SCAN FACTORY

SCAN FACTORY AI

управление уязвимостями
EASM+VM+DAST из одного окна

SCAN FACTORY

Эксперты в управлении уязвимостями и цифровыми рисками

Решение входит в реестр
отечественного ПО

Организация имеет сертификат
ФСТЭК на ТЗКИ и СЗКИ

ScanFactory VM используют
более 50 компаний из разных отраслей:
промышленность, финансы, ИТ, ритейл

5 лет

Защищаем бизнес от киберугроз

100+

Реализованных проектов

500+

Компаний просканировано
с помощью ScanFactory

SCAN FACTORY

Команда

Квалификация

Средний опыт работы специалиста нашей команды — 6 лет. Наши специалисты бывшие участники команд анализа защищенности топовых интеграторов и банков

Выступления на конференциях

PHDays, Offzone, Blackhat, OWASP, Standoff Talks

Сертификаты

OSCE — 1, **OSEP** — 2, **OSWE** — 2,
OSCP — 4, **OSED** — 1, **CRTE** — 2,
CRTP — 1, **CREST** — 1, **HTB CBBH** — 1

Награды

Наши специалисты - члены команд победителей Standoff, Yandex Cloud Bank Security Challenge, номинанты Pentest Award by Awillix

SCAN FACTORY

ScanFactory VM собирает уязвимости в одном окне

EASM
Внешний сканер
Чёрный и серый ящик

VM
Внутренний сканер
Белый и серый ящик

DAST
Сканер веб-приложений

Leaks
Поиск утечек паролей

CPT
Экспертное сопровождение команды пентестеров

SCAN FACTORY

Что делает ScanFactory VM уникальным?

Продуктовая экспертиза №1 на рынке

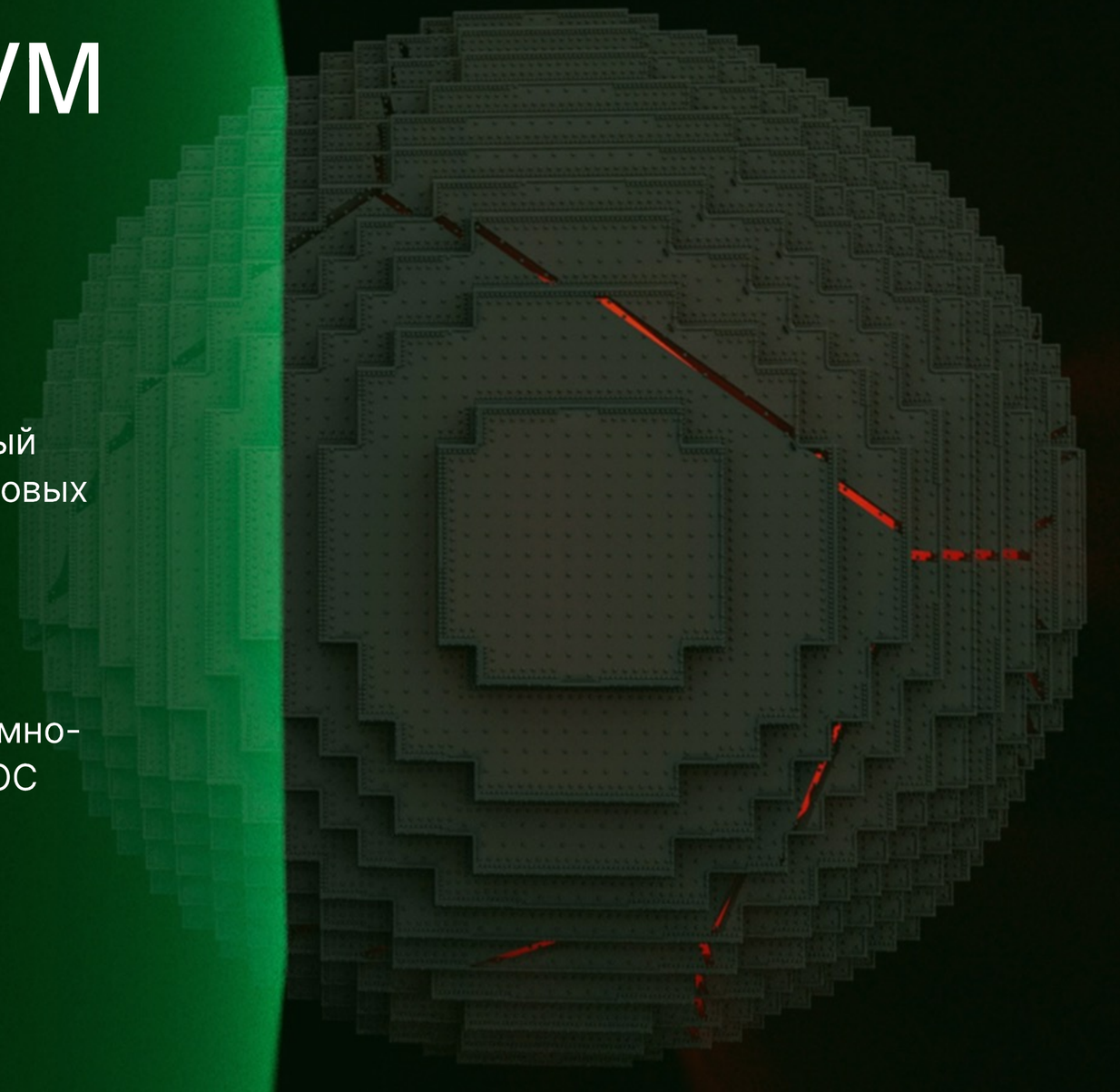
Мы детектируем больше уязвимостей, чем любой отдельно взятый российский вендор за счёт объединения экспертизы лучших мировых инструментов

Гибкость установки

Решение доступно SaaS, On-Premise, а также в формате программно-аппаратного комплекса. Может устанавливаться на российские ОС

СРТ

Предоставляем сервис экспертного сопровождения.



SCAN FACTORY

EASM

- Собственное облако
- OSINT: поиск теневых активов: Netlas, Zoomeye, Shodan, Fofa
- 19 опенсорсных сканеров: Nuclei, nmap, OWASP ZAP, dirsearch, wpscan
- Лучший в мире DAST сканер
- Поставщики CVEDetails, Vulners и БДУ ФСТЭК
- Управление по API

OZON CDEK МАГНИТ beeline cloud СБЕР БАНК

SCAN FACTORY

DAST

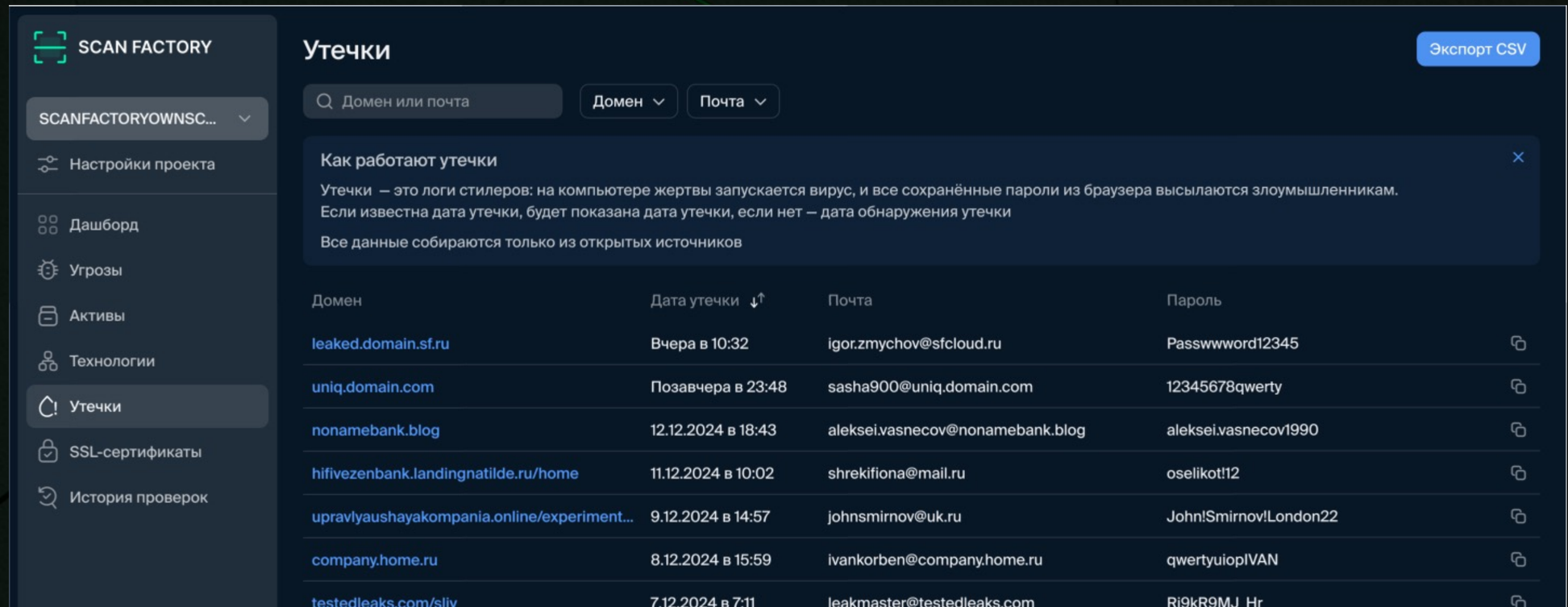
Веб-сканер детектирует 7000+ уязвимостей

- Сканирование чёрным/серым ящиком
- Сканирование Swagger-схем, технология глубокого краулинга
- Использование PKCS12 сертификатов

SCAN FACTORY

Утечки

Пароли сотрудников и клиентов компании,
украденные через стилеры



VM

Мы сильнейший российский вендор
не только в EASM, но и в VM

SCAN FACTORY

Инфраструктурный сканер:

100 000+ CVE

Обновления приходят каждые 12 часов, количество растет ежедневно

260 000+ плагинов

Аудит по PCI DSS, CIS Benchmark

SCAN FACTORY

ЧЁРНЫЙ И БЕЛЫЙ ЯЩИК

Инвентаризация

Версия ОС,
файловой системы

Аптайм,
сетевые параметры

Установленные пакеты
и запущенные процессы

SCAN FACTORY

Поддерживаются

ОС:

WINDOWS

LINUX

MAC OS

Сетевое оборудование:

JUNIPER

CHECKPOINT

CISCO

PALO ALTO

Сканирование на уязвимости СУБД:

PostgreSQL

MySQL

MS SQL

Oracle

Системы виртуализации:

VMware ESXi

vCenter

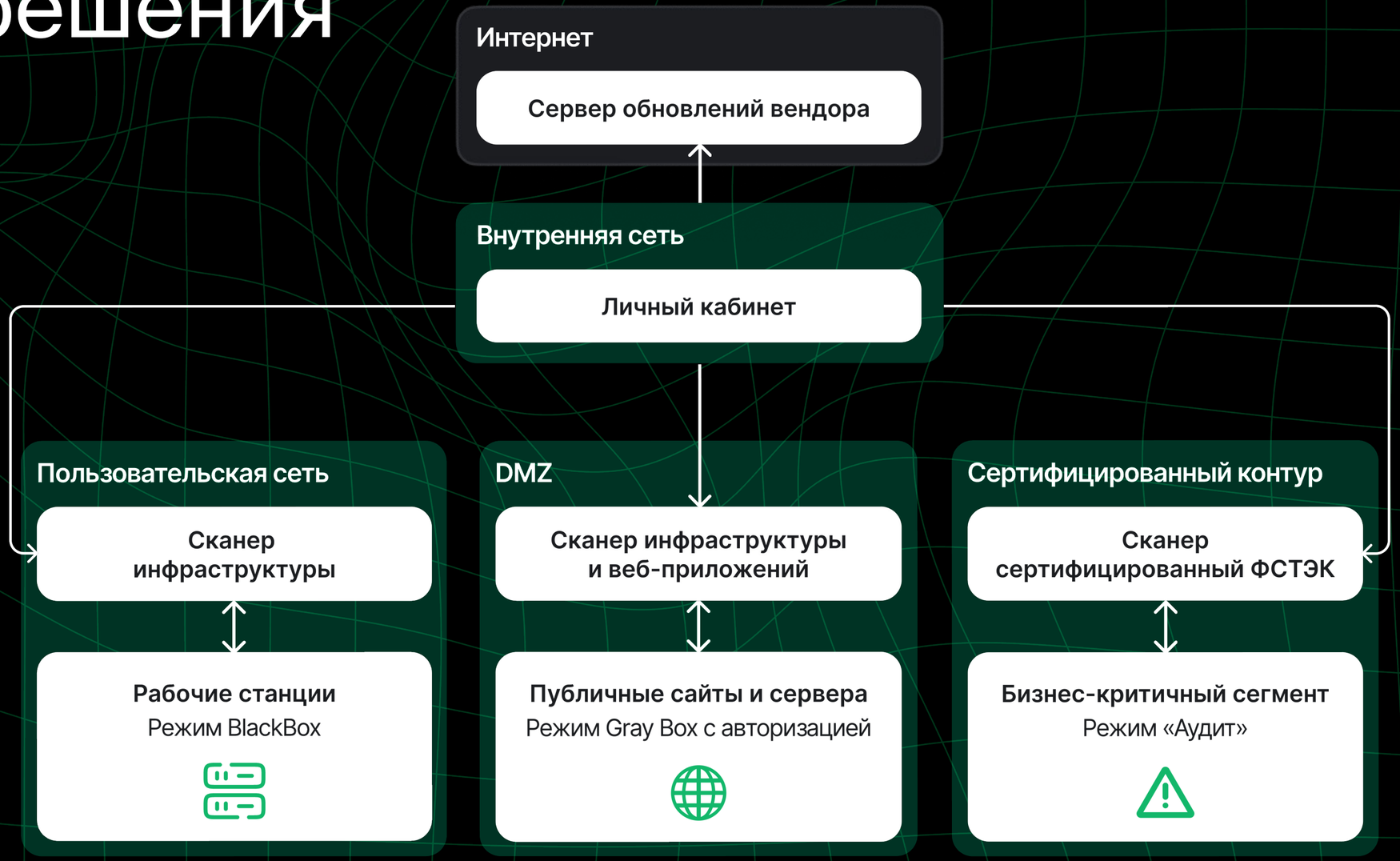
KVM

Citrix Xen

Hyper-V

SCAN FACTORY

Архитектура решения



SCAN FACTORY

Варианты инсталляции

ON-PREMISE

На ВМ Заказчика

SaaS для внешнего периметра

В облаке вендора

ПАК

В ДЦ Заказчика

Remote Scan Agent

Сканирование сети из облака вендора

Перейдём от слов к делу

SCAN FACTORY

SCANFACTORYOWNSC...

- Настройки проекта
- Дашборд
- Угрозы
- Активы
- Утечки
- SSL-сертификаты
- История проверок
- Быстрая проверка
- История действий
- Личный кабинет
- Настройки

Дашборд

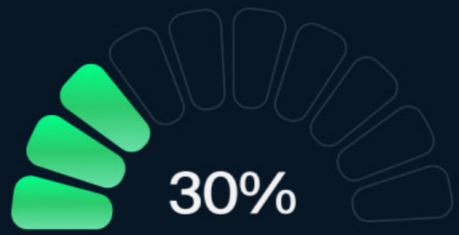
Динамика изменений: Месяц

Скачать отчёт

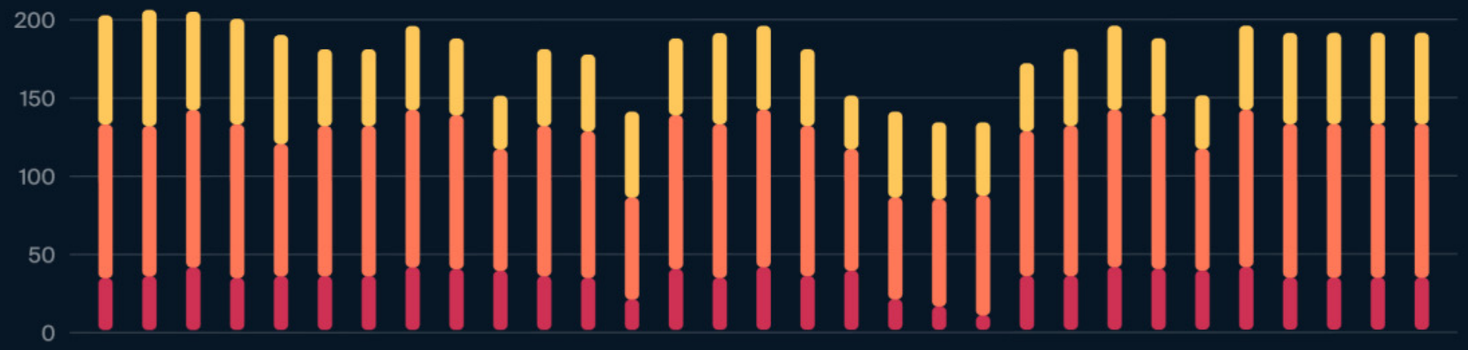
Сканирование идёт

Критические угрозы	Высокие угрозы	Средние угрозы
174 ▲14	223 ▲32	369 ▼29
2	7	14
Неактивные 167 +13	Неактивные 220 +25	Неактивные 298 +45

Защищенность



Динамика изменения угроз



Топ 5 активных угроз

- 12 Debug Endpoint pprof - Expos...
- 8 Outdated software: nginx
- 7 CGI Generic Unseen Paramet...
- 5 TLS Version 1.1 Protocol Depre...
- 2 HSTS Missing From HTTPS Se...

Активы

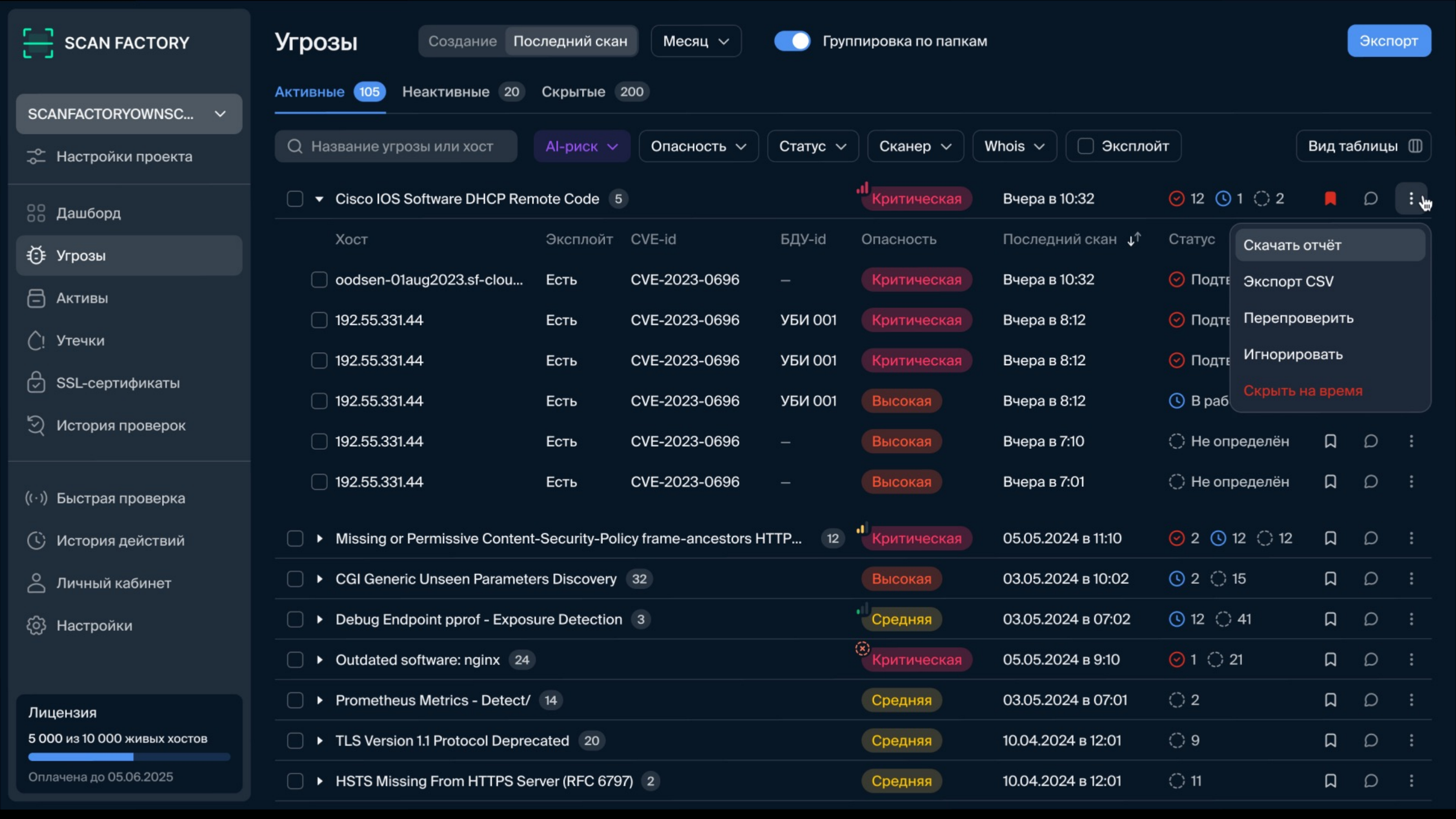
Домены
23 ▲5

IP
672 ▼18

Динамика изменения активов

Самые опасные порты

22 (SSH)	TCP	185.30.97.2
Microsoft IIS httpd 10.0 (Wi...		
23 (Telnet)	UDP	185.30.97.2
Microsoft IIS httpd 10.0 (Wi...		


SCAN FACTORY
SCANFACTORYOWNSC...
Настройки проекта
Дашборд
Угрозы
Активы
Утечки
SSL-сертификаты
История проверок
Быстрая проверка
История действий
Личный кабинет
Настройки
Лицензия
5 000 из 10 000 живых хостов
Оплачена до 05.06.2025
Угрозы
Создание
Последний скан
Месяц
Группировка по папкам
Экспорт
Активные 105
Неактивные 20
Скрытые 200
Название угрозы или хост
AI-риск
Опасность
Статус
Сканер
Whois
Эксплойт
Вид таблицы
Cisco IOS Software DHCP Remote Code 5
Критическая
Вчера в 10:32
12 1 2
Хост
Эксплойт
CVE-id
БДУ-id
Опасность
Последний скан
Статус
oodsen-01aug2023.sf-clou...
Есть
CVE-2023-0696
–
Критическая
Вчера в 10:32
192.55.331.44
Есть
CVE-2023-0696
УБИ 001
Критическая
Вчера в 8:12
192.55.331.44
Есть
CVE-2023-0696
УБИ 001
Критическая
Вчера в 8:12
192.55.331.44
Есть
CVE-2023-0696
УБИ 001
Высокая
Вчера в 8:12
В раб
192.55.331.44
Есть
CVE-2023-0696
–
Высокая
Вчера в 7:10
Не определён
192.55.331.44
Есть
CVE-2023-0696
–
Высокая
Вчера в 7:01
Не определён
Скачать отчёт
Экспорт CSV
Перепроверить
Игнорировать
Скрыть на время
Missing or Permissive Content-Security-Policy frame-ancestors HTTP... 12
Критическая
05.05.2024 в 11:10
2 12 12
CGI Generic Unseen Parameters Discovery 32
Высокая
03.05.2024 в 10:02
2 15
Debug Endpoint pprof - Exposure Detection 3
Средняя
03.05.2024 в 07:02
12 41
Outdated software: nginx 24
Критическая
05.05.2024 в 9:10
1 21
Prometheus Metrics - Detect/ 14
Средняя
03.05.2024 в 07:01
2
TLS Version 1.1 Protocol Deprecated 20
Средняя
10.04.2024 в 12:01
9
HSTS Missing From HTTPS Server (RFC 6797) 2
Средняя
10.04.2024 в 12:01
11

SCAN FACTORY

SCANFACTORYOWNSC...

Настройки проекта

Дашборд

Угрозы

Активы

Утечки

SSL-сертификаты

История проверок

Быстрая проверка

История действий

Личный кабинет

Настройки

Лицензия

5 000 из 10 000 живых хостов

Оплачена до 05.06.2025

Активы

Создание | Последний скан

Месяц

Экспорт CSV

С открытыми портами | Без открытых портов | Не подтверждённые | Не резолвятся в IP | Из чёрного списка

История портов

Домен, ip или порт

Порт | Опасность | Тег | Как добавлен

Вид таблицы

Хост	Порты	Угрозы	Последний скан
uniq.domain.com OSINT 185.18.200.14 и ещё 4		1 22 3	Вчера в 10:32
uniq.domain.com OSINT 185.18.200.14 и ещё 4		1 22 3	05.05.202
185.18.200.14 RU-TILDAPUBLISHING-20230912 (RU)	TCP 22 (ssh) OpenSSH 8.4p1 Ubuntu TCP 48 (ssh) OpenSSH 8.4p1 Ubuntu	1 2 1	Вчера в 1
117.232.15.53 RU-TILDAPUBLISHING-20230912 (RU)	TCP 5050 (http) OpenSSH 8.4p1 Ubuntu (Li... TCP 34 (ssh) OpenSSH 8.4p1 Ubuntu	8 3	03.05.202
82.43.38.141 RU-TILDAPUBLISHING-20230912 (RU)	TCP 22 (ssh) OpenSSH 8.4p1 Ubuntu TCP 48 (ssh) OpenSSH 8.4p1 Ubuntu	2 3	10.04.2024 в 12:01
143.193.147.24 RU-TILDAPUBLISHING-20230912 (RU)	TCP 22 (ssh) OpenSSH 8.4p1 Ubuntu TCP 5050 (http) OpenSSH 8.4p1 Ubuntu	10	03.05.2024 в 07:01
118.20.198.176 RU-TILDAPUBLISHING-20230912 (RU)	TCP 22 (ssh) OpenSSH 8.4p1 Ubuntu TCP 48 (ssh) OpenSSH 8.4p1 Ubuntu	1	10.04.2024 в 12:01
230.161.0.151 RU-TILDAPUBLISHING-20230912 (RU)	TCP 22 (ssh) OpenSSH 8.4p1 Ubuntu TCP 48 (ssh) OpenSSH 8.4p1 Ubuntu	1	03.05.2024 в 07:01
uniq.domain.com OSINT 185.18.200.14 и ещё 4		1 22 3	10.04.2024 в 12:01

Скачать отчёт

Перепроверка портов

Полная перепроверка

История актива

Добавить в чёрный список

SCAN FACTORY

SCANFACTORYOWNSC...

Настройки проекта

Дашборд

Угрозы

Активы

Утечки

SSL-сертификаты

История проверок

Быстрая проверка

История действий

Личный кабинет

Настройки

Настройки проекта

Скачать отчёт

Настройки | Отчеты

ТЕСТОВЫЙ ПРОЕКТ

Сканируется

Активы

Домены	IP	Чёрный список	Исключения из чёрного списка
*.domain.ru ...	95.181.181.49 5.252.64.55 5.252.64.12 185.215.4.57	185.215.4.12 84.201.143.113	academy-adm-v2.domain.ru academy.domain.ru bcscd.domain.ru biolab.domain.ru
Домены: 2; Вайлдкарды: 2	IP 364; Подсети: 16; IP подсетей: 450		

Текст комментария

Расписание сканирования

Часовой пояс	Начало проверки		Конец проверки	
UTC+4 Erevan	Пн	19:00	Пн	19:00
	Вт	19:00	Вт	23:00
	Ср	19:00	Ср	23:00
	Чт	19:00	Чт	23:00

SCAN FACTORY

SCANFACTORYOWNSC...

- Настройки проекта
- Дашборд
- Угрозы
- Активы
- Утечки
- SSL-сертификаты
- История проверок
- Быстрая проверка
- История действий
- Личный кабинет
- Настройки

Лицензия

5 000 из 10 000 живых хостов

Оплачена до 05.06.2025

SSL-сертификаты

Экспорт CSV

Активные 105 | Игнорируемые 20

Домен, ip или порт | Порт

Хост	Порт	Выдан	Алгоритм	Размер ключа	Закончится
185.18.200.14	22	GlobalSign nv-sa BE	sha256WithRSAEncryption	2048	Вчера в 10:32
domain.testssl.com 192.22.12.48	53	GlobalSign nv-sa BE	sha256WithRSAEncryption	2048	Завтра в 19:00
192.255.167.25	2002	GlobalSign nv-sa BE	sha256WithRSAEncryption	2048	23.09.2024
better.call-saul.com	34	Let's Encrypt US	sha256WithRSAEncryption	2048	1.10.2024
fring.gus.rus	5005	Let's Encrypt US	sha256WithRSAEncryption	2048	3.10.2024
192.255.167.25	2005	Let's Encrypt US	sha256WithRSAEncryption	2048	14.10.2024
185.18.200.14	23	Let's Encrypt US	sha256WithRSAEncryption	2048	2.11.2024
mini-trailer.menu.com	55	Sectigo Limited GB	sha256WithRSAEncryption	2048	3.11.2024
scanfactory.top.ru	22	Sectigo Limited GB	sha256WithRSAEncryption	2048	17.11.2024

SCAN FACTORY

SCANFACTORYOWNSC...

Настройки проекта

Дашборд

Угрозы

Активы

Утечки

SSL-сертификаты

История проверок

Быстрая проверка

История действий

Личный кабинет

Настройки

Лицензия

5 000 из 10 000 живых хостов

Оплачена до 05.06.2025

История проверок

Активные 105 | Архивные 167

Вид таблицы

Хост или ID | Сканер | Статус

Шаблон	Тип цели	Хост	Статус	Приоритет	ID	Создана	Обновлена
screenshooter #1	httpreq	185.30.97.29	Завершена	24	...3bb132	Позавчера в 3:02	Позавчера в 10:32
awvs #2	dport	255.166.74.15	В работе	5	...ee3ef3	11.08.2024	12.08.2024
infrascan #1	ipv4port	192.167.1.12	В работе	1	...5522f1	1.08.2024	1.08.2024
nmap #3	ipv4port	185.15.192.48	На паузе	31	...3bb132	24.07.2024	29.07.2024
osinter #2	domain	eklmn.domain-test.ru	Провалена	15	...be9aaf	22.07.2024	25.07.2024
sdto #1	domain	blin.blinskii.univer.ru	Завершена	6	...9b9934	3.04.2024	18.07.2024
sdto #2	domain	silvestranddreevich.s...	Завершена	0	...3bb132	Позавчера в 3:02	16.07.2024
sdto #3	domain	egipetskayasila.online	В работе	0	...16dc51	Позавчера в 3:02	14.07.2024
sdto #4	ipv4port	24.255.255.18	В работе	2	...eec88c	8.07.2024	9.07.2024
webscan #1	ipv4port	255.192.74.12	Завершена	37	...3bb132	1.07.2024	4.07.2024

Строк на странице 10

Перейти на страницу 10

< 1 2 3 ... 9 10 11 >

SCAN FACTORY

SCANFACTORYOWNSC...

- Настройки проекта
- Дашборд
- Угрозы
- Активы
- Утечки
- SSL-сертификаты
- История проверок
- Быстрая проверка
- История действий
- Личный кабинет
- Настройки

Лицензия

5 000 из 10 000 живых хостов

Оплачена до 05.06.2025

Личный кабинет

Установить двухфакторную аутентификацию

Настройки пользователей

ivan@ib.ru — Администратор

seregaib@samosvalbank.ru — Аналитик

Новый пользователь

Имя пользователя

mail@yandex.ru

Пароль

Pa2318ss#2*_428^(word

Права доступа

- (•) Только чтение
- ( ) Аналитик
- ( ) Администратор

Доступ к проектам

Выбрать проекты

Сменить пароль после авторизации

Пользователю будет предложено сменить пароль после первого входа в систему

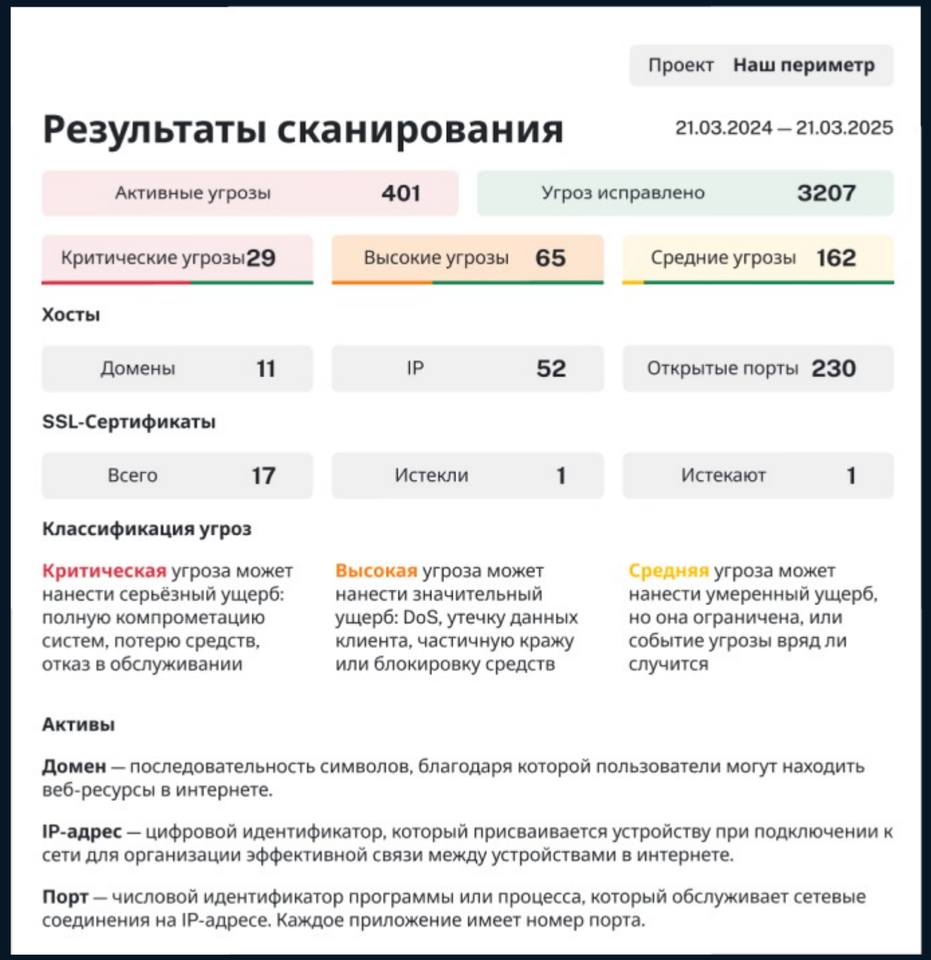
Создать пользователя

Как подключить телеграм-бот с отчётами и уведомлениями

1. Откройте или добавьте в чат бота @scanfactory_reporter_bot
2. Напишите /start
3. Скопируйте и отправьте команду

```
/connect
https://smillychicken.sf-cloud.ru/api/
token eyJhbGcUeadwadawdawdwf...
```

4. Настройте уведомления с помощью команды /settings



Проект Наш периметр

Результаты сканирования

21.03.2024 — 21.03.2025

Активные угрозы	401	Угроз исправлено	3207
Критические угрозы	29	Высокие угрозы	65
Средние угрозы	162		

Хосты

Домены	11	IP	52	Открытые порты	230

SSL-Сертификаты

Всего	17	Истекли	1	Истекают	1

Классификация угроз

Критическая угроза может нанести серьёзный ущерб: полную компрометацию систем, потерю средств, отказ в обслуживании

Высокая угроза может нанести значительный ущерб: DoS, утечку данных клиента, частичную кражу или блокировку средств

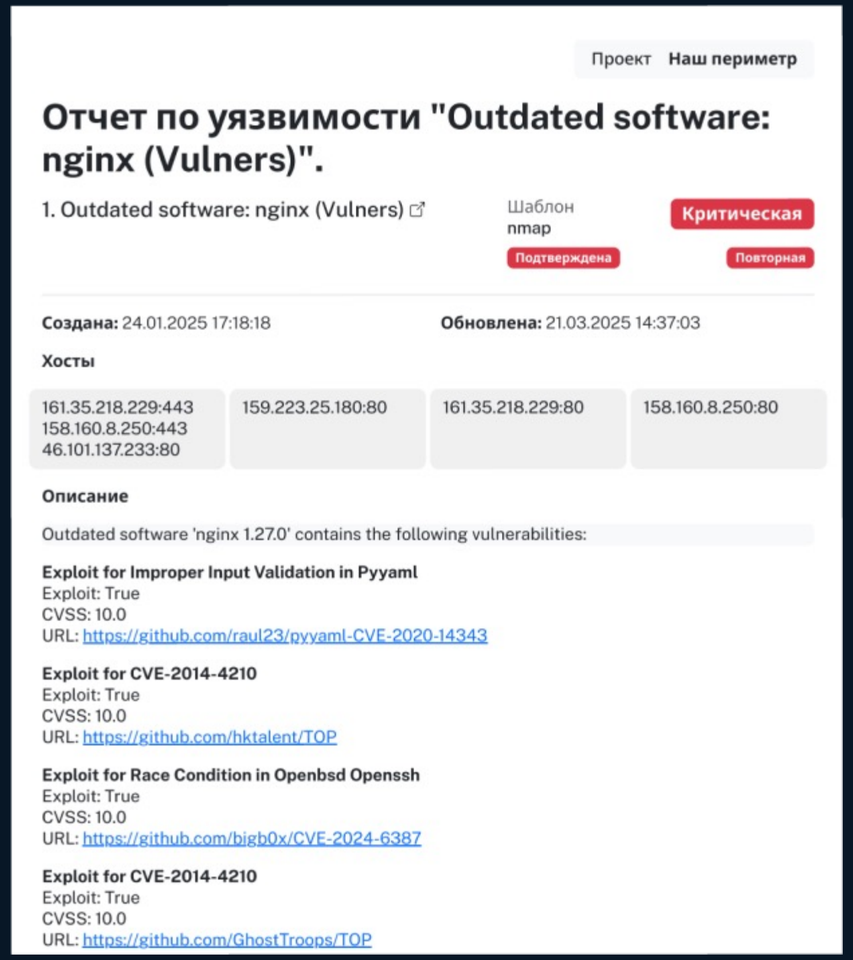
Средняя угроза может нанести умеренный ущерб, но она ограничена, или событие угрозы вряд ли случится

Активы

Домен — последовательность символов, благодаря которой пользователи могут находить веб-ресурсы в интернете.

IP-адрес — цифровой идентификатор, который присваивается устройству при подключении к сети для организации эффективной связи между устройствами в интернете.

Порт — числовой идентификатор программы или процесса, который обслуживает сетевые соединения на IP-адресе. Каждое приложение имеет номер порта.



Проект Наш периметр

Отчет по уязвимости "Outdated software: nginx (Vulners)".

1. Outdated software: nginx (Vulners)

Шаблон nmap

Критическая

Подтверждена

Повторная

Создана: 24.01.2025 17:18:18 **Обновлена:** 21.03.2025 14:37:03

Хосты

161.35.218.229:443 158.160.8.250:443 46.101.137.233:80	159.223.25.180:80	161.35.218.229:80	158.160.8.250:80

Описание

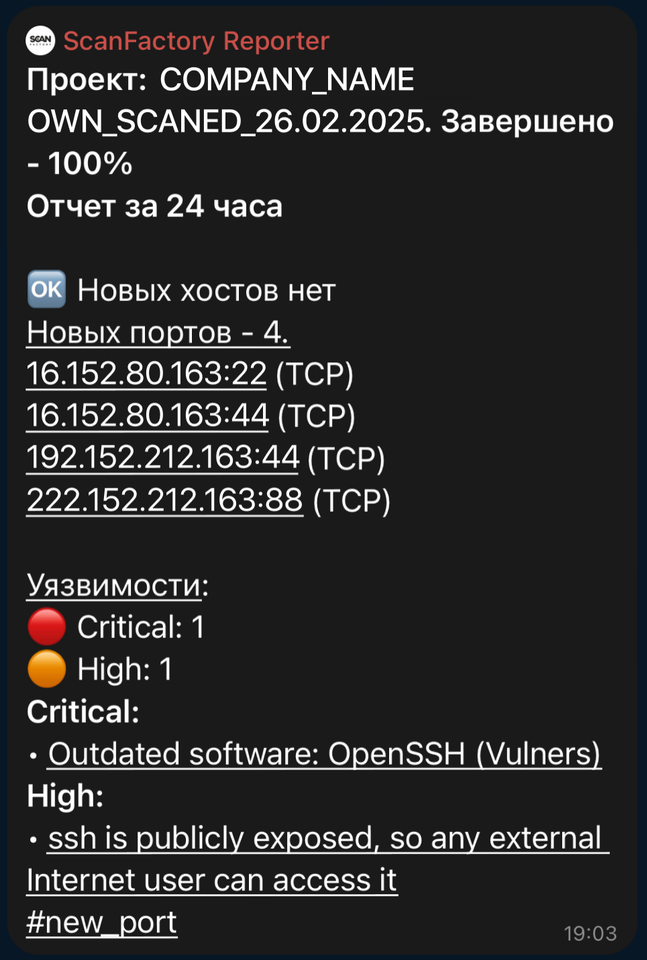
Outdated software 'nginx 1.27.0' contains the following vulnerabilities:

Exploit for Improper Input Validation in Pyyaml
Exploit: True
CVSS: 10.0
URL: https://github.com/raul23/pyyaml-CVE-2020-14343

Exploit for CVE-2014-4210
Exploit: True
CVSS: 10.0
URL: https://github.com/hktalent/TOP

Exploit for Race Condition in Openbsd Openssh
Exploit: True
CVSS: 10.0
URL: https://github.com/bigb0x/CVE-2024-6387

Exploit for CVE-2014-4210
Exploit: True
CVSS: 10.0
URL: https://github.com/GhostTroops/TOP



ScanFactory Reporter

Проект: COMPANY_NAME OWN_SCANED_26.02.2025. Завершено - 100%

Отчет за 24 часа

🆗 Новых хостов нет

Новых портов - 4.

16.152.80.163:22 (TCP)

16.152.80.163:44 (TCP)

192.152.212.163:44 (TCP)

222.152.212.163:88 (TCP)

Уязвимости:

🔴 Critical: 1

🟠 High: 1

Critical:

• Outdated software: OpenSSH (Vulners)

High:

• ssh is publicly exposed, so any external Internet user can access it

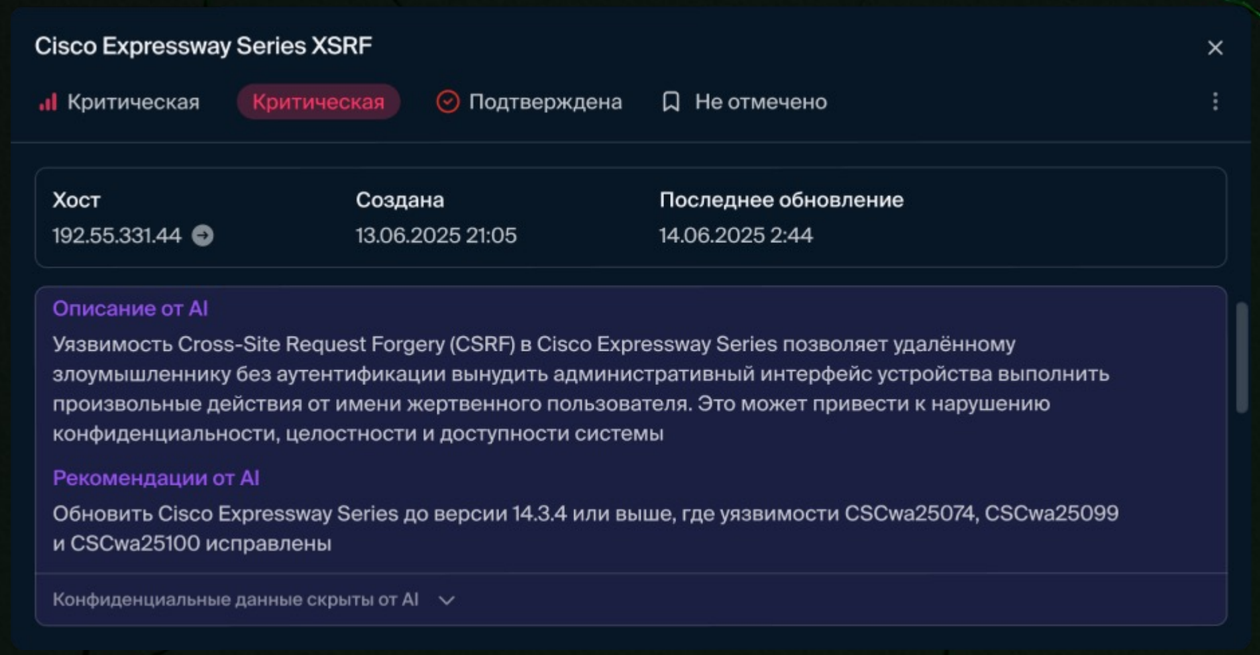
#new_port

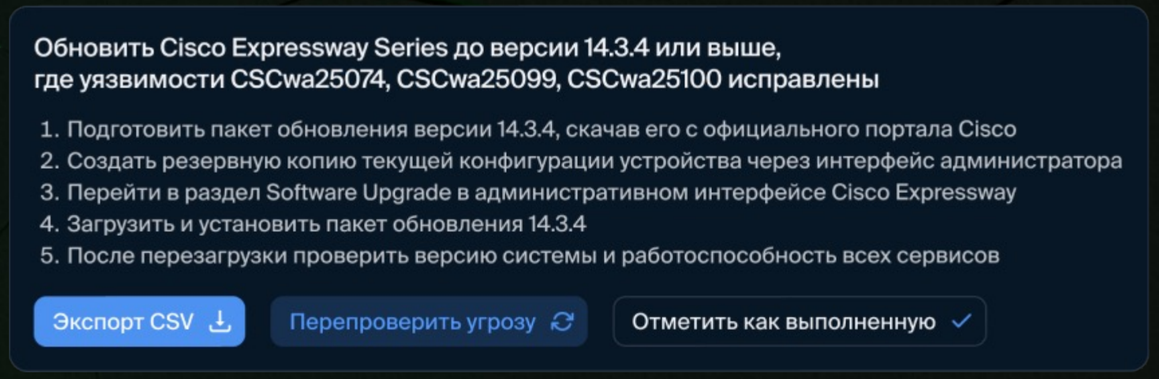
19:03

Регулярно обновляем продукт

SCAN FACTORY

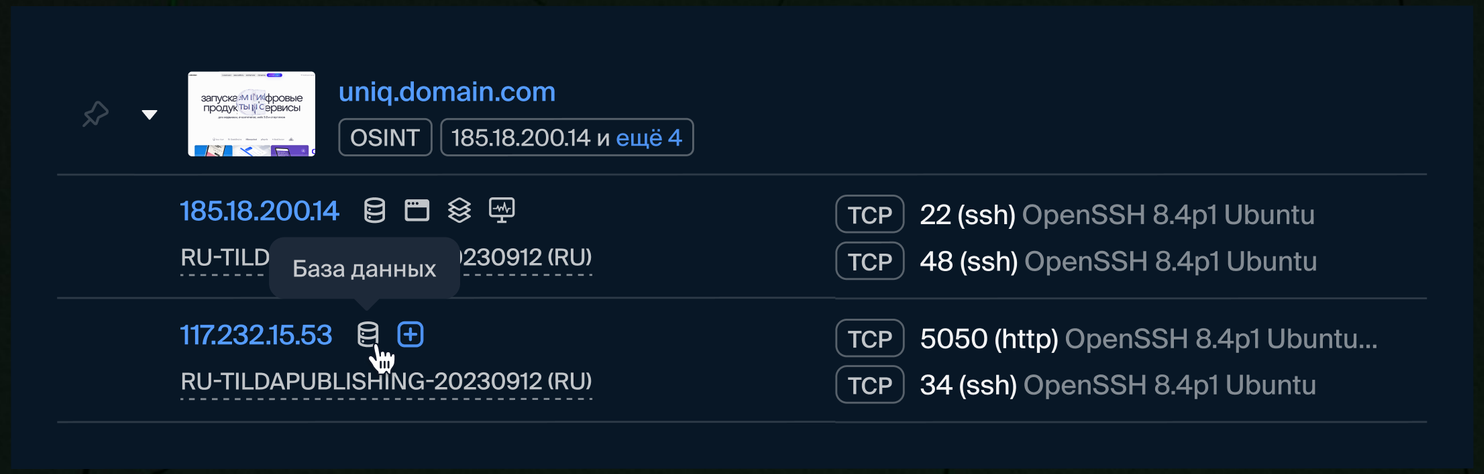
AI для верификации угроз, генерации их описаний и подготовки инструкций по устранению

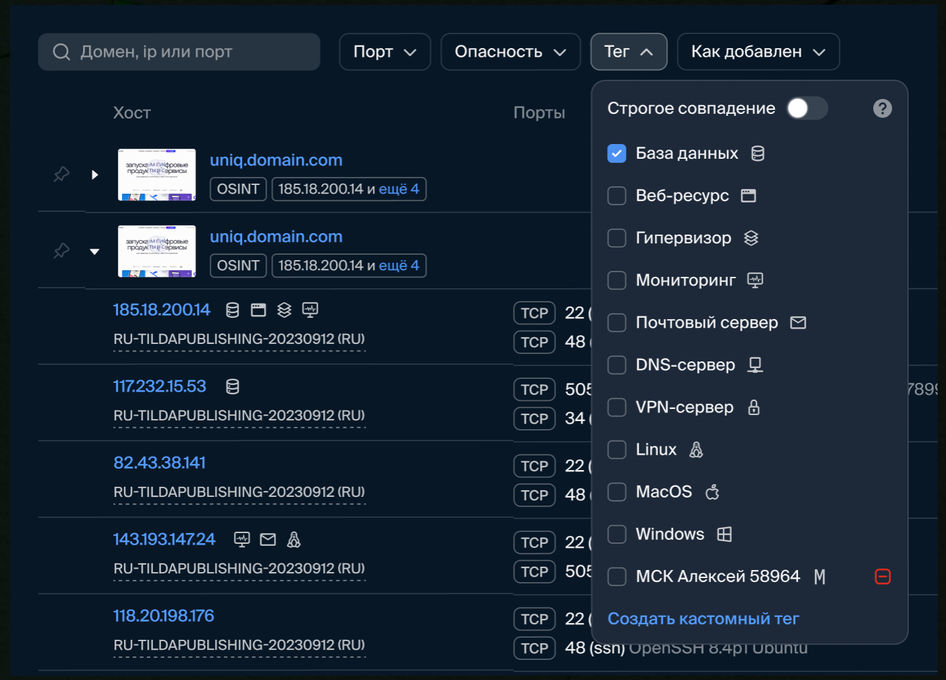




SCAN FACTORY

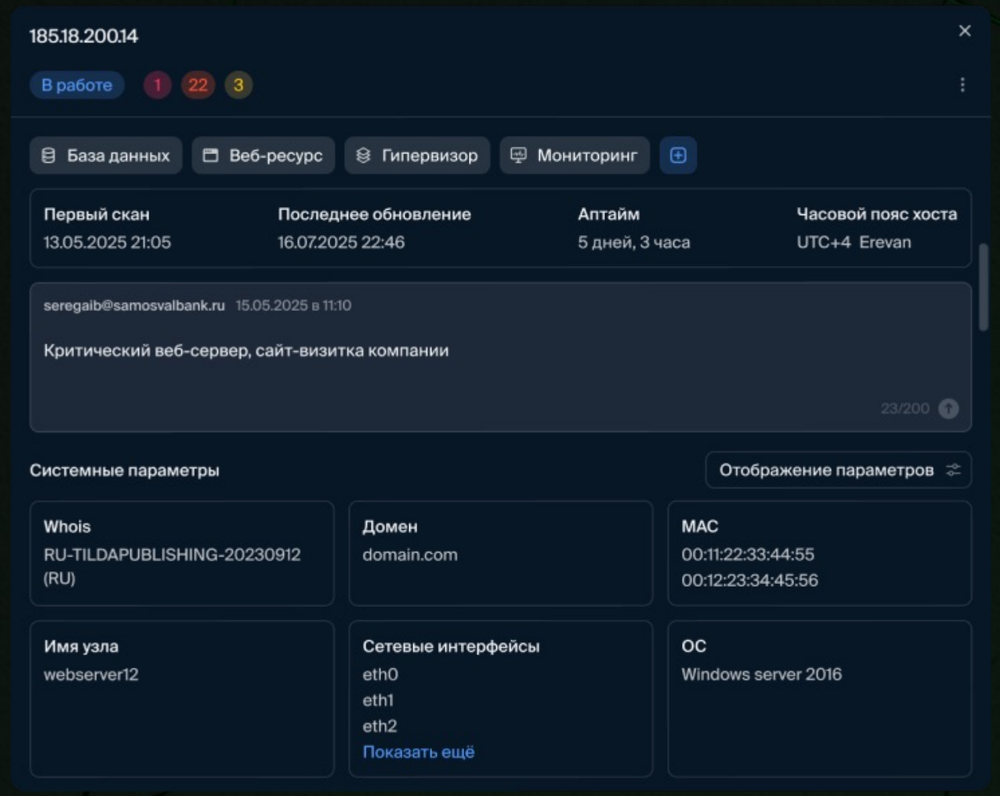
AI-тегирование для разметки и фильтрации групп активов

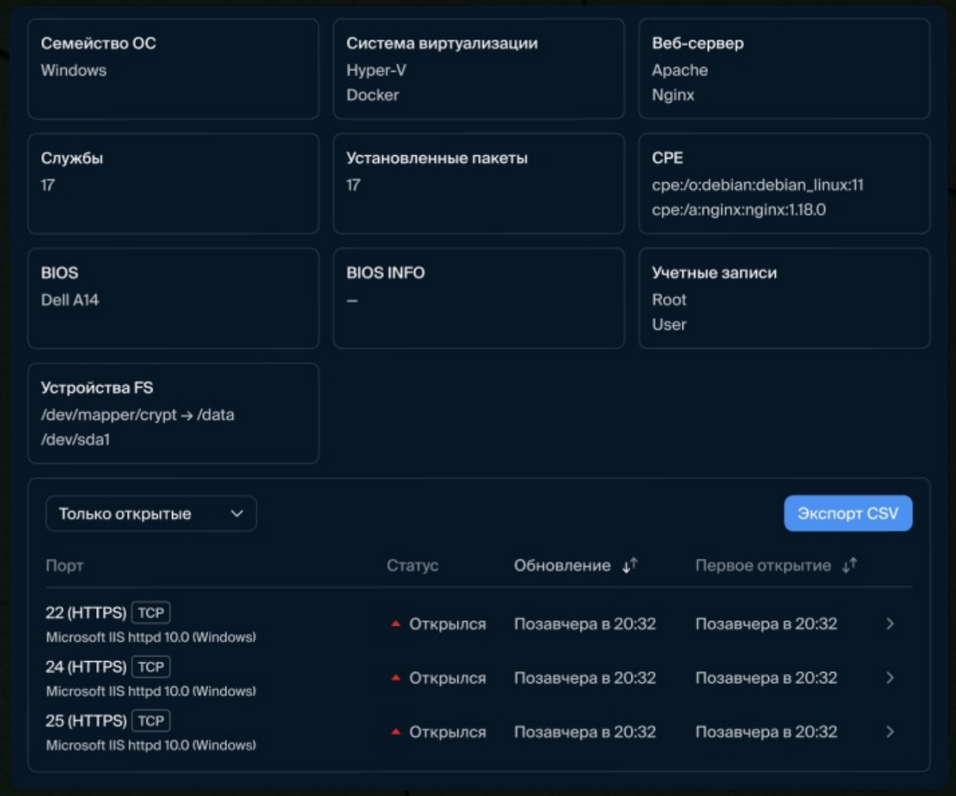




SCAN FACTORY

Карточка актива для отображения всех данных, полученных при сканировании





SCAN FACTORY

Roadmap 2025

Инструкции
для исправления
уязвимостей от AI

Redcheck

ФСТЭК-сертифицированный сканер

Интерактивная
карта атак

SCAN FACTORY

Подписывайтесь на наш телеграм-канал

AM ANTI-MALWARE

CISOCLUB

Все о платформе ScanFactory VM

На CISOCLUB вышел обзор нашей платформы для анализа защищенности.

Из него вы узнаете, как решение помогает управлять уязвимостями на внешнем (EASM) и внутреннем (VM) периметре, и предотвращать утечки паролей для комплексной защиты вашего бизнеса.

В обзоре:
- функциональные возможности
- архитектура решения
- сценарии использования
- системные требования для On-Premise версии
- планы развития

» Читать обзор