Event ID	Название	Описание	MITRE ATTACK
1102	Security log cleared	Может указывать на попытки злоумышленника скрыть следы, очистив журнал безопасности (например, очистка журнала безопасности после несанкционированного входа администратора)	T1070 - Indicator Removal on Host
4624	Successful account logon	Помогает выявлять несанкционированные или подозрительные попытки входа и отслеживать активность пользователей в сети (например, входы за пределами рабочего времени с необычных хостов)	T1078 - Valid Accounts
4625	Failed account logon	Указывает на потенциальные атаки методом перебора паролей при неудачных попытках входа в систему (например, множественные неудачные попытки входа с одного источника за короткое время)	T1110 - Brute Force
4648	Logon attempt with explicit credentials	Может указывать на кражу учетных данных или неправильное использование учетных записей (например, злоумышленник создает новый токен для учетной записи после компрометации текстовых учетных данных)	T1134 - Access Token Manipulation
4662	An operation was performed on an object	Помогает отслеживать доступ к критическим объектам в Active Directory, что может указывать на несанкционированную активность (например, злоумышленник выполняет атаку DCSync, выполняя репликацию с необычного хоста)	T1003 - OS Credential Dumping
4663	Access to an object was requested	Отслеживает попытки выполнения определенных действий над чувствительными объектами, такими как файлы, процессы и ключи реестра, что может указывать на несанкционированный доступ (например, злоумышленник пытается прочитать файл или папку, когда у него явно запрещены такие права)	T1530 - Data from Local System
4670	Permissions on an object were changed	Помогает обнаруживать потенциальное изменение чувствительных файлов или несанкционированное повышение привилегий (например, пользователь с низкими привилегиями изменяет разрешения на чувствительный файл для получения доступа)	T1222 - File Permissions Modification
4672	Administrator privileges assigned to a new logon	Помогает обнаруживать повышение привилегий и несанкционированное использование учетных записей (например, обычному пользователю внезапно предоставляются административные права без запроса на изменение)	T1078 - Valid Accounts
4698	A scheduled task was created	Помогает обнаруживать создание злонамеренных запланированных задач и может указывать на устойчивость, повышение привилегий или горизонтальное перемещение (например, злоумышленник создает запланированную задачу, которая запускает бэкдор)	T1053 - Scheduled Task/Job
4720	New user account created	Отслеживает создание несанкционированных учетных записей или потенциальных внутренних угроз (например, создание новой учетной записи вне обычного рабочего времени без одобрения HR)	T1136 - Create Account
4724	An attempt was made to reset an account's password	Отслеживает попытки сброса пароля учетной записи, которые могут указывать на захват учетной записи (например, злоумышленник сбрасывает пароль учетной записи с высокими привилегиями)	T1098 - Account Manipulation
4728	Member added to a security-enabled global group	Отслеживает изменения важных групп безопасности, которые могут указывать на несанкционированное повышение привилегий (например, злоумышленник добавляет пользователя в группу "Domain Admins")	T1098 - Account Manipulation
4732	Member added to a security-enabled Local group	Отслеживает изменения локальных групп безопасности, которые могут указывать на несанкционированный доступ или повышение привилегий (например, злоумышленник добавляет пользователя в локальную группу "Administrators")	T1098 - Account Manipulation
4768	A Kerberos authentication ticket was requested (TGT Request)	Отслеживает первичные запросы аутентификации для отслеживания входов пользователей и помогает выявлять потенциальное злоупотребление протоколом Kerberos (например, злоумышленник компрометирует NTLM-хэш привилегированной учетной записи и выполняет атаку "перехват хэша", запрашивая TGT с необычного хоста)	T1558 - Steal or Forge Kerberos Tickets
4769	A Kerberos service ticket was requested	Отслеживает потенциальные атаки Kerberoasting или другие подозрительные действия, направленные против протокола Kerberos (например, внезапный рост запросов уникальных служб от одного пользователя)	T1558 - Steal or Forge Kerberos Tickets
4776	The domain controller attempted to validate the credentials	Помогает выявлять неудачные или успешные попытки проверки учетных данных через контроллер домена, что может указывать на несанкционированный доступ или подозрительную аутентификационную активность (например, необычное количество неудачных проверок от одного IP-адреса)	T1110 - Brute Force
7045	New service installed	Отслеживает установку потенциально вредоносных служб, указывающих на горизонтальное перемещение или устойчивость (например, удаленный доступ установлен как служба на нескольких машинах)	T1543 - Create or Modify System Process