

Управление ИБ и анализ угроз на стыке технологий и разных продуктов



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



← Click here



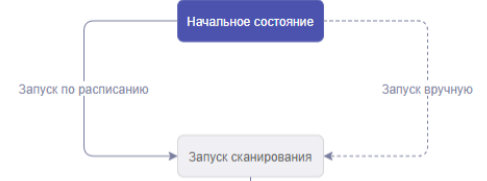
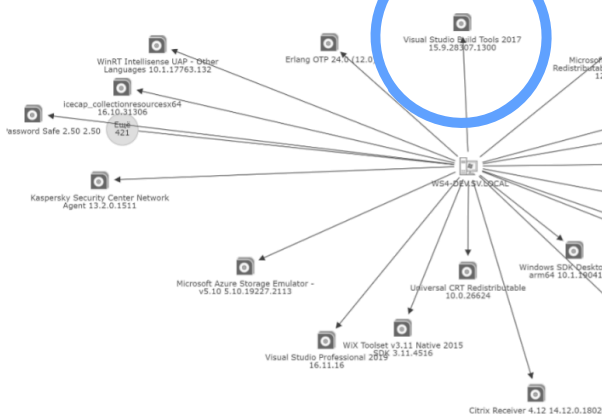
Управление разрозненными ИТ-системами

Управление активами в Security Vision 5

Поиск объектов

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

1



Жизненный цикл

2

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



Обогащение

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

3

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

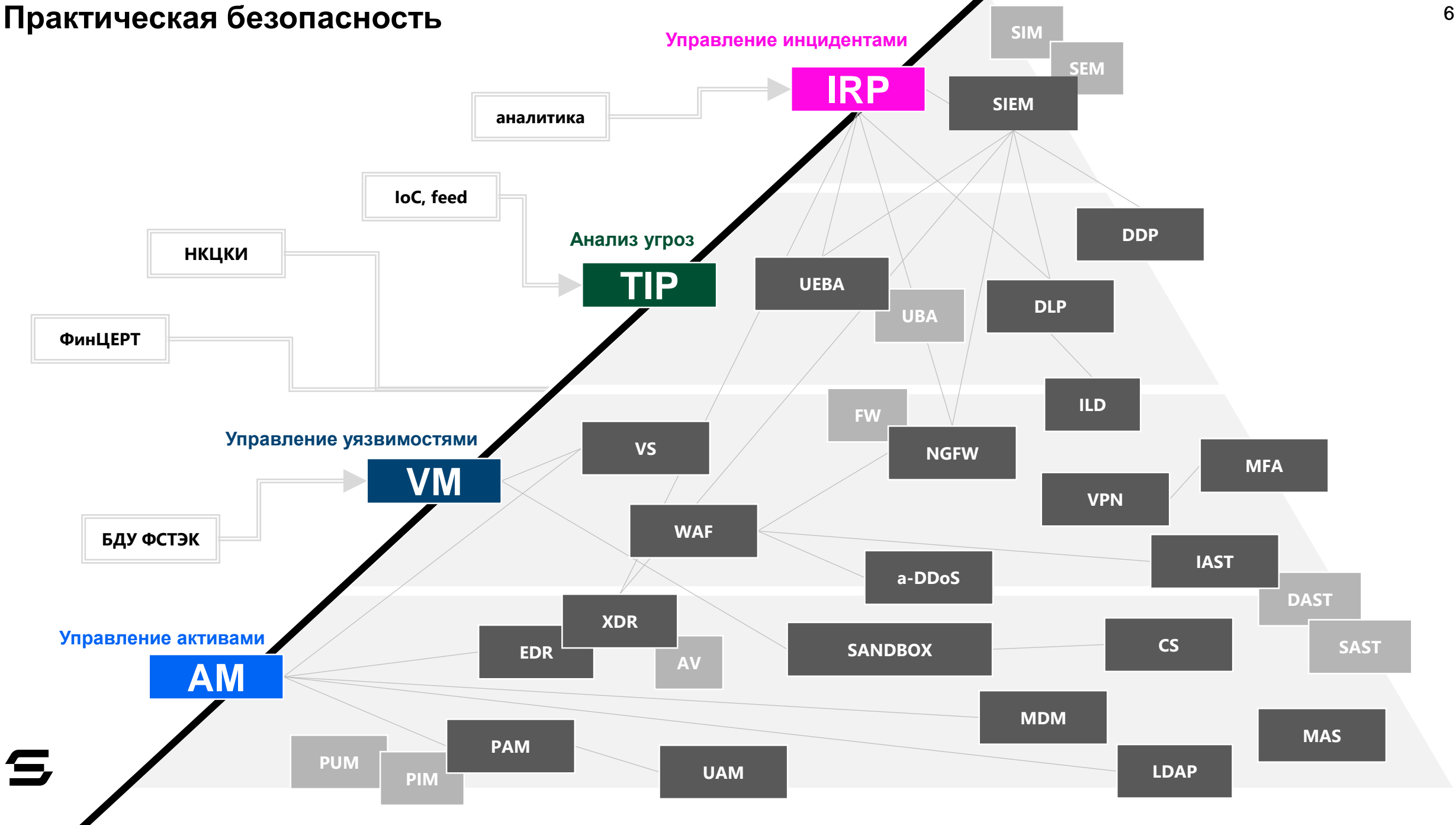
ЖЕЛЕЗО

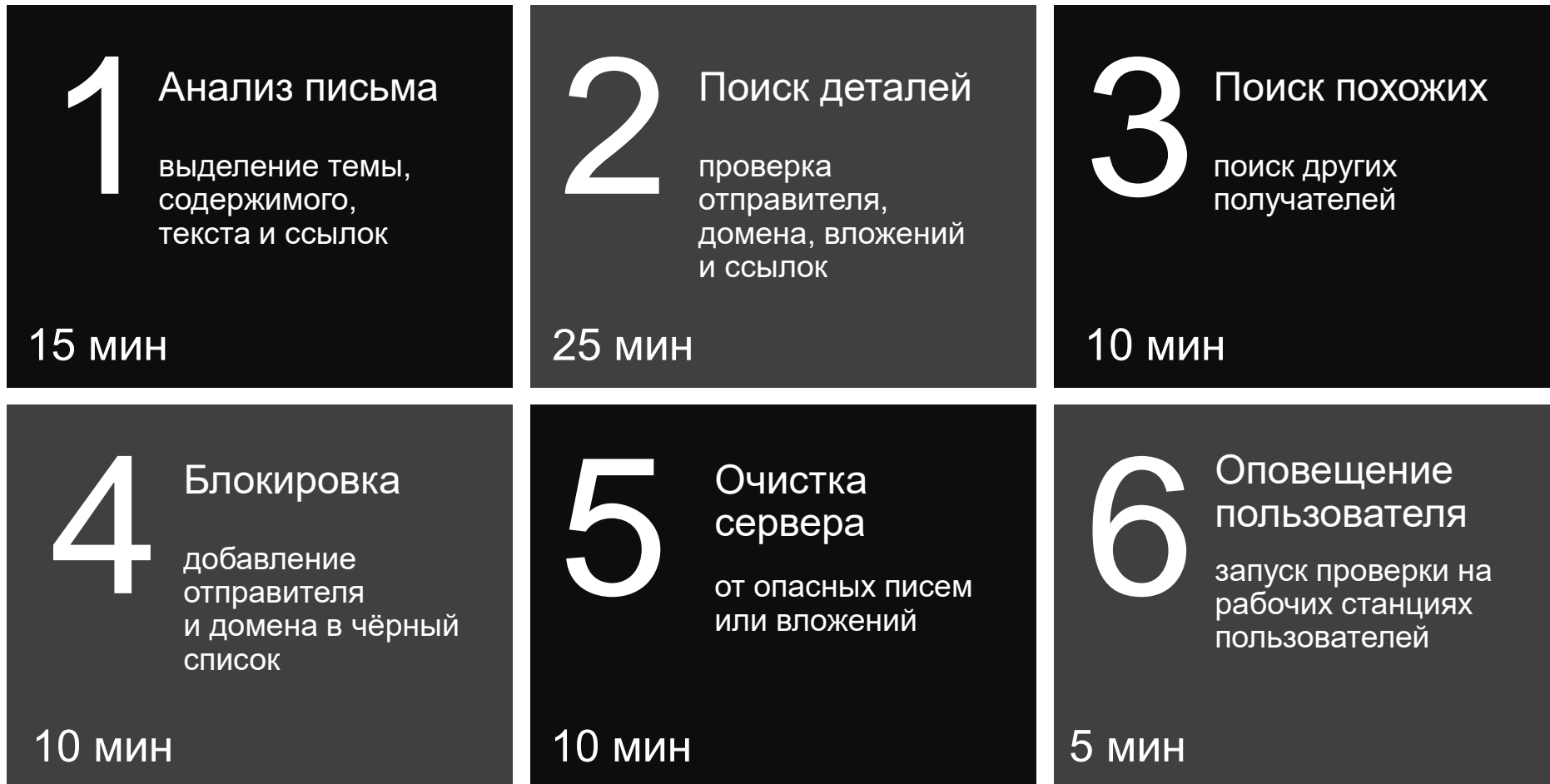
ПОЛЬЗОВАТЕЛИ

ОТЧЕТЫ

ВНЕШНИЕ СИСТЕМЫ

ТАБЛИЦЫ





75 минут
без SOAR





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



интернет, DMZ

периметр компании

сервисы обогащения

IP
URL
Email адрес
Хэш файлов
Best-practices

обнаружение

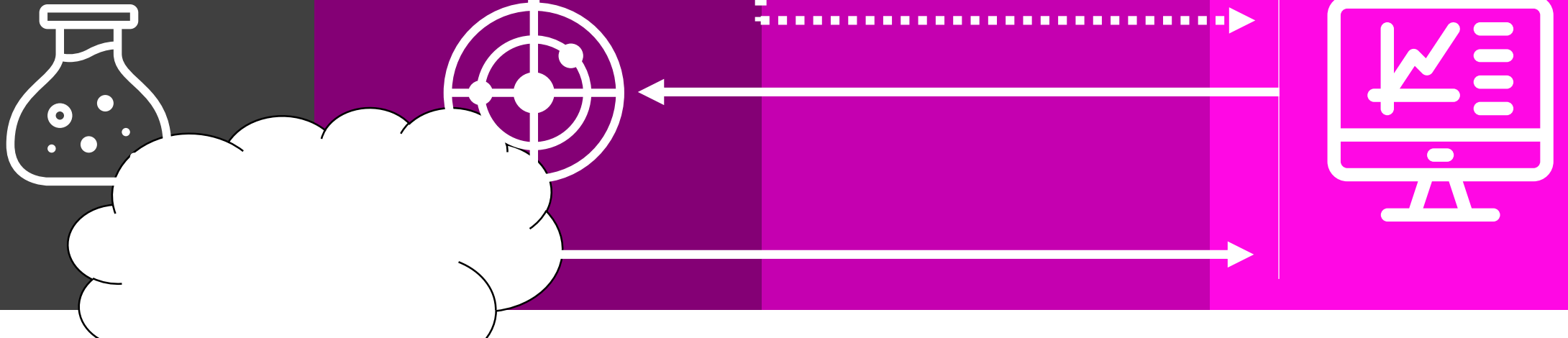
ЛЮБЫЕ СЗИ
FW, NGFW, Proxy, Email, DLP,
AV, EDR, XDR, Sandbox и др.

корреляция

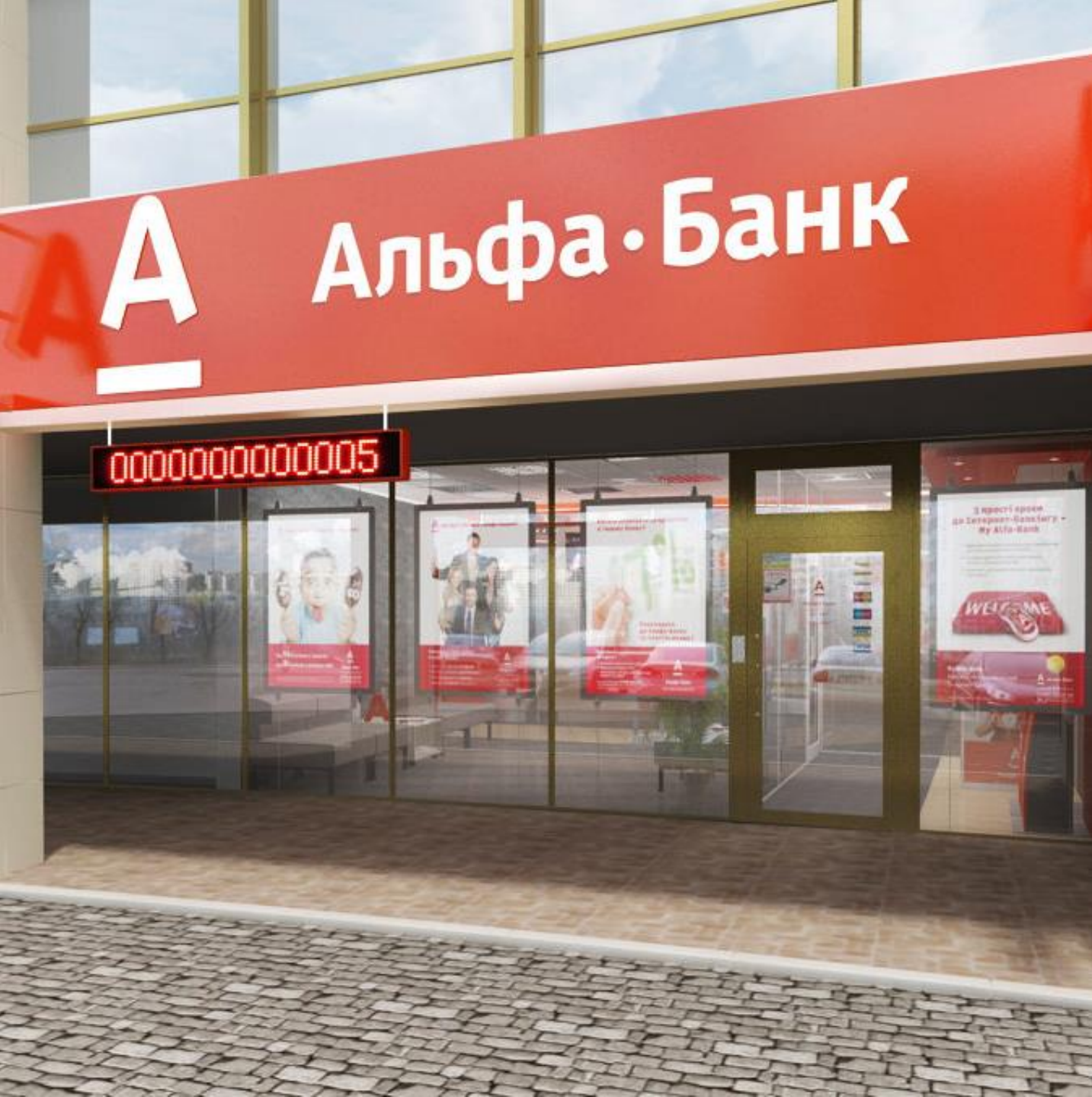
SV TIP
и/или SIEM, UBA/UEBA, ILD

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

Результат анализа <https://tuiaazul.com.br/www.netflix/0cb>

Домен: tuiaazul.com.br
 Страна: US
 Город:
 Сервер: Apache
 IP-адрес: 192.185.177.73
 ASN: AS26337
 Имя ASN: OIS1, US

UrlSCAN Score: 100
 True

Ссылка на результат проверки: <https://urlscan.io/result/1>

Результат анализа сигнатуры EICAR-Test-File

Описание сигнатуры: Под именем "EICAR-Test-SOM-файл, который вирусом НЕ ЯВЛЯЕТСЯ, а возвращает управление DOS.

Дата обнаружения:

Класс: DangerousObject
 Дата публикации в базе: 19/04/2016



2

Тикетинг

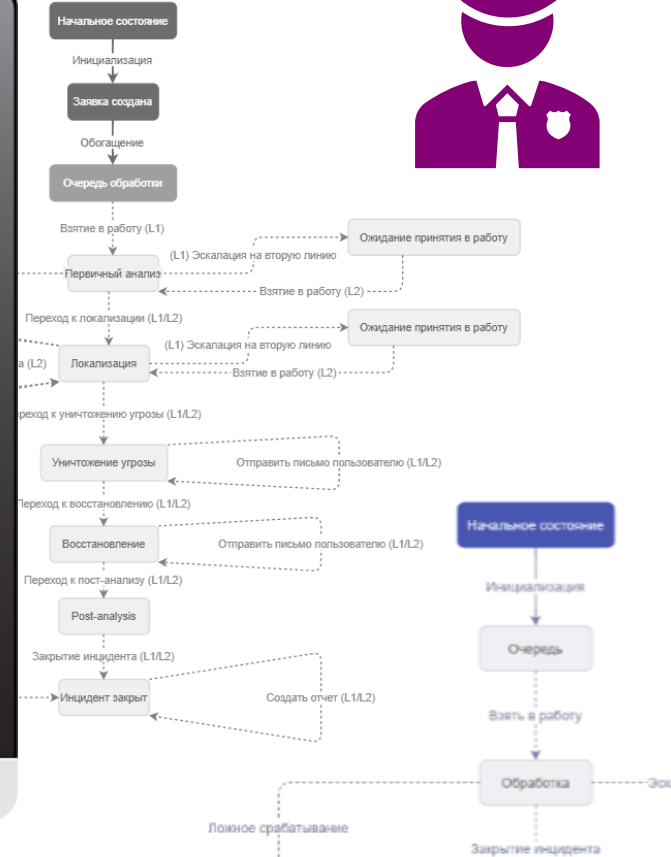
Передача в группу реагирования, обогащение данными из других систем

Id	Тип	Наименование	Описание	Статус	Приоритет	Исполнитель
20.06.2022	Инцидент "Фишинг"	Поступило потенциально фишинговое письмо	Поступило потенциально фишинговое письмо в адрес r.dushkov@yandex.ru от svdemo777@mail.ru	Закрит	Высокий	Непомнящий Петр Борисович
07.06.2022	Инцидент "Фишинг"	Поступило потенциально фишинговое письмо	Поступило потенциально фишинговое письмо в адрес presale4@demo.securityvision.ru от r.dushkov@yandex.ru	Закрит	Высокий	Непомнящий Петр Борисович
04.06.2022	Инцидент (2 линии)	Bruteforce_attempt_atomic_custom	Обнаружена попытка подбора пароля для учетной записи root с узла 172.20.4.114 на узле demo-astra-cmn	Ожидает назначения	Средний	
04.06.2022	Инцидент (2 линии)	Bruteforce_attempt_atomic_custom	Обнаружена попытка подбора пароля для учетной записи KSAvinov с узла 172.20.4.114 на узле demo-astra-cmn	В работе	Высокий	Попов Марк Анатольевич
1781801	Инцидент (2 линии)	Bruteforce_attempt_atomic_custom	Обнаружена попытка подбора пароля для учетной записи root с узла 172.20.4.114 на узле demo-astra-cmn	Ожидает назначения	Низкий	
1781786	Инцидент "Фишинг"	Поступило потенциально фишинговое письмо	Поступило потенциально фишинговое письмо в адрес presale4@demo.securityvision.ru от svdemo777@mail.ru	Закрит	Высокий	Непомнящий Петр Борисович

3

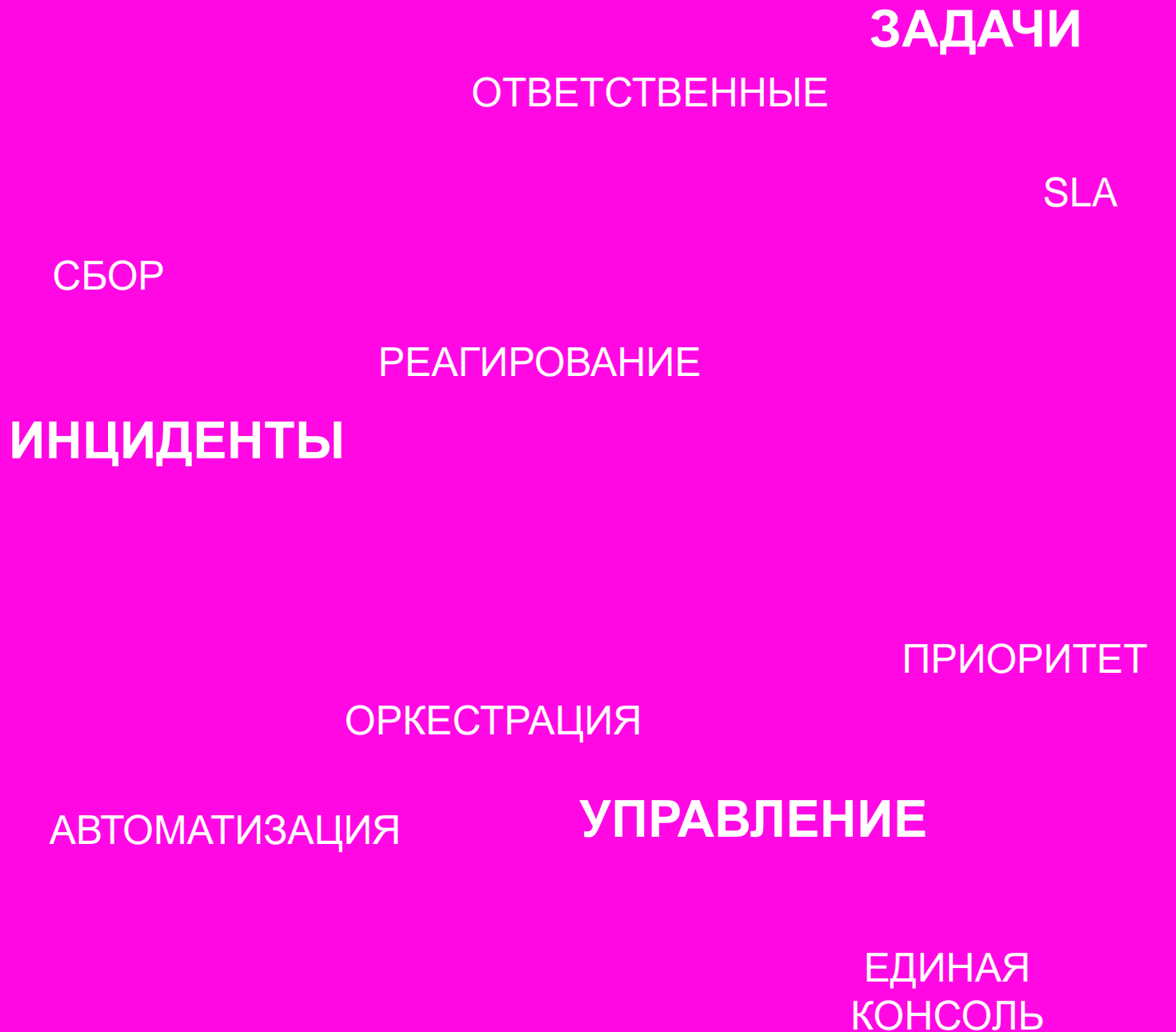
Реагирование

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





ЧЕРКИЗОВО

С 1974

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ



Территориально
распределённая ГК



Интеграция с коммерческим
SOC – «Solar JSOC»



УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ



Управление заявками ИБ как в инцидентах ИТ



Реализация процесса управления уязвимостями

Управление уязвимостями в Security Vision 5

Анализ отчёта

запуск по расписанию и
организация полного
жизненного цикла

1

Входные параметры

IP начала диапазона: 192.168.18.1

IP конца диапазона: 192.168.18.255

Имя профиля: Fast Scan

Путь к папке с заданиями: mp8

Наименование:

Группа:

Включено:

Расписание: Минуты Часы **Дни** Недели Месяцы Годы Cron

Каждые дней начиная с

Каждый день, начиная с 00:00

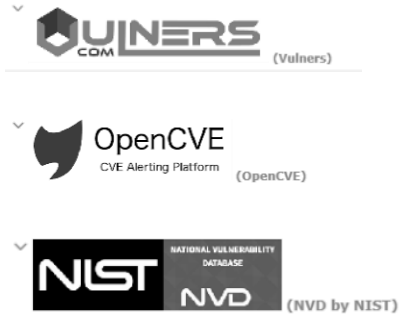
Настройки коннектора

Коннектор:

Конфигурация:

Команда:

Переменные



Обогащение

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

2

ATTACKERKB (AttackerKB)

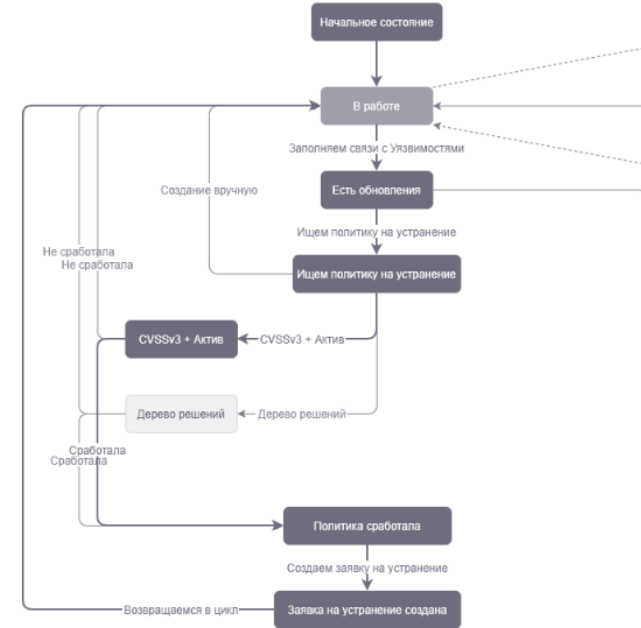
Данные

Наименование: CVE-2019-10072

Дата публикации: 21.06.2019 18:15:00

Дата проверки: 24.07.2020 00:12:06

Id	Дата создания	Наименование	Статус заявки	Срок исполнения	Потрачено планового времени
3179275	14.06.2022 15:57:58	Elevation of Privileges (DEMO-EXCHANGE)	В работе	17.06.2022 15:57:58 Просрочено	100%
3176828	14.06.2022 15:44:46	Integer Overflow (DEMO-DC)	Выполнена	5.06.2022 15:44:46	28%
3179137	14.06.2022 15:57:56	Remote Code Execution (DEMO-DC)	В работе	17.06.2022 15:57:56 Просрочено	100%
3177548	14.06.2022 15:57:02	Cross-Site Scripting (DEMO-DC)	В работе	2.09.2022 15:57:02	31%
3181914	14.06.2022 15:59:16	Elevation of Privileges (DEMO-KSC)	В работе	5.06.2022 15:59:16 Просрочено	100%
3184748	17.06.2022 11:23:28	Debian DLA-2772-1 : taglib - LTS security update (DEMO-ASTRA-CM)	В работе	5.09.2022 11:23:28	28%
3187734	17.06.2022 22:35:07	Debian DLA-2818-1 : ffmpeg - LTS security update (DEMO15.502.SJC01.QUALYS.COM) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2015-3098) (DEMO15.502.SJC01.QUALYS.COM)	Выполнена	5.09.2022 22:35:07	6%
3197050	23.06.2022 21:17:11	Уязвимость в OpenSSL 1.1.1 до 1.1.1j (20210325) ()	В работе	21.09.2022 21:17:11	21%
3177534	14.06.2022 15:57:02	Elevation of Privileges (DEMO-DC)	Новая	17.06.2022 15:57:02 Просрочено	100%
3177535	14.06.2022 15:57:02	Information Disclosure (DEMO-DC)	Новая	12.09.2022 15:57:02	31%
3177536	14.06.2022 15:57:02	Elevation of Privilege (DEMO-DC)	Новая	17.06.2022 15:57:02 Просрочено	100%



Устранение

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

3



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 защищённости

3

Устранение уязвимостей

выстраивание общего процесса для специалистов ИТ и ИБ



УСТРАНЕНИЕ

ЗАДАЧИ

SLA

ОТЧЕТЫ

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

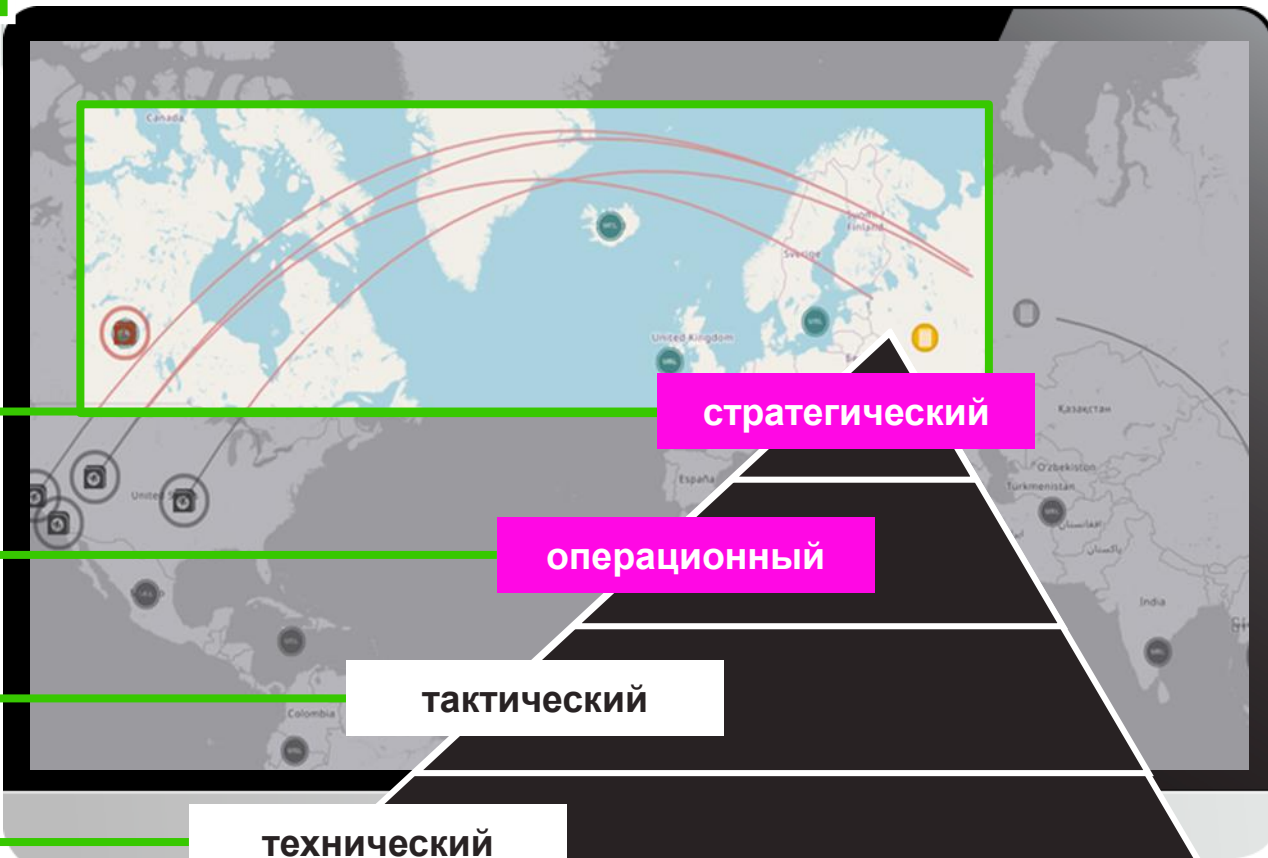


1

Загрузка данных

события, фиды, IoC, бюллетени, источники угроз

- 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.

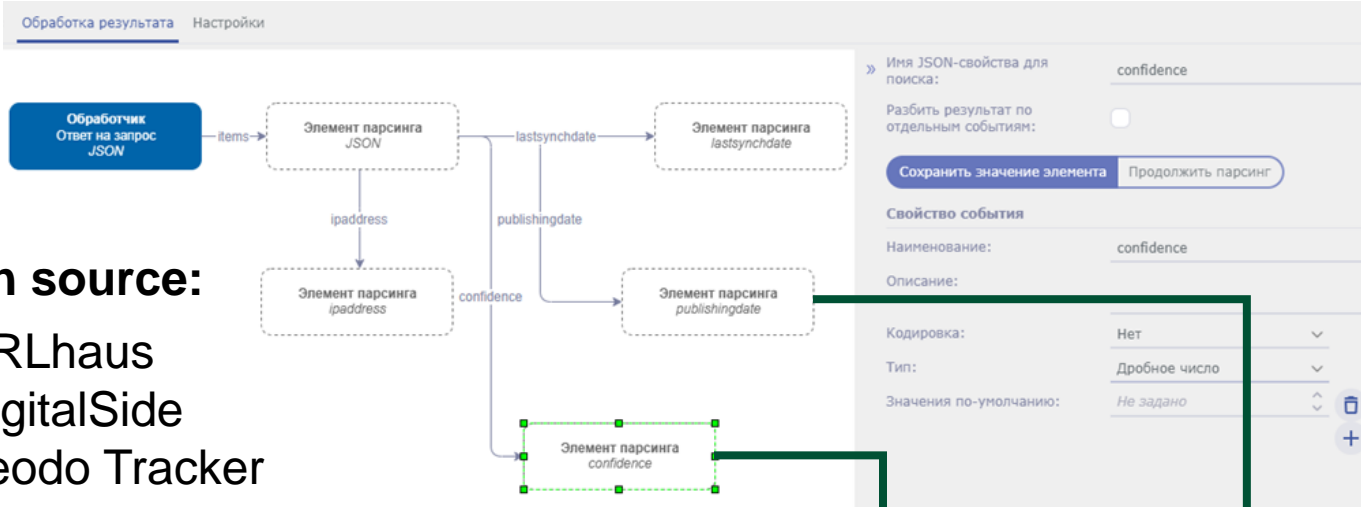
- False-Positive
- Активный
- Не активный
- Отслеживать изменения
- Не отслеживать изменения
- Добавить в Active List
- Поиск в Active list
- Удалить из Active List
- Добавить новый тэг

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/7606PBl16Orc9	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	30	90
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

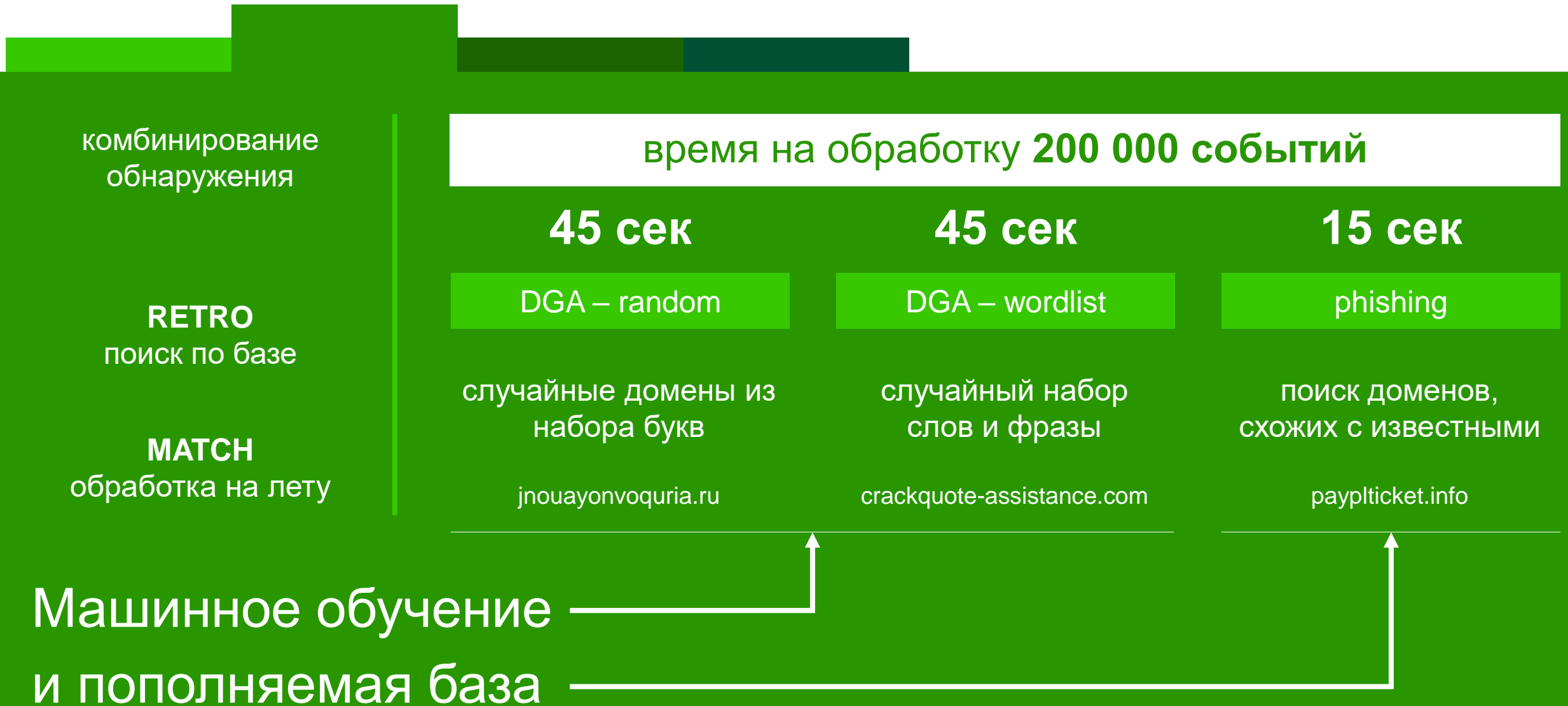
Отправить все IP на FireWall Удалить все IP из FireWall Отметить IOC как FP Отметить IOC как Активный

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

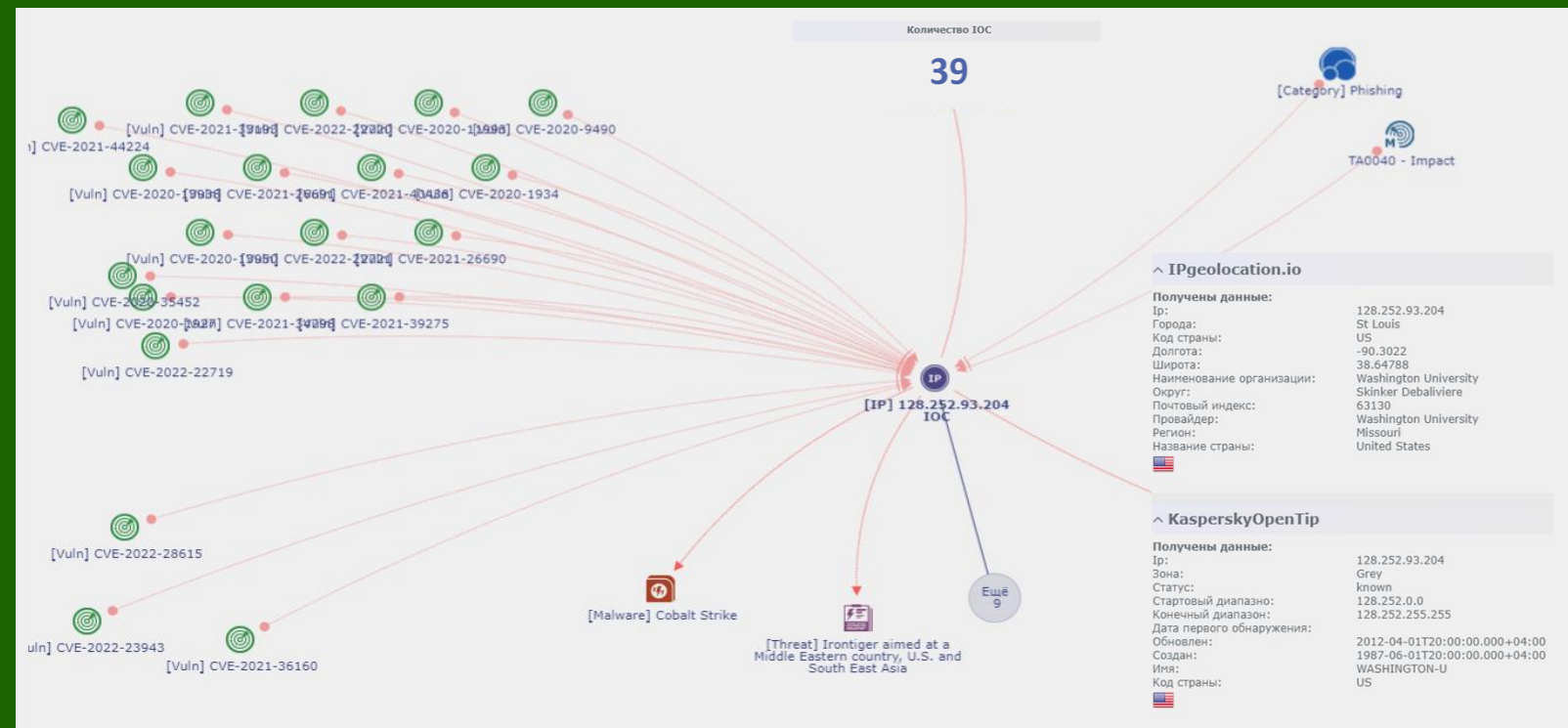
Всего 2 Показывать на странице 20

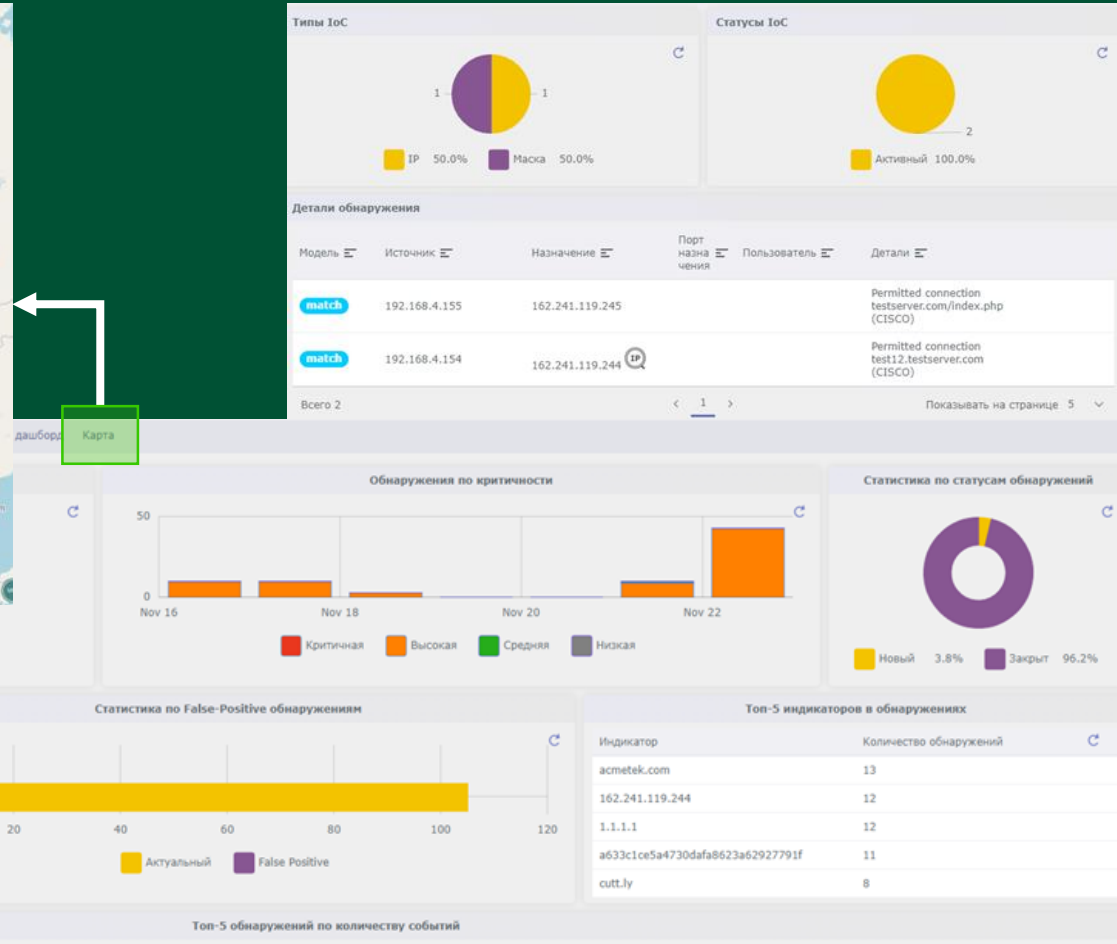
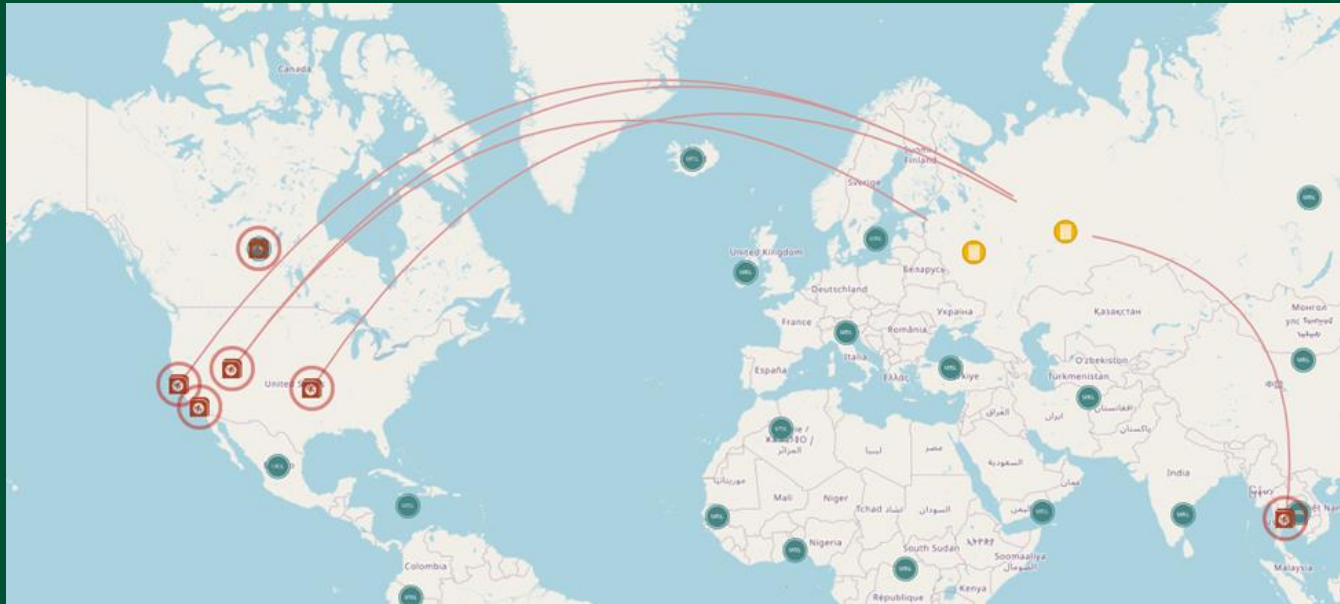
Обнаружение
внутри периметра



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

Стратегический уровень анализа





Полная картина
для реагирования

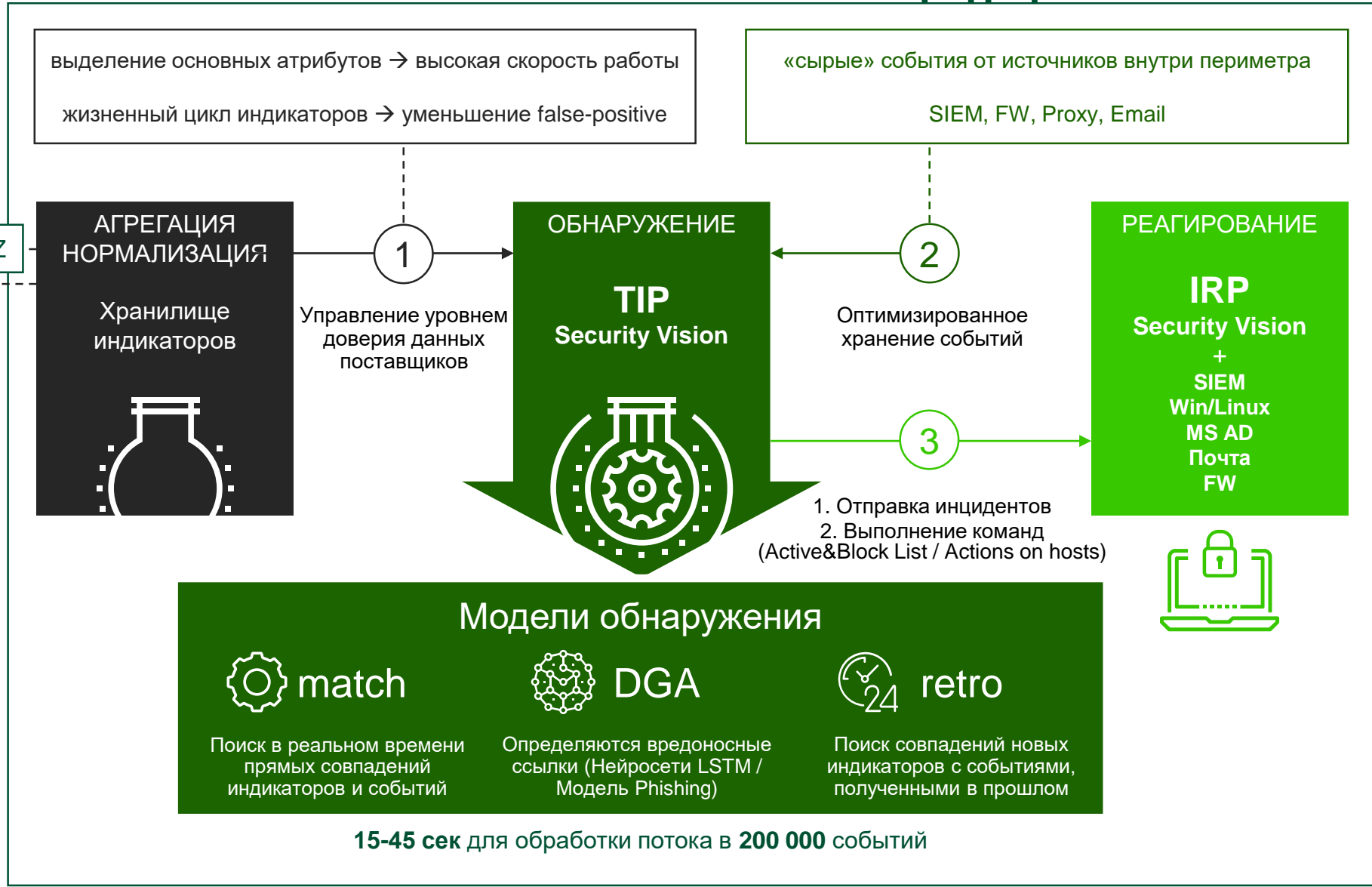
Периметр компании



Поставщики данных
IoC, IoA, IP, URL, хэш



Сервисы обогащения
тактический, операционный и стратегический уровни



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



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

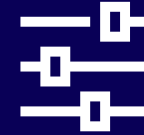


Интеграция с Data Lake и
использование ML модели

~ CRM



Объекты, карточки и
внешний вид



Ролевая модель и
настройка меню

~ BPM

~ BI

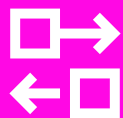


Рабочие процессы и
структура

 **Security
Vision**



Визуализация и
аналитика



Интеграции с внешними
системами



Отчёты и логирование
действий

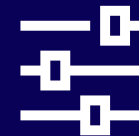
~ RPA

~ Word

~ CRM



Объекты, карточки и
внешний вид



Ролевая модель и
настройка меню

~ BI



Визуализация и
аналитика

~ Word



Отчёты и логирование
действий



массовые операции

фильтрация

сортировка

быстрые ссылки

полнотекстовый поиск

кнопки управления

The screenshot displays a web application interface for object management. 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 contains 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 an object is shown on the right, including fields for ID, creation date, status, and buttons for "Вывод из эксплуатации", "В резерв", "Сломан", and "Категорировать". Below the table, there is a section for "Заявка на устранение" (Incident Report) with fields for ID, creation date, status, and a description of the vulnerability. The description includes a link to a CVE entry: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1064>. The interface also features a pagination control at the bottom of the table.

метки времени

СТИЛИ

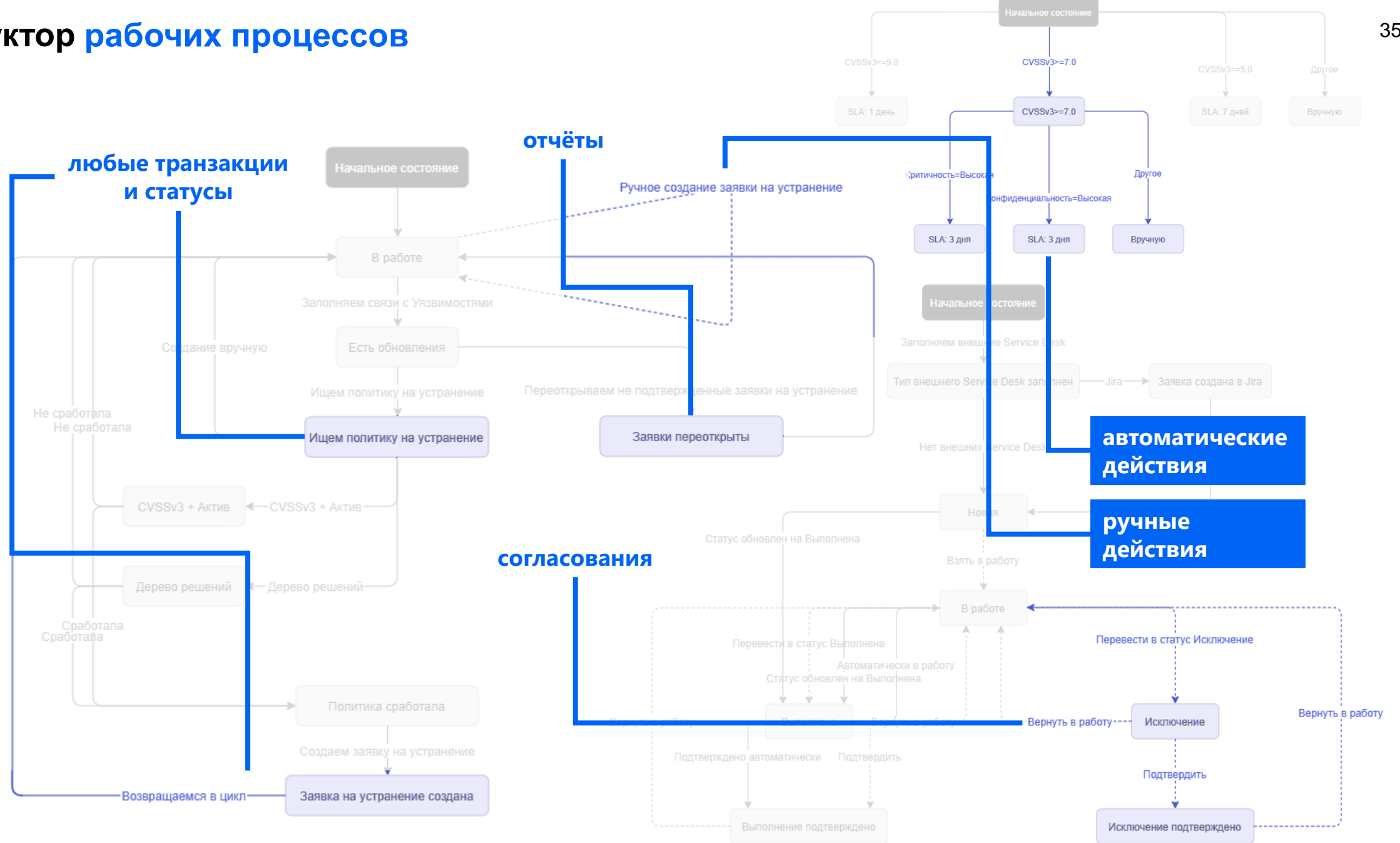
ССЫЛКИ

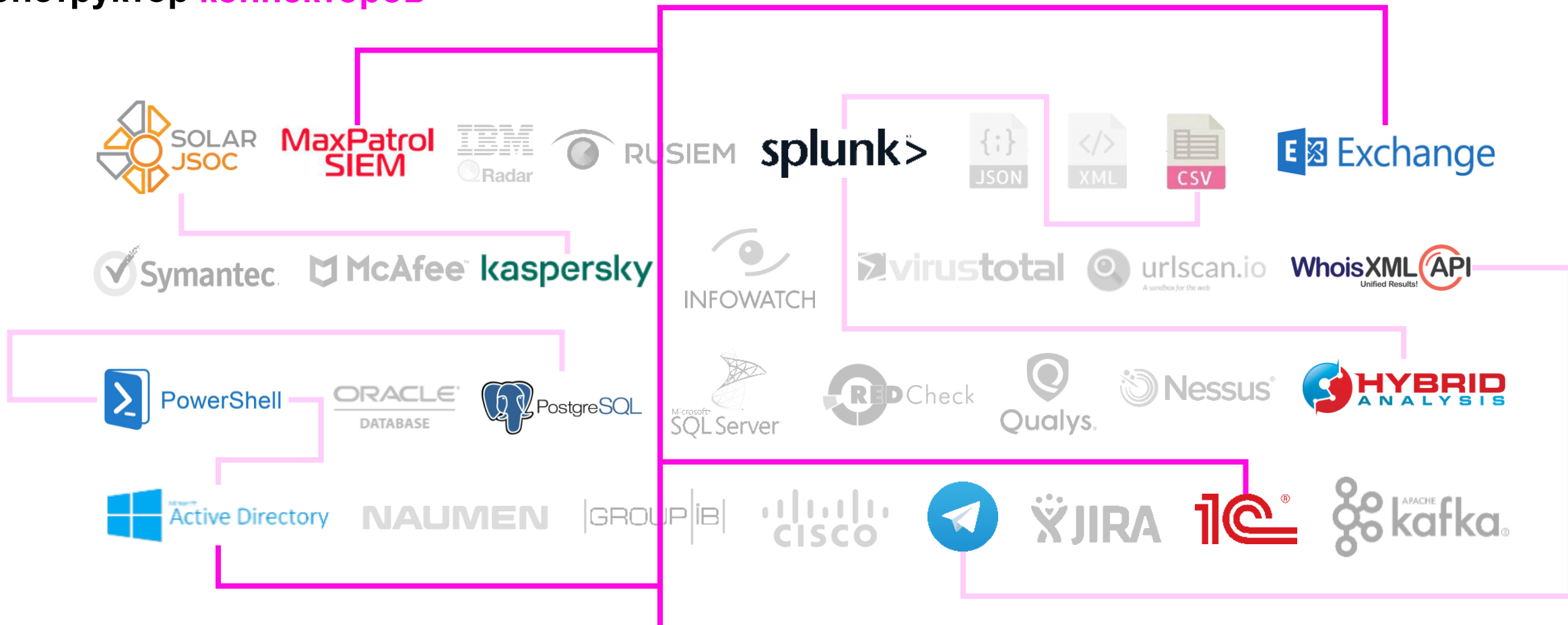
обязательные поля

полная карточка

табличный вид

краткая карточка





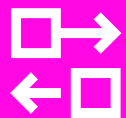
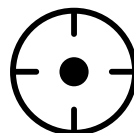
email | Syslog | файлы | БД | API | DNS | SNMP | LDAP | SOAP | скрипты

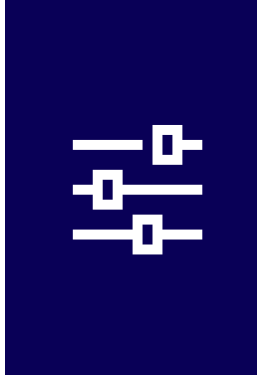
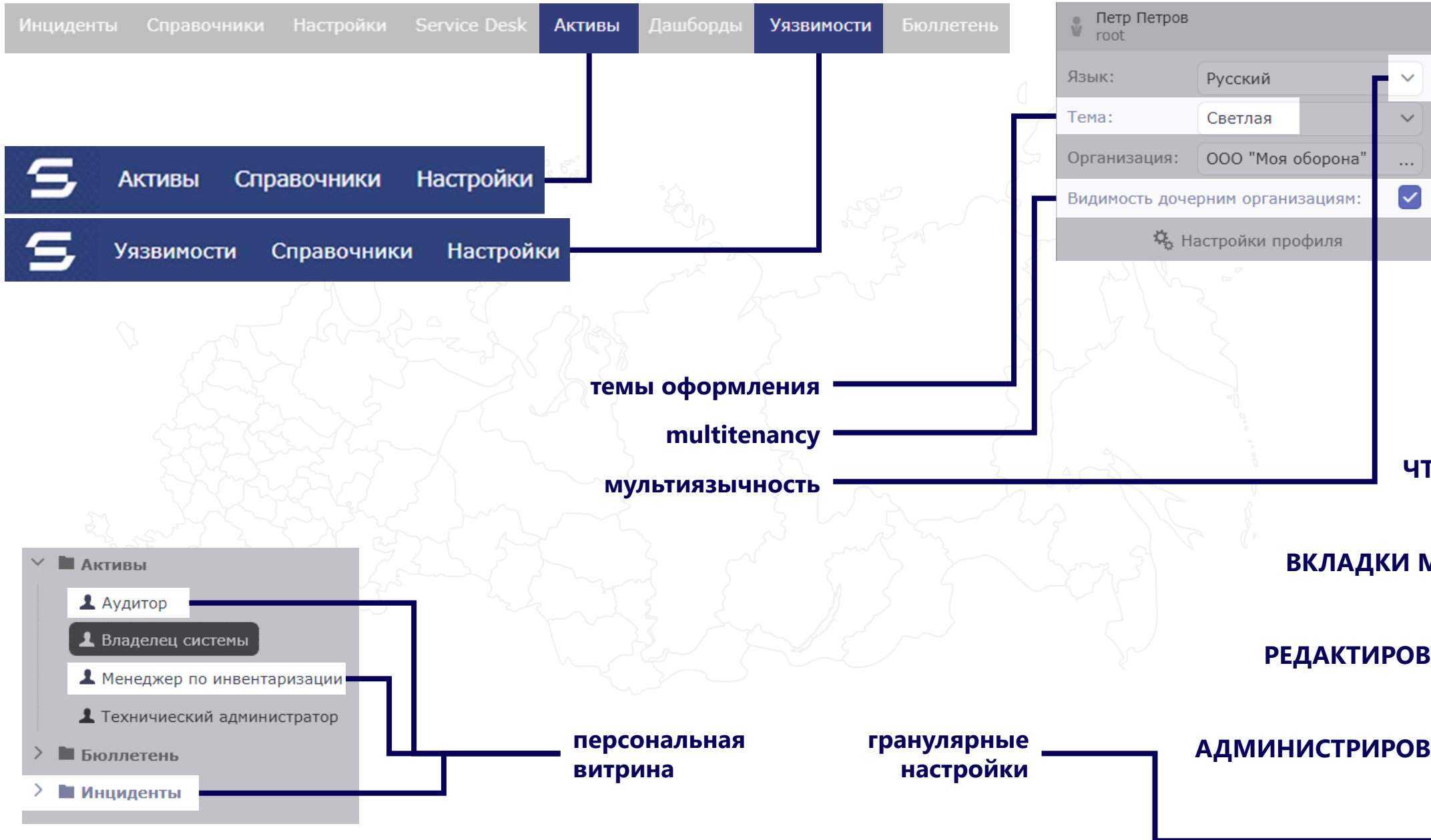
создание новых коннекторов **без участия вендоров**

Сбор и обогащение



Реагирование на события





- ЧТЕНИЕ**
- ВКЛАДКИ МЕНЮ**
- РЕДАКТИРОВАНИЕ**
- АДМИНИСТРИРОВАНИЕ**

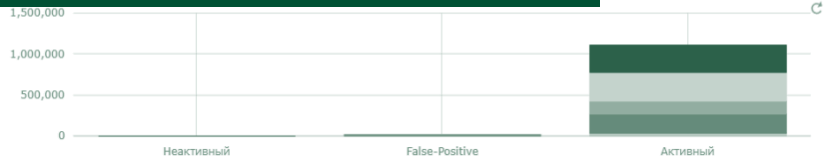
графы связей

карты и планы помещений

различные форматы

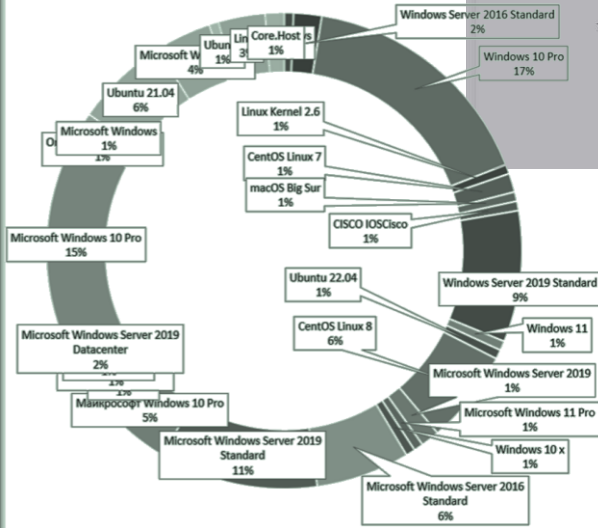


интерактивная аналитика и отчёты по расписанию



The dashboard interface includes a donut chart showing the distribution of servers by OS: Linux (26.5%) and Windows (73.5%). To the right, there are report generation settings such as document format (docx, pdf, etc.), orientation (Portrait, Landscape), and margins. A 'Входной параметр' (Input parameter) field is also visible.

	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 уязвимости:
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

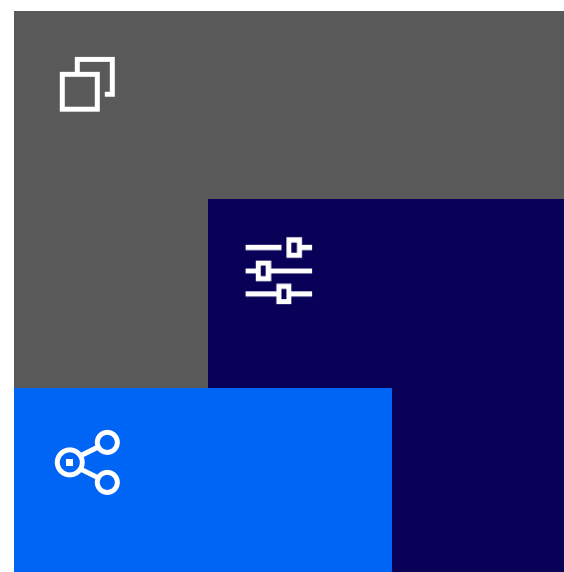
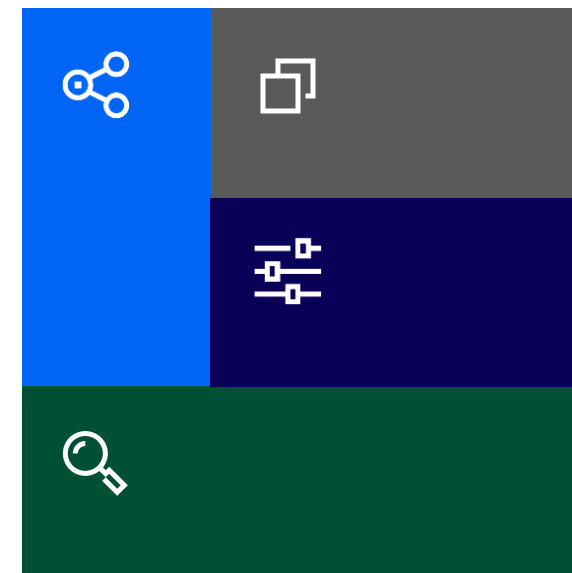
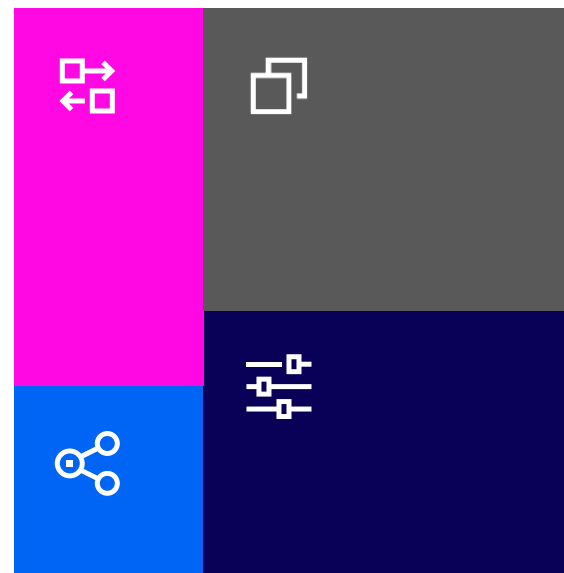
Описание уязвимости:
A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs. An un-authenticated attacker could exploit the vulnerability by sending a specially crafted request to an affected ADFS server. The attacker 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.mscc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1055>

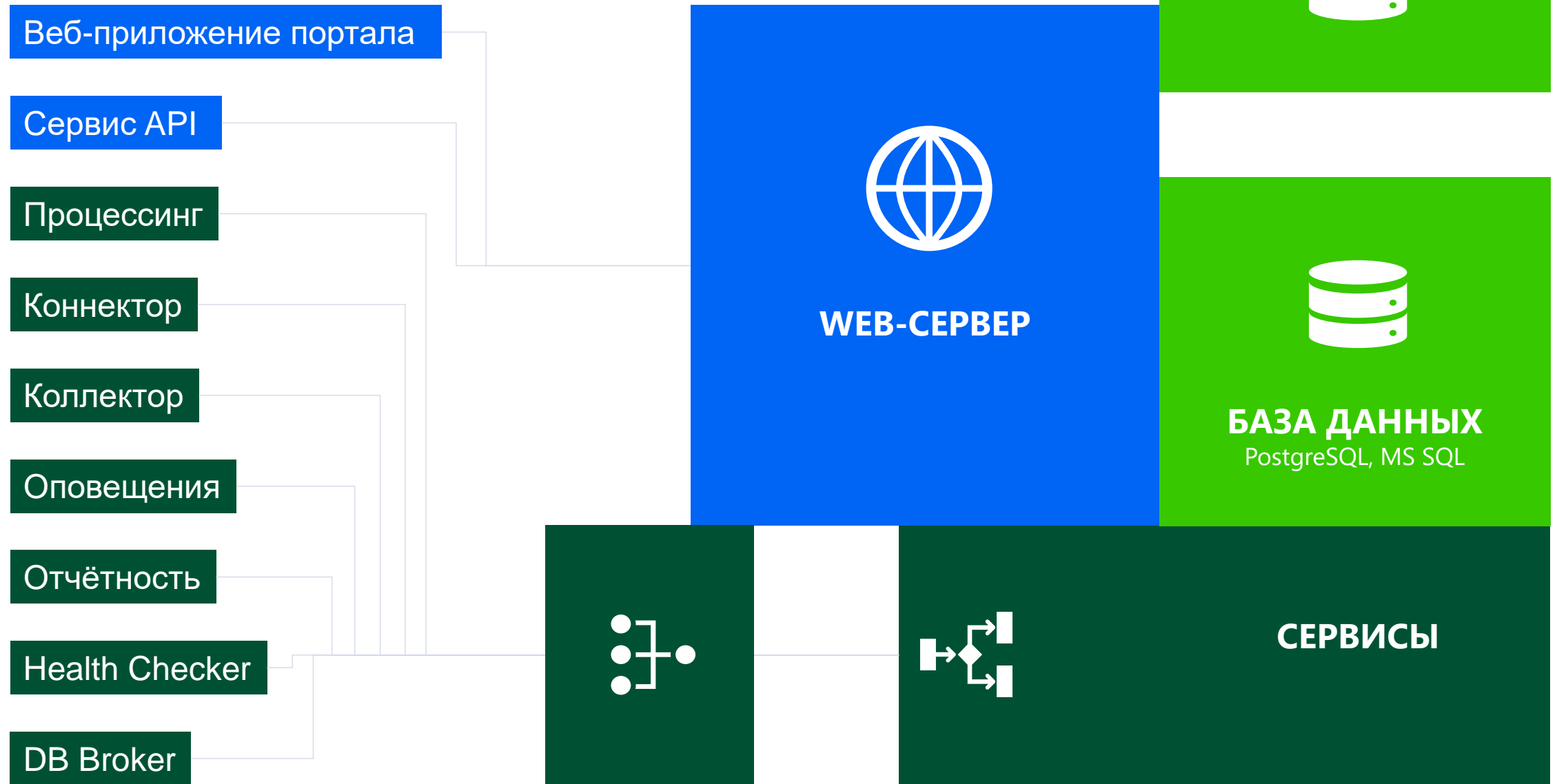


Low-code и No-code
для любых комбинаций

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



Архитектура системы



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



securityvision.ru