




Руководство администратора

Table of contents:

- Руководство администратора
 - Пользовательские и системные настройки
- Администрирование пользователей
 - Смена пароля пользователя
 - Создание новых пользователей
 - Редактирование пользователей
 - Роли пользователей
 -  Среда исполнения
 -  Аппаратные ресурсы
 -  Службы tLab
- Среда исполнения
- Аппаратные ресурсы
- Службы tLab
- Настройки
- Исключения
 - Управление исключением
 - Импорт / экспорт исключений
- Сеть
- Обслуживание
- Лицензия
- Белый список
- Yara
- Управление контейнерами
- Интеграция
- Сетевое хранилище
- ICAP сервер
- Корзина



Руководство администратора

Пользовательские и системные настройки

Кнопка с именем пользователя в верхнем навигационном меню открывает меню настроек.

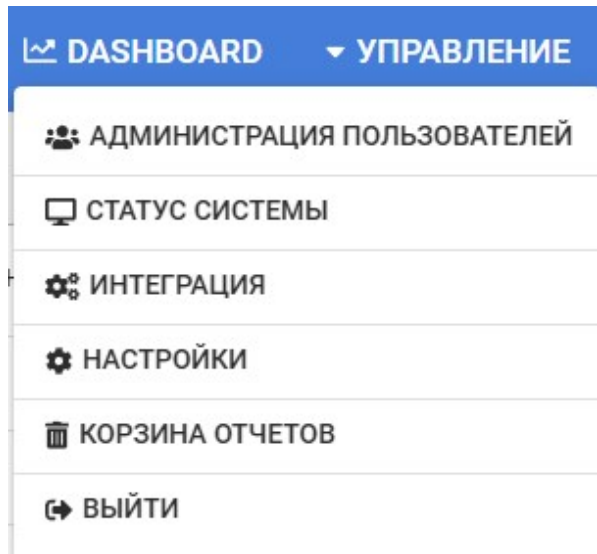


Рис. 1 - Меню настроек

Администрирование пользователей

Отображает список всех пользователей. В данном разделе можно создать нового пользователя (Добавить учетную запись), сменить пароль существующему (Поменять пароль), посмотреть отчеты, принадлежащие пользователям (нажать на логин пользователя).

Добавить учетную запись					АДМИНИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ		
ID	ЛОГИН	ИМЯ ПОЛЬЗОВАТЕЛЯ	ПОЧТА	РОЛЬ	РЕДАКТИРОВАТЬ		
2	script	Scriptus	script@localhost	admin	РЕДАКТИРОВАТЬ	СМЕНИТЬ ПАРОЛЬ	УДАЛИТЬ
3	admin			admin	РЕДАКТИРОВАТЬ	СМЕНИТЬ ПАРОЛЬ	
9	arconly		arc@rest.only	admin	РЕДАКТИРОВАТЬ	СМЕНИТЬ ПАРОЛЬ	УДАЛИТЬ
33	supra	supra	soupe@sup.ra	admin	РЕДАКТИРОВАТЬ	СМЕНИТЬ ПАРОЛЬ	УДАЛИТЬ
35	supra2	supra2	su@p.ra	admin	РЕДАКТИРОВАТЬ	СМЕНИТЬ ПАРОЛЬ	УДАЛИТЬ
36	testadmin	testadmin	tes@tad.min	admin	РЕДАКТИРОВАТЬ	СМЕНИТЬ ПАРОЛЬ	УДАЛИТЬ
40	sampleadmin	sampleadmin	sam@plead.min	admin	РЕДАКТИРОВАТЬ	СМЕНИТЬ ПАРОЛЬ	УДАЛИТЬ

Рис 2.1 - таблица пользователей

Смена пароля пользователя

Смена пароля пользователя производится при нажатии кнопки "Сменить пароль" в соответствующем данному пользователю столбце в таблице. При нажатии кнопки, открывается модальное окно, в котором нужно задать новый пароль

Изменить пароль для Jane

Имя пользователя

Jane

Новый пароль*

6-32 символов

Подтвердите пароль*

6-32 символов

ОТПРАВИТЬ

Рис. 2.2 - окно смены пароля

Создание новых пользователей

Создание новых учетных записей производится администратором на странице "Администрация пользователей" в верхнем правом меню. "Добавить учетную запись" открывает форму для создания нового пользователя. Электронная почта, логин и пароль являются обязательными полями. Пользователь может самостоятельно изменить свой пароль.

Создать пользователя

Полное имя

John Doe

Логин*

3-45 символов

Пароль*

6-32 символов

Подтвердите пароль*

6-32 символов

Email:*

johndoe@gmail.com

Роль

ОТПРАВИТЬ

Рис. 2 - форма создания нового пользователя

Редактирование пользователей

Редактирование данных пользователя производится при нажатии кнопки "Редактировать" в соответствующем данному пользователю столбце в таблице. При нажатии кнопки, открывается модальное окно, в котором нужно задать новые данные.

Редактировать пользователя Jane

Полное имя	<input type="text" value="Jane Doe"/>
Логин*	<input type="text" value="Jane"/>
Email:*	<input type="text" value="janedoe@gmail.com"/>
Роль	<input type="text" value="User"/>

➤ ОТПРАВИТЬ

Рис. 2.3 - окно редактирования пользователя

Роли пользователей

Система поддерживает следующие роли пользователей: обычный пользователь, эксперт и администратор.

В режиме обычного пользователя предоставляются следующие возможности: загрузка файлов для анализа и просмотр отчетов по загруженным файлам. Обычным пользователям видны собственные отчеты и отчеты с открытым доступом.

В режиме эксперта обеспечена возможность для установки вердикта проанализированных объектов, а также все возможности обычного пользователя.

У пользователя системы с ролью администратора присутствуют возможности эксперта и обычного пользователя, а также панель настройки параметров компонентов и управление пользователями. Администратору видны отчеты всех пользователей.

Среда исполнения

Эта страница отображает статус среды исполнения и всех виртуальных машин в ней, статус аппаратных ресурсов, а ...

Аппаратные ресурсы

Страница, показывающая статус аппаратных ресурсов системы в виде интерактивных графиков с возможностью из...

Службы tLab

Компонент, показывающий статусы и логи служб, функционирующих в системе. Статус может быть «АКТИВНЫЙ» ил...

Среда исполнения

Эта страница отображает статус среды исполнения и всех виртуальных машин в ней, статус аппаратных ресурсов, а также служб tLab. Перед использованием динамического анализа среда должна быть включена. Если статус машины горит желтым цветом с названием «ЗАРЕЗЕРВИРОВАНА», то на данной машине выполняется анализ файла. Кликнув на название отчета под заголовком «Задание», можно перейти на данный отчет.

СТАТУС СИСТЕМЫ

☰ Среда исполнения

☰ Аппаратные ресурсы

☰ Службы tLab

Node ID: EXENV_DEBIAN | Статус среды: RUNNING | Количество ВМ 11

w10dev0

Задание: [Отчет №389215](#)

Статус: ● ГОТОВО

Конфигурация: Windows 10 x64 dev 6.1

wXr17o19_o1c0

Статус: ● НЕ ИСПОЛЬЗУЕТСЯ

Конфигурация: Нет

wXr17o19_o110

Статус: ● ГОТОВО

Конфигурация: Windows 10 x64 o11 6.1

wXr17o190

Статус: ● ГОТОВО

Конфигурация: Windows 10 x64 6.1

wXr17o19_o100

Статус: ● ГОТОВО

Конфигурация: Windows 10 x64 o10 6.1

wXr17o19_o111

Статус: ● ГОТОВО

Конфигурация: Windows 10 x64 o11 6.1

w764r15of130

Статус: ● ГОТОВО

Конфигурация: Windows 7 x64 6.1

wXr17o19_o101

Статус: ● ГОТОВО

Конфигурация: Windows 10 x64 o10 6.1

wXr17o19_o112

Статус: ● ГОТОВО

Конфигурация: Windows 10 x64 o11 6.1

wXr17o190_windex_off2

Статус: ● НЕ ИСПОЛЬЗУЕТСЯ

Конфигурация: Нет

wXr17o19_o102

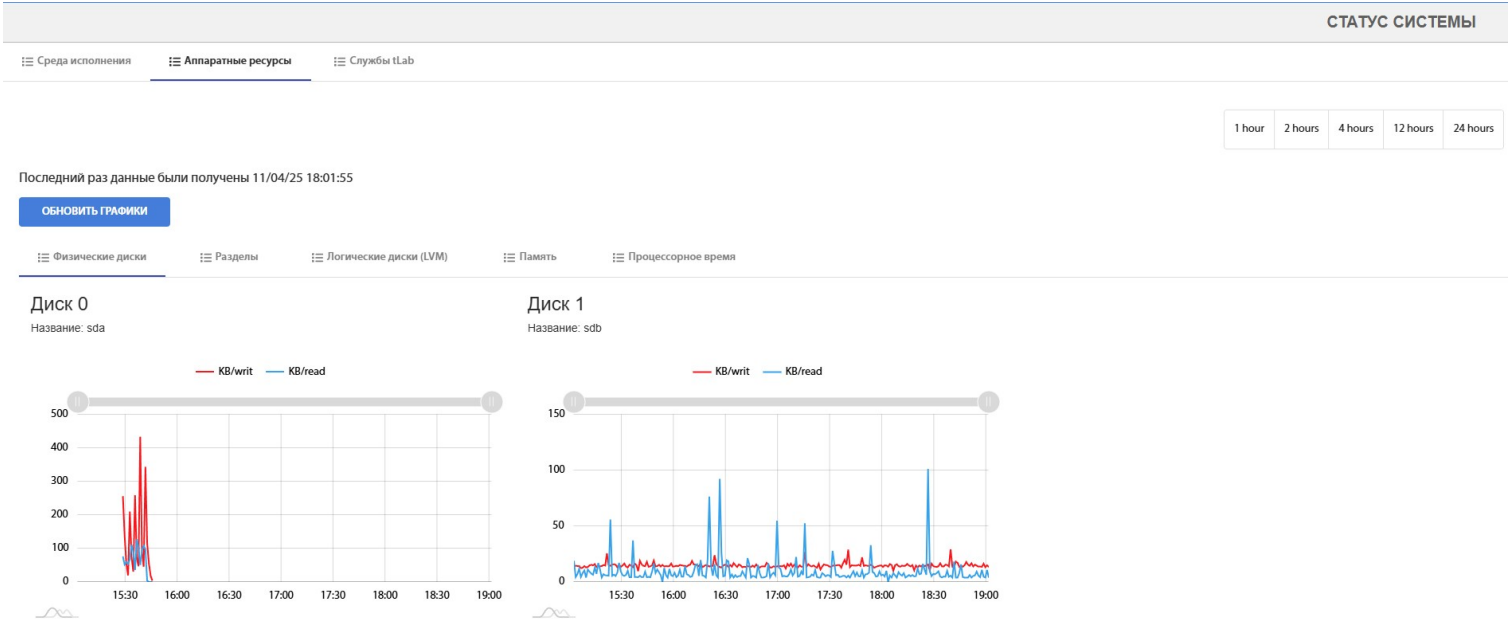
Статус: ● ГОТОВО

Конфигурация: Windows 10 x64 o10 6.1

Рис. 3 - Страница управления

Аппаратные ресурсы

Страница, показывающая статус аппаратных ресурсов системы в виде интерактивных графиков с возможностью изменения периода времени. Информация, доступная для просмотра: физические диски, использование диска,логические диски, память, процессорное время, сетевые интерфейсы, средняя нагрузка процессоров.



Службы tLab

Компонент, показывающий статусы и логи служб, функционирующих в системе. Статус может быть «АКТИВНЫЙ» или «НЕАКТИВНЫЙ».

СТАТУС СИСТЕМЫ

☰ Среда исполнения ☰ Аппаратные ресурсы ☰ Службы tLab

Статусы служб

НАЗВАНИЕ	СТАТУС
tlab-sas	АКТИВНЫЙ
tlab-ees	АКТИВНЫЙ
tlab-exenv-http	АКТИВНЫЙ
tlab-fcs	АКТИВНЫЙ
tlab-yarascan2-mgmt	АКТИВНЫЙ
tlab-wi-web	АКТИВНЫЙ
nginx	АКТИВНЫЙ
elasticsearch	АКТИВНЫЙ
tlab-healthmon	АКТИВНЫЙ
tlab-server	АКТИВНЫЙ
tlab-sasp	НЕАКТИВНЫЙ
tlab-config	АКТИВНЫЙ

Рис 3.2 - Страница служб tLab

Настройки

На данной странице настраиваются различные свойства системы.

Максимальный размер загрузки - максимальный общий объем файлов, отправляемых на анализ.

Задержка исполнения - указывается минимальное время задержки при котором будет обнаруживаться задержка как подозрительное событие и соответственно включаться противодействие.

Автоматическое экспертное заключение - позволяет настроить уровень опасности, при котором файл будет иметь заключение эксперт: Опасно.

Противодействия методам уклонения ВПО - дает возможность выбора метода противодействия задержке исполнения (исключить задержку - задержки не будет; уменьшить задержку в n раз - идет перехват функции задержки и ее сокращения в n раз).

Типы файлов допустимых к анализу - дает возможность запретить анализ определенных типов файлов. После изменения свойства необходимо нажать кнопку "Применить изменения" внутри панели этого свойства для сохранения.

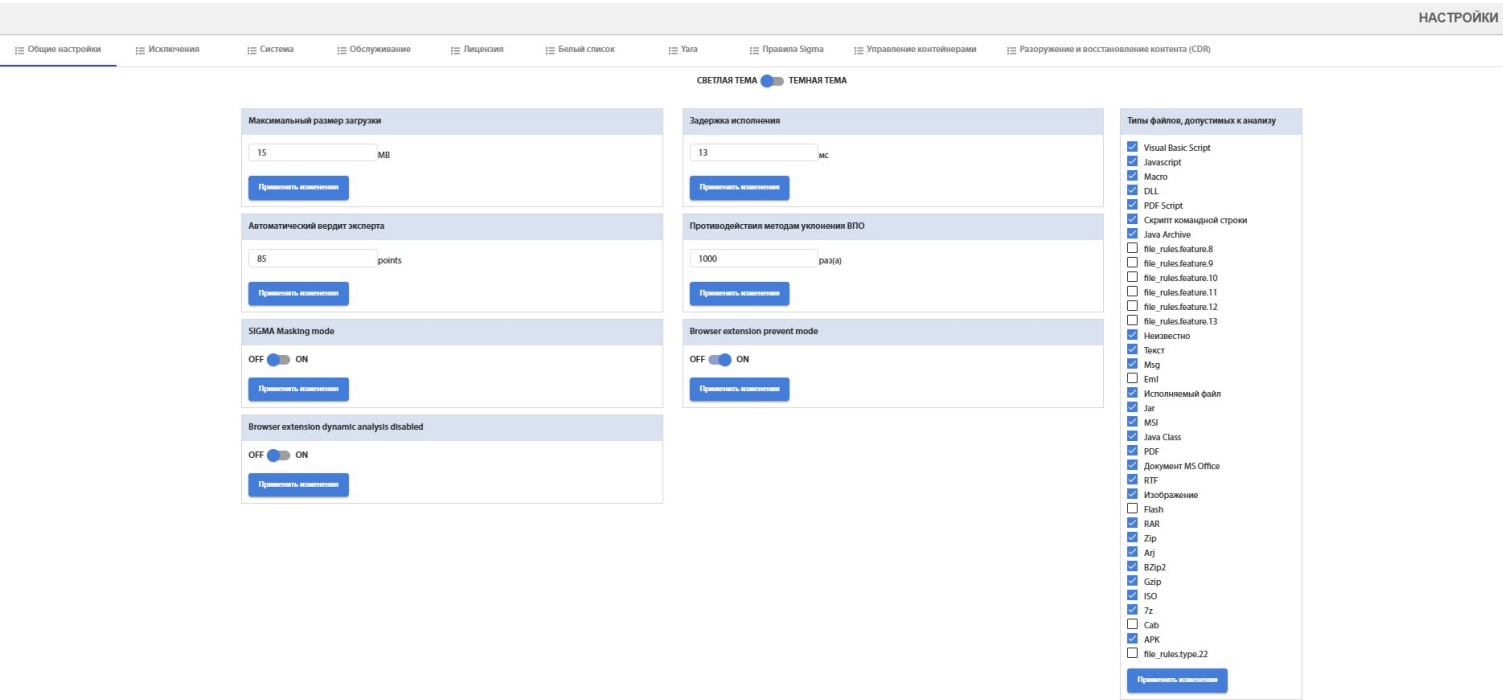


Рис. 4 - Страница настроек системы

Исключения

Таблица со списком добавленных ранее исключений (файлов или директорий). Позволяет редактировать исключения, а также включать или выключать их.

НАСТРОЙКИ

Общие настройки

Исключения

Система

Обслуживание

Лицензия

Белый список

Yara

Правила Sigma

Управление контейнерами

Разоружение и восстановление контента (CDR)

ИМПОРТ

ЭКСПОРТ

ИД	ПУТЬ ИСКЛЮЧЕНИЯ	ОПЕРАЦИОННАЯ СИСТЕМА	СОБЫТИЕ	АТТРИБУТ	ВРЕМЯ СОЗДАНИЯ	СЕМАНТИКА	ПОЛЬЗОВАТЕЛЬ
95	C:\Users\Администратор\...\elfModuleAnalysisCache	Windows 10	x64	Модификация важного файла	Модифицированный файл	15/11/24 19:25:47The file is not critical	admin
94	10.1.0.132	Any	Установлено интернет - соединение	Удаленный адрес		20/08/24 17:34:43download image in document	admin
93	C:\Windows\system32\DllHost.exe	Any	Новый процесс	Командная строка		15/08/24 12:19:44TLAB-1214 - Consider exceptions...racted from behavioral analysis	admin
92	C:\windows\system32\cmd...vent DumpCompleteEvent"	Any	Новый процесс	Командная строка		15/08/24 11:59:03TLAB-1214 - Consider exceptions...racted from behavioral analysis	admin
86	N/A (undefined)	Any	Идентификация уникального компьютера			14/05/24 01:13:28	admin
85	\REGISTRY\REGISTRY\MAC...Name\ActiveComputerName	Any	Идентификация уникального компьютера	Название ключа реестра		14/05/24 01:04:27	admin
84	\REGISTRY\REGISTRY\MAC...Name\ActiveComputerName	Any	Идентификация уникального компьютера	Название ключа реестра		14/05/24 01:02:57	admin
83	\REGISTRY\REGISTRY\MAC...Name\ActiveComputerName	Any	Идентификация уникального компьютера	Название ключа реестра		14/05/24 01:02:44	admin
82	C:\Program Files\Micros...e\Office15\MSACCESS.EXE	Any	Извлечение исполняемого файла	Созданный файл		02/05/24 21:11:24Nominal	dev_amur
81	SvcRestartTask	Any	Установка исполняемого файла на самозапуск (через планировщик задач)	Имя задания в планировщике		02/05/24 12:51:21тесттест	admin
80	\REGISTRY\REGISTRY\MAC...Name\ActiveComputerName	Windows 7	x64 dev	Идентификация уникального компьютера	Название ключа реестра	02/02/24 17:15:54Nominal activity for MS Word	dev_amur
77	C:\Users\Администратор\...4d79-876f-1e46816f6e59	Windows 10	x64 dev	Модификация важного файла	Модифицированный файл	31/10/23 16:30:03Cache file	admin
76	C:\Program Files (x86)\...ader\AcroCEF\RdrCEF.exe	Any	Новый процесс	Файл нового процесса		24/05/23 01:02:29DC 17 Nominal activity	admin

Fig. 4.1 – Страница исключений

Управление исключением

Включение/выключение исключения производится с помощью кнопки - переключателя. Если исключение включено, то оно будет учитываться в привычислении уровня угрозы файла.

Редактирование и удаление исключения выполняется с помощью кнопок в столбце: в виде карандаша и корзины соответственно.

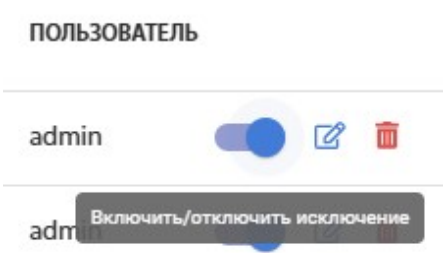


Рис 4.1.1 - кнопки управления исключением

Импорт / экспорт исключений

Для выполнения импорта исключений нужно нажать кнопку "Импорт". В открытом окне нужно выбрать файл формата json, который ранее экспортировался с системы. Итогом импорта будет добавление новых исключений, при этом старые останутся без изменения.

Для выполнения экспорта исключения нужно нажать на кнопку "Экспорт". После нажатия будет скачан файл "exclusions.json"



Рис. 4.1.2 - кнопки импорта и экспорта списка исключений

Сеть

Позволяет применять настройки сети системы.

НАСТРОЙКИ

Общие настройкиИсключенияСистемаОбслуживаниеЛицензияБелый списокYagaПравила SigmaУправление контейнерамиРазоружение и восстановление контента (CDR)

Сеть

Имя хоста

dev-tlab-debian

СОХРАНИТЬ

Адрес

172.16.110.100

Сетевая маска

255.255.254.0

Сетевой шлюз

172.16.110.1

DNS 1:

172.16.110.1

DNS 2:

СОХРАНИТЬ

Рис 4.2 - Страница настроек сети

Обслуживание

Страница, на которой предоставляется возможность выключения или перезагрузки системы tLab. Перезагрузка может занимать несколько минут.

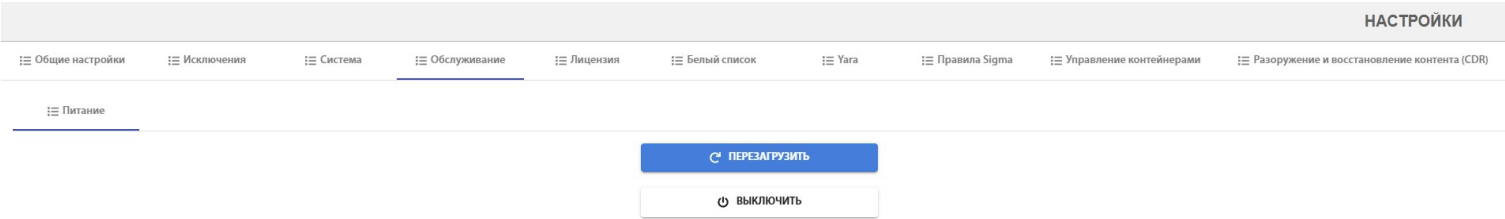


Рис 4.3 - Страница обслуживания системы

Лицензия

Страница, на которой присутствует базовая информация о лицензии и поле активации лицензии.

Информация о лицензии

✔ СИСТЕМА АКТИВИРОВАНА.

Название лицензии tLab Enterprise Software + Support

Тип лицензии: Yearly

Парт-номер лицензии: 5d941cc9-6ad1-4c50-8bcc-a156ddd10b1a

Номер лицензии: -

SKU: -

Выдан: РГУ КНБ РК 12 Департамент

Дата начала: 13/03/2025

Дата истечения: 14/03/2026

✔ ТЕХНИЧЕСКАЯ ПОДДЕРЖКА:

Дата начала: 13/03/2025

Дата истечения: 14/03/2026

Рис. 4.4.1 - окно информации о лицензии

Активировать лицензию

Введите код активации

АКТИВИРОВАТЬ ЛИЦЕНЗИЮ

Рис. 4.4.2 - окно активации лицензии

Белый список

Страница, на которой отображается список доверенных файлов, которые система безопасности считает безопасными. Анализ файлов, включенных в данный список, будет отклоняться со статусом WHITELISTED.

<div>ИМПОРТ</div> <div>ЭКСПОРТ</div> <div>СОЗДАТЬ</div>					
ID	ИМЯ ФАЙЛА	Хэш MD5	Хэш SHA-1	Хэш SHA-256	РАЗМЕР
110610231	calc.exe.exe	42ded57e4e35b23445.....121a8775	d7a7564bcbac07d9b4.....a0d2de92	18c67d03b98a7e2665.....192bbd5a	192.50 KB
110610232	calc.exe.exe	f88cc05134c555d4e1.....78160001	c882f09eafddb75843.....95440001	a103a57d50b32469c5.....821d0001	192.50 KB
110610233	calc.exe.exe	f88cc05134c555d4e1.....78160002	c882f09eafddb75843.....95440002	a103a57d50b32469c5.....821d0002	192.50 KB
110610234	Clean Doc.docx.exe	e33a4b0bd402f7f95b.....2b857c13	340cb322b2b190b829.....c3538554	5fac1a387357418570.....12dc4fb1	6.62 KB
110610235	Clean Doc.pdf.exe	43c9478bf607bb9a76.....e640a1c	031d40b8d61ca23a4e.....55c019f8	83f9fb4f333a04426ab.....2f76dd9e	28.12 KB
110610236	google-tester.exe.exe	46b1dbadb90e948e81.....ca01be0d	7527dd24f6f4b40d7b.....f2488fec	258a5d6523d3b2cb89.....c2f2f349	5.56 MB
110610237	test ThisDocument.cls.exe	eb7cfe4666ce7a8f19.....960fa9bc	3c33e319ec22ebf703.....6e573401	b0d688919ffe7e7d7.....dbb5209a	533.00 bytes
110610238	example.exe	5d41402abc4b2a76b9.....1017c592	7c22fbb2927d828af2.....80637cd	9b74c9897bac770fc.....00000000	120.56 KB
110610241	dsfs	6cd3556deb0da54bca.....39479839	943a702d06f34599ae.....6031d699	315f5bdc76d078c43b.....5894edd3	123.00 bytes

Рис. 4.5.1 - таблица белого списка

Добавление файлов в список производится путём импорта XML файла.

Yara

Страница, на которой отображается список yara-сигнатур. YARA сигнатуры могут быть использованы для обнаружения известных вредоносных программ, вредоносных поведенческих шаблонов и их классификации.

Существует обязательный список сигнатур от вендора, подсвеченных серым цветом.

ИМПОРТ

ОБНОВИТЬ СИГНАТУРЫ ВЕНДОРА

РАЗРАБОТАТЬ YARA

Включить 31/56

?

ID	ВКЛЮЧИТЬ	НАЗВАНИЕ	ОПИСАНИЕ	
1	<input checked="" type="checkbox"/>	EK_Angler.yar		
2	<input checked="" type="checkbox"/>	EK_Zeus.yar		
3	<input checked="" type="checkbox"/>	EK_Phoenix.yar		
4	<input checked="" type="checkbox"/>	Case 4.....	eicar.yar	
5	<input checked="" type="checkbox"/>	Case 5.....	exploit_kits.yar	
6	<input checked="" type="checkbox"/>	Case 6.....	malware.yar	
7	<input checked="" type="checkbox"/>	Case 7.....	packers.yar	
8	<input checked="" type="checkbox"/>	APT_OLE_JSRat	Targeted attack using Excel/word documents	✎ ✖ 📄
9	<input checked="" type="checkbox"/>	DDE Rule	Detect Dynamic Data Exchange protocol in doc/docx	✎ ✖ 📄
10	<input checked="" type="checkbox"/>	Dridex Rule		✎ ✖ 📄
11	<input checked="" type="checkbox"/>	Hidden PE file		✎ ✖ 📄


Items per page: 20

1 – 20 of 56

[|<](#)
[<](#)
[>](#)
[>|](#)

- правило вендора (не может редактироваться/удаляться)

Рис. 4.6.1 - таблица yara-сигнатур

Нажав на кнопку  , можно открыть окно с подробной информацией о модулях и другое.

Информация

Версия модулей:

1.0.3

Дата создания правил вендора:

12/04/21 11:43:41

Дата обновления правил вендора:

12/04/21 11:50:19

Версия правил вендора:

1


Модули Yara:

PE, ELF, Hash, Math, Time, Cuckoo, Magic, Dotnet

Версия Yara:

4.0.2

Рис. 4.6.2 - окно с подробной информацией о Yara

Кнопка  позволяет скачать Yara-сигнатуру файлом формата .yara.

Импорт правила осуществляется кнопкой

 ИМПОРТ

Для импорта нужно указать путь к файлу формата ".yara", название и описание. Сигнатуры вендора доступны к обновлению только через системный функционал с помощью кнопки

ОБНОВИТЬ СИГНАТУРЫ ВЕНДОРА

. На вход подается архивный файл с сигнатурами.

Управление контейнерами

Страница, на которой отображается список контейнеров в системе. Добавленные в таблице контейнеры, доступны для анализа и их статус отображается в Управление - Статус системы.

ЗАГРУЗИТЬ ОБРАЗ



























ID	НАЗВАНИЕ	ОС	ПРИЛОЖЕНИЯ	КОЛ-ВО КОНТЕЙНЕРОВ	РЕДАКТИРОВАТЬ	УДАЛИТЬ
ad92b17d-ed2a-43b4-a504-3ffc2fe9af4e	w764r11of10	Windows 7 x64 SP1 6.1	Default 0, Adobe Reader 11.0.1, MS Office 2010 SP2	0		
37dac045-5048-49fc-aebb-27ec746f58b	w764r15of13	Windows 7 x64 SP1 6.1	Default 0, Adobe Reader DC 15, MS Office 2013	1		
05aa9e2f-6388-4cd1-8874-3022a6b530e0	w7r11of10	Windows 7 SP1 6.1	Default 0, Adobe Reader 11.0.1, MS Office 2010 SP2	0		
74f8bbf1-c3df-452b-8f7b-b7defac09ebd	w7r15of13	Windows 7 SP1 6.1	Default 0, Adobe Reader DC 15, MS Office 2013	0		
22ccb3ef-e62a-46bf-b285-7809b9bab131	w7r17of16	Windows 7 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2016	0		
cd06cbd5-0474-43f1-bba5-3afd1022b612	w81r17o10	Windows 8.1 x64 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2010 SP2	0		
32b6dd26-72fd-48bc-a331-751e94e75352	wXr10of10s1	Windows XP SP3 5.1	Default 0, Adobe Reader 10.1.3, MS Office 2010 SP1	0		
533a0d6e-3f93-4d3b-ad4d-71b43f60fcc4	wXr11of10s2	Windows XP SP3 5.1	Default 0, Adobe Reader 11.0.1, MS Office 2010 SP2	0		
083e333b-a085-4058-8197-87d021121f1	wXr17o19	Windows 10 x64 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2019	1		
083e333b-a085-4058-8197-87d021121f2	wXr17o190_windex_off	Windows 10 x64 off SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2019	1		
e10bc3dc-bf52-41e2-b790-8b64b624395a	wXr17o19_o10	Windows 10 x64 o10 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2019	3		
50f0fa8f-5a1e-41e0-8b09-235c501f6792	wXr17o19_o11	Windows 10 x64 o11 SP1 6.1	Default 0, Adobe Reader DC 17, MS Office 2019	3		
03c5500b-04b1-4d56-bc99-d018aad242ca	wXr9of7s2	Windows XP SP3 5.1	Default 0, Adobe Reader 9.1.0, MS Office 2007 SP2	0		

Рис. 4.7.1. - таблица контейнеров

Для того, чтобы добавить новый контейнер, необходимо нажать на кнопку **ЗАГРУЗИТЬ ОБРАЗ**.
Доступно два вида импорта:

1. Импорт через локальный путь
2. Импорт через URL

Интеграция

В рамках интеграции представлен функционал по интеграции системы с различными внешними сервисами и ресурсами, которые помогают улучшить ее функциональность и эффективность. Здесь доступны различные настройки и подробная информация. Доступен данный функционал в Управление - Интеграция.

Представлены следующие секции: сетевое хранилище, интеграция Trend micro, ICAP сервер.
































Сетевое хранилище

Страница, на которой отображается список сетевых хранилищ (общих папок / shares).В таблице представлены следующие характеристики хранилищ:

1. Включено / выключено сканирование по расписанию
2. Название
3. Сервер (IP)
4. Путь
5. Расписание сканирования (настраивается)
6. Тип сканирования: полное и быстрое. Быстрое - пропускает просканированные файлы по расписанию за период, установленный в поле "Дни до истечения".
7. Имя предустановки

Список хранилищ

ДОБАВИТЬ ХРАНИЛИЩЕ

ID	ВКЛЮЧИТЬ	НАЗВАНИЕ	СЕРВЕР	ПУТЬ	РАСПИСАНИЕ	ТИП СКАНИРОВАНИЯ	ИМЯ ПРЕДУСТАНОВКИ	
1	<input checked="" type="checkbox"/>	Test Share Scan 11	172.16.111.49	share2	В 04:00, только в понедельник	Полное	share	СКАНИРОВАТЬ  
2	<input checked="" type="checkbox"/>	Share22222	172.16.111.49	share1	Каждые 20 минут	Полное	share	СКАНИРОВАТЬ  
5	<input checked="" type="checkbox"/>	Test Path in share	172.16.111.49	share1/hybrid_unknown_malware/exe	Каждый час	Быстрое 	share	СКАНИРОВАТЬ  
6	<input checked="" type="checkbox"/>	Kostya Notebook Share	172.16.100.61	Kostya_Shared_Folder	Не определено	Быстрое 	share	СКАНИРОВАТЬ  
7	<input checked="" type="checkbox"/>	123132131231	123	123	Не определено	Быстрое 	share	СКАНИРОВАТЬ  
8	<input checked="" type="checkbox"/>	New sharsdfgdg	192.168.168.222	common_folder	В 08:00, в 5 число месяца, только в мэй	Быстрое 	mailer	СКАНИРОВАТЬ  
10	<input checked="" type="checkbox"/>	test kostya 2	123	123	В 00:00, только в вторник	Быстрое 	share	СКАНИРОВАТЬ  
11	<input checked="" type="checkbox"/>	test kostya 3	123	123	Каждые 10 минут	Быстрое 	share	СКАНИРОВАТЬ  
12	<input checked="" type="checkbox"/>	test kostya 4	123	123	Каждые 10 минут	Быстрое 	share	СКАНИРОВАТЬ  
13	<input checked="" type="checkbox"/>	test kostya 55	123	123	Каждые 10 минут	Быстрое 	share	СКАНИРОВАТЬ  
14	<input checked="" type="checkbox"/>	test kostya 6	123	123	Каждые 10 минут	Быстрое 	share	СКАНИРОВАТЬ  

Items per page: 201 – 20 of 26|<<>>|

Рис. 4.8.1 - таблица сетевых хранилищ

Для просмотра сессий сканирования определенного хранилища, нужно нажать на название хранилища.

ID	ВКЛЮЧИТЬ	НАЗВАНИЕ
1	<input checked="" type="checkbox"/>	Test Share Scan 11

Рис. 4.8.2 - ссылка на сканирования

НАЧАЛО	КОНЕЦ	ВСЕГО ФАЙЛОВ	ПРОСКАНИРОВАНО	ВРЕДНОСНЫЕ ФАЙЛЫ	ОШИБКА
		13	13	4	
		13	13	5	
		13	13	5	
		13	13	5	
		13	13	5	
		13	13	5	
		13	13	5	
		0	0	0	⚠
		13	12	4	
		13	13	5	
		13	13	5	

Items per page: 201 - 20 of 627|<>>>|

Рис. 4.8.3 - таблица сессий сканирования хранилища

При сканировании хранилища существует вероятность ошибки при выполнении. В случае, если произошла ошибка, в столбце "Ошибка" будет присутствовать знак ⚠. При нажатии на него, появится описание ошибки.

⚠

Описание ошибки

Previous scan in progress

Рис. 4.8.4 - описание ошибки при сканировании

Список хранилищ → Test Share Scan 11 → Scan #833

Рис. 4.8.4.1 - навигация на странице сетевые хранилища

Навигация по странице производится нажатием на ссылки на рисунке 4.8.4.1

Для просмотра списка файлов, которые были проанализированы в рамках сканирования, нужно нажать на ссылку, которая активируется при нажатии на числовое значение в столбце "Всего файлов".

Список хранилищ → Test Share Scan 11

НАЧАЛО	КОНЕЦ	ВСЕГО ФАЙЛОВ
		13

Рис. 4.8.5 - ссылка на таблицу проанализированных файлов

ФИЛЬТР: УРОВЕНЬ УГРОЗЫ		>=		100	СБРОСИТЬ ФИЛЬТРЫ		ВРЕДОНОСНЫЕ ФАЙЛЫ 4 / 13	
№ ОТЧЕТА	ИМЯ ФАЙЛА	ПУТЬ	ХЭШ SHA256	Размер	РЕЗУЛЬТАТ	УРОВЕНЬ УГРОЗЫ	СТАТУС	ОШИБКА
335561,335562	a8e88cda2b50.....5039.exe	a8e88cda2b50.....5039.exe	a8e88...5039	3.96 MB	Угроз не обнаружено	45.28	Завершен	
335563	clean_rtf.rtf	clean_rtf.rtf	0d6af...a01d	7.00 bytes	Угроз не обнаружено	0	Завершен	
335566,335567	da3b2e2db1ba.....4813.exe	da3b2e2db1ba.....4813.exe	da3b2...4813	711.00 KB	Вредоносный	107.7	Завершен	
335568,335569	Defrag.exe	Defrag.exe	f3653...2ba8	182.50 KB	Угроз не обнаружено	49.41	Завершен	
335570,335571	Pafish2.bin	newfolder/ma.....ish2.bin	b8646...0109	168.00 KB	Вредоносный	132.54	Завершен	
335572	prilojenie.doc	newfolder/ma.....enie.doc	6d1f5...a786	677.10 KB	Вредоносный	137.99	Завершен	
335573	rtf1.rtf	newfolder/rtf1.rtf	44d33...2ba5	241.00 bytes	Угроз не обнаружено	0	Завершен	
335574	rtf2.rtf	newfolder/rtf2.rtf	6b42a...894f	239.00 bytes	Угроз не обнаружено	0	Завершен	
335575	f741069631a0.....ead9.pdf	pdf/f7410696.....ead9.pdf	f7410...ead9	59.59 KB	Вредоносный	115.76	Завершен	
335576,335577	cmd.exe	windows_files/cmd.exe	3656f...2ea2	272.00 KB	Угроз не обнаружено	49.41	Завершен	
335578,335581	cmmon32.exe	windows_files/cmmon32.exe	eacbf...7a8e	42.00 KB	Угроз не обнаружено	42.72	Завершен	
						Items per page: 20	1 - 13 of 13	< < > >

Рис. 4.8.6 - таблица проанализированных файлов

Переход на отчёт анализа файла производится путём нажатия на номер отчёта в столбце "№ Отчета".

ICAP сервер

Страница, на которой осуществляются настройки ICAP сервера и настройки фильтра.

☰ Сетевое хранилище

☰ Интеграция Trend Micro

☰ ICAP сервер

☰ Управление расширениями браузера

Настройки фильтра

Включить

OFF ON

Режим работы

Препятствование

Название предустановки

webgateway

Время анализа

30

Макс. время ожидания анализа

300

Пропускать объект в случае таймута

OFF ON

Уровень угрозы для блокировки

80

СОХРАНИТЬ

Настройки сервера

Стартовое кол-во процессов

5

Макс. кол-во процессов

10

Кол-во потоков на процесс

10

Мин. кол-во свободных потоков

10

Макс. кол-во свободных потоков

20

СОХРАНИТЬ

Рис. 4.9.1 - страница настроек ICAP







Корзина

Удаленные администратором отчеты помещаются в корзину. Отсюда их можно восстановить, либо очистить корзину. Отчеты в корзине можно просматривать по прямой ссылке или из корзины.

ОЧИСТИТЬ КОРЗИНУ

ВОССТАНОВИТЬ 1 ОТЧЕТ(А)

СПИСОК УДАЛЕННЫХ ОТЧЁТОВ

	№ ОТЧЕТА	ТИП АНАЛИЗА	ДАТА И ВРЕМЯ	ИМЯ ФАЙЛА	ХЕШ SHA256	ИНДИКАТОРЫ	КОНФИГУРАЦИЯ	ПРОГРАММЫ	СНИМКИ	УРОВЕНЬ УГРОЗЫ	ИНДИКАТОР	ЗАКЛЮЧЕНИЕ
<input checked="" type="checkbox"/>	389215	DYN STA	11/04/25 14:44:01	gualberto2020.pdf	d31092		Windows 10 x64 dev	Adobe Reader DC 17	6	0		UNKNOWN
<input type="checkbox"/>	389214	DYN STA	11/04/25 14:40:52	apwg_trends_report_q2_2023.pdf	2f6d7c		Windows 10 x64 dev	Adobe Reader DC 17	7	0		UNKNOWN
<input type="checkbox"/>	389213	DYN STA	11/04/25 14:37:37	A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning.pdf	278500		Windows 10 x64 dev	Adobe Reader DC 17	6	0		UNKNOWN
<input type="checkbox"/>	389212	DYN STA	11/04/25 14:34:30	Phishing-Detection-with-Machine-Learning (1).pdf	d70157		Windows 10 x64 dev	Adobe Reader DC 17	7	0		UNKNOWN
<input type="checkbox"/>	389211	DYN STA	11/04/25 14:31:21	1465.pdf	ac84d6		Windows 10 x64 dev	Adobe Reader DC 17	7	0		UNKNOWN

Items per page: 5

1 – 5 of 5




Рис. 5 - Страница корзины отчётов