Профилирование в хранилище отпечатков

Использование профилей из хранилища отпечатков позволяет обнаружить возможную подмену MAC-адресов, в случаях, когда устройство переходит из одного класса устройств в другой (например, устройство переходит из класса **Windows** в класс **Принтеры**), и вызвать событие безопасности, а также изолировать конечную точку.

По умолчанию проверка изменений класса устройств отключена. Чтобы активировать ее, перейдите в раздел **Конфигурация → Соответствие → Профилирование/хранилище отпечатков → Обнаружение изменений в устройстве** и переместите переключатель **Срабатывать при изменении класса устройства** в положение **Включено**. После этого появится возможность выбора: запускать событие безопасности при любом изменении класса устройства или при определенном наборе изменений.

Срабатывание связанных событий безопасности при любом изменении класса устройства

При первоначальной активации функции рекомендуется выполнить какие-нибудь действия, вызывающие срабатывание событий безопасности, чтобы проверить, может ли потребоваться внести в белый список какие-либо переходы между классами устройств.

Наиболее простым методом обнаружения является срабатывание при изменении класса устройства, что приводит к возникновению события безопасности при обнаружении перехода устройства из одного класса в другой. Некоторые из таких переходов могут считаться допустимыми. Их можно включить белый список переходов с помощью параметра Белый список изменений в классе устройства. Пример включения в белый список — переход Windows OS в Mac OS X или macOS.

Пример события безопасности с использованием этого триггера является предустановленным в поставляемой конфигурации AxelNAC (идентификатор события безопасности — **1300006**, имя — **Fingerbank device class change**).

Пользовательское срабатывание связанных событий безопасности

Вместо срабатывания при любом переходе можно выполнить обнаружение и срабатывание события безопасности на определенных изменениях класса устройства. Для этого нужно указать все варианты изменения класса устройства, которые должны вызывать срабатывание события безопасности, в поле **Пользовательские триггеры изменения класса устройства**.

ID статьи: 972
Последнее обновление: 17 июл., 2024
Обновлено от: Егоров В.
Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство администратора -> Хранилище отпечатков -> Профилирование в хранилище отпечатков
https://docs.axel.pro/entry/972/