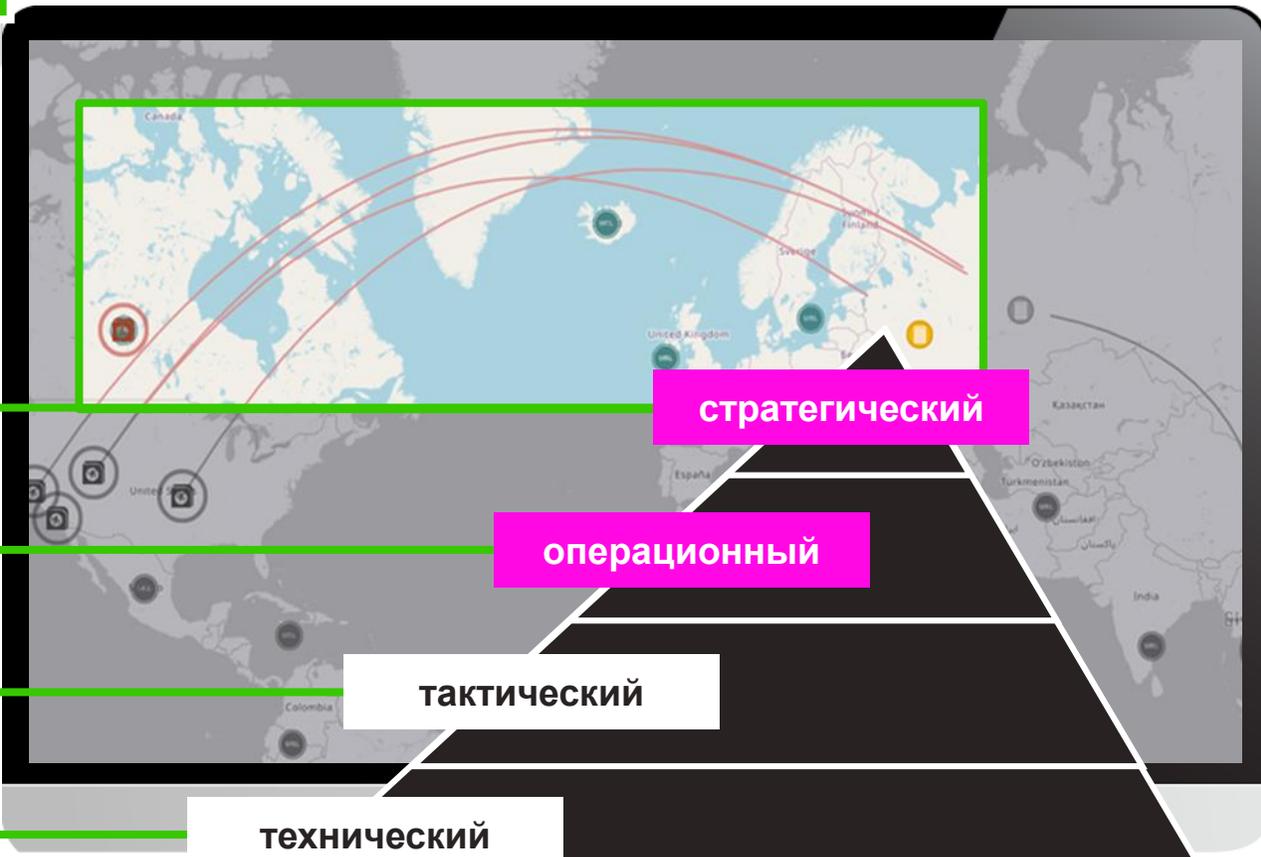


1

Загрузка данных

события, фиды, IoC, бюллетени, источники угроз

- злоумышленники
- ВПО
- угрозы
- уязвимости
- IoA
- домены
- URL
- хэши
- IP



Работа с IoC

2

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.

False-Positive

Активный

Не активный

Отслеживать изменения

Не отслеживать изменения

Добавить в Active List

Поиск в Active list

Удалить из Active List

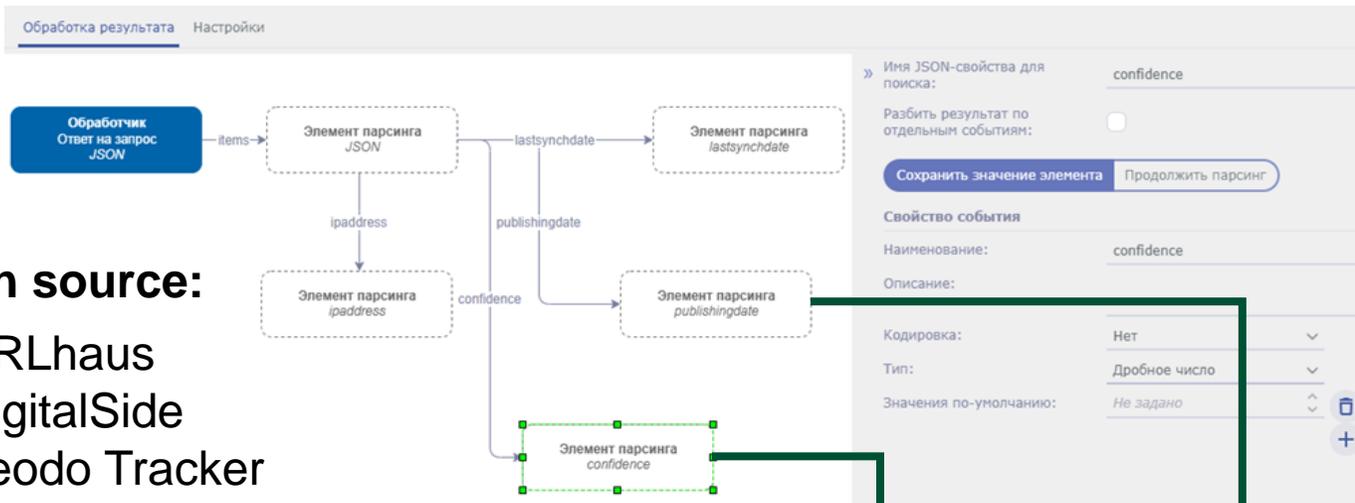
Добавить новый тэг

Реагирование

управление политиками в едином продукте

4





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://kontenserciesddi.baserves.com/app?783003312514/qEOp89s yiukMSLVDnuc5WrbBn1 mNLtvU/5408e8QlnlfdNy 3MPXivh2uMZkBgUAxLtv rTAUSz1frGCJG	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://kontenserciesddi.baserves.com/app?323185532344/lyezASi3 4PWk7H1GBvuReKnQ8D mpUk5z/7606PBI16Orc9	07.11.2022 16:22:50	Активный	Критичная (100)	GroupIB	

Сбор индикаторов от поставщиков

Настройки > Дополнительные > Время жизни IOC

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

Время участия в обнаружении и жизни внутри системы

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

Описание:
Дата первого обнаружения: 09.01.2021 00:21:06
Дата последнего обнаружения: 01.11.2022 15:38:25
Отрасль: Не задано
Категория IOC/IOA: TorNode
MITRE ATT&CK: Не задано
OWASP Top 10: Не задано
Kill-Chain фазы: Не задано
Добавлен в Active List: Нет
Нахождение в табличных списках (SIEM): Не задано
Находится в блок-листе FW:
Ссылки: Не задано

Распространенность: Не задано
TLP: Green
Whois / ASN
Город: Не задано
Широта: Не задано
Долгота: Не задано
ASN: Не задано
ISP: Не задано
Дата создания в ASN: 02.12.2022 00:00:00
Дата обновления в ASN: 02.12.2022 00:00:00
Срок истечения в ASN: 02.12.2022 00:00:00
Организация ASN: Не задано
Первый IP в ASN: IPv4 IPv6
Последний IP в ASN: IPv4 IPv6

Только актуальные данные, меньше False Positive

Обнаружение

Главная Событие Индикаторы Активы Вложения Аналитика История

Статус: ● В работе
Критичность: ● Критичная
Количество событий: 39

Общая информация

Обнаружение
Id: 9470859
Наименование: Отправка письма с подозрительного домена: acmetek.com
Описание:

Инцидент в SOAR: [3200155](#)
Отправлен в SIEM по SysLog:

История

Дата создания: 10.11.2022 10:20:31
Взят в работу: 10.11.2022 10:21:58
Время первого события: 05.09.2022 18:33:00
Время последнего события: 05.09.2022 18:33:00

Реагирование

Ответственный: Петров Петр
Время в работе: 5.05:56
Решение по инциденту:

Типы IoC
Домен 100.0%

Статусы IoC
Активный 100.0%

Наименование	Количество событий	Время первого события	Время последнего события	Время закрытия	Статус обнаружения	Критичность
Обращение на подозрительный домен vk.com	116	10.11.2022 20:31:29	10.11.2022 20:33:48	10.11.2022 20:38:00	Закрит	Высокая
[retro] Обращение на подозрительный IP 172.67.166.99	14	31.10.2022 17:29:30	31.10.2022 17:29:30		Новый	
Обращение на подозрительный IP 128.252.93.204 (qsdictydb.wustl.edu)	38	10.11.2022 10:25:59	10.11.2022 10:26:39		В работе	Высокая
Обращение с подозрительного IP 128.252.93.204 (qsdictydb.wustl.edu)	16	10.11.2022 10:19:38	10.11.2022 10:20:09	10.11.2022 10:24:01	Закрит	Высокая
Отправка письма с подозрительного домена: acmetek.com	13	05.09.2022 18:33:00	05.09.2022 18:33:00		В работе	Критичная
Обращение с подозрительного IP 128.252.93.204 (qsdictydb.wustl.edu)	12	10.11.2022 10:11:37	10.11.2022 10:12:01	10.11.2022 10:15:17	Закрит	Высокая

Основная информация

IP адрес: 51.15.61 IPv4 IPv6
Страна: Netherlands
Описание:
Дата первого обнаружения: 09.01.2021 00:21:06
Дата последнего обнаружения: 01.11.2022 15:38:25
Отрасль: Не задано
Категория IOC/IOA: TorNode
MITRE ATT&CK: Не задано
OWASP Top 10: Не задано
Kill-Chain фазы: Не задано
Добавлен в Active List: Net
Нахождение в табличных списках (SIEM): Не задано
Находится в блок-листе FW:
Ссылки: Не задано

Оценки

Оценка критичности: 50
Оценка доверия: 50
Оценка источника: Не задано
Оценка категории: Не задано
Распространенность: Не задано
TLP: Green

Whois / ASN

Город: Не задано
Широта: Не задано
Долгота: Не задано
ASN: Не задано
ISP: Не задано
Дата создания в ASN: 02.12.2022 00:00:00
Дата обновления в ASN: 02.12.2022 00:00:00
Срок истечения в ASN: 02.12.2022 00:00:00
Организация ASN: Не задано
Первый IP в ASN: Не задано
Последний IP в ASN: Не задано

URL

Domain
Email
HostName
Ports
OS
Software
Hash SHA1
Hash MD5
Hash SHA256
JA3S
JARM

Закрывать для редактирования
Отслеживать изменения
False-Positive
Неактивный
Добавить новый тэг
Добавить в Active List
Проверить в Active List
Выгрузить в формате STIX2
Выгрузить отчет

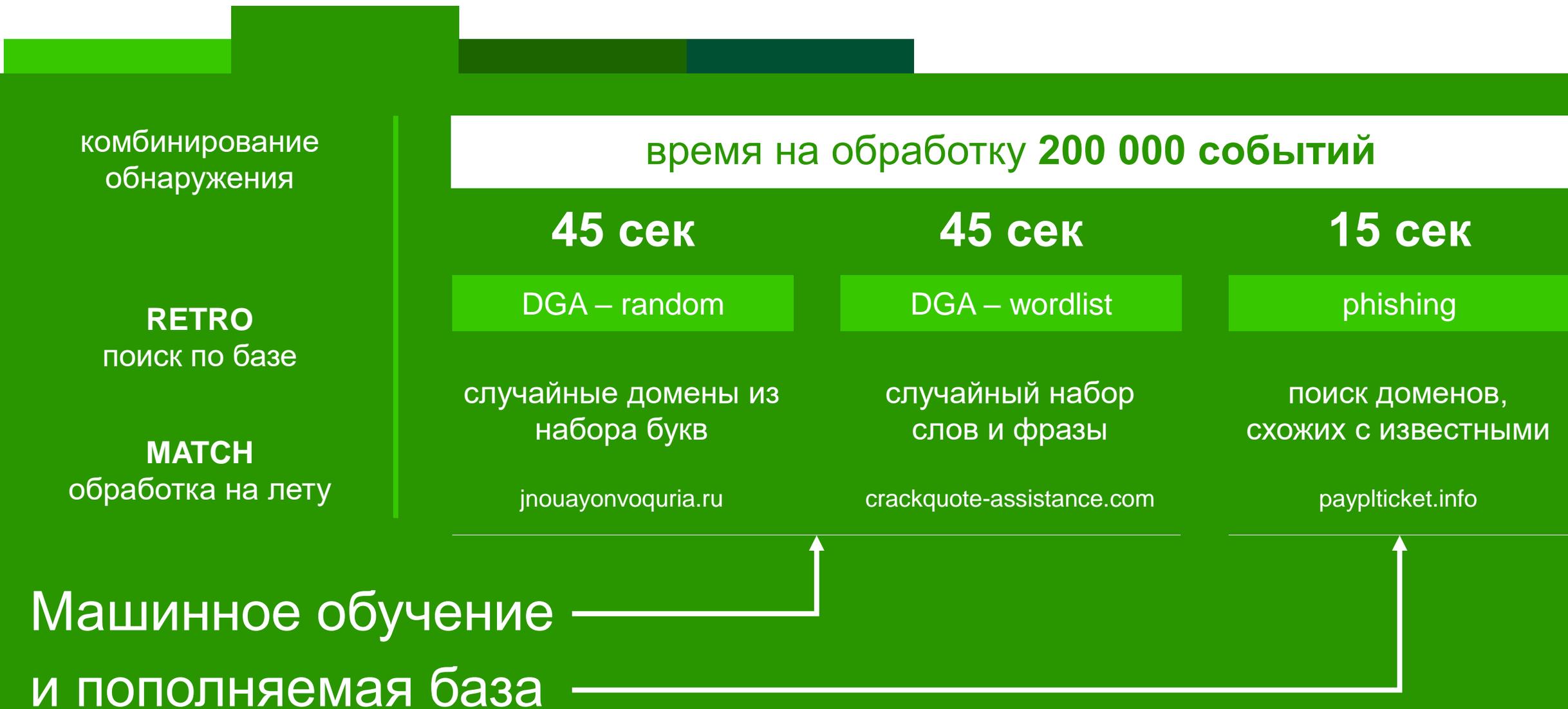
Отправить все IP на FireWall Удалить все IP из FireWall Отметить IOC как FP Отметить IOC как Активный

IoC	Тип	Статус IOC	Критичность	Находится в блок-листе
<input checked="" type="checkbox"/> 206.116.23.54	IP	Активный	Высокая (70)	False
<input checked="" type="checkbox"/> 128.252.93.204	IP	Активный	Критичная (100)	False

Выбрано 2 Действия Отменить выбор

Всего 2 Показывать на странице 20

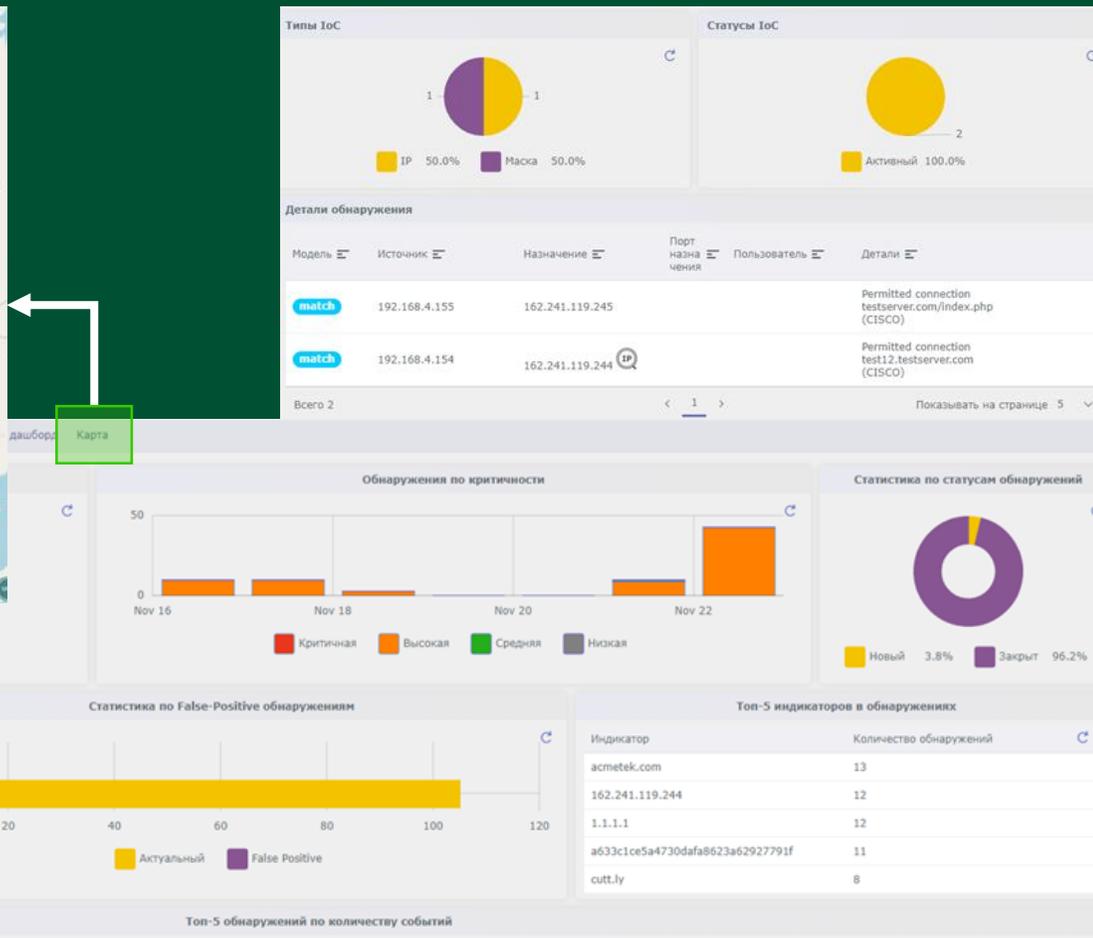
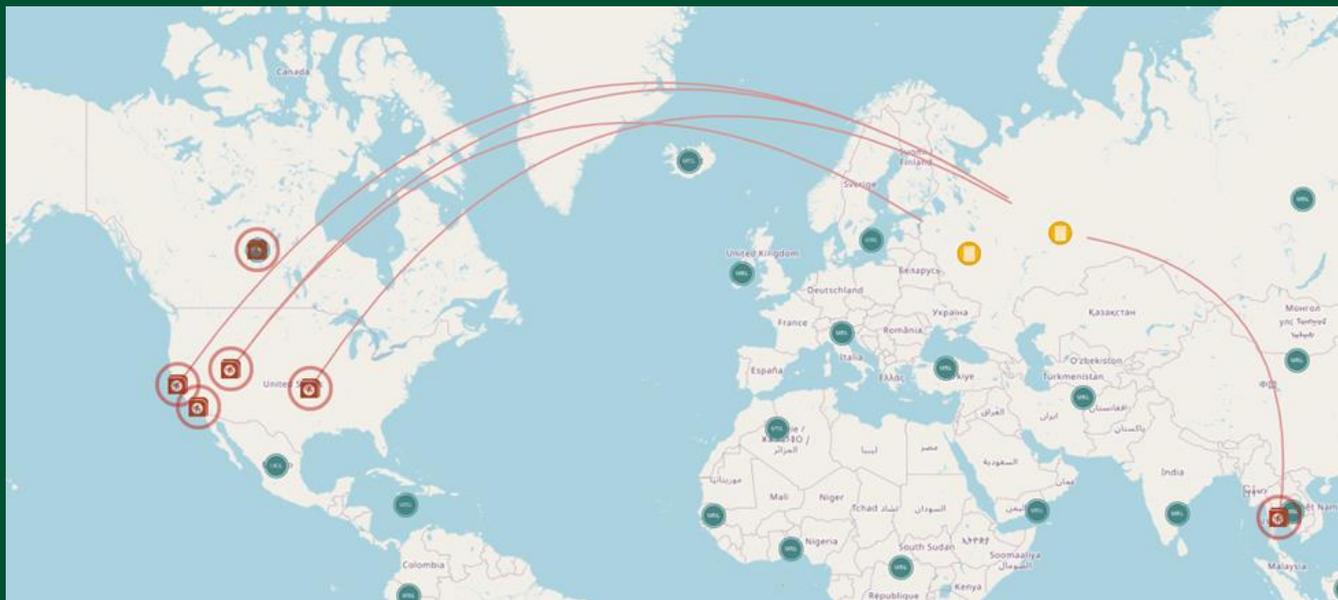
Обнаружение
внутри периметра



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

Стратегический уровень анализа





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

Интеллектуальная
платформа
информационной
безопасности и ИТ



securityvision.ru