При расследовании инцидентов в Windows важно анализировать различные события, которые могут указывать на подозрительную или нежелательную активность. Вот основные категории событий, которые следует учитывать:

**1. События входа в систему (Logon/Logoff)**

- **Event ID 4624** - Успешный вход в систему. Важно определить, кто и когда вошел в систему, а также каким образом (например, интерактивный вход или удаленный доступ).
- **Event ID 4625** - Неудачная попытка входа. Это может указывать на попытки взлома или ошибочные попытки доступа.
- **Event ID 4634** - Успешный выход из системы.
- **Event ID 4648** - Вход с использованием альтернативных учетных данных (например, при использовании RunAs).

**2. События связанные с учетными записями (Account Management)**

- **Event ID 4720** - Создание новой учетной записи.
- **Event ID 4722** - Включение учетной записи.
- **Event ID 4725** - Отключение учетной записи.
- **Event ID 4726** - Удаление учетной записи.
- **Event ID 4732/4733** - Добавление или удаление учетной записи из группы безопасности (например, администраторов).

**3. События изменения прав (Privilege Use)**

- **Event ID 4672** - Применение привилегий специального назначения, например, привилегии администратора.
- **Event ID 4673** - Попытка использования привилегии, например, для выполнения действий, требующих повышенных прав.

**4. События связанные с доступом к объектам (Object Access)**

- **Event ID 4663** - Попытка доступа к объекту (файл, папка, ключ реестра и т.д.).
- **Event ID 4656** - Запрос на доступ к объекту.
- **Event ID 4698** - Создание задания в планировщике задач, что может указывать на возможное наличие вредоносного ПО.

**5. События системных изменений (System Integrity)**

- **Event ID 104** - Изменение настроек аудита, что может свидетельствовать о попытке скрыть следы.
- **Event ID 1102** - Очистка журнала событий безопасности, что часто является признаком компрометации.

**6. События использования служб (Service Events)**

- **Event ID 7045** - Установка новой службы. Если служба установлена без ведома администратора, это может свидетельствовать о вредоносной активности.

**7. События сетевой активности (Network Events)**

- **Event ID 5156** - Разрешенное соединение через брандмауэр.
- **Event ID 5140** - Доступ к общему ресурсу, что может свидетельствовать о попытке несанкционированного доступа к файлам.

**8. События, связанные с PowerShell (PowerShell Events)**

- **Event ID 4104** - Скрипты, выполняемые через PowerShell, могут указывать на попытки эксплуатации системы через сценарии.
- **Event ID 4103** - Загрузка модулей PowerShell.
- **Event ID 4105** - Начало удаленной сессии PowerShell.

**9. События использования приложений (Application Events)**

- **Event ID 4688** - Создание нового процесса, что может указывать на запуск подозрительных программ.
- **Event ID 4697** - Установка новой службы, которая может быть связана с вредоносным ПО.

Анализ этих событий позволяет выявить несанкционированные действия и определить, каким образом произошел инцидент.