

Общие сведения

События безопасности — это модуль, который позволяет реагировать на действия и состояния конечных устройств. AxelNAC позволяет реагировать на смену профиля устройства (тип устройства, MAC-вендера, отпечаток DHCP и т.д.), на несоответствие политикам ИБ устройства, а также реагировать на превышение устройством порогового уровня потребляемого трафика.

Функционал **событий безопасности** позволяет комбинировать уведомление администраторов ИБ и изолирование устройства, вызвавшего событие, от общей сети с последующим указанием инструкций и действий на портале администратора AxelNAC.

Глобально, события безопасности позволяют выполнять следующие действия с конечными устройствами, которые попали под настроенные условия:

- Снять устройство с регистрации;
- Зарегистрировать устройство в сети;
- Изолировать устройство;
- Отправить уведомление на электронную почту Администратора сети ;
- Отправить уведомление на электронную почту владельца конечного устройства ;
- Отправить уведомление на определенную электронную почту ;
- Выполнить скрипт;
- Завершить активное событие безопасности .

Список событий безопасности

Все события безопасности доступны в разделе **Конфигурация → Соответствие → События безопасности**.

Статус	Идентификатор	Описание	Приоритет	Шаблон	
Включено	1300006	Fingerbank device class change	1	device_transition	<button>Клонировать</button> <button>Предпросмотр</button>
Включено	1300007	Fingerbank profile anomaly	4	generic	<button>Клонировать</button> <button>Предпросмотр</button>
Включено	1300008	Fingerbank detected blacklisted communication	4	generic	<button>Клонировать</button> <button>Предпросмотр</button>
Отключено	2000000	Malware	4	malware	<button>Клонировать</button> <button>Предпросмотр</button>
Отключено	2000032	LSASS Exploit	4	lsass	<button>Клонировать</button> <button>Предпросмотр</button>
Отключено	2001569	NetBIOS Scan	6	scanning	<button>Клонировать</button> <button>Предпросмотр</button>
Отключено	2001904	Telnet Scan	6	scanning	<button>Клонировать</button> <button>Предпросмотр</button>
Отключено	2001972	Remote Desktop Scan	6	scanning	<button>Клонировать</button> <button>Предпросмотр</button>
Отключено	2002030	IRC Trojan	3	trojan	<button>Клонировать</button> <button>Предпросмотр</button>

На данной странице вы можете просмотреть список всех созданных событий безопасности, задать параметры поиска, активировать работу, клонировать, выполнить предпросмотр отображаемой HTML-страницы и экспортовать список.

Вы также можете отсортировать список по любой из колонок. Для этого нажмите на иконку сортировки слева от имени колонки.

Статус	Идентификатор	Описание
Включено	1100001	Nessus Scan

Поиск событий безопасности

Для того, чтобы выполнить поиск событий безопасности, нажмите на строку поиска в верхней части списка, введите ключевое слово для поиска и нажмите **Поиск**. В качестве ключевого слова может использоваться идентификатор или описание события безопасности, а также имя шаблона HTML-страницы, который будет использоваться при срабатывании события.

События безопасности

Статус	Идентификатор	Описание	Приоритет	Шаблон
Отключено	3000001	Block all mobile devices	10	banned_devices
Отключено	3000002	Block Apple iPod, iPhone or iPad	10	banned_devices
Отключено	3000003	Block BlackBerrys	10	banned_devices
Отключено	3000004	Block PS3 and PSP	10	banned_devices
Отключено	3000005	Block Slingbox	10	banned_devices

Для того, чтобы сбросить условия поиска, нажмите **Очистить**.

Быстрая активация событий безопасности

Для того, чтобы активировать/деактивировать работу события безопасности, нажмите на переключатель в колонке **Статус**.

События безопасности

Статус	Идентификатор	Описание	Приоритет
Включено	1100001	Nessus Scan	4
Включено	1100002	OpenVAS scan	4
Отключено	1100003	MAC Vendor isolation example	4
Отключено	1100004	Ancient OS isolation example	4

Клонирование событий безопасности

Для того, чтобы клонировать событие безопасности, нажмите **Клонировать** в правой части таблицы. После этого откроется окно конфигурации нового события безопасности.

Шаблон
failed_scan

Клонировать Предпросмотр ▾

failed_scan

Клонировать Предпросмотр ▾

banned_devices

Клонировать Предпросмотр ▾

Предпросмотр HTML-страницы

Для того, чтобы выполнить предпросмотр HTML-страницы, отображаемой при срабатывании события безопасности, нажмите **Предпросмотр** в правой части таблицы. При нажатии вам будет предложено выбрать профиль подключения, для которого вы хотите выполнить предпросмотр. После выбора профиля подключения будет отображена HTML-страница.

The screenshot shows a table with columns: Описание (Description), Приоритет (Priority), and Шаблон (Template). There are six rows of data:

Описание	Приоритет	Шаблон
Nessus Scan	4	failed_scan
OpenVAS scan	4	failed_scan
MAC Vendor isolation example	4	banned_devices
Ancient OS isolation example	4	banned_os
P2P Isolation (snort example)	4	p2p
Auto-register Device example	1	generic

A dropdown menu is open on the right side of the table, listing various connection profiles. An arrow points from the 'banned_devices' entry in the table to the corresponding entry in the dropdown menu. The dropdown menu includes:

- Профиль подключения
- Conn_profile_multi
- Conn_profile_provisioning
- EAP_connect_test
- EAP_connect_test-copy
- EAP_connect_test_1
- Guest_access_locale_auth
- SMS-test_profile
- conn_AD_test
- default
- open_ssid_test
- secure_ssid_test
- stress_test_conn_profile
- test_connect_noEAP
- test_connect_noEAP-WLC
- test_connect_noEAP-copy1

At the bottom of the dropdown menu are two buttons: Клонировать (Clone) and Предпросмотр (Preview).

ID статьи: 588

Последнее обновление: 8 окт., 2024

Обновлено от: Егоров В.

Ревизия: 4

База знаний AxeINAC -> Документация -> Система контроля доступа к сети «AxeINAC». Версия 2.0.1 -> AxeINAC. Руководство администратора -> События безопасности -> Общие сведения

<https://docs.axel.pro/entry/588/>