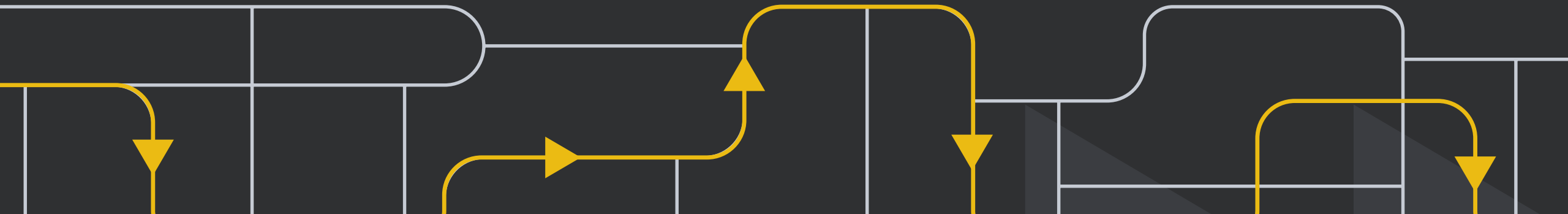
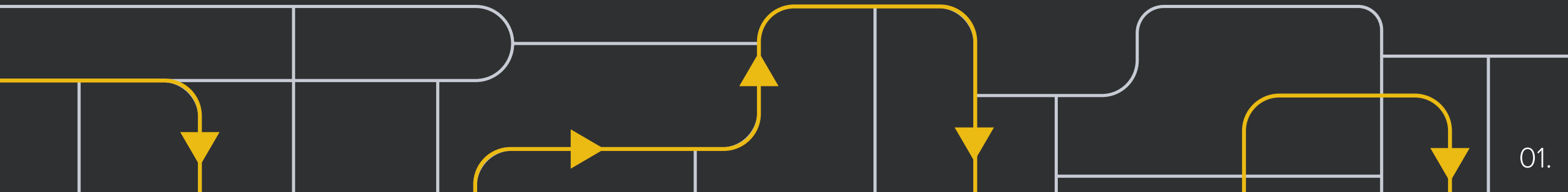
RT Protect EASM

Сервис непрерывного исследования защищённости всех внешних активов и ресурсов организации

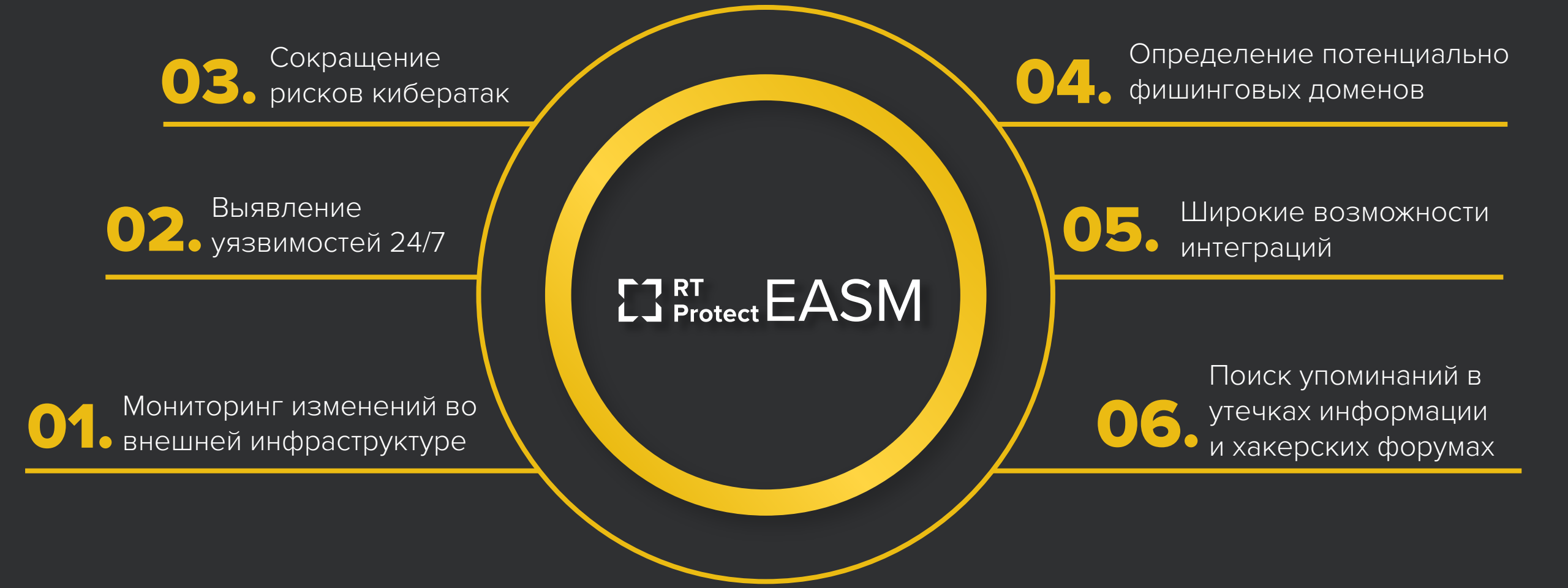


RT Protect EASM

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



01. Мониторинг изменений во внешней инфраструктуре

02. Выявление уязвимостей 24/7

03. Сокращение рисков кибератак

04. Определение потенциально фишинговых доменов

05. Широкие возможности интеграций

06. Поиск упоминаний в утечках информации и хакерских форумах

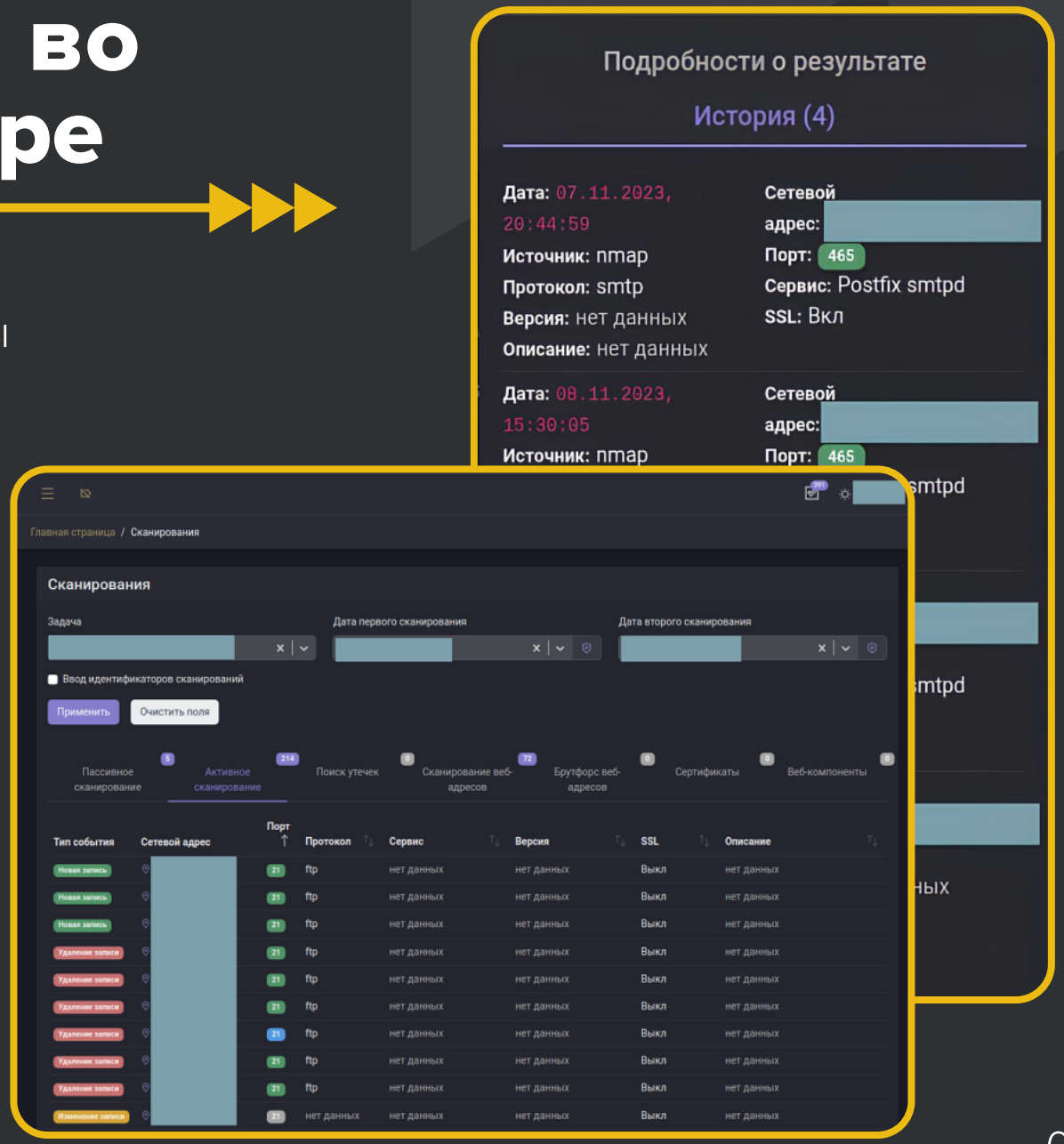
Мониторинг изменений во внешней инфраструктуре

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 тд);



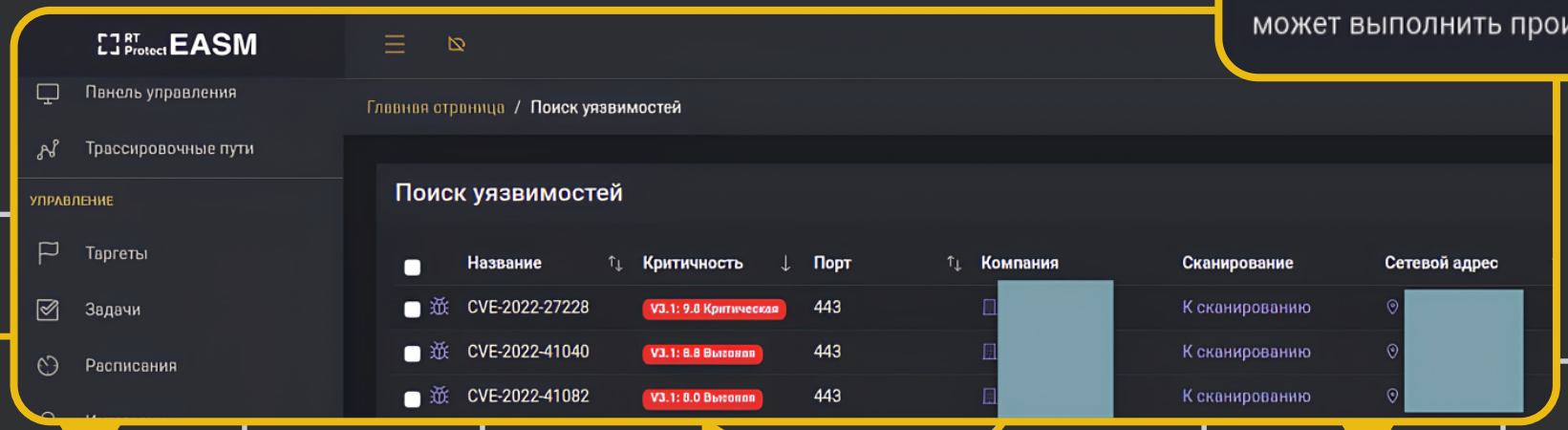
Выявление уязвимостей 24/7

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;

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.

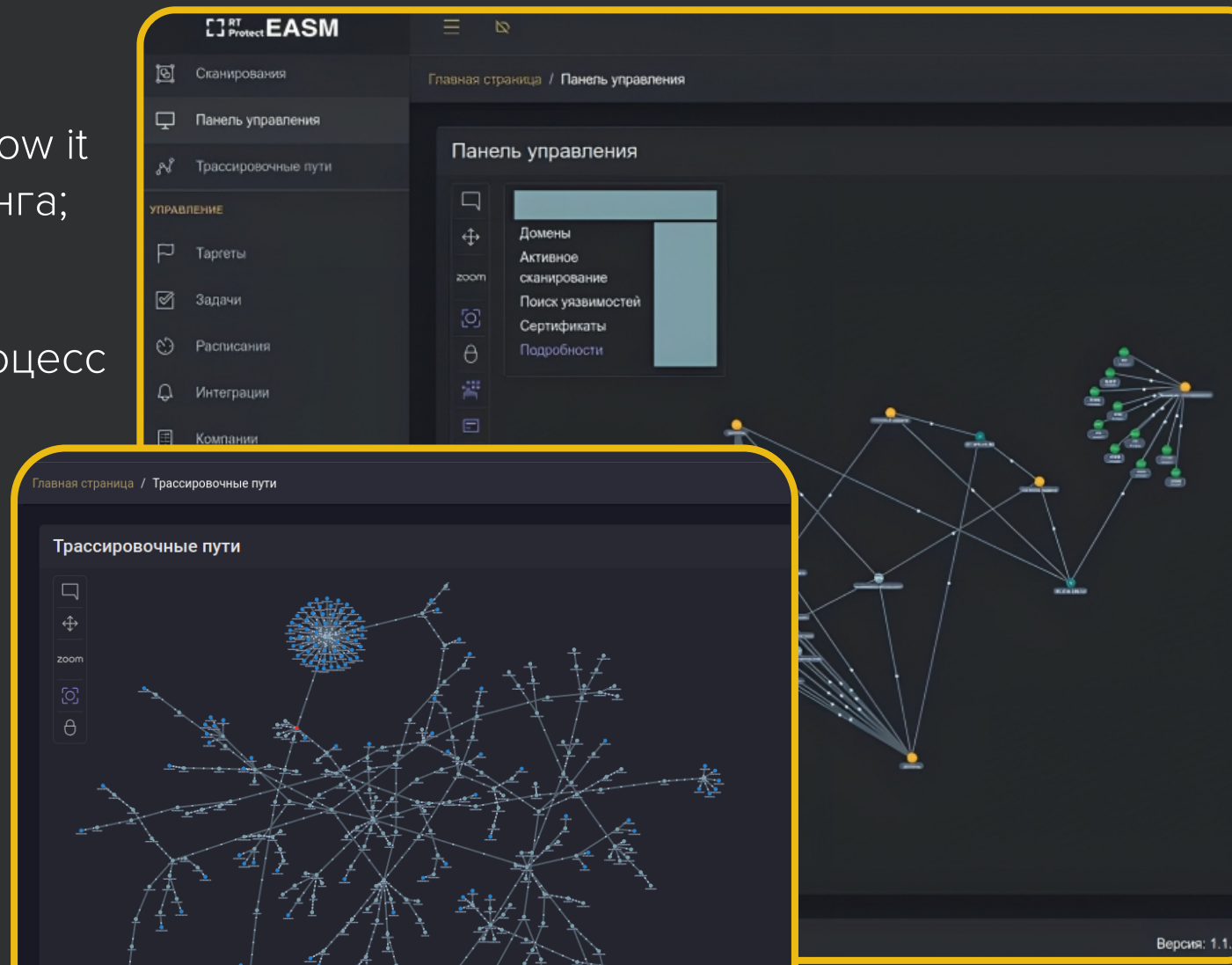


Сокращение рисков кибератак

01. Уменьшает вероятность появления shadow it ресурсов за счёт постоянного мониторинга;

02. Позволяет качественно выстраивать процесс управления уязвимостями благодаря их своевременному обнаружению;

03. Автоматически выполняет часть тех действий, которые APT-группировки выполняют вручную;

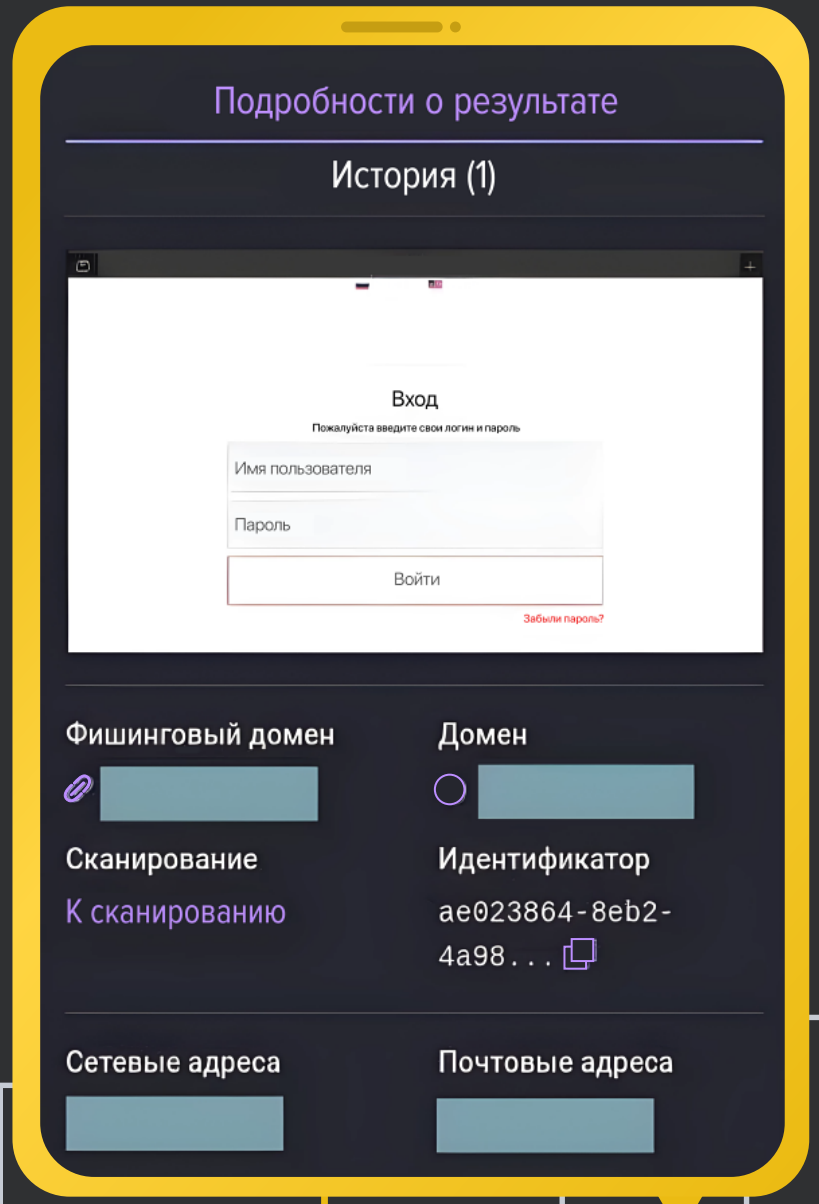


Определение потенциально фишинговых доменов

01. Позволяет своевременно реагировать на появление фишинговых доменов;

02. Уменьшает вероятность успешного выполнения фишинговых атак;

03. Позволяет сохранить репутацию благодаря быстрому обнаружению фишингового домена;



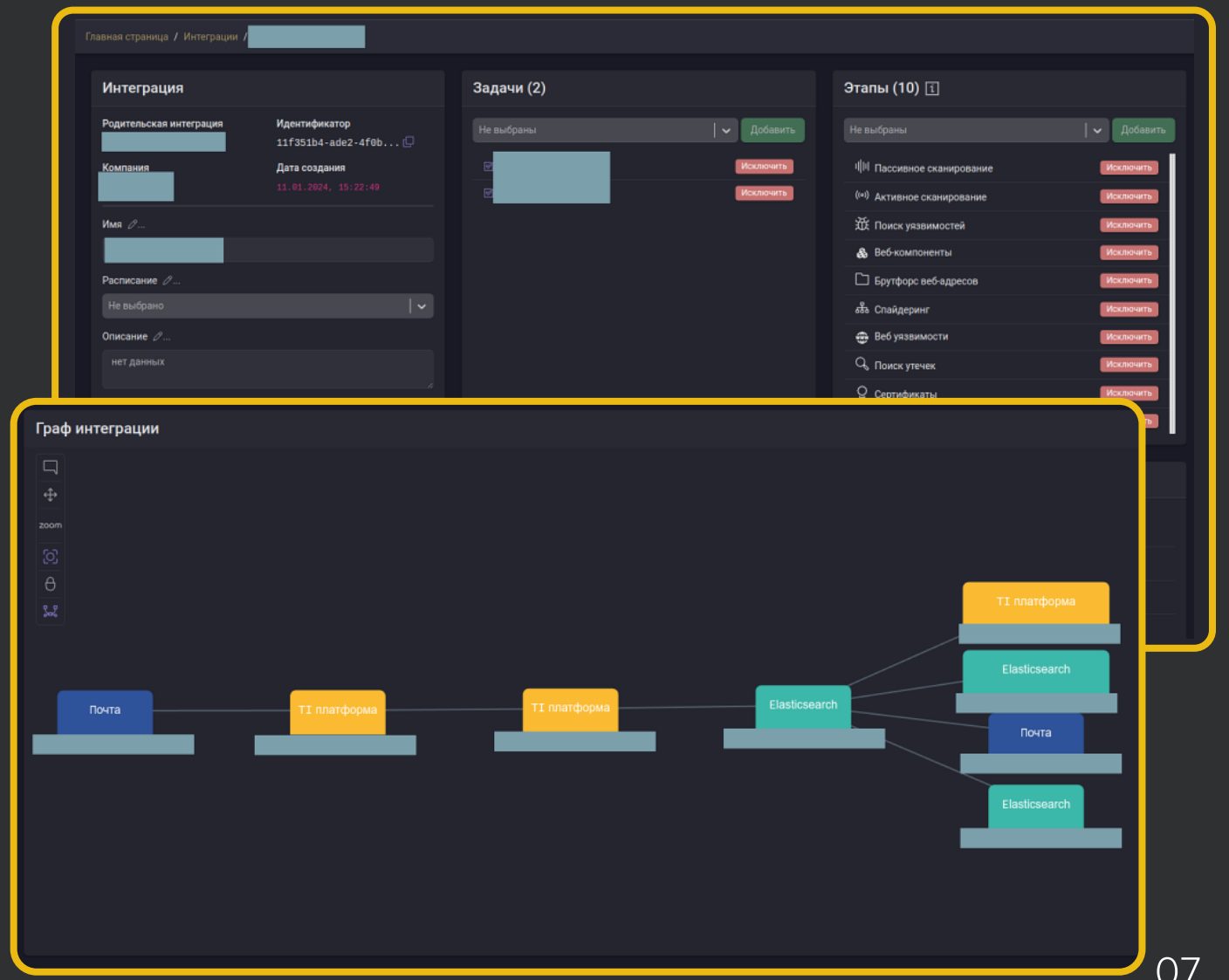
Широкие возможности интеграций

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;

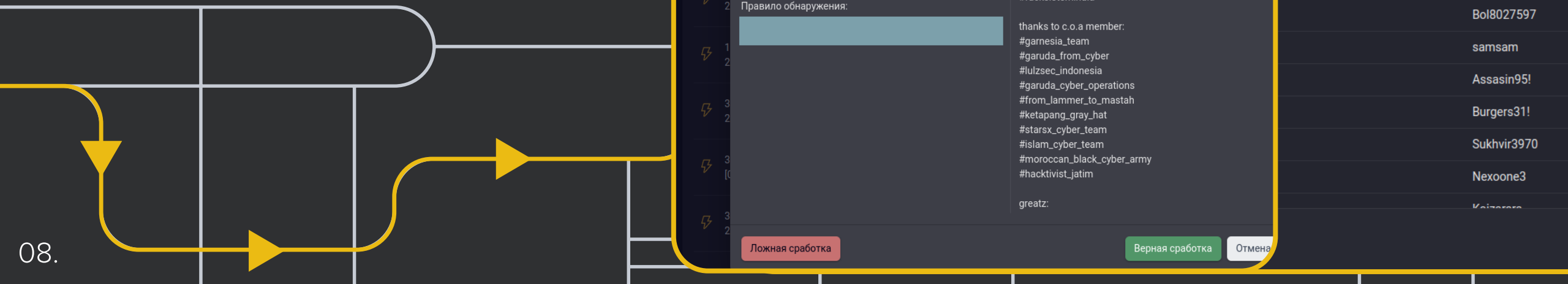


Поиск упоминаний в утечках информации и хакерских форумах

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;



Почта	Логин	Пароль
Kaarineluz@hotmail.com	нет данных	paramore729
theo_12004@hotmail.com	нет данных	Antonomasia9!
mery_moon89@hotmail.com	нет данных	Iluminatti89
alex_hernandez_89@hotmail.com	нет данных	Eh19449656
		lazyback30
		Ethan6262.
		parola41
		lillo1965
		Serafina1.
		Scorpion22
		Bol8027597
		samsam
		Assasin95!
		Burgers31!
		Sukhvir3970
		Nexoone3

Задачи требующие рассмотрения

Обнаружено новое упоминание компании

Отправитель:

Ссылка на сообщение:

Правило обнаружения:

type attack:ddos

#idiotallackersindia
#fuckhackersindia
#fucksistemindia

thanks to c.o.a member:
#garnesia_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:

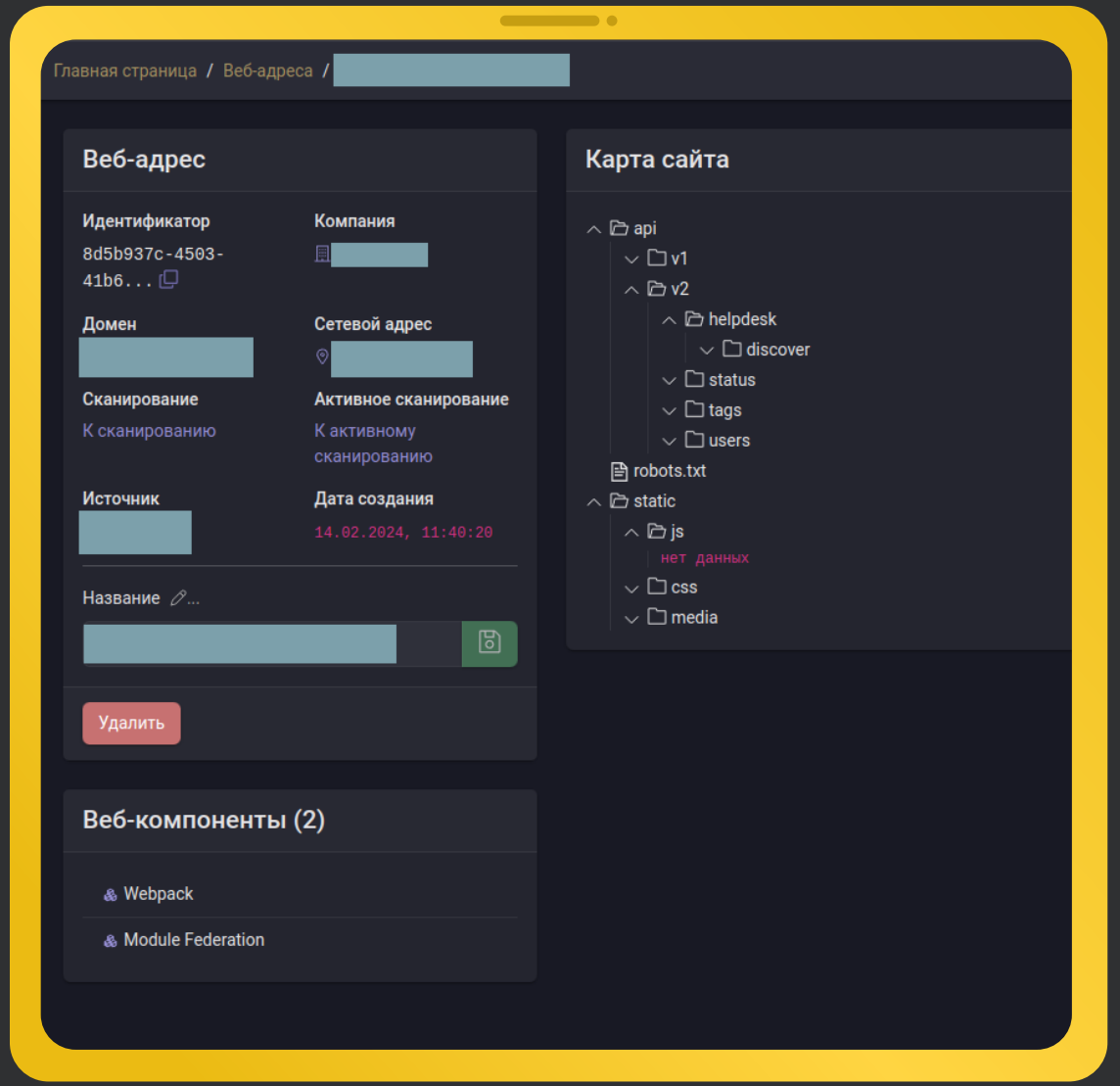
Ложная сработка

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 имён;
06. **Поиск учётных записей** в публичных утечках информации;
07. **Поиск фишинговых доменов**;
08. **Поиск упоминаний** в утечках информации и хакерских форумах;



RT Protect EASM

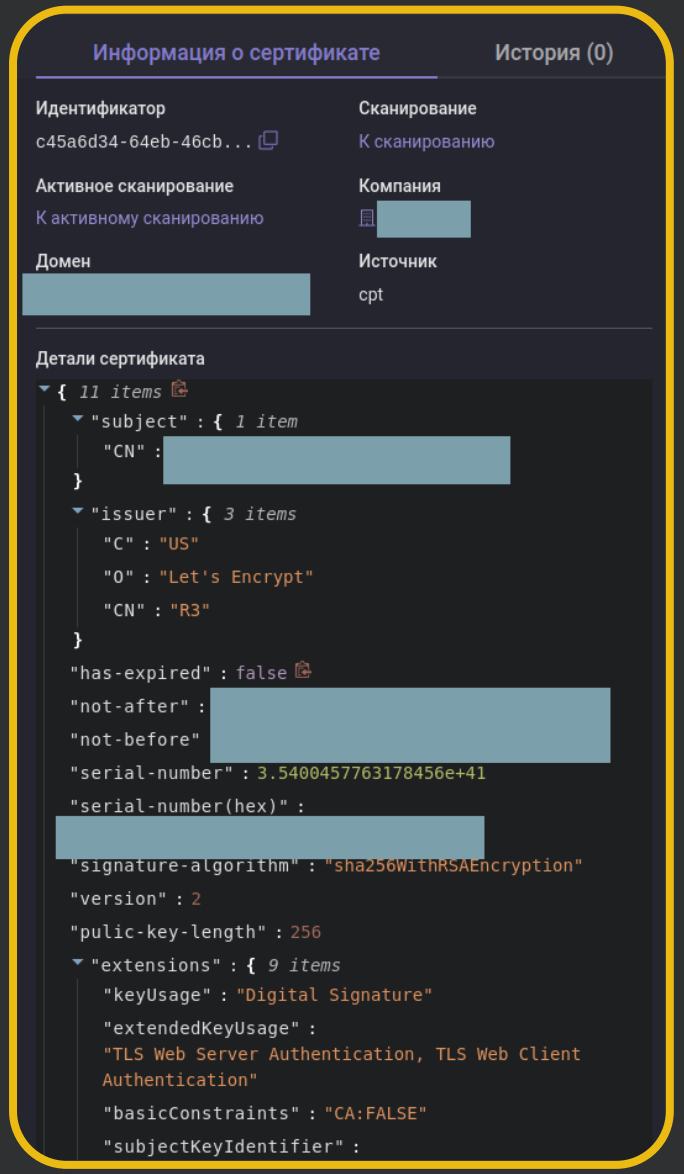
Решение позволяет:

- Определять изменения на внешнем сетевом периметре Организации;
- Находить уязвимости и эксплуатировать их;
- Искать утечки учётных записей в открытых источниках;
- Определять уязвимые компоненты на веб сервисах;
- Обнаруживать ресурсы, доступные из сети Интернет;
- 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.



Нам доверяют

Ростех
РТ-Энергоэффективность

РТ
Развитие бизнеса

Ростех
Техприемка

Ростех

KAMAZ

ОАК
Объединенная авиастроительная корпорация

ОДК

КБП

СИБЕР

Нацимбио

Высокоточные комплексы

УВЗ

НОВИКОМБАНК

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