

# Детальный отчет

Детальный отчет – интерактивный список активностей с возможностью фильтрации по типу событий. Список всех активностей с параметрами приведен в [Приложении 2](#). При нажатии *Правой кнопки мыши* на параметр активности отображается контекстное меню с дополнительными для данного параметра фильтрами. Каждая активность имеет уровень опасности. Список возможных уровней опасности представлен в [Приложении 3](#).

Краткий отчет

Детальный отчет

Цепочка событий

Логи производительности

СБРОСИТЬ ФИЛЬТРЫ

ФИЛЬТР ПО ТИПУ СОБЫТИЙ

ИНДИКАТОР	ПАРАМЕТР	ХЭШ SHA256	ВРЕМЯ
> Новый процесс			18:43:01
> Идентификация уникального компьютера			18:43:02
> Новый процесс			18:43:02
> Идентификация уникального компьютера			18:43:02
▼ Идентификация уникального компьютера			18:43:02
▼ Процесс-инициатор	C:\Windows\System32\WScript.exe	ce9f70_d97b	18:43:02
Подписано	N/A (undefined)		18:43:02
Название ключа реестра	\REGISTRY\MACHINE\Software\Microsoft\Cryptography		18:43:02
Атрибут компьютера (используемый для идентификации)	2		18:43:02
▼ Внедрение кода			18:44:35
▼ Процесс-инициатор (инжектор)	C:\Windows\System32\lschlient.exe	5a299f_e900	18:44:35
Подписано	N/A (undefined)		18:44:35
▼ Процесс-цель инъекции	System		18:44:35
Подписано	N/A (undefined)		18:44:35

Items per page: 1001 – 6 of 6

Рис. 16 – Список зафиксированных активностей

СБРОСИТЬ ФИЛЬТРЫ

ФИЛЬТР ПО ТИПУ СОБЫТИЙ

☒ Выбрать все

☐ Исключить все

☒ Новый процесс

☒ Идентификация уникального компьютера

☒ Внедрение кода

Apply

Рис. 17 – Фильтры списка зафиксированных активностей

ИНДИКАТОР	ПАРАМЕТР	ХЭШ SHA256	ВРЕМЯ
> Новый процесс			18:43:01
▼ Идентификация уникального компьютера			18:43:02
> Процесс-инициатор	\SystemRoot\System32\Conhost.exe		18:43:02
Название ключа реестра	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName		
Атрибут компьютера (используемый для идентификации)	1		
> Новый процесс			
> Идентификация уникального компьютера			
> Идентификация уникального компьютера			
> Внедрение кода			

Все действия процесса

Все действия над процессом

Все действия подозрительного предка(источника)

Все действия над подозрительным предком(источником)

Полная цепочка подозрительных событий

Все действия процесса с таким названием

Все действия над процессом с таким названием

Рис. 18 – Фильтры списка зафиксированных активностей, доступные через контекстное меню

Система предоставляет возможность добавления файл или путь в исключение для анализа. Выделив путь или его часть и нажав правой кнопкой, откроется меню, в котором можно открыть окно

добавления исключения.






>  Процесс-инициатор	C:\MAPKЕPbin	⋮
 Открываемый файл	C:\Users\Администратор\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat	⋮
>  Открытие важного файла	<div>Добавить строку в исключения Скопировать в буфер</div>	
>  Открытие важного файла		
>  Считывает настройки интернета		

Рис 18.1 – Определение пути файла/директории исключения

Добавить исключение

Событие:	Идентификация уникального компьютера
Родитель:	\SystemRoot\System32\Conhost.exe
Процесс-инициатор	\SystemRoot\System32\Conhost.exe
Исключить путь:	<input type="text" value="\SystemRoot\System32\Conhost.exe"/>
Операционная система	<div>Any</div>
Семантика	<div></div>

➤ ОТПРАВИТЬ

Рис 18.2 – Окно добавления исключения

 [Отредактировать эту страницу](#)