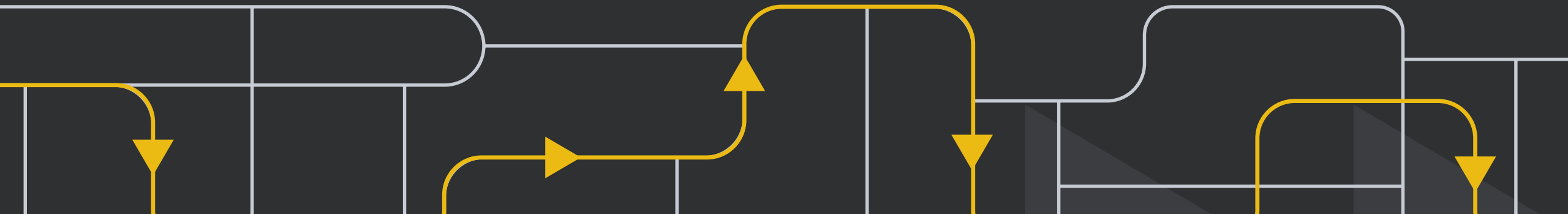


The logo features a stylized white square icon on the left, composed of four L-shaped segments. To its right, the text 'RT Protect' is stacked vertically in a bold, sans-serif font. Further to the right, the word 'EASM' is written in a significantly larger, bold, sans-serif font.

# 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



# 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 переменные на внешних ресурсах (смена сертификата, открытие порта и тд);

Подробности о результате

История (4)

Дата: 07.11.2023, 20:44:59	Сетевой адрес: [redacted]
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: [redacted]
Источник: nmap	Порт: 465

Главная страница / Сканирования

### Сканирования

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

Ввод идентификаторов сканирований

Применить | Очистить поля

Пассивное сканирование: 5 | 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	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Новая запись	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Новая запись	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Удаление записи	[redacted]	21	ftp	нет данных	нет данных	Выкл	нет данных
Изменился записи	[redacted]	21	нет данных	нет данных	нет данных	Выкл	нет данных

# 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>

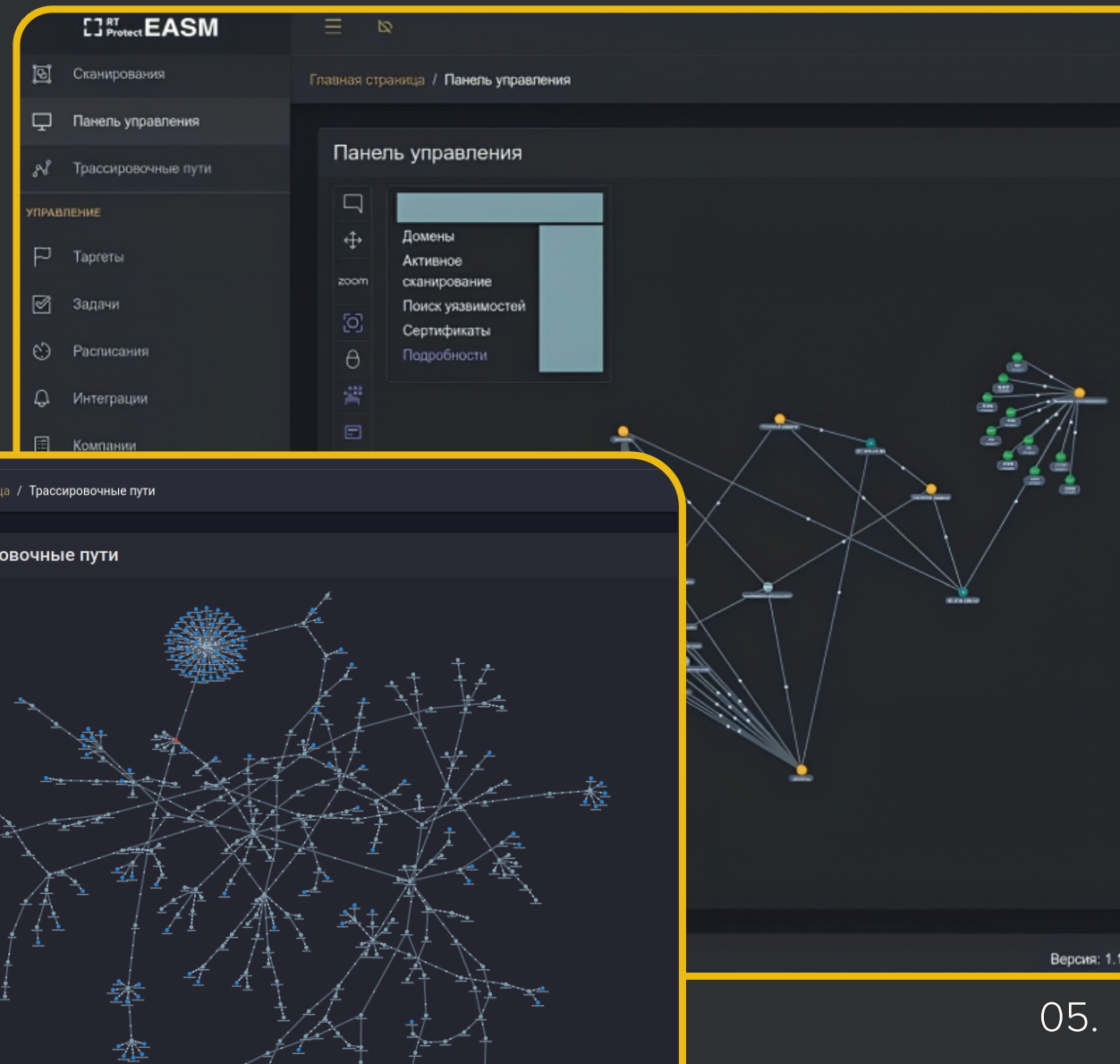
Решение: Разработчик продукта рекомендует обновить модуль «Опросы, голосования» (Polls, Votes (vote)) до версии 21.0.100

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

	Название	Критичность	Порт	Компания	Сканирование	Сетевой адрес
<input type="checkbox"/>	CVE-2022-27228	<b>V3.1: 9.8 Критическая</b>	443		К сканированию	
<input type="checkbox"/>	CVE-2022-41040	<b>V3.1: 8.8 Высокая</b>	443		К сканированию	
<input type="checkbox"/>	CVE-2022-41082	<b>V3.1: 8.0 Высокая</b>	443		К сканированию	

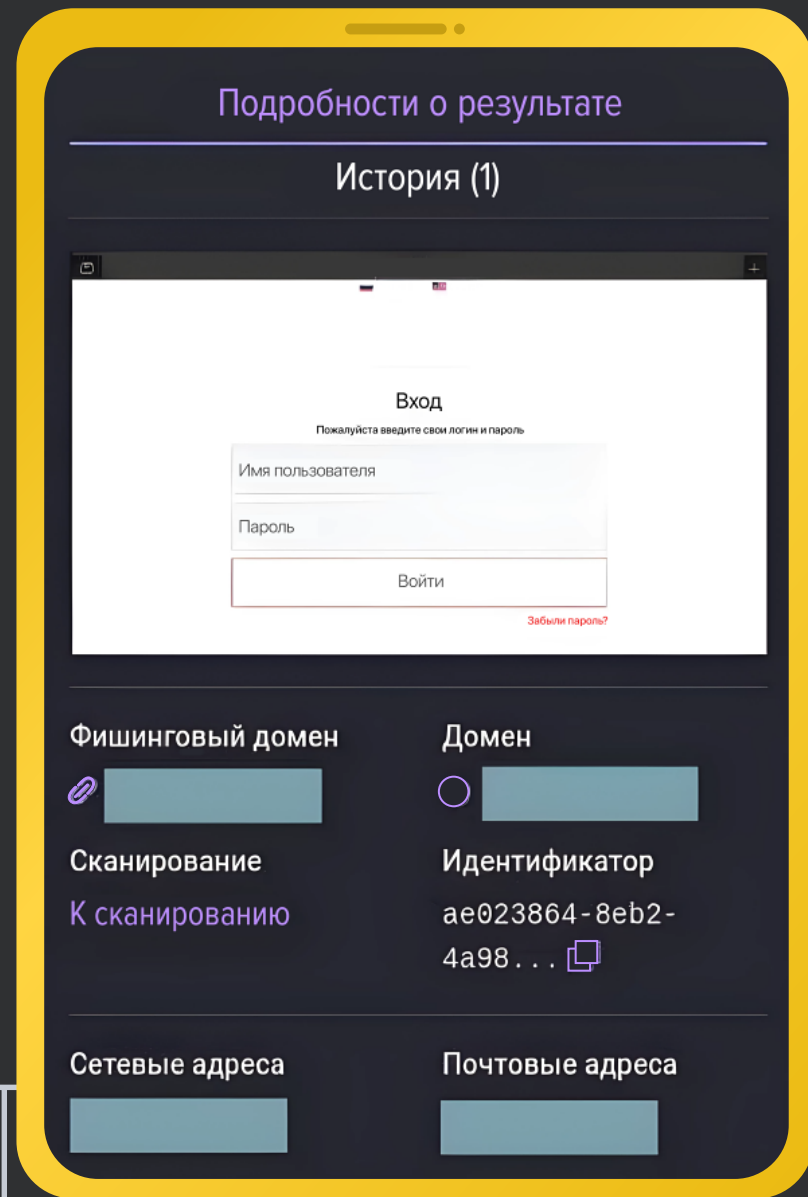
# Сокращение рисков кибератак

- 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 АРТ-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;

The image displays two screenshots from a security management interface. The top screenshot shows the configuration page for an integration, with fields for 'Родительская интеграция', 'Идентификатор', 'Компания', 'Имя', 'Расписание', and 'Описание'. It also features a 'Задачи (2)' section with a 'Добавить' button and a list of tasks with 'Исключить' buttons. The 'Этапы (10)' section lists various scanning and search tasks, each with an 'Исключить' button.

The bottom screenshot shows a 'Граф интеграции' (Integration Graph) with a toolbar on the left containing icons for zooming and locking. The graph consists of several nodes: 'Почта' (Email), two 'TI платформа' (TI platform) nodes, and three 'Elasticsearch' nodes. Lines connect the nodes, illustrating the relationships and data flow between different integration components.



# 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	lluminatti89
alex_hernandez_89@hotmail.com	нет данных	Eh19449656

Задачи, требующие рассмотрения

Обнаружено новое упоминание компании

Отправитель: [redacted] type attack:ddos

Ссылка на сообщение: [redacted]

Правило обнаружения: [redacted]

#diotallackersindia  
#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  
#hactivist\_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



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

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	Статус Активен
Название организации [redacted]	Дата окончания аренды [redacted]
Дата регистрации 04.10.2013, 21:59:00	Дата возможности выкупа [redacted]

### Сетевые адреса (2)

Не выбраны | Добавить

[redacted]	Исключить
[redacted]	Исключить

### Таргеты (0)

Не выбраны | Добавить

Нет данных для отображения

## 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;
- ▶ Сбирать 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 c45a6d34-64eb-46cb...	Сканирование К сканированию
Активное сканирование К активному сканированию	Компания 
Домен 	Источник cpt

### История (0)

### Детали сертификата

```
{ 11 items
  "subject": { 1 item
    "CN": 
  }
  "issuer": { 3 items
    "C": "US"
    "O": "Let's Encrypt"
    "CN": "R3"
  }
  "has-expired": false
  "not-after": 
  "not-before": 
  "serial-number": 3.5400457763178456e+41
  "serial-number(hex)": 
  "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



Ростех  
RT-Энергоэффективность



РТ  
Развитие  
бизнеса



Ростех  
Техприемка



Ростех



KAMAZ



OAK

ОБЪЕДИНЕННАЯ  
АБСТРАКТНАЯ  
КОРПОРАЦИЯ



ОДК



КБП



СИБЕР



Нацимбио



ВЫСОКОТОЧНЫЕ  
КОМПЛЕКСЫ



НОВИКОМБАНК

## Контакты

Адрес: 117587, г. Москва,  
Варшавское шоссе,  
дом 118, корпус 1

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

E-mail: [info@rt-ib.ru](mailto:info@rt-ib.ru)

Сайт: [rt-ib.ru](http://rt-ib.ru)



РТ

Информационная  
безопасность

