

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-вендора, 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**.

The screenshot shows the 'События безопасности' (Security Events) configuration page in the AxelNAC interface. The page has a dark header with the 'AxelNAC' logo and navigation links: 'Статус', 'Отчёты', 'Аудит', 'Узлы', 'Пользователи', and 'Конфигурация'. The user is logged in as 'admin'. The left sidebar contains a 'Фильтр' (Filter) section and a list of configuration options under 'Соответствие' (Compliance), including 'Основные настройки', 'Определение изменений в устройстве', 'Комбинации устройства', 'Отпечатки DHCP', 'DHCP-вендоры', 'Отпечаток DHCPv6', 'DHCPv6 Enterprises', 'MAC-вендоры', 'Агенты пользователя', 'Обнаружение сетевых аномалий', 'Механизмы сканирования', and 'События безопасности' (which is highlighted). The main content area is titled 'События безопасности' and features a search bar, a 'Очистить' (Clear) button, and a 'Поиск' (Search) button. Below the search bar is a 'Новое событие безопасности' (New security event) button and a table with 25 rows. The table has columns for 'Статус' (Status), 'Идентификатор' (Identifier), 'Описание' (Description), 'Приоритет' (Priority), and 'Шаблон' (Template). The first row shows a 'Включено' (Enabled) status for 'Fingerbank device class change' with priority 1. The second row shows 'Включено' for 'Fingerbank profile anomaly' with priority 4. The third row shows 'Включено' for 'Fingerbank detected blacklisted communication' with priority 4. The fourth row shows 'Отключено' (Disabled) for 'Malware' with priority 4. The fifth row shows 'Отключено' for 'LSASS Exploit' with priority 4. The sixth row shows 'Отключено' for 'NetBIOS Scan' with priority 6. The seventh row shows 'Отключено' for 'Telnet Scan' with priority 6. The eighth row shows 'Отключено' for 'Remote Desktop Scan' with priority 6. The ninth row shows 'Отключено' for 'IRC Troian' with priority 3. Each row has 'Клонировать' (Clone) and 'Предпросмотр' (Preview) buttons.

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

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

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

The diagram illustrates the sorting mechanism in the 'События безопасности' table. It shows the first three columns: 'Статус' (Status), 'Идентификатор' (Identifier), and 'Описание' (Description). Each column header has a sorting icon (a small square with up and down arrows) to its left. Arrows point from these icons to the column headers, indicating that clicking the icon will sort the data by that column. The first row of data shows 'Включено' (Enabled) status, identifier '1100001', and description '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

🔍 Block

Очистить

Поиск

Новое событие безопасности

25

« < 1 > »

<input type="checkbox"/>	Статус	Идентификатор	Описание	Приоритет	Шаблон	
<input type="checkbox"/>	Отключено	3000001	Block all mobile devices	10	banned_devices	<div>Клонировать</div> <div>Предпросмотр</div>
<input type="checkbox"/>	Отключено	3000002	Block Apple iPod, iPhone or iPad	10	banned_devices	<div>Клонировать</div> <div>Предпросмотр</div>
<input type="checkbox"/>	Отключено	3000003	Block BlackBerries	10	banned_devices	<div>Клонировать</div> <div>Предпросмотр</div>
<input type="checkbox"/>	Отключено	3000004	Block PS3 and PSP	10	banned_devices	<div>Клонировать</div> <div>Предпросмотр</div>
<input type="checkbox"/>	Отключено	3000005	Block Slingbox	10	banned_devices	<div>Клонировать</div> <div>Предпросмотр</div>

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

🔍 Введите критерии поиска

Новое событие безопасности

<input type="checkbox"/>	Статус	Идентификатор	Описание	Приоритет
<input type="checkbox"/>	Включено	1100001	Nessus Scan	4
<input type="checkbox"/>	Включено	1100002	OpenVAS scan	4
<input type="checkbox"/>	Отключено	1100003	MAC Vendor isolation example	4
<input type="checkbox"/>	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	<div>Клонировать</div> <div>Предпросмотр</div>
failed_scan	<div>Клонировать</div> <div>Предпросмотр</div>
banned_devices	<div>Клонировать</div> <div>Предпросмотр</div>

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.

25

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

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

Клонировать

Предпросмотр