Богоутдинова Алина.

1. Выберите правильный вариант

Это всего лишь универсальная Категория «Catch-All», которая регистрирует различные события, влияющие на компьютер, безопасность системы или журнал безопасности

(Системные события)

А) Системные события

Б) Целостность системы

В) Общая папка

1. Выберите правильный вариант. О каком аудите речь?

В Windows есть десятки прав и разрешений пользователя (например, вход в качестве пакетного задания и работа в составе операционной системы). Этот параметр политики определяет, следует ли выполнять аудит каждого экземпляра субъекта безопасности

(Аудит использования привилегий)

А) Аудит изменений политики

Б) Аудит отслеживания процессов

В) Аудит использования привилегий

1. Вставьте пропущенные слова в текст

Эта подкатегория сообщает, когда осуществляется доступ к объектам … Только объекты файловой системы с SACL вызывают создание событий аудита и только тогда, когда доступ к ним осуществляется способом, соответствующим их записям SACL. Сам по себе этот … не приведет к аудиту каких бы то ни было событий. Он определяет, следует ли выполнять аудит событий пользователя, обращающегося к объекту файловой системы, имеющему указанный системный список управления доступом (SACL), фактически позволяя выполнять аудит.

(Б и В)

А) Разрешений пользователя

Б) Файловой системы

В) Параметр политики

Г) Общая папка

1. Перечислите все правильные аудиты

(Б В Д)

А) Аудит безопасности данных

Б) Аудит изменений политики

В) Аудит использования привилегий

Г) Аудит удаления пользователей

Д) Аудит системных событий

1. Соотнесите понятия

1 Управление учетными записями пользователей

2 Управление учетными записями компьютеров

3 Управление группами безопасности

4 Управление группами распространения

5 Управление группой приложений

А) Эта подкатегория сообщает о каждом событии …. , например при создании, изменении или удалении группы рассылки, а также при добавлении или удалении участника из группы рассылки. Если этот параметр политики аудита включен, администраторы могут отслеживать события для обнаружения вредоносного, случайного и полномочного создания учетных записей групп.

Б) Эта подкатегория сообщает о каждом …. , например при создании, изменении или удалении группы приложений, а также при добавлении или удалении члена …. . Если этот параметр политики аудита включен, администраторы могут отслеживать события для обнаружения вредоносного, случайного и полномочного создания учетных …. .

В) Эта подкатегория сообщает о каждом событии … , например при создании, изменении или удалении …. , а также при добавлении или удалении члена … . Если этот параметр политики аудита включен, администраторы могут отслеживать события для обнаружения вредоносного, случайного и полномочного создания учетных записей …..

Г) Эта подкатегория сообщает о каждом событии …. , например о создании, изменении или удалении ….. . ….. переименована, отключена или включена; или пароль установлен или изменен. Если этот параметр политики аудита включен, администраторы могут отслеживать события для обнаружения вредоносного, случайного и полномочного создания …. .

Д) Эта подкатегория сообщает о каждом событии …. , например, когда создается, изменяется, удаляется, переименована, отключена или включена ….. .

(1-г, 2-д, 3-в, 4-а, 5-б)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| В | А | Г | Б |  |

1. Соотнесите понятия по концовки определения.

1 Регистр

2 Файловая система

3 Объект ядра

4 Общая папка

А) Если параметр аудита доступа к объектам настроен на успешное выполнение , запись аудита создается каждый раз, когда пользователь успешно обращается к объекту с указанным списком SACL. Если для этого параметра политики задано значение сбой , запись аудита создается каждый раз, когда пользователь не пытается получить доступ к объекту с указанным списком SACL.

Б)  Он определяет, следует ли выполнять аудит событий пользователя, обращающегося к объекту файлового ресурса, имеющему указанный системный список управления доступом (SACL), фактически позволяя выполнять аудит.

В) Сам по себе этот параметр политики не приведет к аудиту каких бы то ни было событий.

Г) Обычно объекты получают только списки SACL, если включены параметры аудита Аудитбасеобжектс или Аудитбаседиректориес.

(1-В, 2-А, 3-Г, 4-Б)

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
|  |  |  |  |