R-Vision

Incident Response Platform **(IRP/SOAR)**

www.rvision.ru

Линейка продуктов R-Vision

IRP

Автоматизация мониторинга и реагирования на инциденты

SENSE

Продвинутая аналитика для выявления угроз и аномалий

TIP

Платформа анализа информации об угрозах

TDP

Автоматизированное обнаружение атак с помощью имитации ИТ-инфраструктуры

КИИ

Автоматизация категорирования объектов КИИ и процесса обеспечения соответствия 187-ФЗ

SGRC

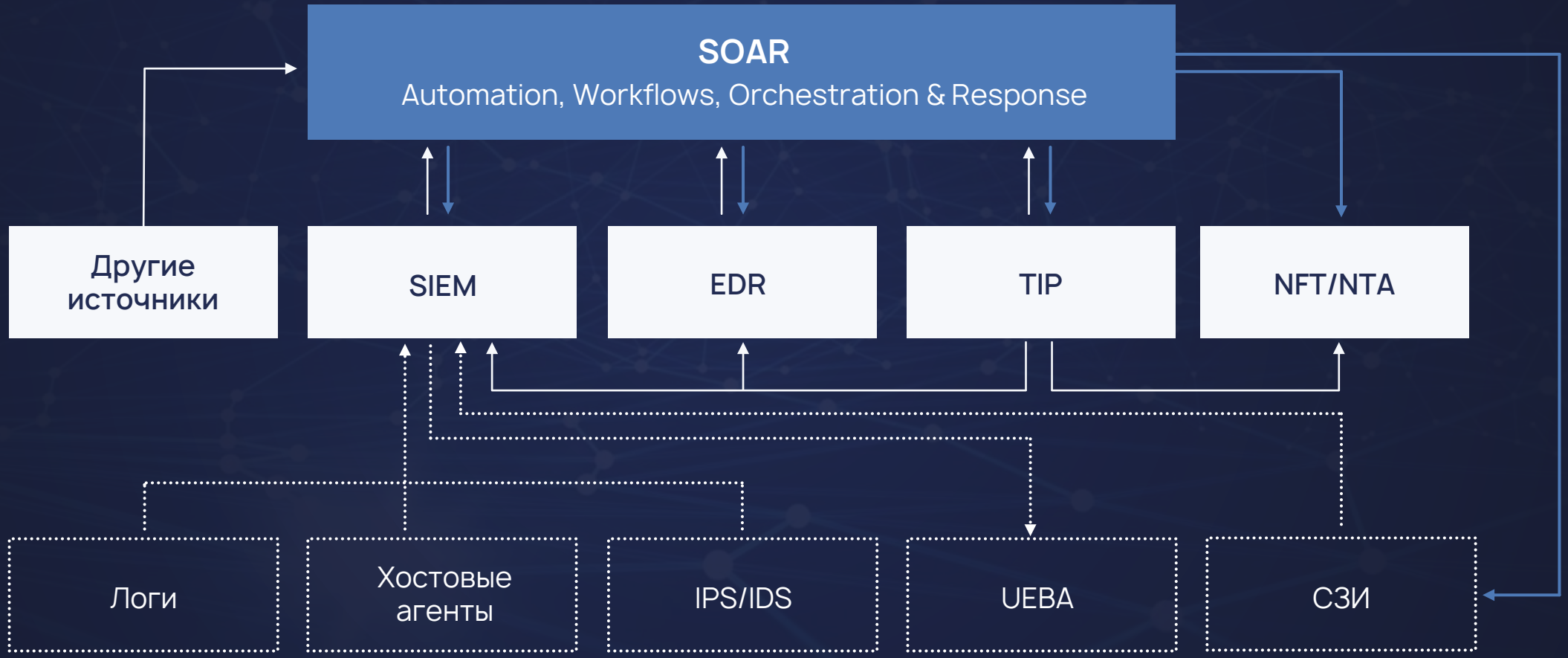
Управление ИБ, оценка рисков и комплаенс-контроль

CERS

Построение центра реагирования на угрозы и уязвимости

Решения класса SOAR

Место IRP/SOAR в SOC



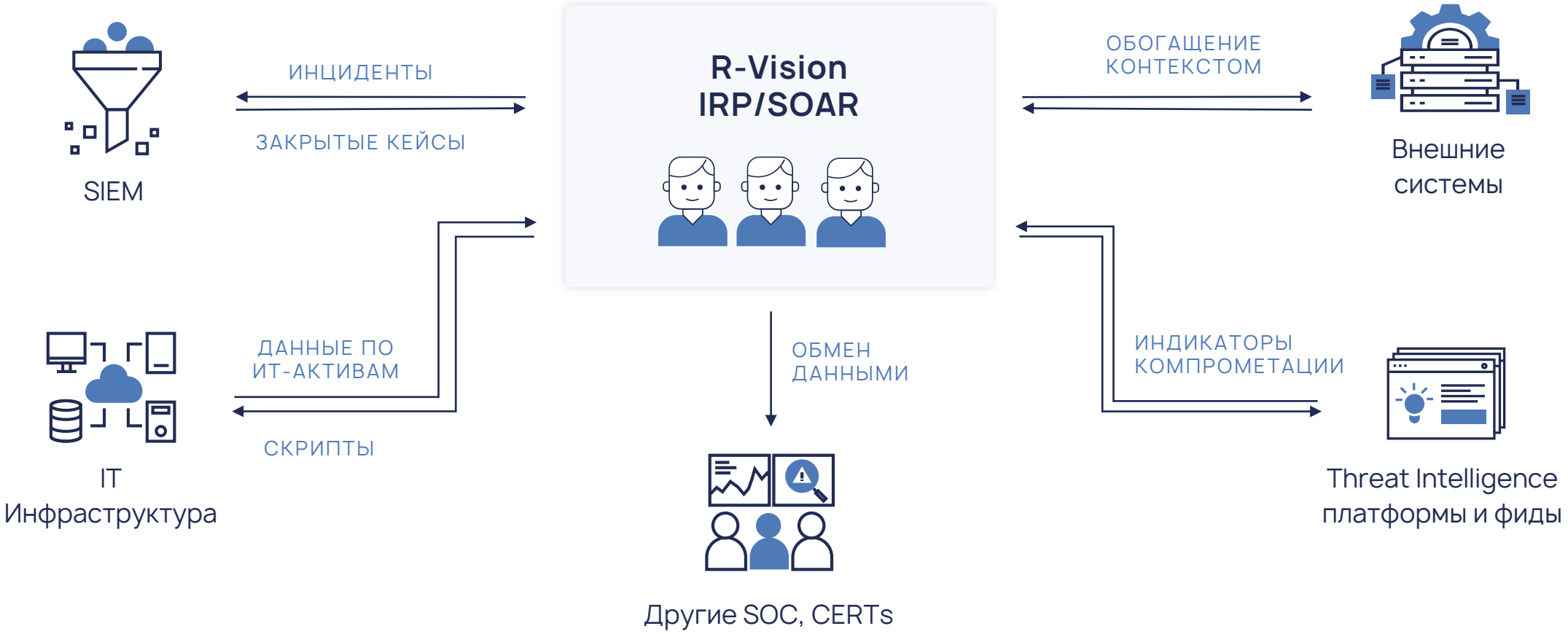
IRP/SOAR vs SIEM vs Service Desk

Решаемые задачи	SIEM	IRP/SOAR	SD
Сбор событий, логов	✓		
Сбор, формирование инцидентов	✓	✓	
Управление жизненным циклом инцидентов (workflow)	✓	✓	✓
Автоматизация реагирования на инциденты		✓	
Обогащение контекстом, сбор данных из сторонних систем		✓	
Динамические сценарии реагирования		✓	
Оркестрация средств защиты и других систем		✓	
Контроль за выполнением задач во внешних системах		✓	✓
Визуализация (отчеты, метрики, KPI)	✓	✓	✓
Контроль инфраструктуры (включая инвентаризацию)	✓	✓	✓
Ресурсно-сервисная модель		✓	✓
Обмен информацией по инцидентам		✓	

Схема работы R-Vision IRP

- Уведомление
- Локализация
- Внедрение мер
- Восстановление
- Расследование
- Отчетность

R-Vision IRP - единая точка работы аналитика по инциденту



Ключевые возможности R-Vision IRP

Агрегация

инцидентов, сведений и контекста в единой системе

Интеграция

с любыми решениями и СЗИ (SIEM, ITSM, AV, VS и другими)

Визуализация

информации на различных уровнях представления

Контроль

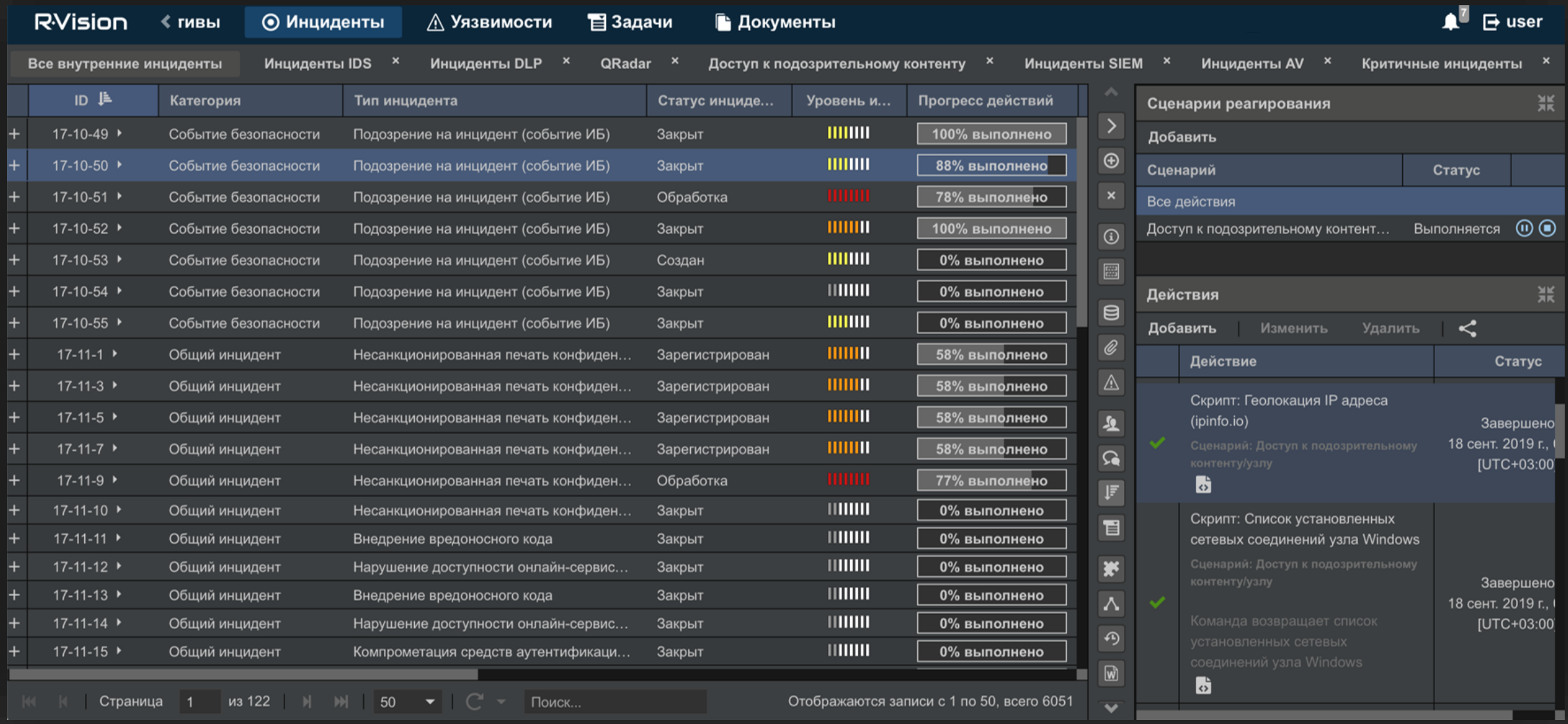
Активов, установленного ПО, привилегий пользователей, метрик ИБ

Автоматизация

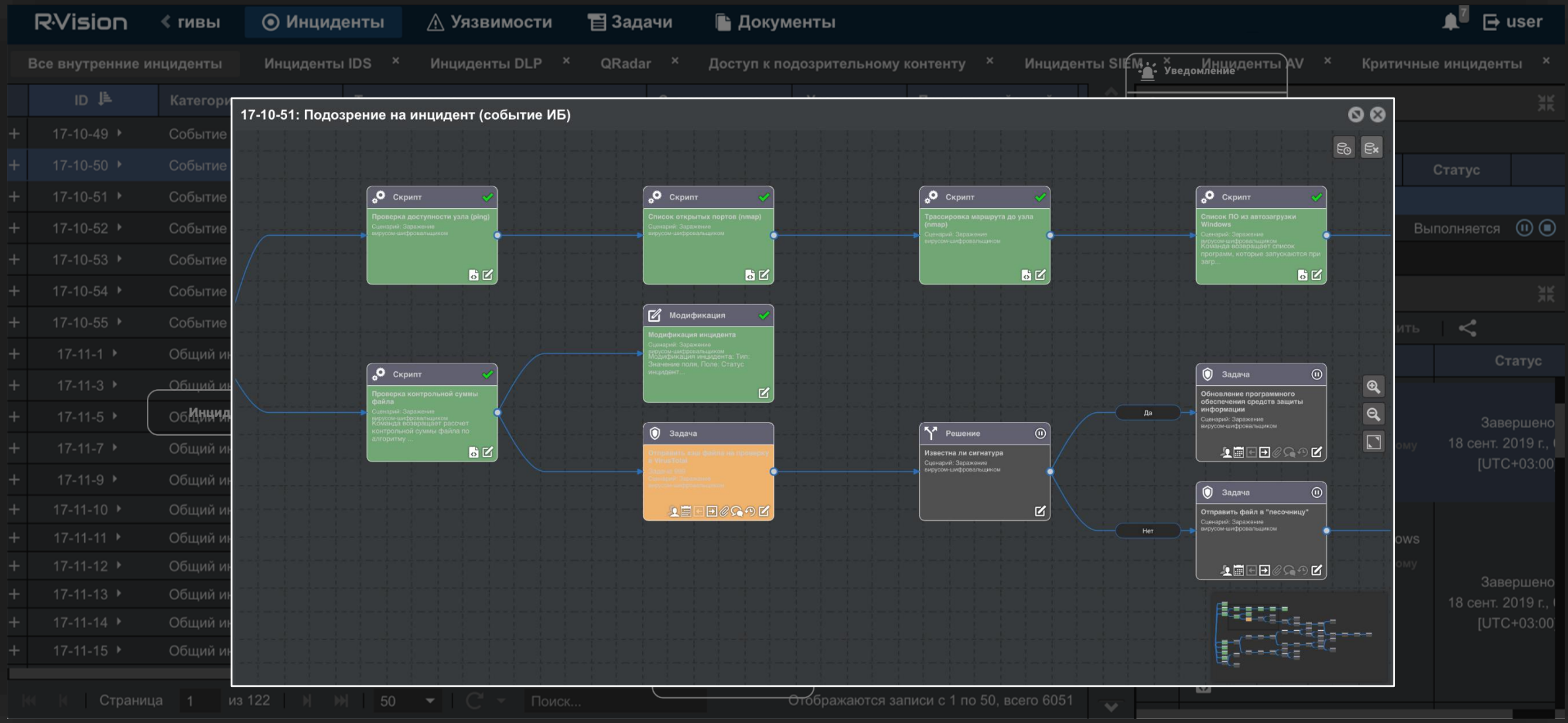
реагирования на инциденты, workflow обработки инцидентов в SOC, управления уязвимостями

Отчетность

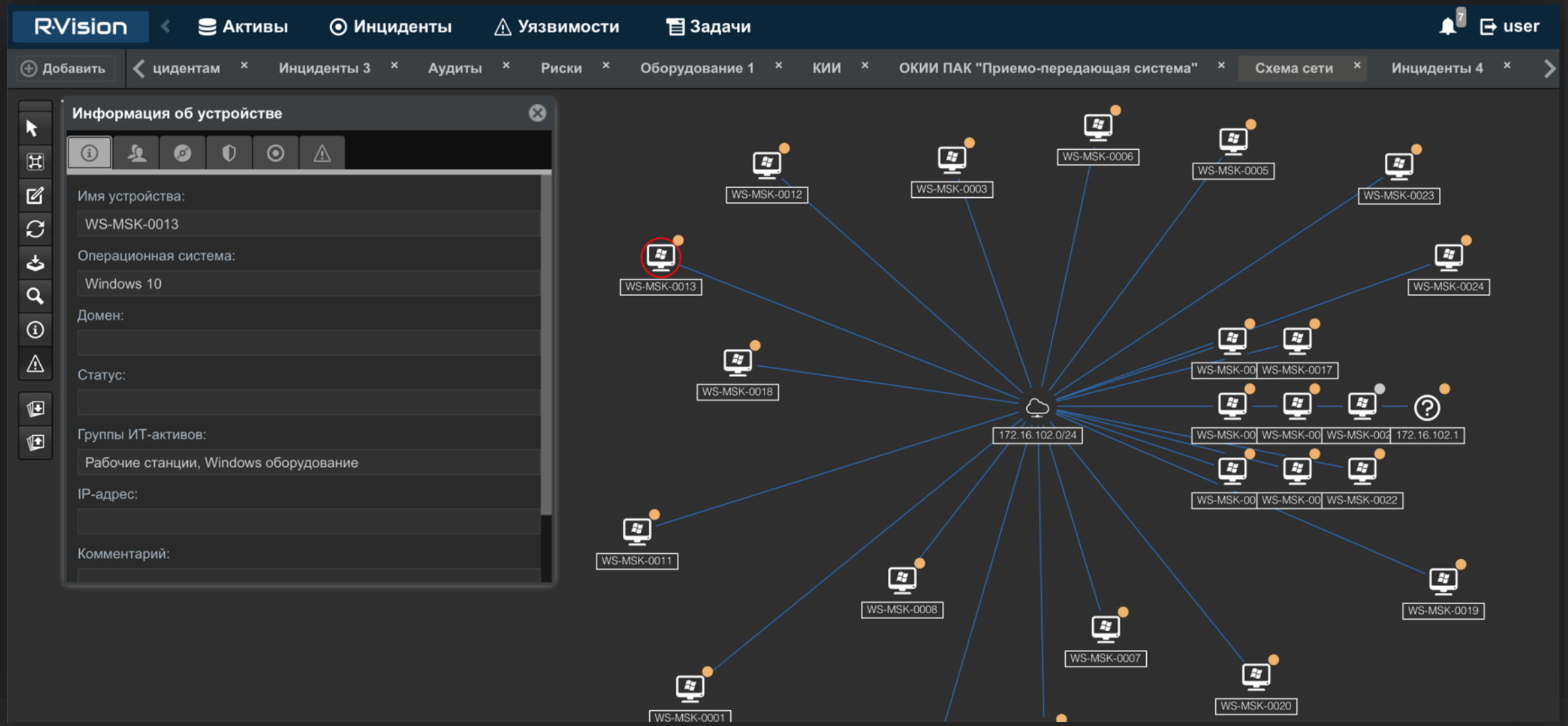
Формирование и экспорт отчетов


RVision
гивы
Инциденты
Уязвимости
Задачи
Документы
user
Все внутренние инциденты
Инциденты IDS
Инциденты DLP
QRadar
Доступ к подозрительному контенту
Инциденты SIEM
Инциденты AV
Критичные инциденты
ID
Категория
Тип инцидента
Статус инциде...
Уровень и...
Прогресс действий
17-10-49 Событие безопасности Подозрение на инцидент (событие ИБ) Закрыт 100% выполнено
17-10-50 Событие безопасности Подозрение на инцидент (событие ИБ) Закрыт 88% выполнено
17-10-51 Событие безопасности Подозрение на инцидент (событие ИБ) Обработка 78% выполнено
17-10-52 Событие безопасности Подозрение на инцидент (событие ИБ) Закрыт 100% выполнено
17-10-53 Событие безопасности Подозрение на инцидент (событие ИБ) Создан 0% выполнено
17-10-54 Событие безопасности Подозрение на инцидент (событие ИБ) Закрыт 0% выполнено
17-10-55 Событие безопасности Подозрение на инцидент (событие ИБ) Закрыт 0% выполнено
17-11-1 Общий инцидент Несанкционированная печать конфиден... Зарегистрирован 58% выполнено
17-11-3 Общий инцидент Несанкционированная печать конфиден... Зарегистрирован 58% выполнено
17-11-5 Общий инцидент Несанкционированная печать конфиден... Зарегистрирован 58% выполнено
17-11-7 Общий инцидент Несанкционированная печать конфиден... Зарегистрирован 58% выполнено
17-11-9 Общий инцидент Несанкционированная печать конфиден... Обработка 77% выполнено
17-11-10 Общий инцидент Несанкционированная печать конфиден... Закрыт 0% выполнено
17-11-11 Общий инцидент Внедрение вредоносного кода Закрыт 0% выполнено
17-11-12 Общий инцидент Нарушение доступности онлайн-сервис... Закрыт 0% выполнено
17-11-13 Общий инцидент Внедрение вредоносного кода Закрыт 0% выполнено
17-11-14 Общий инцидент Нарушение доступности онлайн-сервис... Закрыт 0% выполнено
17-11-15 Общий инцидент Компрометация средств аутентификаци... Закрыт 0% выполнено
Страница 1 из 122 50 Поиск... Отображаются записи с 1 по 50, всего 6051
Сценарии реагирования
Добавить
Сценарий Статус
Все действия
Доступ к подозрительному контент... Выполняется
Действия
Добавить Изменить Удалить
Действие Статус
Скрипт: Геолокация IP адреса (ipinfo.io)
Сценарий: Доступ к подозрительному контенту/узлу
Завершено 18 сент. 2019 г., [UTC+03:00
Скрипт: Список установленных сетевых соединений узла Windows
Сценарий: Доступ к подозрительному контенту/узлу
Команда возвращает список установленных сетевых соединений узла Windows
Завершено 18 сент. 2019 г., [UTC+03:00

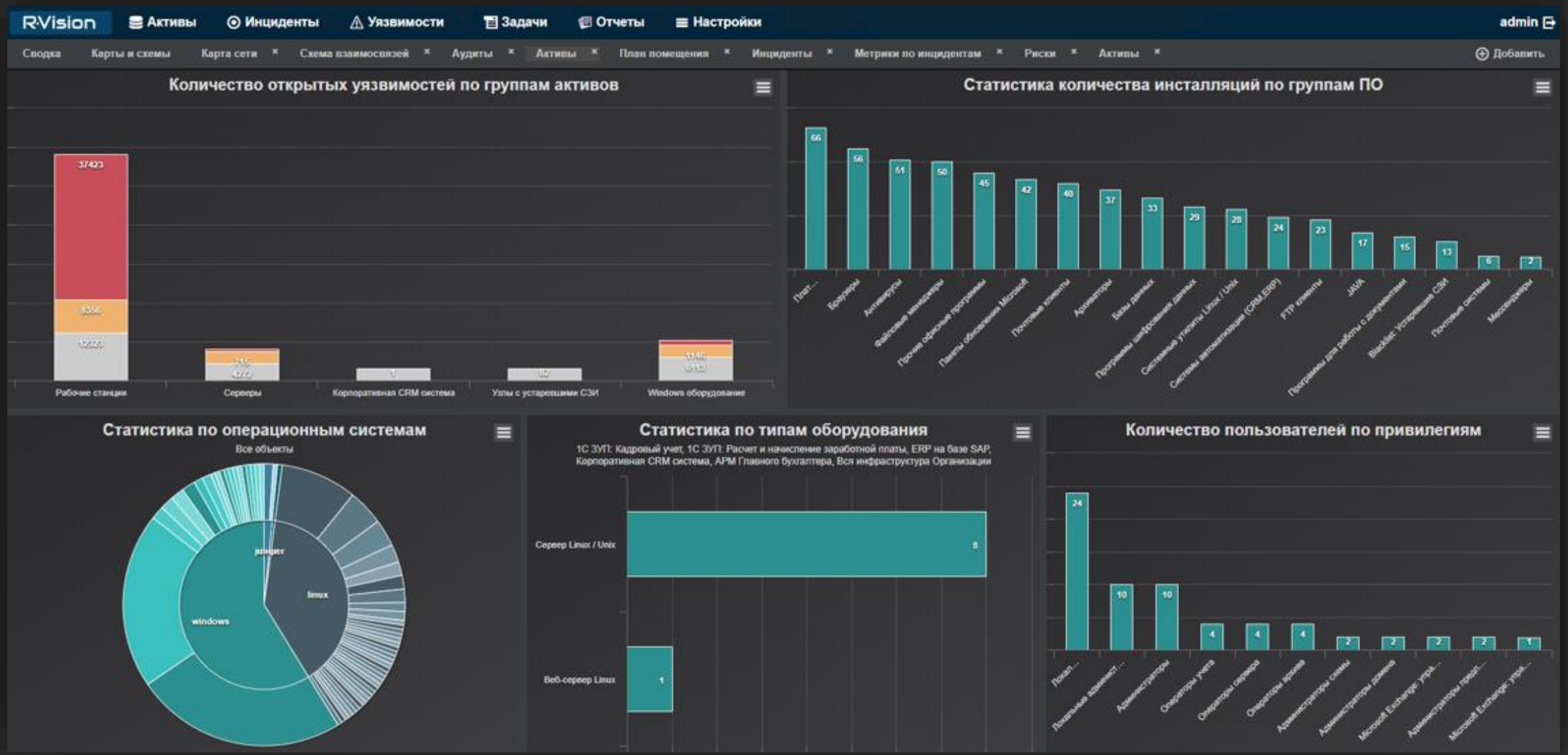
Инциденты



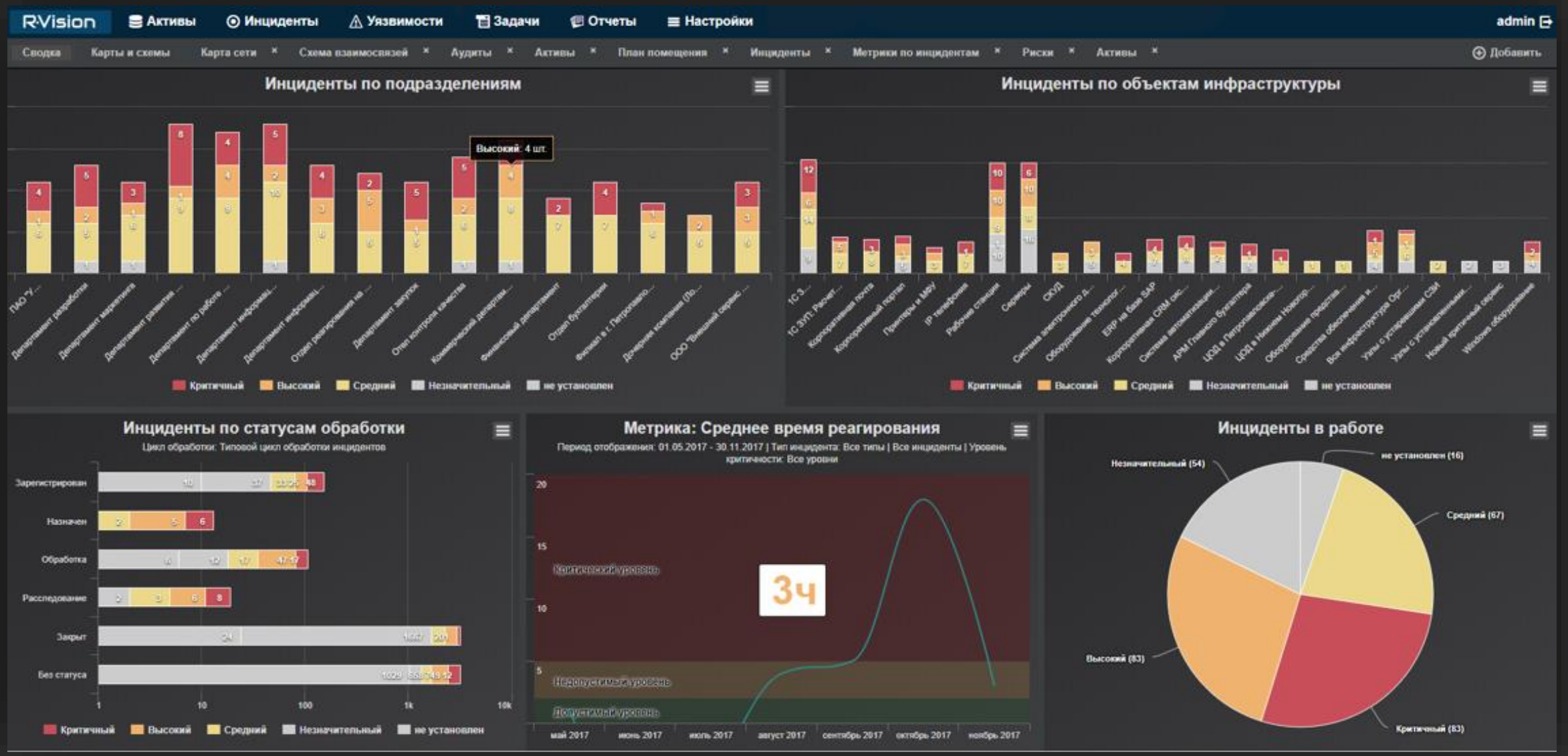
Сценарии реагирования



Контроль инфраструктуры



Сводная информация



Метрики по инцидентам

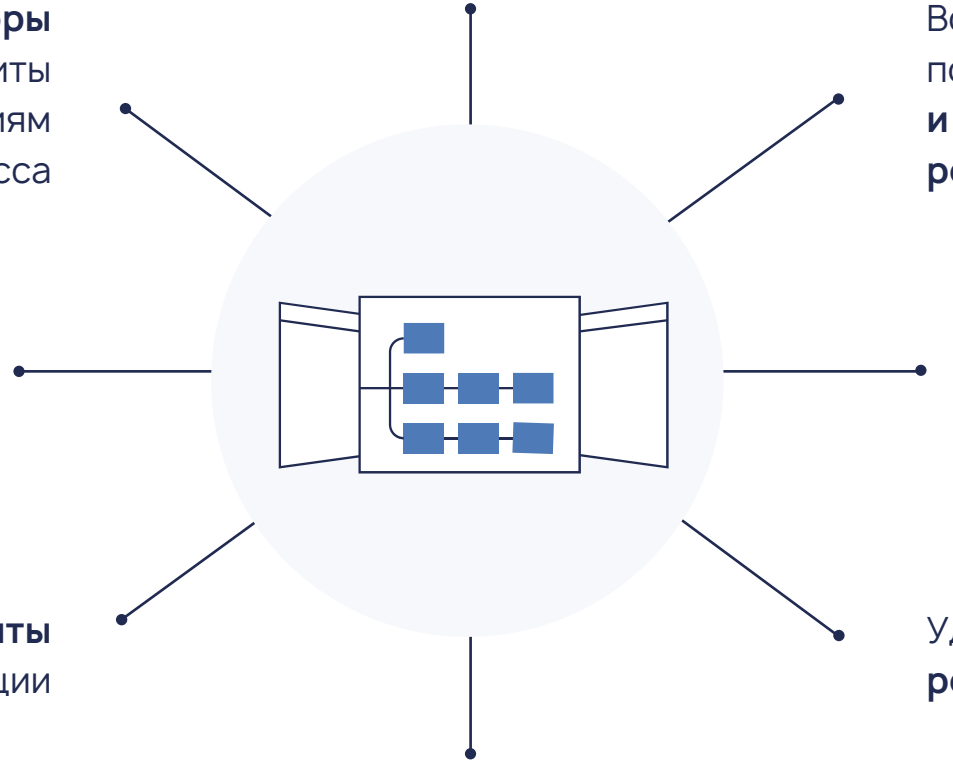
Инциденты на геокарте

Преимущества R-Vision IRP

Поддержка **мульти-арендной архитектуры**

Готовые коннекторы к средствам защиты и ИБ-решениям различного класса

Встроенные возможности по управлению активами **и формирования единого реестра активов**



Уникальный механизм интеграции с любыми сторонними системами

Гибкая настройка под выстроенные процессы

Готовые скрипты автоматизации

Удобный графический **редактор плейбуков**

Взаимодействие **с ГосСОПКА и ФинЦЕРТ**

Интеграции с другими системами

SIEM systems	Vulnerability scanners	AV & DLP solutions	Firewalls/ NGFW / WAF	CMDB / ITSM systems	Other systems	
MaxPatrol SIEM	MaxPatrol	Kaspersky Security Center	Check Point	Micro Focus UCMDB	MS Active Directory	VMWare vCenter
IBM QRadar	Алтэкс-софт RedCheck	Infowatch TrafficMonitor/ DeviceMonitor	Cisco	Micro Focus SM	MS Exchange / Lotus Domino / Communigate	Trend Micro DDAn / DDEI
Micro Focus ArcSight	Tenable Nessus/SC	Triton AP-DATA	Palo Alto Networks	MS SCCM	E-Mail парсинг	Symantec BlueCoat
Splunk	Rapid7 Nexpose	Symantec Endpoint Protection	Fortinet	Naumen CMDB	MS SQL, My SQL, Postgre SQL, Oracle DB direct connectors	FortiSandbox / Fortimail
McAfee ESM	Qualys	McAfee ePolicy Orchestrator	Juniper	OmniTracker CMDB/SM	Конструктор коннекторов (REST API, SOAP, Powershell, SSH, LDAP, SNMP)	Imperva DAM
RSA NetWitness	OpenVAS	ESET	Huawei	iTOP	Собственные REST API методы	Lieberman ERPM
FortiSIEM			Gigamon GigaVue FM / OS	JIRA	Zabbix	VirusTotal/ ThreatCrowd/ AlienVault/...
			Imperva WAF			Skybox

Результат

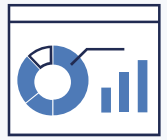
Повышение **скорости реагирования** на инциденты

Минимизация **потенциального ущерба** и простоя бизнеса

Компенсация **нехватки персонала** в условиях роста числа инцидентов

Повышение эффективности работы корпоративного SOC

Контроль ИТ-инфраструктуры и защищенности ресурсов



Полная картина о состоянии ИБ, отчетность и метрики для принятия решений

Кейсы использования R-Vision IRP/SOAR

Автоматизация SOC крупной нефтегазовой компании, осуществляющего мониторинг и реагирование на инциденты для более 100 дочерних предприятий в 30 регионах страны

Автоматизация управления жизненным циклом инцидентов в крупной промышленной компании с объемом инфраструктуры в 10 тыс. хостов и множеством дочерних предприятий

Автоматизация реагирования на инциденты и обмена данными с ФинЦЕРТ в ряде крупнейших российских банков

Автоматизация workflow в коммерческих SOC и возможность предоставления дополнительных услуг по модели MSSP

R-Vision

+ 7 (499) 322 80 40

sales@rvision.ru

www.rvision.ru

Подписывайтесь на наш дайджест ИБ: **rvision.ru/blog**