Платформа Security Vision IRP

ИНТЕЛЛЕКТУАЛЬНАЯ
БЕЗОПАСНОСТЬ ГРУППА КОМПАНИЙ

Sk Сколково

АРХИТЕКТУРА

SECURITY VISION: АРХИТЕКТУРА

Архитектура универсальной платформы автоматизации

API
Работа с данными

РАБОТА С ДАННЫМИ

WORKFLOW
Рабочие процессы

ГРАФИЧЕСКИЙ РЕДАКТОР И ДВИЖОК РАБОЧИХ ПРОЦЕССОВ

UI/UX
Гибкий интерфейс

УНИКАЛЬНЫЙ ИНТЕРФЕЙС ПОД КАЖДУЮ РОЛЬ: Preview | Role skin

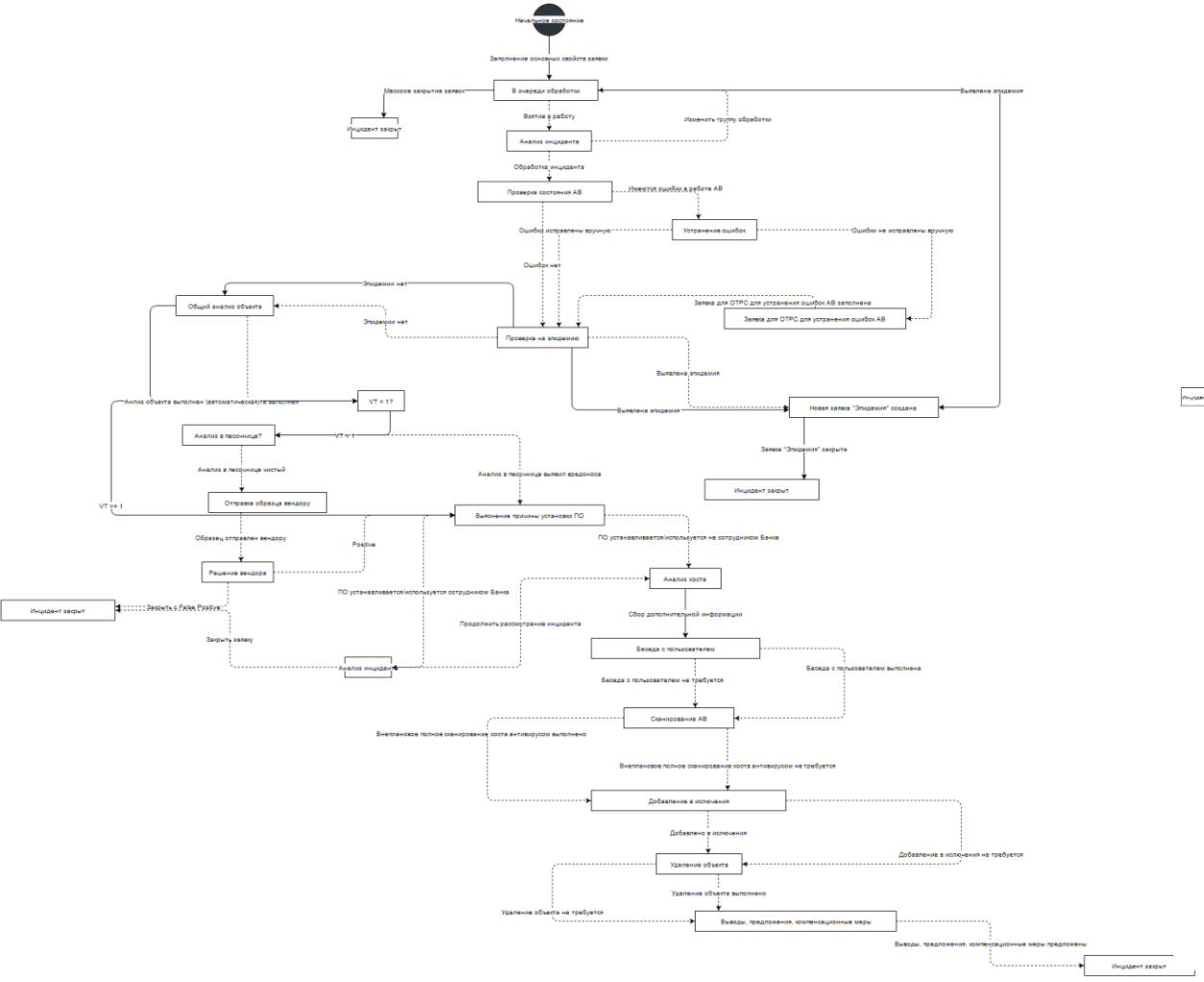
DATA CONNECTOR
Коннекторы данных

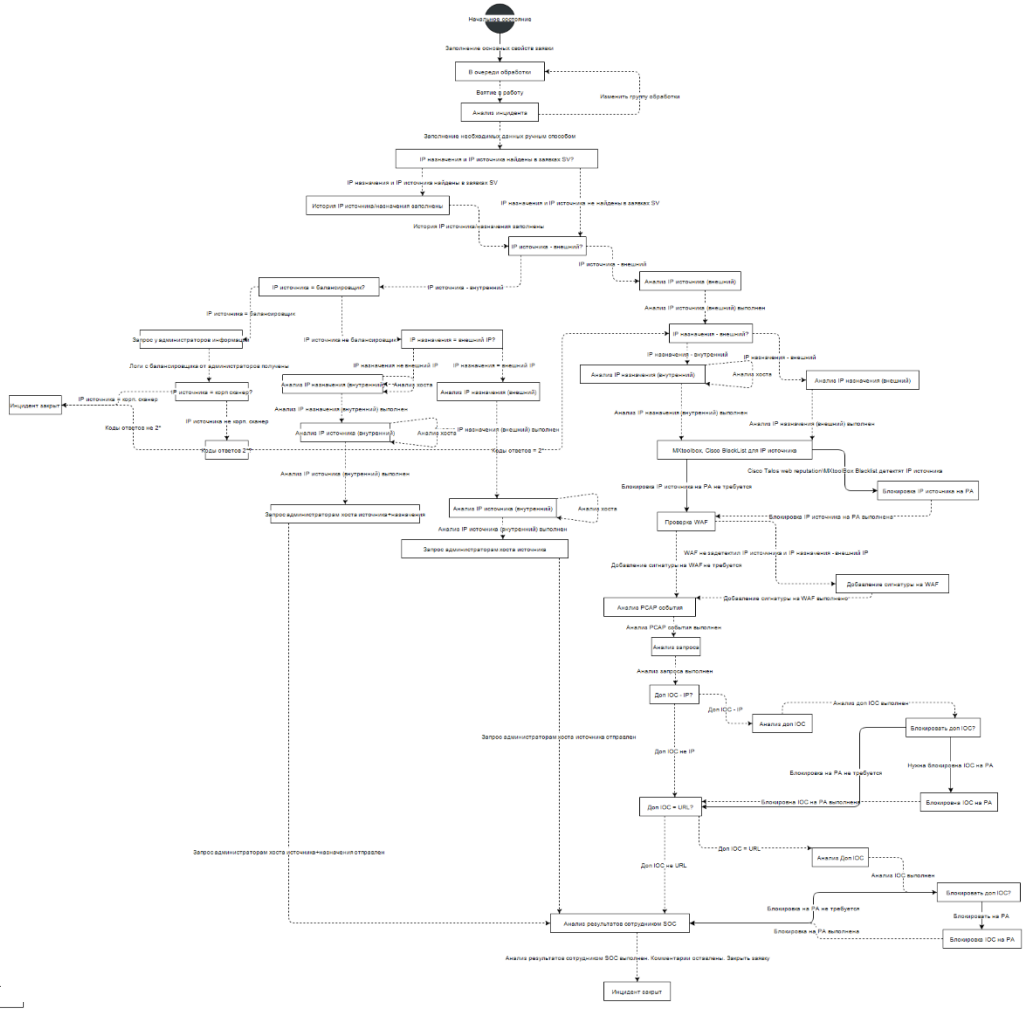
РАБОТА С ПОТОКОМ: Очистка|Валидация|Дедупликация | Фильтрация|Обогащение|Правила корреляции

EXT CONNECTOR
Внешние коннекторы

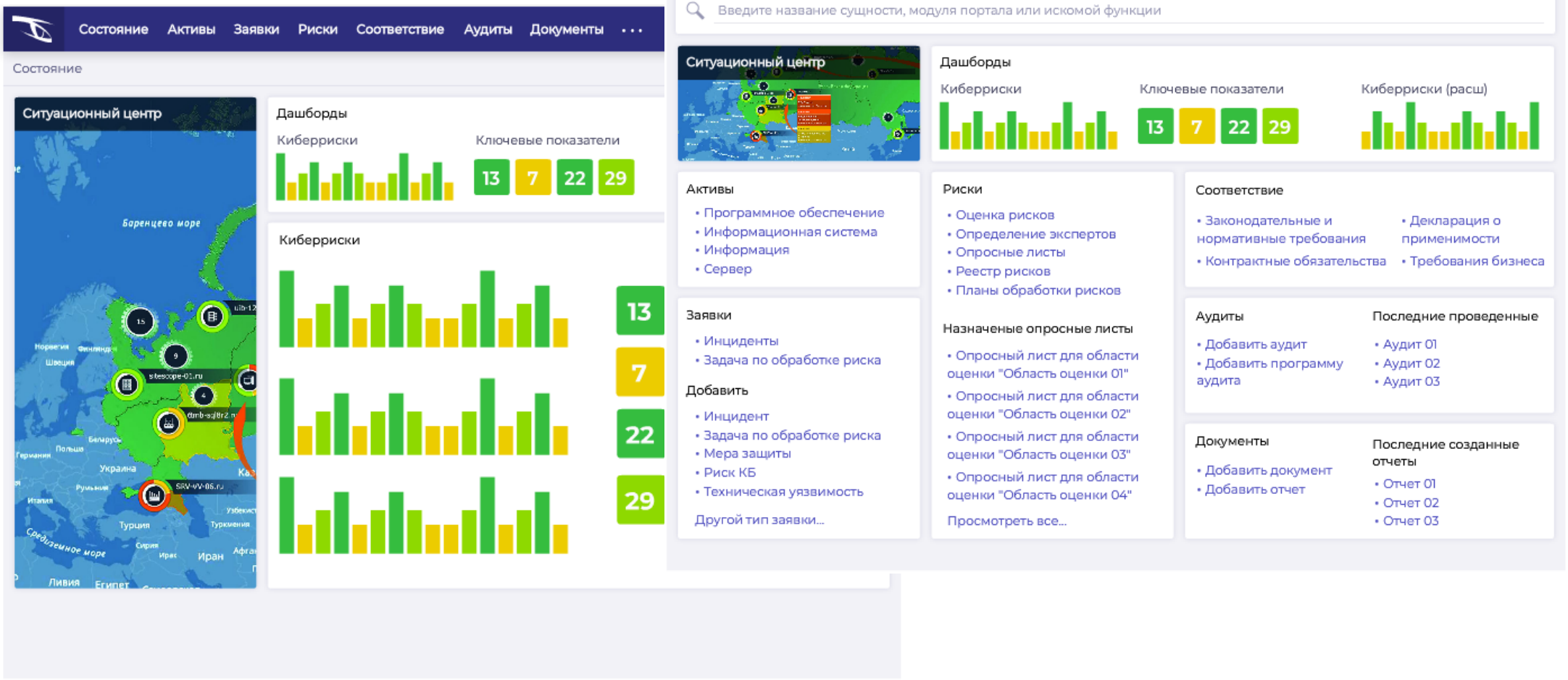
РАБОТА С ИТ и ИБ СИСТЕМАМИ: Обогащение | Выполнение команд

SECURITY VISION: WORKFLOW





SECURITY VISION: UI UX



SECURITY VISION: КОННЕКТОРЫ СБОРА

Коннекторы сбора данных с внешних систем (примеры из практики):

Универсальные коннекторы данных:

- обработка файлов в форматах XML, JSON, CSV, TXT, Binary;
- IMAP;
- POP3;
- MS SQL;
- MySQL;
- PostgreSQL;
- REST;
- SOAP;
- Syslog.

Преднастроенные коннекторы на получение событий с внешних систем:

- Nessus/Tenable
- Skybox (Firewall changes, Vulnerabilities)
- QRadar SIEM
- MaxPatrol SIEM
- Kaspersky Security Center / Kaspersky Security Center IPS
- Symantec Endpoint Protection / Symantec Endpoint Protection IPS
- FireEye / FireEye IPS
- PaloAlto (Reports / Spyware / Virus)
- Tripwire
- Ironport
- OTRS
- FinCERT
- MS SQL
- MySQL
- PosgtreSQL

SECURITY VISION: ВНЕШНИЕ КОННЕКТОРЫ

Коннекторы реагирования и обогащения данных (примеры из практики):

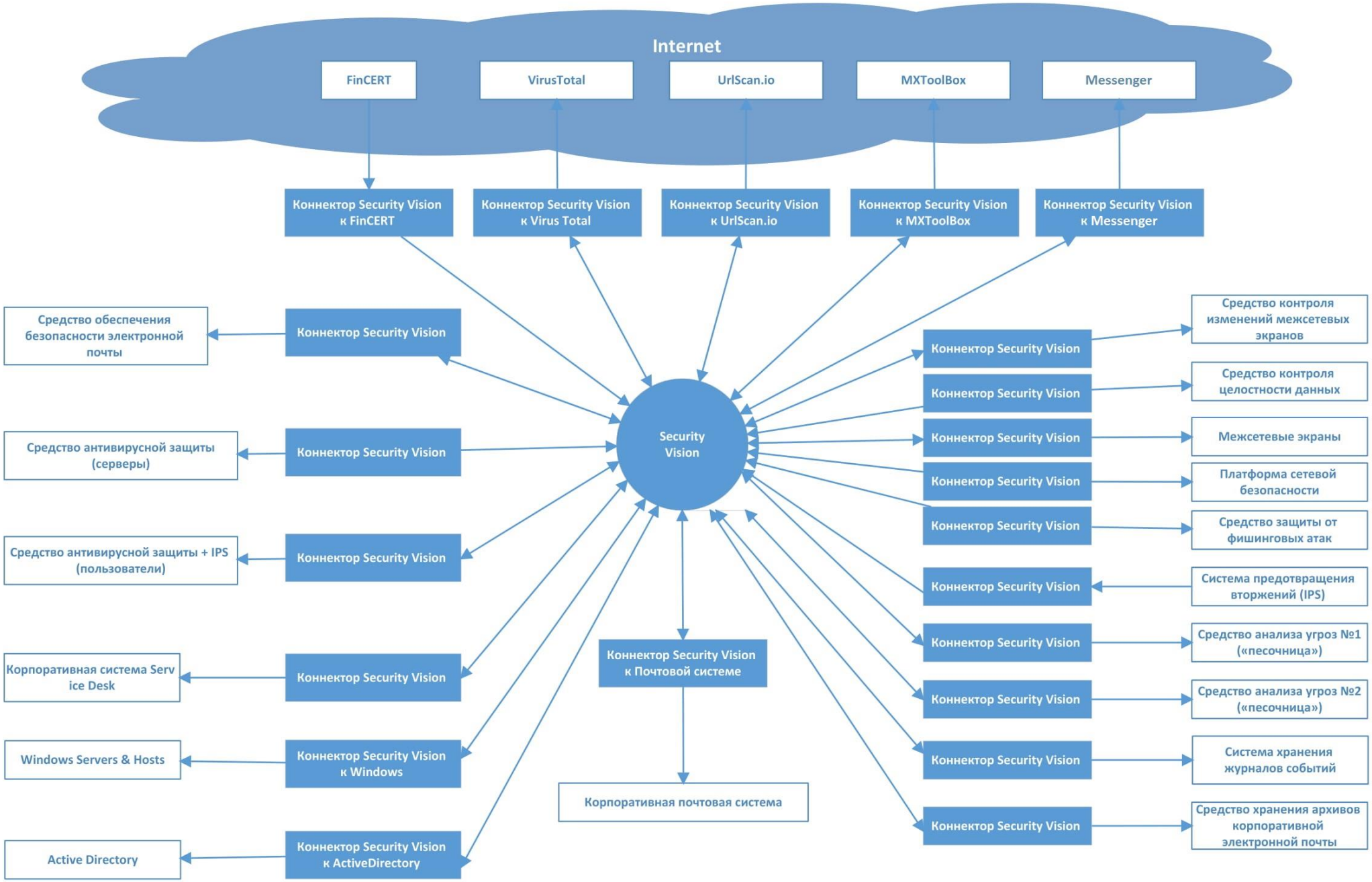
Универсальные коннекторы:

- ActiveDirectory
- DNS
- MS Exchange
- IMAP
- File
- MS SQL
- MySQL
- Oracle
- POP3
- PostgreSQL
- PowerShell
- REST / SMTP / SNMP / SOAP
- SSH / SSH Shell
- MS Windows

Преднастроенные коннекторы взаимодействия с внешними системами:

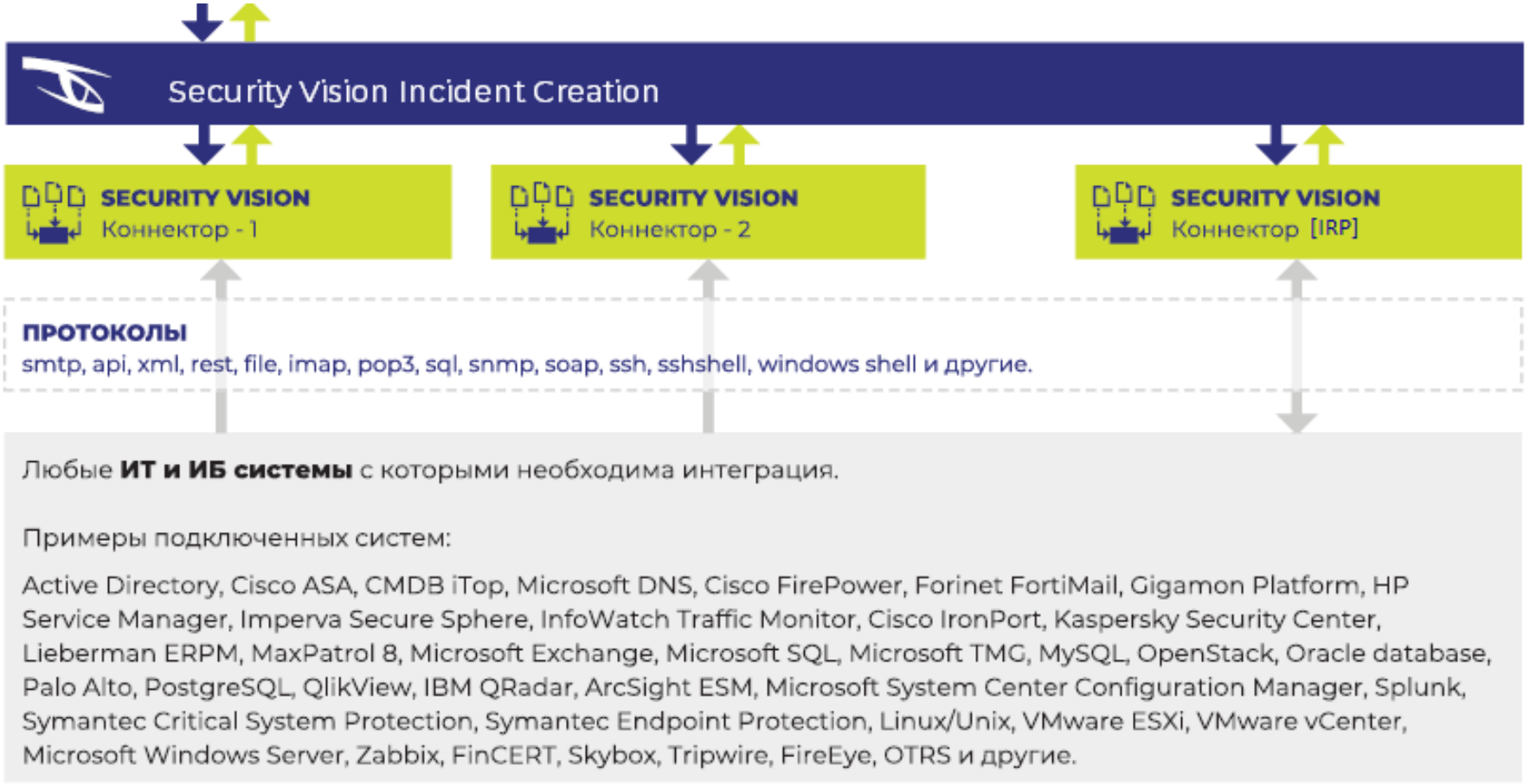
ActiveDirectory , ArcSight Logger , CheckPoint Sandblast, Cisco (API/SNMP/SSH), CMDB iTop, DNS, FirePower, FortiMail, Gigamon (GigaVue-Fm), HPSM (REST/SOAP), Hybrid-Analysis, IMAP, Imperva Secure Sphere, InfoWatch Traffic Monitor, IronPort (REST/SSH), Kaspersky Security Center, Lieberman ERPM, MailArchiva, MaxPatrol 8, MS Exchange (EWS / PowerShell), MS SQL, MS Windows Servers / Desktops, Microsoft TMG, MySQL, MXtoolBox, OpenStack, Oracle DB, PaloAlto, POP3, PostgreSQL, QlikView, Qradar, SCCM, Security Vision, SMTP, Splunk (SMART MONITOR), Symantec Critical System Protection, Symantec Endpoint Protection, TrendMicro, Tripwire, Unix, URLScan.io, VirusTotal, VMware ESXi, VMware vCenter, Zabbix, ФПСУ-IP, ФПСУ-TLS

Схема взаимодействий с Security Vision



SECURITY VISION IRP: СХЕМА ЧАСТЬ 1

SECURITY VISION IRP: СХЕМА ЧАСТЬ 2



Security Vision позволяет осуществлять мониторинг и роботизированное реагирование на инциденты кибербезопасности в режиме реального времени.

Security Vision
IRP

SECURITY VISION IRP: РЕШАЕМЫЕ ЗАДАЧИ

- ✓ Централизованный сбор и корреляция событий безопасности
- ✓ Роботизированная обратная реакция на инциденты
- ✓ Визуализация и принятие управленческих решений
- ✓ Автоматизация процессов ИБ
- ✓ Снижение времени реакции на инциденты

SECURITY VISION IRP

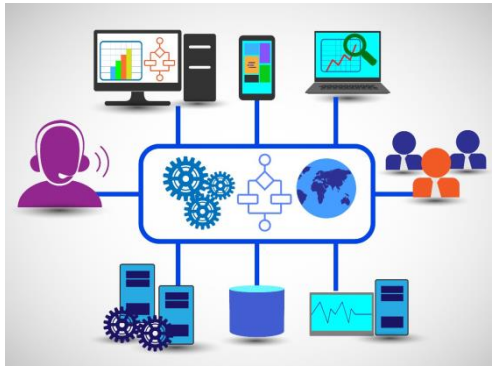
Incident Response Platform [**IRP**] – основные предпосылки построения IRP:

- Снижение риска человеческого фактора и ошибок персонала, привлекаемого на реагирование инцидентов кибербезопасности; [две трети киберинцидентов связаны с человеческим фактором]

- Роботизация [24x7x365] выполнение дежурных процедур оператора в режиме реального времени; [после громких эпидемий вирусов и троянцев шифровалильщиков, стало очевидным, что реагирование это не оповещение, а это автоматическое выполнение действий оператора]

SECURITY VISION IRP

Incident Response Platform [**IRP**] – основные предпосылки построения IRP:

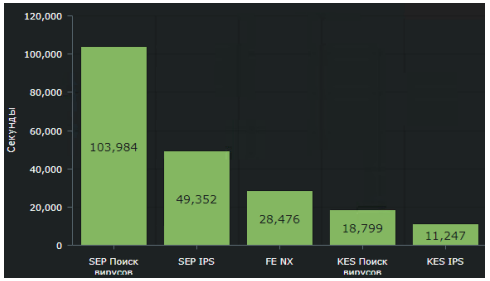


- Автоматическое насыщение и обогащение инцидента информацией о событиях со смежных ИТ и ИБ систем; [двусторонний обмен между ИТ и ИБ системами обеспечивает необходимое и достаточное условия отсутствия белых пятен]

- Глубина проверок (количество и качество); [ручной режим тратит на разбор стандартного инцидента 2 часа с минимальной глубиной проверок – до 10, автоматический за несколько минут способен провести сотни проверок]

SECURITY VISION IRP

Incident Response Platform [**IRP**] – основные предпосылки построения IRP:



- Снижение воздействия инцидентов ИБ за счёт снижения времени реагирования; [время реакции снижает пагубное воздействие случившихся инцидентов]

- Систематизация интеграций: Active Directory, Cisco ASA, CMDB iTop, Microsoft DNS, Cisco FirePower, Forinet FortiMail, Gigamon Platform, HP Service Manager, Imperva Secure Sphere, InfoWatch Traffic Monitor, Cisco IronPort, Kaspersky Security Center, Lieberman ERPM, MaxPatrol 8, Microsoft Exchange, Microsoft SQL, Microsoft TMG, MySQL, OpenStack, Oracle database, Palo Alto, PostgreSQL, QlikView, IBM QRadar, ArcSight ESM, Microsoft System Center Configuration Manager, Splunk, Symantec Critical System Protection, Symantec Endpoint Protection, Linux / Unix, VMware ESXi, VMware vCenter, Microsoft Windows Server, Zabbix, FinCERT, Skybox, Tripwire, FireEye, OTRS и другие.

SECURITY VISION IRP

Incident Response Platform [**IRP**] – основные предпосылки построения IRP:

Удобство и наглядность:

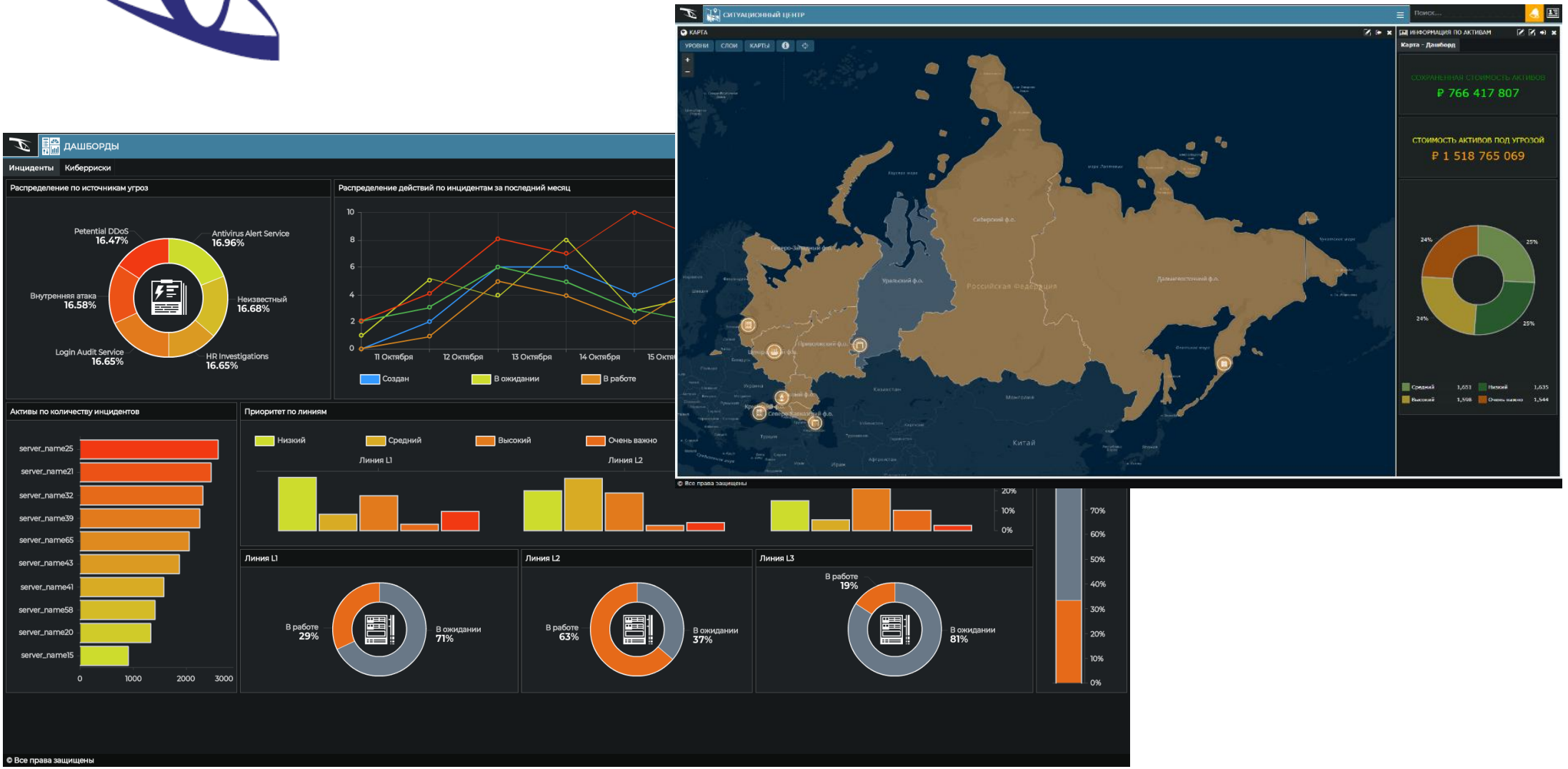
- Построение картинки активных инцидентов на **географической карте;**
- Построение графических схем инцидентов (**взаимосвязь объектов в рамках расследования**);
- Интеграция с более чем одной **SIEM** системой, зонтичная технология;
- Построение отчетов и дашбордов для разных **ролей;**
- **Оповещение** о критичных инцидентах – email, sms, IM.

SECURITY VISION IRP

Примеры проверок:

- Наличие на АРМ антивирусного ПО;
- Проверка URL, хэшей, почтовых адресов на внешних сервисах (VirusTotal, URLScan.io, MxToolBox0);
- Длина пароля в соответствии с политикой безопасности;
- Отсутствие уязвимостей на АРМ или на сервере;
- Проверка файлов в песочницах;
- Контроль целостности;
- Формирование чек-листов и их обработка
- Блокировка IP-адресов на межсетевых экранах;
- Анализ запросов регуляторов;
- Сбор информации об узле/ УЗ в домене;
- Получение параметров и категорирование значимости объекта;
- Контроль изменений параметров АС;
- Наличие обновлений на АРМ;
- Формирование актов и отчетов по стандартам и нормативам;

SECURITY VISION МОДУЛИ: ДАШБОРДЫ

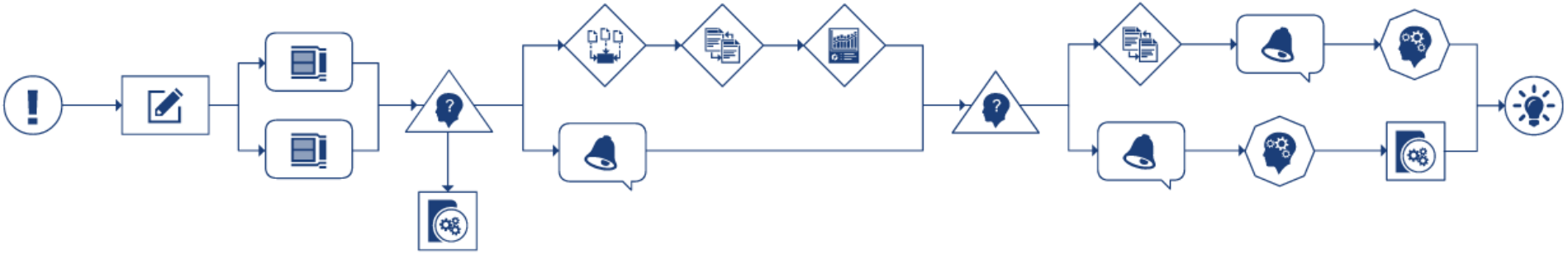


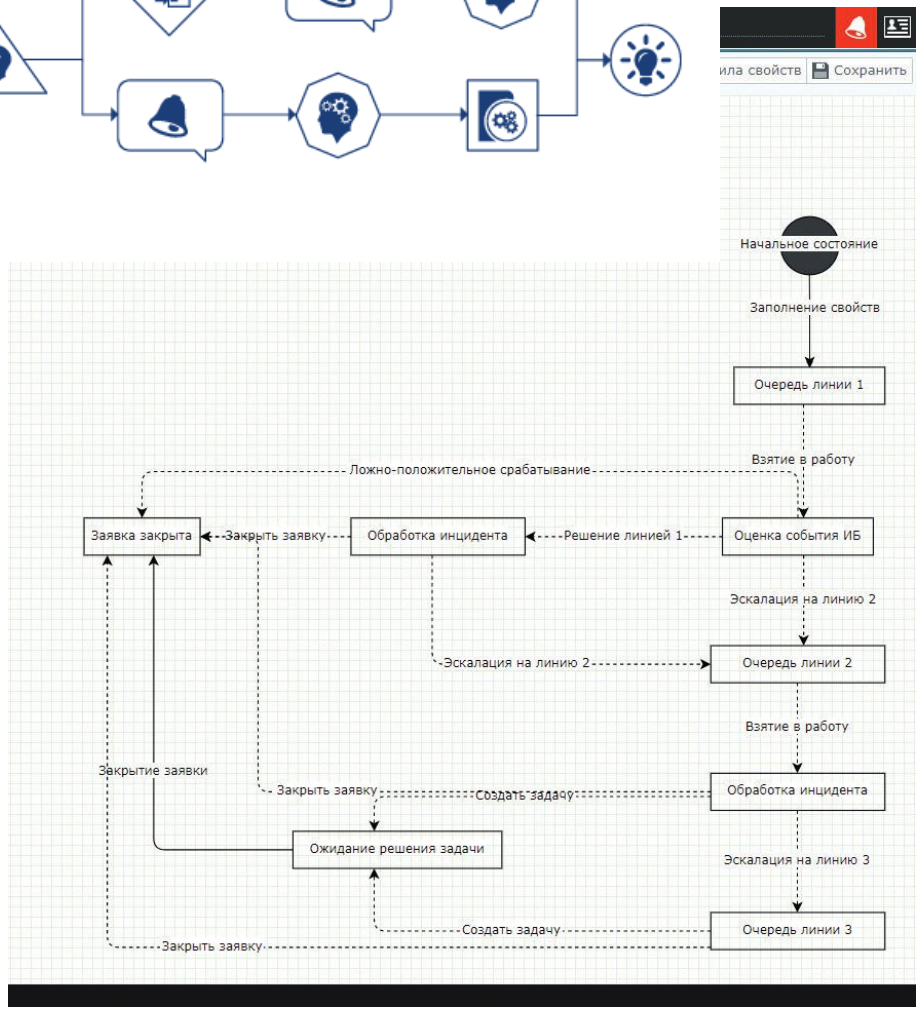
Пример визуализации конструктора **витрины дашбордов** для оператора.
Могут быть представлены **любые формы и представления**.
Доступно разграничение отображения **по ролям и географии.**

SECURITY VISION МОДУЛИ: КАРТА

Пример визуализации **картографической панели** управления оператора в режиме 2D**.** Возможно представление в 3D.

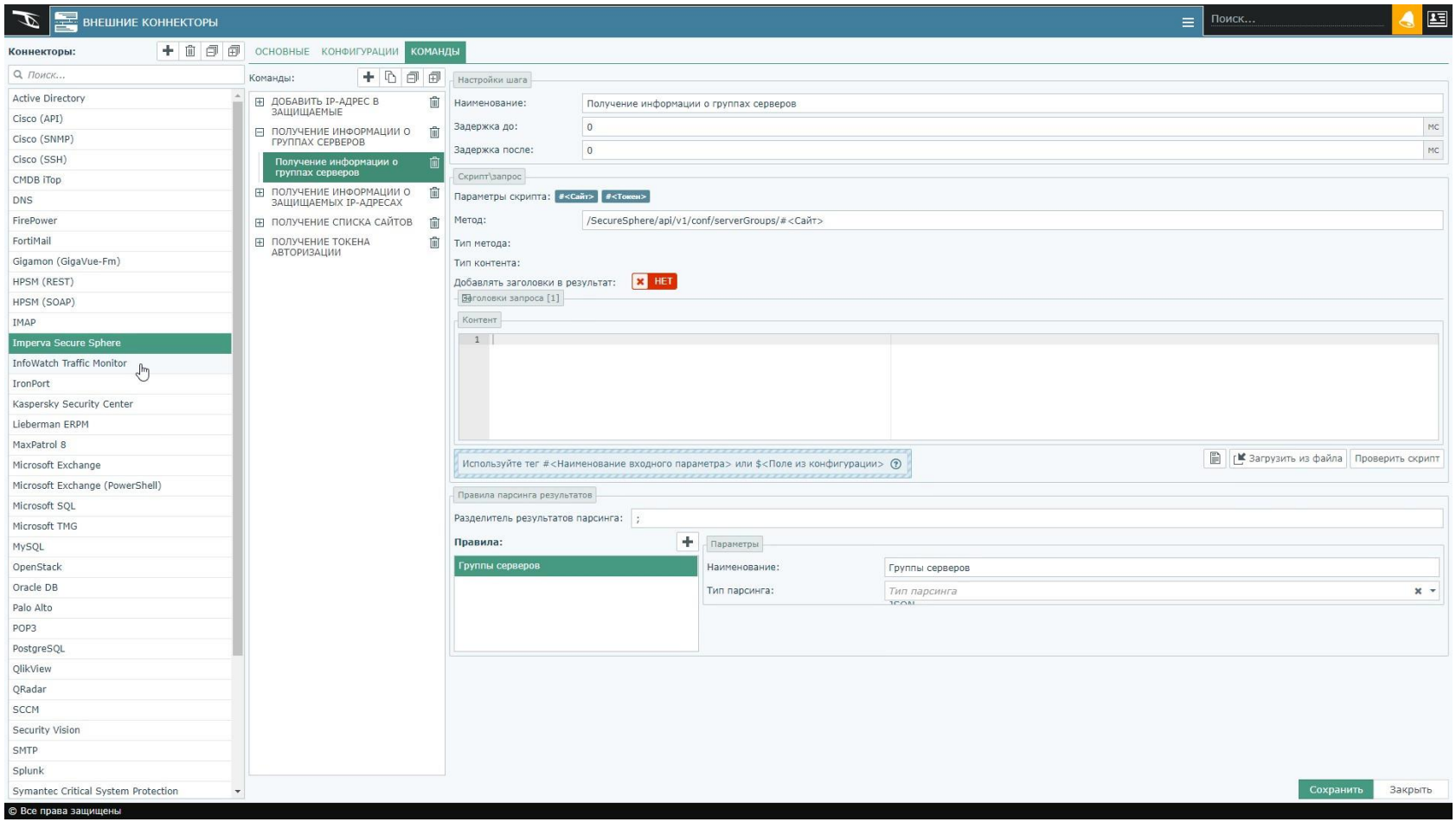
SECURITY VISION МОДУЛИ: РАБОЧИЕ ПРОЦЕССЫ





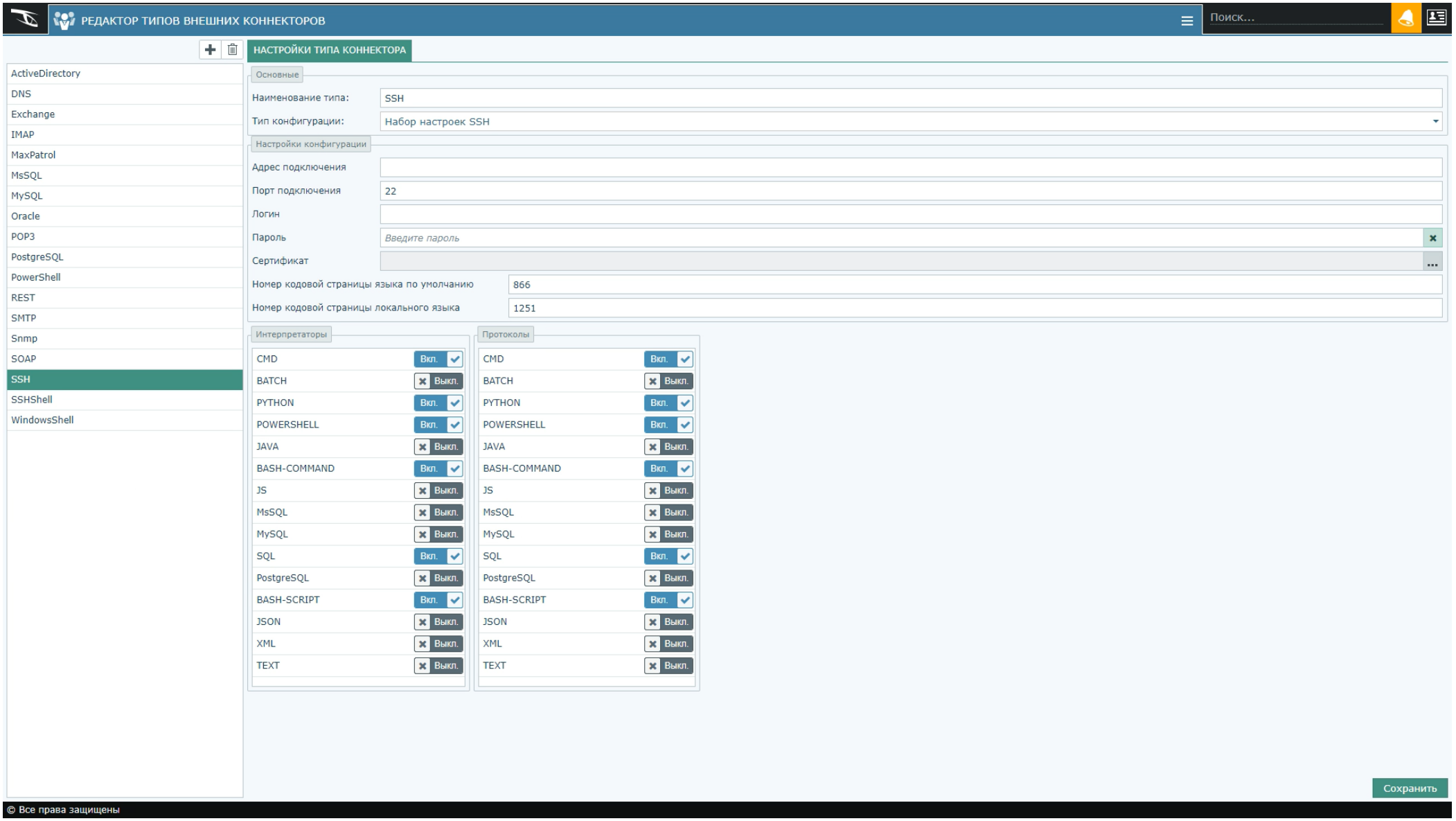
- графическое моделирование рабочих процессов управления инцидентами;
- интерактивное сопровождение процесса управления инцидентами в режиме реального времени;
- управление командами SOC: L1/L2/L3 в режиме реального времени.

SECURITY VISION МОДУЛИ: КОННЕКТОРЫ ДАННЫХ



Пример визуализации **универсальных коннекторов** связи, позволяющих обеспечить односторонние и двусторонние связи системы с ИТ и ИБ системами для достижения обратной автоматической реакции в соответствии со сценариями реагирования.

SECURITY VISION МОДУЛИ: КОННЕКТОРЫ ДАННЫХ



SECURITY VISION МОДУЛИ

Проектные внедрения могут быть дополнены опционными или индивидуальными модулями, такими как:

1. Конструктор активов
2. Конструктор заявок/инцидентов
3. Конструктор рабочих процессов
4. Географическая карта 2D/3D
5. Конструктор/витрина дашбордов
6. Конструктор отчётов
7. Конструктор оповещений
8. Конструктор управления рисками
9. Конструктор управления реагированием
10. Конструктор коннекторов данных
11. Конструктор внешних коннекторов
12. Управление жизненным циклом уязвимостей
13. Конструктор управления соответствием и база документов, регламентирующих порядок обеспечения ИБ
14. Конструктор аудитов

SECURITY VISION МОДУЛИ

Проектные внедрения могут быть дополнены опционными или индивидуальными модулями, такими как:

14. Конструктор аудитов
15. Управления соответствием GDPR
16. Управления соответствием КИИ (Критическая информационная инфраструктура)
17. Конструктор мониторинга доступности
18. Управление осведомленностью (Awareness) в области ИБ
19. Учет лицензий и сервисных контрактов
20. Ядро корреляции
21. Интеграция с CERT (ГосСОПКА, FinCERT)
22. Инвентаризация и контроль целостности
23. Контроль за изменениями в ИТ-инфраструктуре
24. Кластер аналитики BigData: ML, OLAP, Hadoop sample
25. Взаимодействие с корпоративными системами и др.

SECURITY VISION: ПРИМЕРЫ ЗАКАЗЧИКОВ

Среди клиентов компании: Сбербанк России, Банк Открытие, РОСТЕХ, Мультикарта, Гознак, Главгосэкспертиза, Федеральная служба охраны Российской Федерации, СДМ Банк, Министерство спорта России, Газпроммедиа Холдинг, Майтро Интернейшнл, Гидромашсервис и другие.

SECURITY VISION: СЕРТИФИКАЦИЯ

Идет сертификация по **4 уровню контроля отсутствия НДВ**. Получено решение во ФСТЭК и положительное заключение лаборатории.

Включен в **Единый реестр российских программ для электронных вычислительных машин и баз данных.**

SECURITY VISION

УВИДЕТЬ БЕЗОПАСНОСТЬ

www.securityvision.ru

Участник