

Систематизация и автоматизация процесса управления уязвимостями



Екатерина Урбах

Менеджер по работе с партнерами
Security Vision



Максим Репко

Пресейл-менеджер
Security Vision

100%

русская компания, специализирующаяся на автоматизации процессов обеспечения ИБ



сертифицирован
ФСТЭК по 4 уровню
доверия



включён в Единый
реестр российского
ПО



сертифицирован
ОАЦ в республике
Беларусь



государственные
структуры



промышленность и
энергетика



финансовые и
страховые организации



ритейл и другие
компании



телеком-операторы
и коммерческие SOC



*securityvision.ru/projects/
**securityvision.ru/about/partners
***csr.ru/ru/research/prognoz-razvitiya-rynka-kiberbezopasnosti-v-rossiyskoy-federatsii-na-2024-2028-gody



АО «ГОЗНАК»



ФГБУ НИИ «ИНТЕГРАЛ»



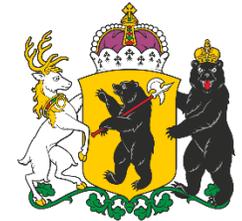
ФЕДЕРАЛЬНАЯ СЛУЖБА ОХРАНЫ РФ



ПРАВИТЕЛЬСТВО КРАСНОЯРСКОГО КРАЯ



ПРАВИТЕЛЬСТВО ТЮМЕНСКОЙ ОБЛАСТИ



ПРАВИТЕЛЬСТВО ЯРОСЛАВСКОЙ ОБЛАСТИ



СОВЕТ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОГО СОБРАНИЯ РФ



АО «ДОМ.РФ»



АО НПП «ИСТОК ИМ. ШОКИНА»



ПАО «СЕВЕРСТАЛЬ»



ООО «ЕВРАЗ»



АО КОНЦЕРН «РОСЭНЕРГОАТОМ»



АО ОХК «УРАЛХИМ»



ПАО ГМК «НОРИЛЬСКИЙ НИКЕЛЬ»



ПАО «ИНТЕР РАО»



ПАО «РУСГИДРО»



ПАО «СБЕРБАНК»



АО «АЛЬФА-БАНК»



ПАО «РОСБАНК»



АО «Т-БАНК»



АО «БАНК ГПБ»



ПАО БАНК «ФК ОТКРЫТИЕ»



АО «СМП БАНК»



ПАО «СДМ-БАНК»



АО «АБ РОССИЯ»



ООО «X5 GROUP»



ПАО «МАГНИТ»



ГРУППА «ЧЕРКИЗОВО»



ООО ГК «РУСАГРО»



АО «ПЕРВЫЙ КАНАЛ»



АО «ПОЧТА РОССИИ»



ГОСКОРПОРАЦИЯ «РОСТЕХ»



ХОЛДИНГ «CAPITAL GROUP»



ПАО «МЕГАФОН»



ПАО «ВЫМПЕЛКОМ»



ООО «СОЛАР СЕКЬЮРИТИ»



ООО «АТ ГРУП»



ООО «ТТК-СВЯЗЬ» (ТРАНСТЕЛЕКОМ)



ООО «ИНФОСЕКЬЮРИТИ СЕРВИС»



КОММЕРЧЕСКИЙ СОС «РОСТЕХ»



МГТУ им. Баумана



Иннополис



НГТУ



НИЯУ МИФИ



СибГУ им. Решетнёва



УГНТУ



Сириус



УНИТ



Московский политех



ПЛАТФОРМА



Единая гибкая платформа

с кастомизацией



Объекты, карточки и
табличные представления



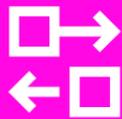
Роли и меню, доступ к
данным и внешний вид



Рабочие процессы и
автоматизация действий



Аналитика, интерактивные
виджеты и дашборды



Интеграции с внешними
системами (коннекторы)



Отчёты, выгрузка файлов
и логирование действий

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. A table lists various devices with columns for selection, ID, creation date, status, 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 vulnerabilities with columns for type, FQDN, IP address, and operation system.

метки времени

стили

ссылки

обязательные поля

полная карточка

табличный вид

краткая карточка

Настройки > Рабочие процессы > Рабочие процессы

Группа Рабочий процесс

Поиск...

Активы

- Жизненный цикл
 - Жизненный цикл устройства
 - Категорирование (дерево решений)
 - Категорирование (ручное и справочник)
- Ресурсно-сервисная модель
- Экспресс отчеты
 - Добавление типов в справочник оборудования
- Общее
 - Закреть на редактирование
 - Открыть на редактирование
- Управление рисками
 - ТМР
 - Жизненный цикл
 - Моделирование мер
 - Моделирование риска
- Мониторинг рисков
- Общие
- Оценка рисков
- Управление мерами

Жизненный цикл устройства

Группа : Жизненный цикл

Типы объектов : Все типы объектов

Версия : 3 - 04.03.2024 11:14:01

Отправить письмо

Тип: Почта (MS Exchange EWS)

Отправить сообщение

Тип: Telegram

Категорирование (ручное и справочник)

Состояний: 2, Переходов: 3

Действия: 5, 4

Активные процессов: 16

Последняя обработка: 13.09.2024, 13:31:51

Использование процесса в разделах

Активы

- Серверы и рабочие станции > [103]
- Сетевое оборудование > [110]
- Сервер\АРМ > [105]
- Базы данных > [119]
- Телефоны\VoIP > [117]

Ещё (3)

Жизненный цикл устройства

Начальное состояние

IP заполнен

IP заполнен

Введение в эксплуатацию

Используется

Поставить актио на учет

В эксплуатацию автоматически

Ввод в эксплуатацию

Отправить оповещения

Установить значение настроек

Оповещение почта

Оповещение telegram

Очистка

Очистка

Вывод из эксплуатации

Вывод из эксплуатации

Утилизировать

Утилизировать

ручные и автоматические транзакции

каталог РП

отображение дочерних объектов и результатов

статистика применения

управление версиями

создание интеграций
через интерфейс

The screenshot displays the 'Security Vision' connector configuration in the interface. The connector is named 'Security Vision Управление Активами' and is of type 'HTTP'. It is part of the 'Security Vision Assets Management' group. The configuration shows a search for 'Учетная запись' (Account) and 'Хост' (Host). A custom command is defined to find host IDs in the Security Vision CMDB. The command is a POST request to 'ip/entity/search' with a JSON body containing search criteria for host IDs. The interface also shows a list of available connectors in the marketplace on the left, including 'Kali tools', 'Kaspersky OpenTip', 'Shodan', and 'Security Vision TIP'.

возможность
переключения лицензий

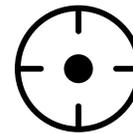
кастомные команды и
переменные

коннекторы, доступные
в маркетплейсе

тестирование
команд

WMI | PS | SSH | файл | почта | БД | HTTP (API) | LDAP | EventLog | Syslog | DNS | скрипты и др.

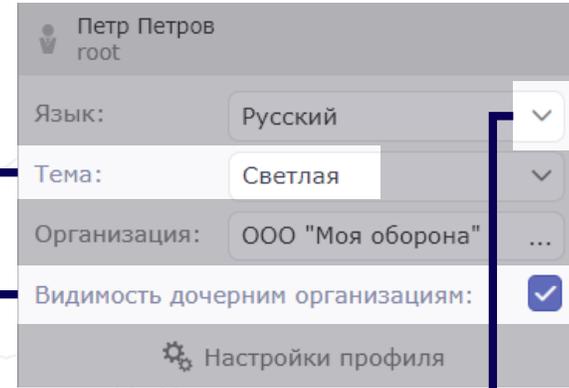
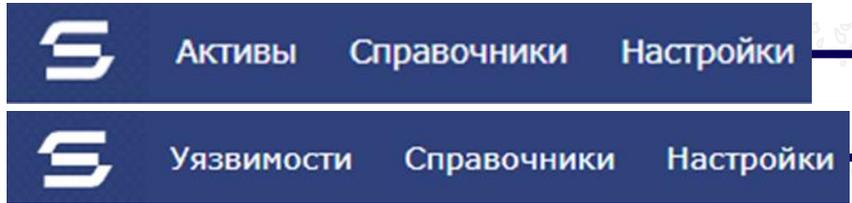
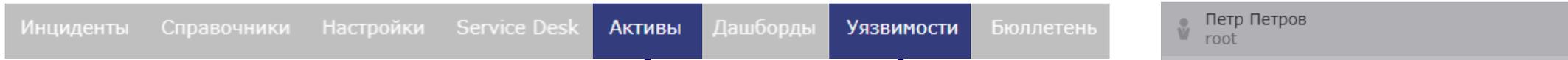
Сбор и обогащение



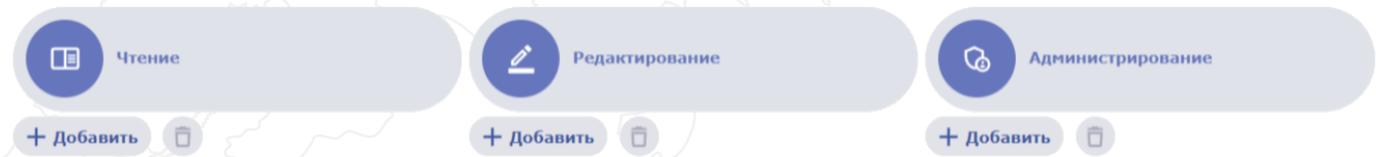
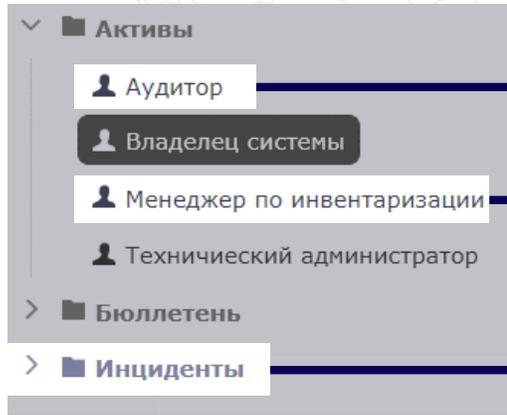
Реагирование на события

создание новых коннекторов **без участия вендоров**





темы оформления
multitenancy
мультиязычность

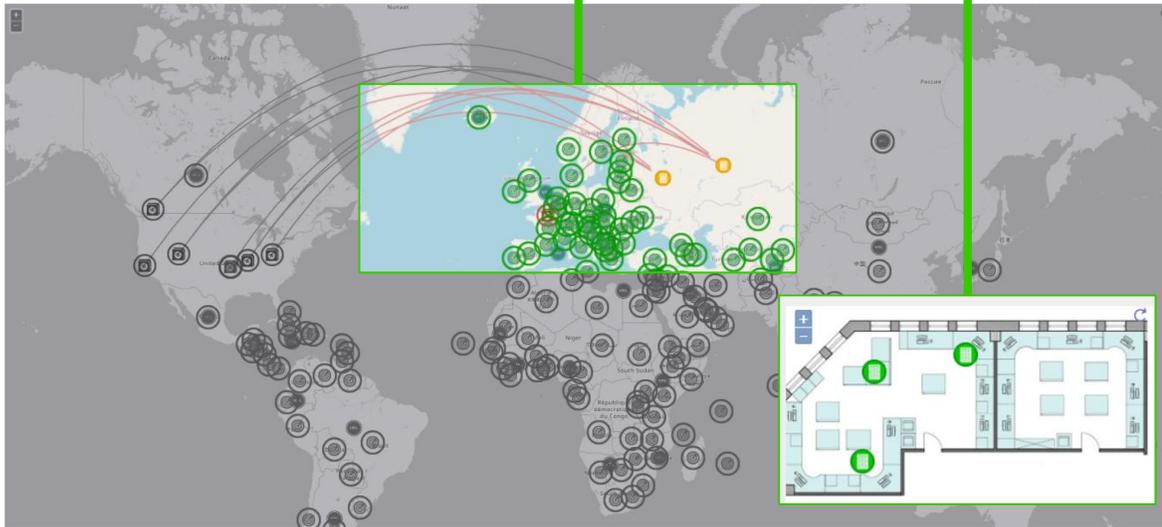


персональная витрина
гранулярные настройки



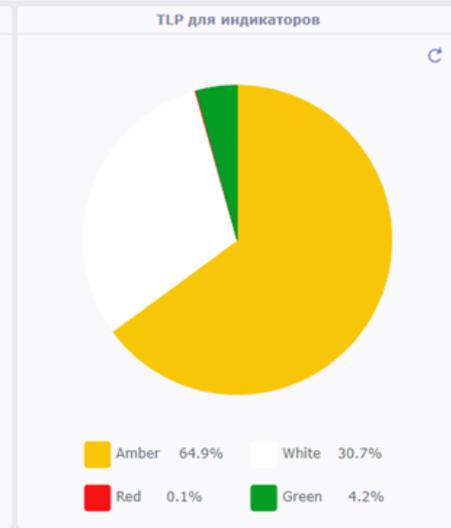
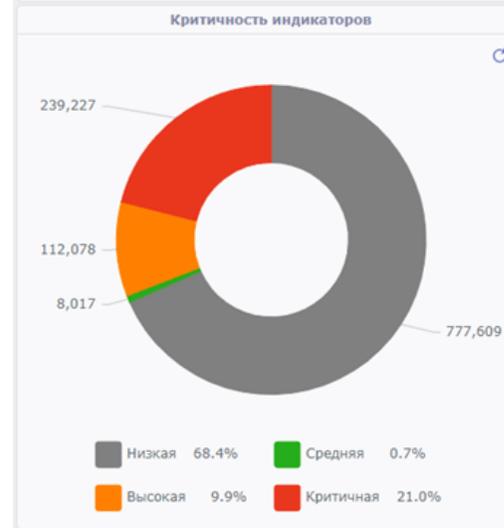
карты и планы помещений

дашборды

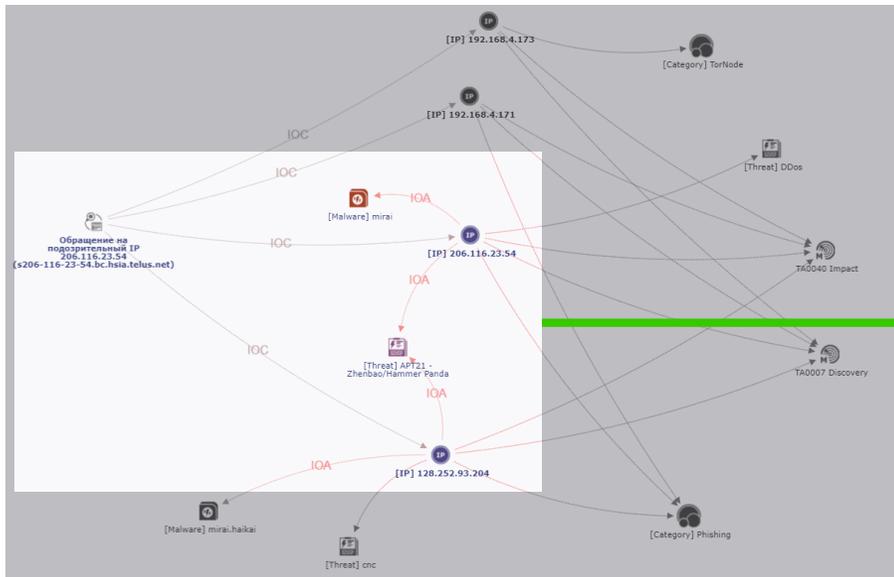


Топ-5 активных критичных инцидентов

Наименование	Критичность	Статус
Отправка письма с подозрительного домена: acmetek.com	Критичная	Новый
Обращение на подозрительный домен cutt.ly	Высокая	Новый
Обращение на подозрительный домен conect-app.com	Высокая	Новый
Обращение с подозрительного IP 192.168.4.173 (ws4-dev.sv.local)	Высокая	Новый

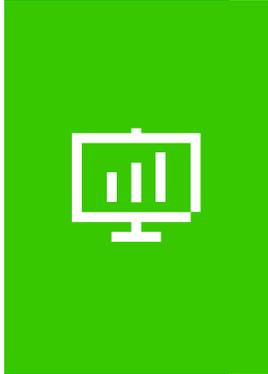


графы связей



интерактивная аналитика и связанные графики

Количество активных индикаторов за период	Количество активных инцидентов за период
934676	7



различные форматы

Security Vision

Отчет по активам

Дата выгрузки: 04.06.2024 14:56:44

Период: 01.02.2023 - 27.06.2024

Статистика активов

Новые активы	Новые критичные активы
135	14
Инвентаризовано	Ошибка инвентаризации
9	45

Активы по статусам

Подготовка	Используется	Не используется	Утилизирован
4	119	4	11

Активы по критичности

11	3	5
----	---	---

Диаграмма в...

	A	B	C
1	Подготовка	11	
2	Используется	119	
3	Не используется	4	
4	Утилизирован	1	

Сохранить Отмена

Размер и положение: Относительное Абсолютное

Сгенерировать отчет docx pdf xls ods odt txt csv

Таблица всех активов

Тип устройства	Количество
Сетевое устройство	10
Другое устройство	1
Сервер\АРМ	116
Принтер\МФУ	6
Интерфейс удаленного управления	1
Телефон\VoIP	4
Система хранения данных	1

Процентное соотношение количества устройств

Сетевое устройство 7%	Другое устройство 1%	Сервер\АРМ 83%	Принтер\МФУ 4%
-----------------------	----------------------	----------------	----------------

Импортировать настройки из дашборда Переменные

Наименование: Подробная статистика о всех активах

Описание: Не задано

Группа: Активы

Использовать из действия:

Формат страниц: A5 A4 A3

Ориентация документа: Портретная Альбомная

Отступы документа: Настроить

Язык: Русский

Цвет фона: Не задано

Автоматически разделить по страницам:

Формат документа: Docx Pdf Xlsx Ods Odt Txt Csv

Word

Входной параметр

Дата начала

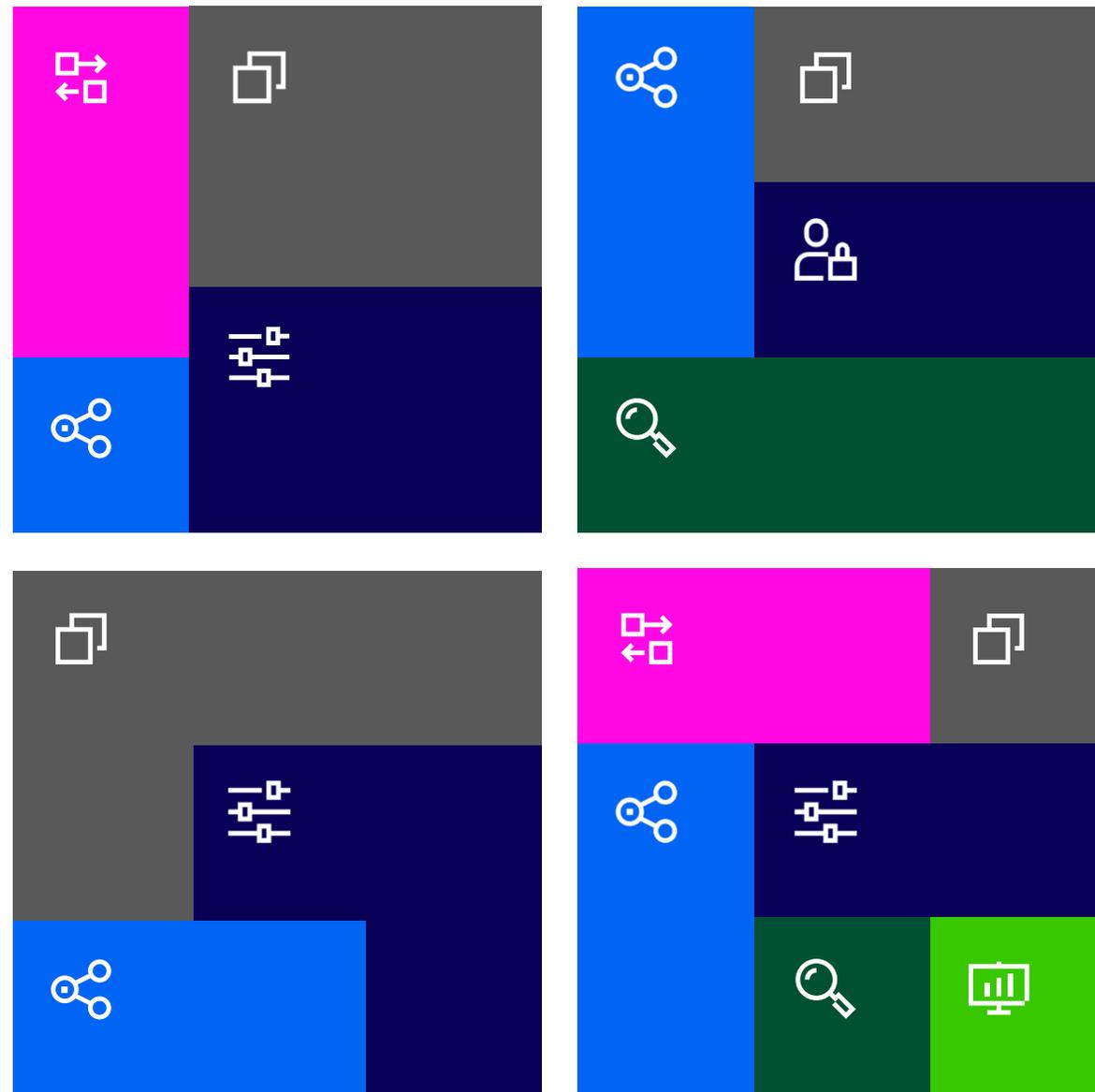
Дата окончания

редактор шаблонов

хранение исходных данных



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



NG SOAR
Расширенное управление инцидентами

SOAR
Управление инцидентами

ГосСОПКА
Взаимодействие с НКЦКИ

FinCERT
Взаимодействие с ЦБ РФ

AM
Управление активами и инвентаризацией

VM + VS*
Управление уязвимостями *со сканером

SPC
Управление конфигурациями безопасности

КИИ
Управление соответствием ФЗ-187

RM
Управление рисками кибербезопасности

ORM
Управление операционными рисками

CM
Управление соответствием НМД

BCM
Управление непрерывностью бизнеса

SA
Портал самооценки ДЗО

TIP
Анализ угроз кибербезопасности

UEBA
Поведенческий анализ и поиск аномалий



[Блог]
securityvision.ru/blog



[Хабр]
habr.com/ru/companies/securityvision



[Telegram]
t.me/svplatform



[YouTube]
youtube.com/@securityvision2421

ПРОЦЕССЫ

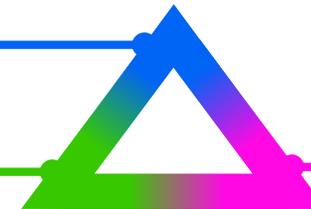
Governance, Risk Management and Compliance

ТЕХНОЛОГИИ

Security Orchestration Tools

АНАЛИТИКА

Security Data Analysis



Цикл управления уязвимостями

