

The logo features a stylized white icon of two overlapping squares on the left. To its right, the text 'RT Protect' is stacked vertically in a bold, sans-serif font. Further to the right, the letters 'EASM' are displayed in a significantly larger, bold, sans-serif font.

RT Protect EASM

Сервис непрерывного исследования защищенности всех
внешних активов и ресурсов организации



RT Protect EASM



RT Protect EASM — решение, включающее в себя инвентаризацию и непрерывное отслеживание всех внешних активов и ресурсов организации, механизмы для обнаружения фишинговых доменов, упоминаний организации в утечках информации и на хакерских форумах, а также оценку и управление рисками в отношении потенциальных уязвимостей и угроз информационной безопасности.

Решаемые задачи RT Protect EASM



03. Сокращение рисков кибератак

04. Определение потенциально фишинговых доменов

02. Выявление уязвимостей 24/7

05. Широкие возможности интеграций

01. Мониторинг изменений во внешней инфраструктуре

06. Поиск упоминаний в утечках информации и на хакерских форумах

 RT Protect EASM

Мониторинг изменений во внешней инфраструктуре

The image shows a screenshot of a security monitoring interface. The main window displays a table of scan results with columns for event type, network address, port, protocol, service, version, SSL status, and description. Below the table are navigation tabs for different scan types. A detailed view of a scan history is shown in a separate window, listing scan dates, times, sources, protocols, and services.

Сканирования

Задача: [] x | Дата первого сканирования: [] x | Дата второго сканирования: [] x

Ввод идентификаторов сканиваний

Пассивное сканирование 3 | Активное сканирование 214 | Поиск утечек 0 | Сканирование веб-адресов 72 | Брутфорс веб-адресов 0 | Сертификаты 0 | Веб-компоненты 0

Тип события	Сетевой адрес	Порт	Протокол	Сервис	Версия	SSL	Описание
Новая запись	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Новая запись	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Новая запись	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[]	21	ftp	нет данных	нет данных	Выкл	нет данных
Измененная запись	[]	21	нет данных	нет данных	нет данных	Выкл	нет данных

Подробности о результате

История (4)

Дата: 07.11.2023, 20:44:59	Сетевой адрес: []
Источник: nmap	Порт: 465
Протокол: smtp	Сервис: Postfix smtpd
Версия: нет данных	SSL: Вкл
Описание: нет данных	
Дата: 08.11.2023, 15:30:05	Сетевой адрес: []
Источник: nmap	Порт: 465

- 01.** Формирует «слепок» внешней инфраструктуры на момент сканирования;
- 02.** Уведомляет об изменениях на периметре;
- 03.** Строит таймлайн изменений;
- 04.** Позволяет выявить перемены на внешних ресурсах (смена сертификата, открытие порта и т.д.);

Выявление уязвимостей 24/7

Критичность: **V3.1: 9.8 Критическая**

Сканирование: К сканированию

Семейство: RCE

Ссылки: <https://helpdesk.bitrix24.com/open/15536776/>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-27228>
<https://nvd.nist.gov/vuln/detail/CVE-2022-27228>

Решение: Разработчик продукта рекомендует обновить модуль «Опросы, голосования» (Polls, Votes (vote)) до версии 21.0.100

Описание: В модуле голосования (он же «Опросы, Голосования») до 21.0.100 Bitrix Site Manager удаленный неаутентифицированный злоумышленник может выполнить произвольный код.

Название	Критичность	Порт	Компания	Сканирование	Сетевой адрес
CVE-2022-27228	V3.1: 9.8 Критическая	443		К сканированию	
CVE-2022-41040	V3.1: 8.8 Высокая	443		К сканированию	
CVE-2022-41082	V3.1: 8.0 Высокая	443		К сканированию	

01

Выполняет периодическое сканирование внешнего периметра;

02

Выявляет уязвимости как на основе версий, так и активным методом;

03

Ищет уязвимости как в общесистемном ПО, так и в WEB-приложениях;

Сокращение рисков кибератак

- 01.** Уменьшает вероятность появления shadow it ресурсов за счет постоянного мониторинга;
- 02.** Позволяет качественно выстраивать процесс управления уязвимостями благодаря их своевременному обнаружению;
- 03.** Автоматически выполняет часть тех действий, которые АРТ-группировки выполняют вручную;

RT Protect EASM

Сканирования
Панель управления
Трассировочные пути

управление

Таргеты
Задачи
Расписания
Интеграции
Компании

Главная страница / Панель управления

Панель управления

Домены
Активное сканирование
Поиск уязвимостей
Сертификаты
Подробности

Главная страница / Трассировочные пути

Трассировочные пути

Версия: 1.1.

Определение потенциально фишинговых доменов

- 01.** Позволяет своевременно реагировать на появление фишинговых доменов;
- 02.** Уменьшает вероятность успешного выполнения фишинговых атак;
- 03.** Позволяет сохранить репутацию благодаря быстрому обнаружению фишингового домена;



Подробности о результате

История (1)

Вход

Пожалуйста введите свои логин и пароль

Имя пользователя

Пароль

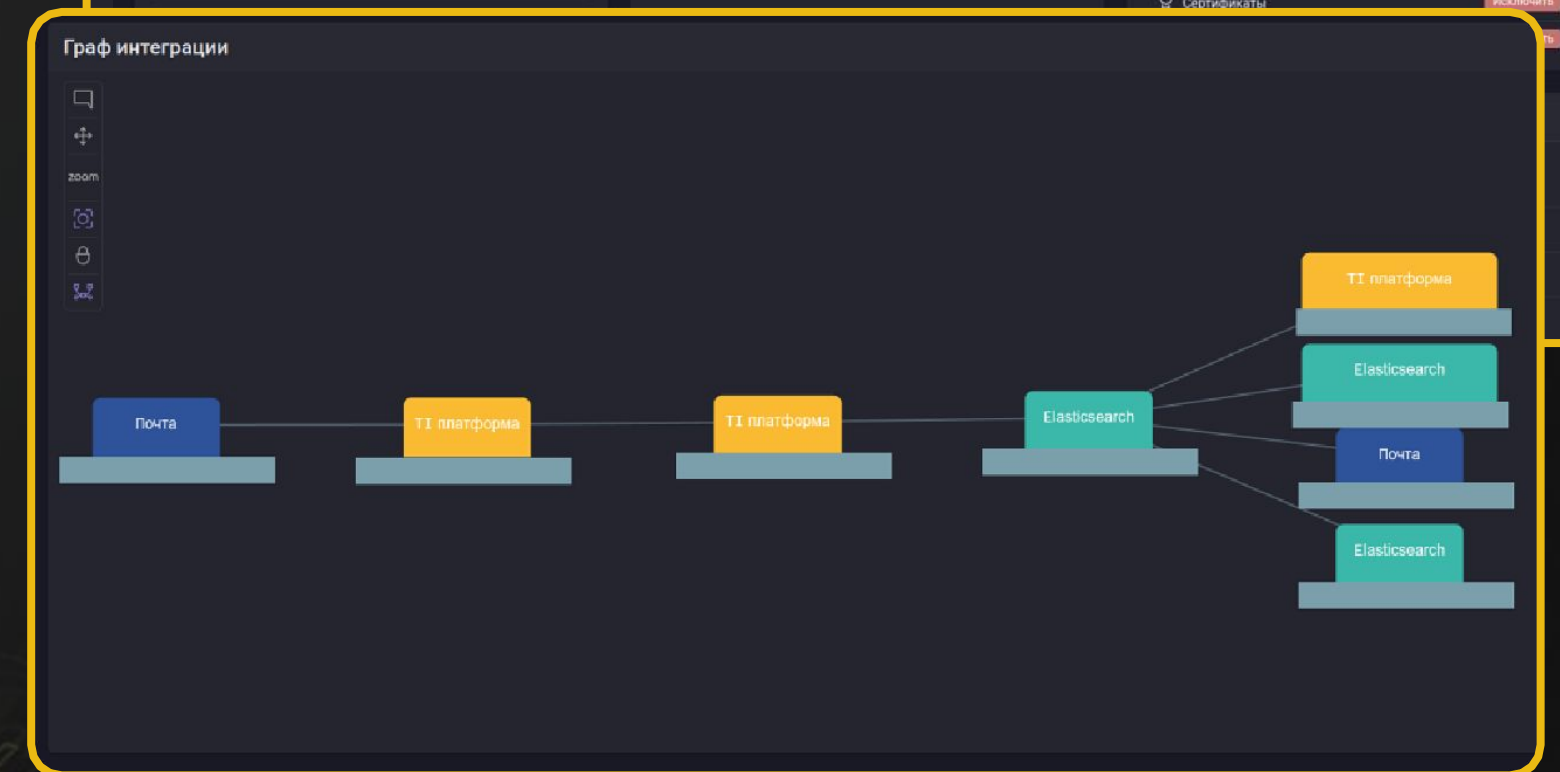
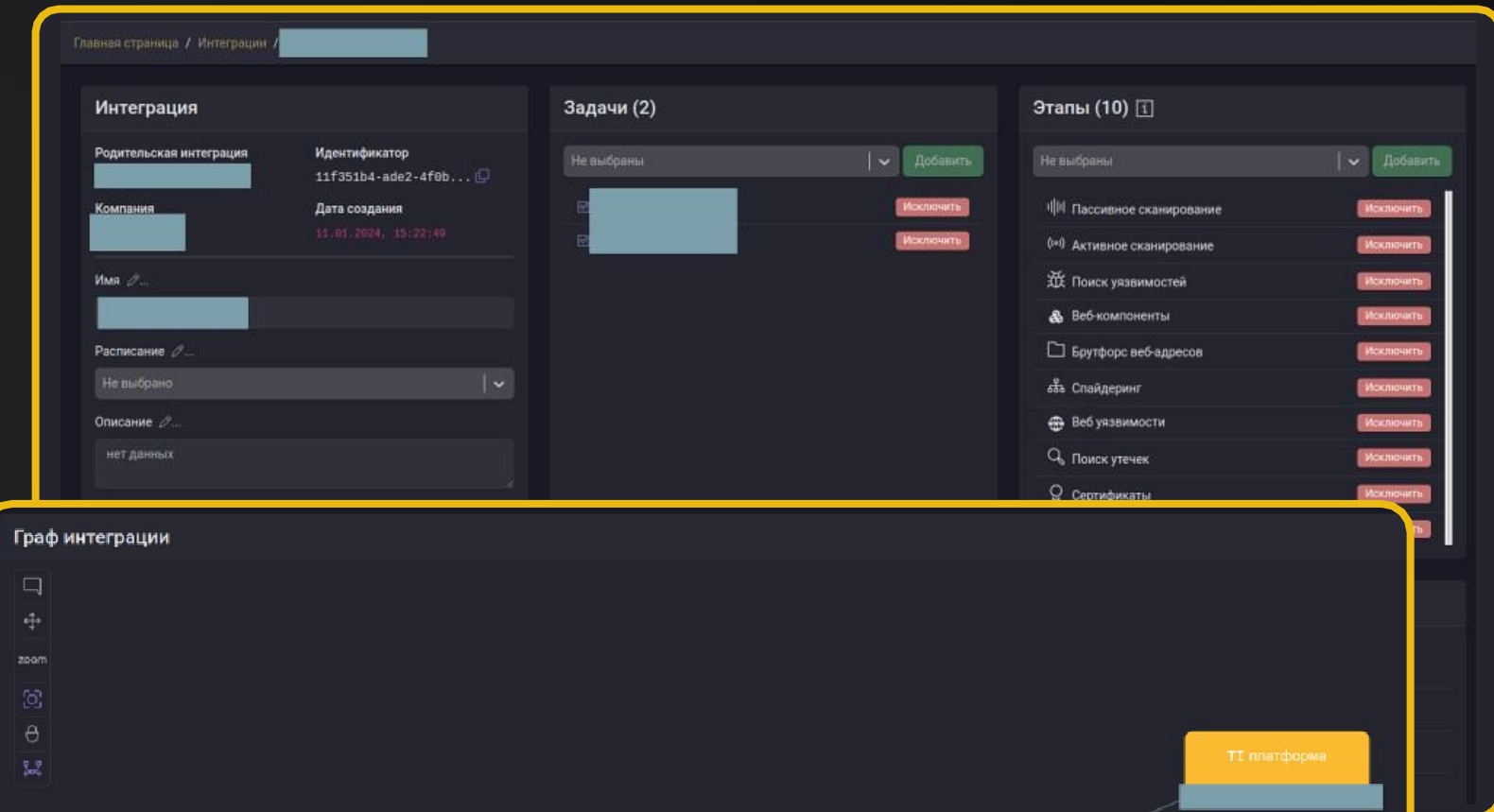
Войти

[Забыли пароль?](#)

Фишинговый домен	Домен
Сканирование	Идентификатор
К сканированию	ae023864-8eb2-4a98...
Сетевые адреса	Почтовые адреса

Широкие возможности интеграций

- 01.** Интеграция с RT Protect TI позволяет улучшить качество определения фишинговых доменов;
- 02.** Интеграции с системами класса IRP, SOAR, SIEM позволяют оперативно реагировать на инциденты;
- 03.** Присутствует возможность связи интеграций в граф;
- 04.** Каждая из интеграций в графе может проводить преобразование и обогащение данных;



Поиск упоминаний в утечках информации на хакерских форумах

- 01.** Выявляет готовящиеся атаки;
- 02.** Определяет пользователей, зарегистрировавших личный аккаунт на рабочую почту;
- 03.** Помогает проверить соответствуют ли пароли (из утечек) пользователей парольной политике компании;

The screenshot displays a security tool interface. At the top, there is a table with columns for 'Почта' (Email), 'Логин' (Login), and 'Пароль' (Password). Below this, a modal window titled 'Задачи требующие рассмотрения' (Tasks requiring attention) is open, showing a notification: 'Обнаружено новое упоминание компании' (New company mention detected). The notification details include the sender, a link to the message, and the detection rule used. The rule text lists various hashtags and phrases related to cyberattacks and hacker groups.

Почта	Логин	Пароль
Kaarineluz@hotmail.com	нет данных	paramore729
theo_12004@hotmail.com	нет данных	Antonomasia9!
mery_moon89@hotmail.com	нет данных	Illuminatti89
alex_hernandez_89@hotmail.com	нет данных	Eh19449656
		lazyback30
		Ethan6262.
		parola41
		lillo1965
		Serafina1.
		Scorpion22
		Bol8027597
		samsam
		Assasin95!
		Burgers31!
		Sukhvir3970
		Nexoone3
		Keinara

Задачи требующие рассмотрения

Обнаружено новое упоминание компании

Отправитель: [redacted] type attack.ddos

Ссылка на сообщение: [redacted]

Правило обнаружения: [redacted]

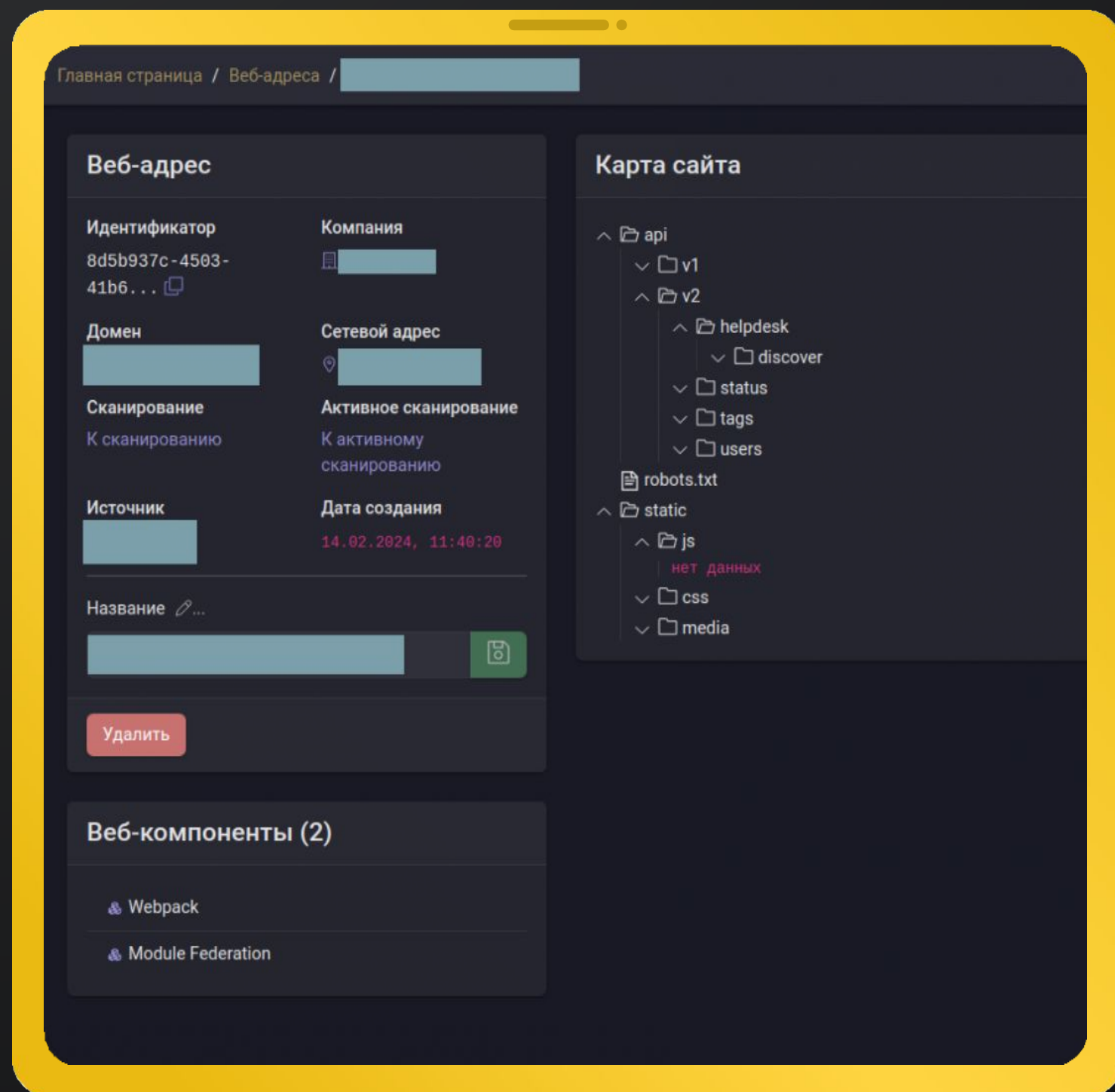
#idiotallackersindia
#fuckhackersindia
#fucksistemindia

thanks to c.o.a member:
#gamesia_team
#garuda_from_cyber
#lulzsec_indonesia
#garuda_cyber_operations
#from_lammer_to_mastah
#ketapang_gray_hat
#starsx_cyber_team
#islam_cyber_team
#moroccan_black_cyber_army
#hacktivist_jatim

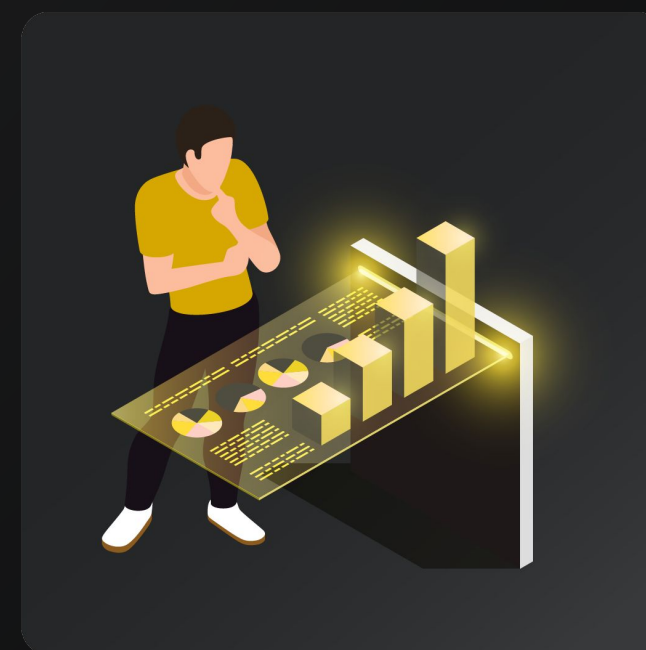
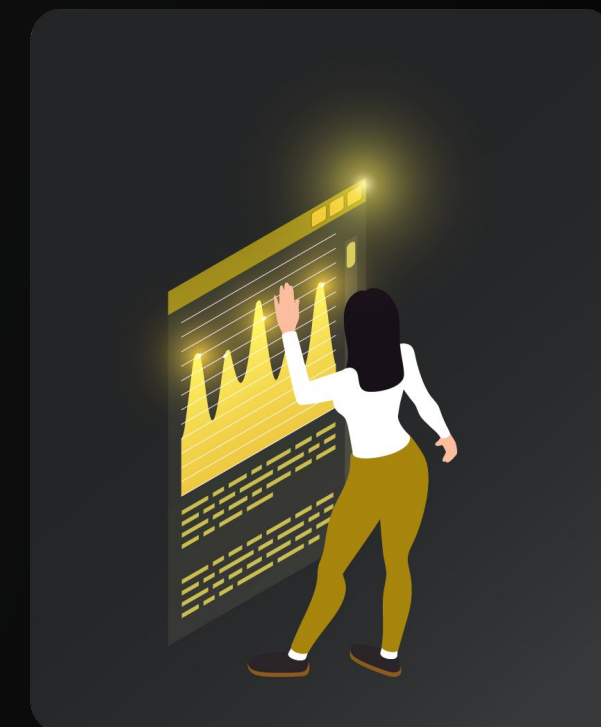
greatz:

Ложная сработка Верная сработка Отмена

Возможности RT Protect EASM

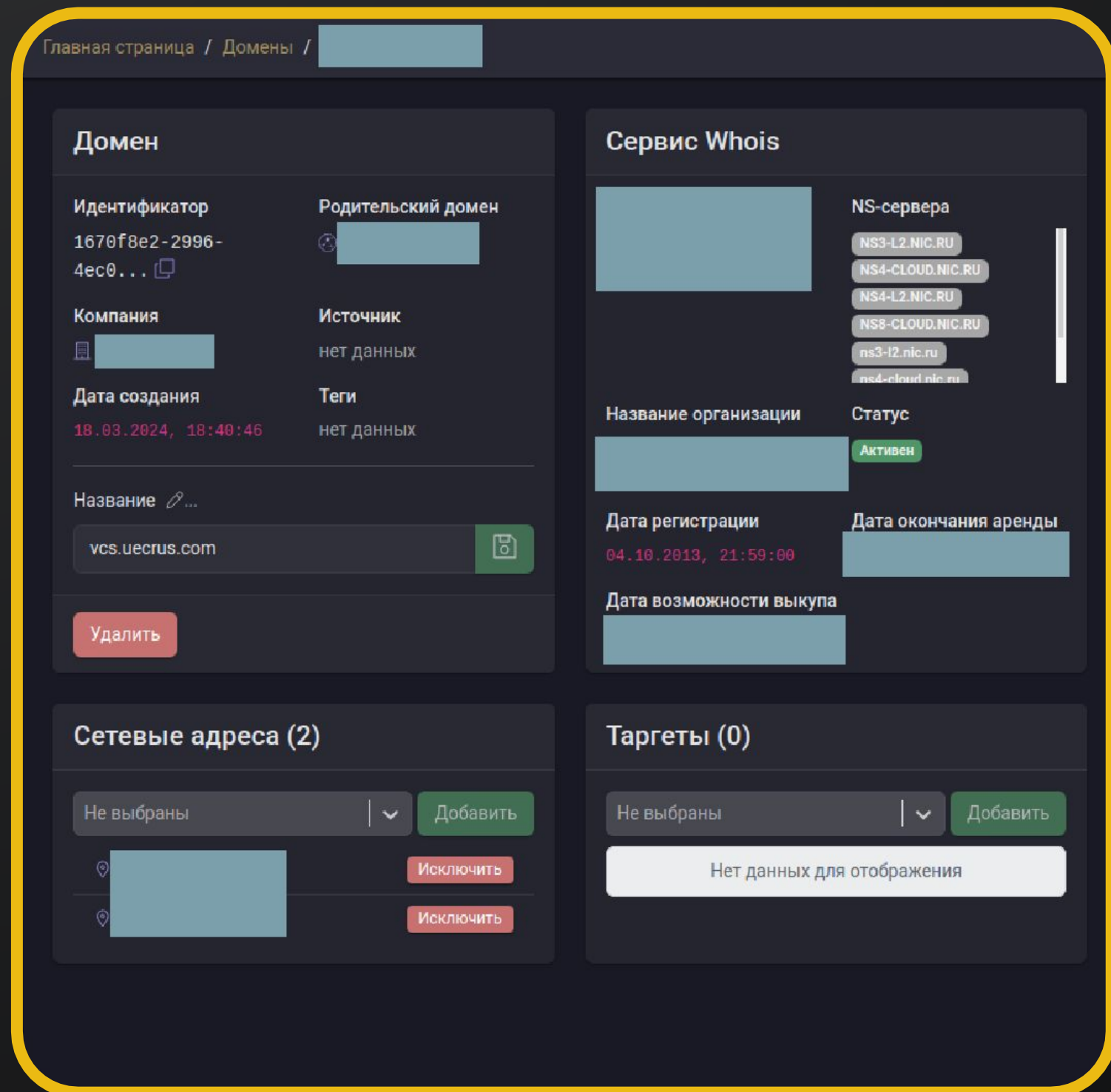


- 01.** Пассивное сканирование – поиск поддоменов и ip-адресов;
- 02.** Активное сканирование – определение открытых портов, сервисов и служб;
- 03.** Поиск уязвимостей в доступных сервисах;
- 04.** Анализ веб-сервисов – поиск уязвимых и устаревших компонентов, пассивный поиск уязвимостей на основании версии сервиса;



- 05.** Брутфорс - перебор директорий на сайте и dns имен;
- 06.** Поиск учетных записей в публичных утечках информации;
- 07.** Поиск фишинговых доменов;
- 08.** Поиск упоминаний в утечках информации и хакерских форумах;

Решение позволяет:



Главная страница / Домены / [redacted]

Домен

Идентификатор: 1670f8e2-2996-4ec0...
Родительский домен: [redacted]
Компания: [redacted] | Источник: нет данных
Дата создания: 18.03.2024, 18:40:46 | Теги: нет данных
Название: vcs.uecrus.com
Удалить

Сервис Whois

NS-сервера: NS3-L2.NIC.RU, NS4-CLOUD.NIC.RU, NS4-L2.NIC.RU, NS8-CLOUD.NIC.RU, ns3-l2.nic.ru, ns4-cloud.nic.ru
Название организации: [redacted] | Статус: Активен
Дата регистрации: 04.10.2013, 21:59:00 | Дата окончания аренды: [redacted]
Дата возможности выкупа: [redacted]

Сетевые адреса (2)

Не выбраны | Добавить
[redacted] | Исключить
[redacted] | Исключить

Таргеты (0)

Не выбраны | Добавить
Нет данных для отображения

01

Определять изменения на внешнем сетевом периметре Организации;

02

Находить уязвимости и эксплуатировать их;

03

Искать утечки учётных записей в открытых источниках;

04

Определять уязвимые компоненты на веб сервисах;

05

Обнаруживать ресурсы, доступные из сети Интернет;

06

Собирать информацию о сертификатах на внешних сервисах.

RT Protect EASM

Веб-интерфейс RT Protect EASM позволяет в реальном времени отображать информацию о сканируемых доменах.

Продукт построен по принципу микросервисной архитектуры, что позволяет масштабировать необходимые сервисы в зависимости от нагрузки.

Информация о сертификате

Идентификатор с45a6d34-64eb-46cb...	Сканирование К сканированию
Активное сканирование К активному сканированию	Компания [Redacted]
Домен [Redacted]	Источник cрт

Детали сертификата

```
{ 11 items
  "subject": { 1 item
    "CN": [Redacted]
  }
  "issuer": { 3 items
    "C": "US"
    "O": "Let's Encrypt"
    "CN": "R3"
  }
  "has-expired": false
  "not-after": [Redacted]
  "not-before": [Redacted]
  "serial-number": 3.5400457763178456e+41
  "serial-number(hex)": [Redacted]
  "signature-algorithm": "sha256WithRSAEncryption"
  "version": 2
  "public-key-length": 256
  "extensions": { 9 items
    "keyUsage": "Digital Signature"
    "extendedKeyUsage":
      "TLS Web Server Authentication, TLS Web Client Authentication"
    "basicConstraints": "CA:FALSE"
    "subjectKeyIdentifier":
```

Нам доверяют



Контакты

Адрес: 117587, г.

Москва, Варшавское шоссе, дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru



РТ

Информационная
безопасность

