Веб-сервис RT Protect TI

Руководство пользователя

Версия 1.0.20 от 17 октября 2024 Разработано компанией АО «РТ-Информационная безопасность»

CJ RT **J** Protect

Оглавление



1. Общие положения	2
2. Общие сведения	3
3. Назначение программы	4
3.1 Основные задачи и возможности	4
3.2 Способы отражения предметной области в программе	4
4. Роли пользователей, взаимодействующих с Сервисом	5
5. Порядок взаимодействия с сервисом	6
6. Операции, доступные пользователю программы	7
6.1 Общие сведения	7
6.2 Главная страница	7
6.3 Организация	11
6.4 Активность	11
6.5 Отчеты	19
6.6 Граф связей	21
7. Сообщения об ошибках	26
8. Термины и определения	27
9. Заключение	28

1. Общие положения

Настоящий документ является руководством для пользователя вебсервиса «RT Protect TI» работающего в организации не являющейся владельцем платформы.

В документе приведены общие сведения, рекомендации по использованию программы и решению типичных проблем.

Данное руководство кратко можно идентифицировать согласно таблице 1.

Название документа	«Веб сервис RT Protect TI»
	Руководство Пользователя
Версия документа	Версия 1.0.20
	(актуальна для версии продукта
	frontend 0.8.3/backend 2.9.4)
Идентификация программы	Сервис по предоставлению аналитики «RT Protect TI»
Идентификация разработчика	АО «РТ-Информационная безопасность»

Таблица 1 – Идентификация документа

2. Общие сведения

Программа RT Protect TI – сервис компании АО «РТ-Информационная безопасность», предназначенный для сбора и анализа данных угроз информационной безопасности. Решение предоставляет актуальные сведения об угрозах, что позволяет оперативно выявлять события информационной безопасности и эффективно расследовать инциденты. Кроме того, посредством портала пользователи получают глобальные исследовательские и аналитические материалы о киберугрозах.

3. Назначение программы

3.1 Основные задачи и возможности

Основные задачи и возможности сервиса «RT Protect TI» можно кратко описать согласно следующему списку:

1) Проверка артефактов вредоносной активности (IP-адрес, доменное имя, URL, файлы, email);

2) Предоставление вердикта по артефактам.

3.2 Способы отражения предметной области в программе

Программа предназначена для проверки артефактов вредоносной активности, полученных из различных источников.

Сервис развертывается на мощностях предприятия-разработчика. Сервис является облачным решением, для взаимодействия с которым пользователю предоставляется открытое API. Взаимодействие с сервисом возможно через браузер.

4. Роли пользователей, взаимодействующих с Сервисом

Для обеспечения эффективного функционирования Сервиса необходимо наличие следующих групп пользователей, которые взаимодействуют с Сервисом:

– пользователь;

– аналитик;

– администратор безопасности.

Пользователь – может загружать для анализа на сервисе различные артефакты, просматривать отчеты по проверке артефактов, просматривать связи артефактов в виде графов, просматривать отчеты по активности.

Администратор – выполняет корректную настройку программы в соответствии с руководством администратора, регистрирует новых пользователей, подключенных к сервису, и осуществляет другие функции, описанные в руководстве администратора;

Аналитик – пользователь, ответственный за анализ поступающих от программы данных.

5. Порядок взаимодействия с сервисом

Взаимодействие с Сервисом возможно по открытому API, либо через браузер по ссылке <u>http://ti.rt-protect.ru</u>. Для входа на Сервис требуется пройти процедуру авторизации, описанную в документе «Веб-сервис RT Protect TI Руководство Администратора».

6. Операции, доступные пользователю программы

6.1 Общие сведения

Интерфейс сервиса «RT Protect TI», доступный для учетных записей с ролью «Пользователь» (для пользователей организации не являющейся владельцем платформы) позволяет выполнять следующие действия:

– используя функционал главной страницы просматривать сводную информацию по активности в организациях, подключенных к сервису;

 просматривать информацию о клиентах, подключенных к сервису в рамках одной организации;

используя функционал разделов аналитики просматривать информацию
 об артефактах и обнаружениях;

– просматривать отчеты об анализе артефактов;

- просматривать связи артефактов между собой в разделе «Граф связей».

6.2 Главная страница

Интерфейс Главной страницы сервиса «RT Protect TI», доступный для учетных записей с ролью «Пользователь» (для организации не владельца платформы), представлен на рисунке 1.

E3 Protect TI	ם Ξ			C a
😡 Главная страница	Проверка артефактов			
Организация				
аналитика	Введите IP-адрес, доменное имя. URL етаії или контрольную сум	ау файла для проверки		Отпр
О Активность	СТАТИСТИКА ДОБАВЛЕНИЯ АРТЕФАКТОВ ЗА МЕСЯЦ			
🖹 Отчеты	Файлы Доменные имена	IP-Appeca	Uri	Email
और Граф связей	754563 34302	1320392	70933	(1) 21
	АКТИВНОСТЬ	E La		
		🗢 Файлы 🔶 IP-Адреса 🐟 Домен	нные имена 😽 Url 🛶 Email	
	800-			
	162627 172627 182627 182627 202627 212627 2	12627 282627 002827 012627 022627 032627	042627 052627 062627 072627 08263	17 09/26/27 10/26/27 11/26/27 12/26/27 1
	топ 5 распространенных угроз (файлы)	1	ТОП 5 ПОСЛЕДНИХ УГРОЗ (ФАЙЛЫ)	
	KM5SS.exe (11469) UnMinor.exe (838) Cada22204427(dda49) winterv.exe (563) r24415641641ccc59171ac	wethdb633a (6052) 38e9bd533af (840)	0.0 %	Jarbo 7 te8772545a36f28b3a4f3769251 (5) bb5bbs2e42c7642efeaad2e9c2c3233 (4) wmcraxer (893) 555aver (11469) 56603fdcb7a2eb5770705990ct9ef37a (1363)

Рисунок 1 – Главная страница

Пользователь может проводить проверки артефактов (домены, ip-адреса, EMAIL, URL и хеш-суммы по алгоритмам SHA-256, SHA-1 и MD5). Чтобы выполнить проверку, необходимо ввести значение артефакта в строке **Проверка артефактов** и нажать кнопку **Отправить**. Кроме того, пользователь может загрузить для проверки исполняемый файл для его анализа в песочницах и с использованием сервисов, предоставляющих аналитику онлайн, по запросу (например, VirusTotal), для этого необходимо нажать кнопку **Загрузить файл** (1), после чего выбрать в проводнике соответствующий файл и нажать кнопку **Отправить**.

В области Проверка артефактов администратор также может проверить

целый список артефактов, нажав по иконке 📒, после чего откроется окно для загрузки списка артефактов, представленное на рисунке 2.

10



В данном окне артефакт добавляется по одному в каждой строчке.

Проверка артефактов списком ограничена количеством в 100 строк.

После отправки артефактов на анализ любым из указанных способов откроется страница с отчетом. Отчет содержит несколько вкладок, которые позволяют подробно проанализировать артефакт.

В зависимости от типа артефакта список вкладок будет отличаться – это вкладки песочниц, внешних источников (например, база данных MalwareBazaar) и вкладка с данными сервиса VirusTotal.

В правом верхнем углу страницы имеются иконки 🤅 💪 для смены цветовой схемы экрана (темной или светлой тем).

Также в правом верхнем углу находится иконка с именем, идентифицирующая пользователя, который произвел вход в программу на данный момент. При нажатии по данной иконке происходит переход в окно выбора действий, представленное на рисунке 3.



Рисунок 3 – Окно выбора действий для пользователя

В данном окне имеется возможность просмотреть профиль пользователя, либо осуществить выход из профиля.

При нажатии по иконке «Выход» появляется окно подтверждения для выхода из профиля, представленное на рисунке 4.



Рисунок 4 – Окно подтверждения действия выхода из приложения

Для подтверждения выхода из профиля необходимо нажать по иконке «Выход».

Окно просмотра профиля пользователя представлено на рисунке 5.

рофиль	
nail	
ль	
Тользователь	
A9	
RMAM	
зганизация	
пукойл	
лисание	
менить пароль	

Рисунок 5 – Окно просмотра профиля пользователя

В данном окне редактировать информацию о пользователе нельзя.

Для смены пароля требуется нажать по иконке «Сменить пароль», после

чего откроется окно смены пароля, представленное на рисунке 6.

Сменить пароль	\times
Ваш текущий пароль *	
	\odot
Новый пароль *	
	\odot
Повторите пароль *	
	\odot
Требования к паролю Пароль должен быть не менее 8 символов. Должен содержать хотя бы одну заглавную букву. Должен содержать хотя бы одну строчную букву. 	
Сохранить	

Рисунок 6 – Окно смены пароля

После смены пароля требуется нажать по иконке «Сохранить».

На Главной странице Пользователь имеет возможность просмотреть информацию в графическом виде об активности, распространенных и последних угрозах, а также по отчетам по различным артефактам на основе источников.

6.3 Организация

В разделе «Организация», представленном на рисунке 7, пользователь организации, подключенной к платформе RT Protect TI через-веб сервис (и не являющейся владельцем платформы), может просмотреть информацию об организации и клиентах, подключенных к сервису в рамках своей организации.

Организация				
<u></u>	Poccas Crisus est cuit			
лукойл	Добуча полезных иссолаемых свотор			
TAXOAA				
101 000. Procenicias Φεχαραμμα, r. Morcas, Cpremouni dynasap, 11 lukol@blabil.com +76956275444 +76956253706 εκτιτικτώ				
АУТОЙЛ — одна их крупнейших вертикально интерированных нелтегазовых компаний в имре, на доло которой пригодится более 2% мировой добычи нефти и около 1% доказанных запаков уллеодородов списание				
Клиенты				
I I I I I I I I I I I I I I I I I I I				
Имя				
> Load test				
> tan-35				
x 31				
> 666				
> mm				
> 1111				
> 111				
>1				
a v 1 v a flormann rei 20 v				

Рисунок 7 – Окно раздела «Организация»

Пользователь может скачать отчет в формате pdf по обнаружениям в организации, нажав по иконке .

6.4 Активность

В разделе **Активность** в табличной форме представлена информация о последних угрозах, которые обнаружены в инфраструктуре организации, подключенной к сервису аналитики.

В верхней части страницы **Активность** имеются следующие активные вкладки **Артефакты**, **Клиенты**.

При переходе по каждой вкладке на странице **Активность** отображается информация, соответствующая данной вкладке, при этом вкладка, на которую был произведен переход, отмечается серым цветом.

Вид страницы Активность в зависимости от того, по какой вкладке был произведен вход, показан на рисунках 8 - 9.

Активность			Сбросить фильтры
Артефакты			
Тип артефакта Вердикт	Период регистрации (на сервере)		• Список 🔿 Календарь
Не задан 🛛 🗸 🔘 🛛 Вредоносный х Подозрительный х 🛛 Х 🗸 🖓	1 месяц		~)
дополнительные фильтры	ACNO/INITE/BHSE GWIDSTW		
Teru			
Не задан 🛛 🗸 🧳			
ГРАФИКИ ОБНАРУЖЕНИЙ			4
			Найдено: 5387, показано с 1 по 10
Название артефакта	Предыдущий вердикт / Время	Количество обнаружений 斗	Время последнего обнаружения ↓
> <u>61(08108/2558cf422a6ba+f7654566108331c7a4124(365c206a05261b20821</u> ,0	Неизвестный 29.05.2024, 16:57:50	797	15.07.2024, 15:08:56
>fd7499214abaa13bf56d006ab7de78eb8d6adf17926c24ace024d067049bc81d() 51000 prefamiliant	Вредоносный е6.е5.2024, 17:41:08	11326	15.07.2024, 10:32:19
> <u>cb56c246a38292c224d1aabe5c33a671fc8ac8acd28cdc8c4fbc767c4c7b82f5</u>	Подозрительный 03.06.2024, 09:27:51	8851	15.07.2024, 10:03:08
> 9794d943685bbbb3878f952e05bdebadec13cfe51d47ce858f84eb84e813856d(0	Безопасный 25.85.2824, 16:39:21	2287	12.07.2024, 21:03:17
> <u>a695431272644b6dbd2b66787cc162bd5a52e1ccb0592ac6955e7664de5da50</u>	Неизвестный 16.05.2024, 18:49:00	35	12.07.2024, 15:26:20
> b283415c9df96f9e53b7d452d3e5c840c5bd7a6ce734a30bae4a869a57974a0g		1554	12.07.2024, 11:31:31
> inst. bostly. Com ()	Неизвестный 13.06.2024, 17:24:36	47	12.07.2024, 10:25:30
> e1af498f95432a4f2f666a8cbec7bd6ab9deb4d1695c6e7cde7acb9bd488e688		2	08.07.2024, 15:01:43
> http://188.127.237.46:9000/winlog.cnf (1	08.07.2024, 10:34:24
> < <u>c19c785782eea66881.dd7cbf9e4fef88b41384e8bd6ce26b7229e8251f24272.</u>	Неизвестный 06.07.2024, 17:34:52	113	06.07.2024, 18:03:58
1 2 3 4 > ≫ Rokaswanu no: 10 ✓			Найдено: 5387, показано с 1 по 10

Рисунок 8 – Общий вид страницы Активность вкладки Артефакты

Активность				Сбросить фильтры
Артефакты Клиенты				
Тип артефакта	Вердикт	Период регистрации (на сервере)		• Список 🔿 Календарь
Не задан 🛛 🗸 🗸 О	Вредоносный х Подозрительный х 🛛 🗙 🖓	1 месяц		×
дополнительные фильтры				v
Клиенты				
Не задан				
ГРАФИКИ ОБНАРУЖЕНИЙ				
a c 1 x x Transformer and the second se				
Название	артефакта	Предыдущий вердикт / Время	Количество обнаружений $\uparrow \downarrow$	Время последнего обнаружения 🔱
fd7499214abaa13bf56d006ab7de78eb8d6adf17926c24ace024d067049bc81d (Д Лукойл (1)			11310	26.06.2024, 10:14:36
97b4d943665bbb3878f952e05bdebadec13cfa51d47ce858f84ebd04e013056d			2197	26.06.2024, 10:04:18
<u>132.148.72.192</u> лукойл (1)			2848	25.06.2024, 17:46:17
mcc.brrkst.dynamic-dns.net () лукойл (Load test)			650	25.06.2024, 17:42:16
f24415c41d41cccc59171ace38e9bd533af6c78a02bd9a8117e1a6341df9c645 (Д лукойл (1)			1	17.06.2024, 15:10:01
е8fd9eb522961fa5bc8211e948f9f26397d268d9e378c700fa7abd204dd5012e (Д Лукойл (1)			13	17.06.2024, 14:27:17
< < 1 > >> Noxaawaans no: 10 V				Найдено: б. показано с 1 по б

Рисунок 9 – Общий вид страницы Активность вкладки Клиенты

Таблица имеет следующие поля:

– Название артефакта (в данном столбце в зависимости от типа артефакта отображается различная информация: контрольная сумма файлаугрозы в формате SHA-256, IP-адреса, доменные имена, URL);

 – Предыдущий вердикт/Время (предыдущий вердикт по артефакту и время вынесения вердикта);

– Количество обнаружений (отображается общее количество обнаружений по данному артефакту);

- **Время последнего обнаружения** (отображается время последнего обнаружения файла с угрозой).

Для удобства и наглядного отображения вердикта по артефакту в столбце «Название артефакта» информация отображается разным цветом шрифта:

<u>630ae106a99ae7da5d8dd33e7704b27701f6</u>
 вредоносный артефакт (шрифт красного цвета);

_ 02f0c498bb4e5f62722ab5e8a63f5b3779db88ef – безопасный артефакт

(шрифт зеленого цвета);

(шрифт серого цвета);

— 61F897ED69646E0509F6802FB2D7C5E88C3E3B93C4CA86942E24D203AA878863
— подозрительный артефакт (шрифт оранжевого цвета).

В столбце **Название артефакта** справа от информации, характеризующей артефакт (контрольной суммы файла, IP-адреса, email или доменного имени), имеется иконка ^[], нажав ЛКМ по которой, можно скачать данную информацию в буфер обмена.

Контрольная сумма файла угрозы, а также информация по другим типам артефактов является активной ссылкой, при нажатии по которой ЛКМ открывается окно отчета TI-платформы, представленное на рисунке 10.

C3 Protect TI		Файл: 85ed8506f3ea081c12a0eab17ed	Fbd8f900af0fbaa43a42ca46d8e5ad8c2e	865		Безопасный
Потоковый анализ >	Прочее >					
Основная информация VirusTotal Pu	blic TI RST Cloud Внешние источники YARA IOC Заи	лючение аналитика 2				
		Основная	информация			2
Безопасный ЕБДИЛ			28.03.2024, 05:30 ВПЕРВЫЕ ОБНАРУУ	69 КЕН		
Вердикт		5	езопасный (вердикт основан на от	vere VirusTotal)		JSON
Впервые обнаружен		2	8.03.2024, 05:36:09			
Таги						
Размер файла		1	8.08 MB			
SHA-256		8	5ed8506f3ea081c12a0eab17edfbd8	900af0fbaa43a42ca46d8e5ad8c2e8b5		
SHA-1	u1 e16941e14661a6024750ecd195:048189033182a					
MD5	96256c71t00cc5528118049f60e07360					
TLSH	112817df02839415575790348902865594760c356031c2cf1280751e3d32b68534b32					
Imphash	b06444055cccd4e4077d815448db1cf84					
39921 f6qx/jihjqgiotznyf2+9mcp9x9giop376iy1tag/fjqgiogcncpcgdphmiyp						
Обнаруженные имена	ARQYAREHINE MMENA			7651.exe		
Связанные артефакты 🗞 🔨						
Артефакт	Тип артефакта Количе	ство обнаружении	Комментарий	Дата создания / Автор	Дата последнего сохранения / Автор	Управление
Нет данных 🔗						
		Обнару	жения 限			5
Организация	ПАО «Азрофлот» 🥌		Организация		ООО Вычислительные решения	
Клиент	test		Клиент		Stage cepsep EDR	
Количество обнаружений	266		Количество обнаружений		1	
Время последнего обнаружения	02.04.2024, 15:18:18		Время последнего обнаружен	ия	28.03.2024, 12:34:18	

Рисунок 10 – Страница отчета сервиса по обнаруженной угрозе

Страница отчета программы об угрозе разделена на следующие области:

1) область краткой информации об угрозе;

2) область вкладок;

3) область основной информации;

4) область связанных с артефактом других артефактов;

5) область обнаружения (показывает другие организации на которых были обнаружения по данному артефакту).

В области краткой информации отображена информация об анализируемой угрозе в зависимости от типа артефакта (контрольная сумма проанализированного файла в формате SHA-256, IP-адрес, доменное имя, URL, email и вердикт TI-портала по данной угрозе).

В области вкладок отображается вкладка основной информации отчета TI-платформы, вкладки отчетов по угрозе от сторонних подключенных сервисов, разделенных по группам:

1) потоковый анализ (Virus Total, Public TI, RST Cloud и т.д.);

2) остальные (Внешние источники, YARA, IOC, Заключение аналитика).

Состав этих вкладок может меняться в зависимости от интегрированных модулей и интеграций.

Если в области вкладок запись отображается серым цветом, запрос информации по данному артефакту в том или ином сервисе недоступен. При нажатии ЛКМ по одной из вкладок появляется окно результатов по анализу артефакта (рис. 11).

VirusTotal 🧭			Virus Total
24.68	mediaget idle (overlay (peaz) (lighted) detected	11.51 MB Paswep	12.04.2023, 05.56-53 Дята последнейто знакитая 28.04.2023, 10:06:38 Время получения отчета 28.04.2023, 10:06:36 Время постановки отчета в очередь
DETECTION DETAILS			JSON
Avast	Win32:MiscX-Gen [PUP]	AVG	Win32:MiscX-Gen [PUP]
Cylance	Unsafe	Cyren	W32/ABRisk.DNTM-2624
DeepInstinct	MALICIOUS	DrWeb	Program.MediaGet.165
Elastic	Malicious (High Confidence)	ESET-NOD32	A Variant Of Win32/MediaGet.AK Potentially Unwanted
Fortinet	Riskware/MediaGet	Google	Detected
Gridinsoft	PUP.MediaGet.SdIC	Jiangmin	Downloader.MediaGet.Bla
K7AntiVirus	Adware (004ce1671)	K7GW	Adware (004ce1671)
Kaspersky	Not-A-Virus:HEUR:Downloader:Win32.MediaGet.Gen	Lionic	Riskware.Win32.MediaGet.11C
Malwarebytes	Floxif, Virus, FileInfector, DDS	MaxSecure	Downloader.W32.MediaGet.Gen_236651
Rising	Downloader.MediaGetl8.13A69 (TFE:5:Yf9JqlorrOtT)	Sangfor	Downloader.Win32.Mediaget.Vxzo
Sophos	Generic Reputation PUA (PUA)	TrendMicro-HouseCall	TROJ_GEN.R002H0CIQ22
Webroot	W32.Adware.Gen	ZoneAlarm	Not-A-Virus:HEUR:Downloader:Win32.MediaGet.Gen
Acronis	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected

Рисунок 11 – Результаты анализа артефакта на странице Virus Total

Окно основной информации по результатам анализа артефакта в формате

HTML представлено на рисунке 12.

Вердикт	Вредоносный (вердикт основан на отчете VirusTotal)
Впервые обнаружен	05.07.2022, 12:37:44
Размер файла	11.51 MB
SHA-256	630ae106a99ae7da5d8dd33e7704b27701f698ce81c6d859be07e1157563cd24
SHA-1	ace104fb3a778773752d21d334a8beabeebf3b29
MD5	5ff37d5bd1f55421a18829e52a804108
TLSH	t1f3c6cf2337058c29d52110b06ea9d79a9319fd238b2167cfb38d6a6d1a7c1c24f35bf6
Imphash	9f72a91bb07c782d841b9af20ada6733
SSDEEP	196608: nng zjhii o 95314 hne 0 lm dosa 3 jtot jt 6 so 4 qasa 4 meq/f wa 6 mz mz: nng zjhir 3 lqe 0 lq loj twtg 4 qasa 4 tw s x a so 100 ms so 1
Обнаруженные имена	mediaget.exe mediaget

Рисунок 12 – Информация отчета об артефакте в формате HTML

Окно основной информации по результатам анализа артефакта в формате

JSON представлено на рисунке 13.

7 { 27 items	HTML
"id": 57066978	
"sha256" : "630ac106a99ac7da5d8dd33c7704bc27701f698cc81c6d859bc07c1157563cd24"	
"sha1" : "ace104fb3o778773752d2Ld334s8beabeebf3b29"	
"md5" : "\$ff37d5bd1f55421a18829e52a804108"	
"t1sh" : "T1F3C6CF2337058C29052110806EA9079A9319FD23882167CF83806A601A7C1C24F358F6"	
"imphash" : "9f72a91bb07c782d841b9af20ada6733"	
"ssdeep" : "196688:NWg27hi1095334hNe0LmD0sA3jToT316so4q4sA4MeQ/FWa6mzmZ:NWg27hi731Qe0LQ10jTNT64q4sA4TNsX"	
"artifactClass": 3	
"artifactName" : "NaliciousFile"	
"artifactSeverity": 4	
"nsrlInfold" : Nucl	
"sophosInfoId" : MULL	
"vtReportId" : 164411	
"kasperskyReportId" : 6173	
"yaraReportId" : MULE	
"fileExpertOpinionId": "6e454816-030f-4481-0940-fd4766175b82"	
"iocId" : NULL	
"ptMsReportId": Mai	
"sthenaReportId" : 26	
"firstTimeSeen" : "2022-07-05T09:37:44.7012592"	
"info": "Вердикт основан на отчете VirusTotal"	
"fileNames": [2 items	
0 : "mediaget.exe"	
1 : "mediaget"	
1	
"fileSize" : 12070544	
"hasFileInfileStorage" : false	
"uploadTime" : Image	
"uploadInProgress" : false	
* "feedsToHashInfos": [] 0 items	
}	

Рисунок 13 – Информация отчета об артефакте в формате JSON

В области Связанные артефакты показывается таблица с описанием артефакта, связанного с тем артефактом, отчет по которому просматривается на

данный момент. При нажатии по иконке Привязать артефакт открывается окно для привязки артефактов друг к другу (см. рисунок 14).

~

Рисунок 14 – Окно для привязки артефакта

В данном окне добавляется один или несколько артефактов, тип артефакта и комментарий.

После добавления информации следует нажать по иконке «Привязать». После привязки артефакт появится в списке связанных артефактов.

Важно

Привязка разных типов артефактов допускается. Т.е. ip-адрес и хешсумма могут быть привязаны друг к другу.

Для фильтрации информации на странице **Активность** вкладки **Артефакты** предусмотрена система фильтров, представленная в следующем списке:

- Тип артефакта (файл, IP-адрес, доменное имя, URL);

– Вердикт (неизвестный, безопасный, вредоносный, подозрительный);

— **Период регистрации (на сервере)**, может задаваться в виде списка (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца), либо в виде календаря (начальная и конечная даты);

– Артефакт (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);

- **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);

– **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);

– Предыдущий вердикт;

– Предыдущий вердикт (период регистрации на сервере);

– Время последнего изменения вердикта.

На странице **Активность** вкладки **Артефакты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 15).

ГРАФИКИ РАСПРЕДЕЛЕНИЯ УГРОЗ	۵
Статистика обнаружений по типам	Статистика обнаружений по вердиктам
35790	35790
■Контрольные суммы (27642) ■IP-Адреса (2317) ■Доменные имена (5831) ■ Url (0)	Неизвестный (21111) = Безопасный (14675) = Вредоносный (3) = Подозрительный (1)

Рисунок 15 – Область графического отображения информации по обнаруженным угрозам вкладка «Артефакты»

В данной области для наглядности представления информации имеются графики, отображающие следующие статистические данные:

– статистика обнаружений по типам;

– статистика обнаружений по вердиктам;

Для фильтрации информации на странице **Активность** вкладка **Клиенты** предусмотрена система фильтров, представленная в следующем списке:

- Тип артефакта (файл, IP-адрес, доменное имя, URL);

– Вердикт (неизвестный, безопасный, вредоносный, подозрительный);

– **Период регистрации (на сервере)**, может задаваться в виде списка (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца), либо в виде календаря (начальная и конечная даты);

 – Артефакт (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);

– **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);

– **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);

– Предыдущий вердикт;

– Время последнего изменения вердикта;

– Клиенты.

На странице Активность вкладки Клиенты имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 16).



Рисунок 16 – Область графического отображения информации по обнаруженным угрозам вкладка Клиенты

В данной области для наглядности представления информации имеется график, отображающий следующие статистические данные обнаружений по клиентам, подключенным к сервису в рамках организации, не являющейся владельцем платформы.

6.5 Отчеты

В разделе **Отчеты** в табличной форме представлена информация о проверенных внешними анализаторами артефактах, для которых настроена интеграция. Общий вид страницы представлен на рисунке 17.

Отчеты			
Источник Тип артефакта			
Virus Total v Файл	~		
ГРАФИК ОТЧЕТОВ			
« < 1 2 3 4 > » Показывать по: 10		Найдено:	272380, показано с 1 по 10
Артефакт	Статус	Время обращения	Действия
f24415c41d41cccc59171ace38e9bd533af6c78a02bd9a8117e1a6341df9c645 🗗	Отчет не был получен (Артефакт не найден)	19.09.2023, 10:25:54	Посмотреть отчет
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b859	Отчет не был получен (Артефакт не найден)	18.09.2023, 16:16:49	Посмотреть отчет
e3bec44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b857	Отчет не был получен (Артефакт не найден)	18.09.2023, 16:16:05	Посмотреть отчет
e3b8c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b851 🗗	Отчет не был получен (Артефакт не найден)	18.09.2023, 16:14:20	Посмотреть отчет
1ae4161b3c197c5274d55dc63378c4ab30e9f688a08223a4b6510f3ef6c4c01b	Отчет не был получен (Артефакт не найден)	18.09.2023, 12:14:01	Посмотреть отчет
49d7c335b19b6b6ba58619583567dbca4c4d0ec22e96eb74106aae5aa3b631c9 💭	Отчет получен успешно	18.09.2023, 12:06:11	Посмотреть отчет
9111099efe9d5c9b391dc132b2faf0a3851a760d4106d5368e30ac744eb42706 💭	Отчет получен успешно	18.09.2023, 11:59:43	Посмотреть отчет
b75ef0d9be5c111341dab495301c5939495487c2a76eb2ec1d1eac393e6efc5e	Отчет получен успешно	18.09.2023, 11:55:58	Посмотреть отчет
3fa149b1165a3ff84e3e8524ece4ff86b91352f0686a1fded3e141ccec0f0a2d	Отчет получен успешно	18.09.2023, 11:55:42	Посмотреть отчет
9ecb5f24d9e3090aeecf6929fa69cf4e0648d726f7c7797279e1df9e7178fe5b	Отчет получен успешно	18.09.2023, 11:55:27	Посмотреть отчет
« 1 2 3 4 > > Показывать по: 10 ❤		Найдено:	272380, показано с 1 по 10

Рисунок 17 – Окно раздела «Отчеты»

В таблице имеются следующие поля:

 – Артефакт (в столбце отображается информация о проверенном артефакте в зависимости от типа артефакта (хеш сумма, IP-адрес, доменное имя, URL);

 – Статус (в столбце отображается информация о получении отчета (отчет получен успешно, отчет не был получен));

- Время обращения (время, в которое был запрошен отчет);
- Действия (получить отчет).

Информация об артефакте отображается разными цветами:

- шрифт красного цвета (артефакт является вредоносным);
- шрифт зеленого цвета (артефакт является безопасным);
- шрифт серого цвета (неизвестный артефакт);
- шрифт оранжевого цвета (артефакт является подозрительным).

Над таблицей для фильтрации информации имеются следующие фильтры:

- Источник (Virus Total, Public TI, Athena, RST Cloud);
- Тип артефакта (файл, IP-адрес, доменное имя, URL.

Над таблицей для отображения визуальной информации имеется область

с графиком полученного числа отчетов за определенный период в зависимости

от установленного в фильтре источника данных (рисунок 18).



Рисунок 18 – Отчеты Virus Total

Для просмотра отчета по артефакту нужно нажать по иконке Страница отчета по артефакту представлена на рисунке 19.

Отчет			
VirusTotal 💋			∑ VirusTota
М	BEDaisy.sy	s 3.19 M8 annoty country count Passuep ann	08.09.2023, 21.5650 Для поскеднето анализа 16.09.2023, 12.0611 Время получения отчета 18.09.2023, 12.0609 Время постченовки отчета в очерева.
DETECTION DETAILS			ISO
Fortinet	W64/FRS.AITr	Acronis	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
APEX	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
8kav	Undetected	CAT-QuickHeal	Undetected
ClamAV	Undetected	CMC	Undetected
CrowdStrike	Undetected	Cybereason	Undetected
Cylance	Undetected	Cynet	Undetected

Рисунок 19 – Страница отчета по артефакту от источника Virus Total

6.6 Граф связей

Страница «Граф связей» с незаполненным полем артефакта представлена на рисунке 20.



Рисунок 20 – Общий вид пустой страницы «Граф связей»

На странице имеется две области:

 – область с иконками-подсказками для управления визуальной частью графа;

– область для введения информации по артефакту, для которого требуется построить граф.

В области управления визуальной частью графа находятся иконки, при наведении на которые указателя мыши появляются всплывающие сообщения (подсказки) для управления графом.

Пример отображения графа после заполнения поля артефакта в виде ipадреса представлен на рисунке 21.



Рисунок 21 – Отображение графа связей для артефакта типа ір-адрес

Пример отображения графа связей для артефакта типа домен с привязанными артефактами представлен на рисунке 22.



Рисунок 22 – Отображения графа связей для артефакта типа домен с привязанными артефактами

На данной странице графа в правой части имеется столбец «Легенда», отображающий связанные с артефактом другие артефакты.

Для того, чтобы скрыть столбец с информацией по привязанным артефактам, следует нажать ЛКМ по иконке .

При нажатии ЛКМ по круглой области отрисовки графа отображается информация об артефакте (смотри рисунок 23).

P	Вредоносный ВЕРДИКТ
0	28.09.2022, 15:32:23 ВРЕМЯ ОБНАРУЖЕНИЯ
<u></u>	тестовая привязка_2 КОММЕНТАРИЙ
Зердикт блокиг	г основан на индикаторе компрометации зовка сайта погоды"

Рисунок 23 – Информация по артефакту

При нажатии по активной области «Связи» появится окно, показывающее список связей данного артефакта (рисунок 24).

Артефакт	Комментарий	Тип
85.198.79.8	тестовая привязка_2	ІР-Адрес
login.live.com	тестовая привязка_2	Домен
www.eldorado.ru	тестовая привязка_2	Домен

Рисунок 24 – Связи по данному артефакту

При нажатии по иконке, идентифицирующей артефакт, происходит переход на страницу отчета по данному артефакту.

Для привязки нового артефакта к выбранному артефакту следует нажать

по иконке 🧖, после чего появляется окно для внесения информации по

привязанному артефакту, представленное на рисунке 25.

Привязать артефакты	×
Артефакты 🕕 *	
Комментарий	/
	Привязать

Рисунок 25 – Окно добавления информации для привязывания артефакта

После добавления информации в данном окне следует нажать по иконке «Привязать». Привязанный артефакт будет отображаться на странице **Граф связей.**

Для удаления связи между двумя артефактами из привязанных артефактов следует нажать по иконке , после чего появится окно указания того, какую связь и для какого узла требуется удалить (рисунок 26).

Удаление связей для узла www.eldorado.ru	\times
Связи	
Выберите связи	· ~
	Удалить

Рисунок 26 – Удаление связей между артефактами

Для подтверждения удаления связи требуется нажать по иконке «Удалить».

7. Сообщения об ошибках

Большинство ошибок можно разделить на следующие типы:

1) Ошибки конфигурации:

– некорректные настройки параметров безопасности;

– некорректная установка компонентов программы;

– некорректные действие со стороны пользователя/администратора;

– критические ошибки.

2) Ошибки оборудования:

выход из строя аппаратных средств, на которых установлена программа;

 выход из строя сервера (или компонентов на сервере), с которыми взаимодействуют компоненты Изделия, установленные на оборудовании пользователя;

– перебои питания со стороны клиентской или серверной части.

При возникновении ошибки пользователю не следует самостоятельно заниматься устранением ошибки. Пользователю необходимо обращаться к производителю программы.

8. Термины и определения

Перечень терминов и определений указан в таблице 2.

Таблица 2 – Термины и определения

Информационная безопасность (ИБ)	Сфера науки и техники, охватывающая совокупность проблем, связанных с обеспечением защищенности объектов информационной сферы в условиях существования угроз. Под информационной безопасностью также понимают защищенность информации от несанкционированного ознакомления, преобразования и уничтожения, защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности	
Инцидент ИБ	Нарушение или угроза нарушения ИБ компании	
URL	Унифицированный указатель ресурса	
API	Интерфейс прикладного программирования	
SOC	Центр обеспечения компьютерной безопасности	
OC	Операционная система	
Событие ИБ	Любое идентифицированное явление в системе или сети	
Угроза ИБ	Потенциально возможное событие, действие (воздействие), процесс или явление, создающее опасность возникновения инцидента ИБ	
Уязвимость		
информационной	Недостаток в ИС, используя который внешний злоумышленник может	
системы (ИС)	намеренно реализовать угрозу и в	

9. Заключение



Цитирование документа допускается только со ссылкой на настоящее руководство. Руководство не может быть полностью или частично воспроизведено, тиражировано или распространено без разрешения АО «РТ-Информационная безопасность».