

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

ID	ПУТЬ ИСКЛЮЧЕНИЯ	ОПЕРАЦИОННАЯ СИСТЕМА	СОБЫТИЕ	АТРИБУТ	ВРЕМЯ СОЗДАНИЯ	СЕМАНТИКА	ПОЛЬЗОВАТЕЛЬ
95	C:\Users\Администратор\AppData\Local\Temp\ModuleAnalysisCache	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\AppData\Local\Temp\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)_loader\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 при вычислении уровня угрозы файла.

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

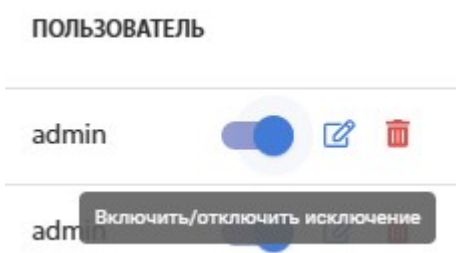


Рис 4.1.1 - кнопки управления исключением

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

 [Отредактировать эту страницу](#)