Данный материал содержит информацию о событиях безопасности Windows с перечень ID событий (их основные поля с содержимым и назначением). События собраны по группам в зависимости от выявляемой активности, в рамках группы описаны типовые кейсы применения в рамках мониторинга и реагирования.

4688 Событие Создания процесса

Creator Subject \ Субъект-создатель:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию создания процесса. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, запустившей процесс
Account Domain \ Домен учетной записи	Домен учетной записи, запустившей процесс
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведен запуск.
Target Subject \ Целевой субъект:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи в рамках контекста которой был произведен запуск
Account Name \ Имя учетной записи	Имя учетной записи, запустившей процесс
Account Domain \ Домен учетной записи	Домен учетной записи, запустившей процесс
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведен запуск.
Process Information \ Информация о процессе:	
New Process ID \ ИД Нового процесса	Шестнадцатеричный ИД нового процесса. По данному значению можно определить цепочку процессов за счет смежного поля Creator Process ID \ ИД процесса-создателя
New Process Name \ Имя нового процесса	Полный путь и имя исполняемого файла
Creator Process ID \ ИД процесса-создателя	Шестнадцатеричный ИД процесса-создателя. По данному значению можно определить цепочку процессов за счет смежного поля New Process Name \ Имя нового процесса
Creator Process Name \ Имя процесса-создателя	Полный путь и имя исполняемого файла процесса-создателя
Process Command Line \ Командная строка процесса	Командная строка, с которой был выполнен процесс.

4689 Событие завершение процесса

Subject \ Субъект	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию завершения процесса. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, запустившей процесс
Account Domain \ Домен учетной записи	Домен учетной записи, запустившей процесс
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведено завершение процесса.
Process Information \ Информация о процессе:	
Process ID \ ИД процесса	Шестнадцатеричный ИД завершенного процесса. По данному значению можно определить цепочку процессов за счет смежного поля Creator Process ID \ ИД процесса-создателя в событиях 4689
Process Name \ Имя процесса	Полный путь и имя исполняемого файла

- Запуск процесса из нетипичной директории
- Запуск процесса от нетипичного родительского процесса или цепочки процессов
- Запуск процесса с подозрительной командной строкой
- Запуск процесса
  от непривилегированной учетной записи
- Остановка процессов в системе

4697 Событие создания службы в системе

Subject \ Субъект	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию создания службы. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, создавшей службу
Account Domain \ Домен учетной записи	Домен учетной записи, создавшей службу
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии было произведено создание.
Service Information \ Информация о сервисе:	
Service Name \ Имя службы	Имя созданной службы
Account File name \ Имя файла службы	Полный путь к исполняемому файлу службы и параметры запуска, если таковые имеются
Service Type \ Тип службы	Тип, указывающий в каком режиме запускается служба
Service Start Type \ Тип запуска службы	Тип запуска указывается в какой момент и как запускается служба
Service Account \ Учетная запись службы	Контекст, в рамках которого будет произведен запуск службы

4698 Событие Создания задачи в планировщике задач

Subject \ Субъект	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию создания задачи в. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, создавшей службу
Account Domain \ Домен учетной записи	Домен учетной записи, создавшей службу
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии было произведено создание.
Service Information \ Информация о сервисе:	
Task Name \ Имя Задачи	Имя задачи, позволяет определить задачу в планировщике.
Task Content \ Содержимое задачи	Полное содержание задачи в XML формате

4657 Событие изменения записи в реестре

Subject \ Субъект:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию создания службы. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, изменившей запись
Account Domain \ Домен учетной записи	Домен учетной записи, изменившей запись
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии было произведено изменение.
Process Information \ Информация о процессе:	
Process ID \ ИД процесса	Шестнадцатеричный ИД процесса, который произвел изменение. По данному значению можно определить

	цепочку процессов за счет смежного поля Creator Process ID \ ИД процесса-создателя в событиях 4688, 4689
Process Name \ Имя процесса	Полный путь и имя исполняемого файла
Object \ Объект:	
Object Name \ Имя объекта	Путь до фактического расположения записи реестра
Object value name \ Имя значения объекта	Имя значения ключа реестра
Operation type \ Тип операции	Действие, выполненное над записью в реестре
Change Information \ Информация:	
Old value type \ Тип старого значения	Тип значения до изменения(если применимо)
Old value \ Старое значение	Старое значение (если применимо)
New value type \ Тип нового значения	Тип значения после изменения
New value \ Новое значение	Новое значение

- Запуск процесса из нетипичной директории
- Запуск процесса от нетипичного родительского процесса или цепочки процессов
- Запуск процесса с подозрительной командной строкой
- Запуск процесса
  от непривилегированной учетной записи
- Остановка процессов в системе

4624 Событие успешного входа

Subject \ Субъект:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию входа. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, которая пытается произвести вход
Account Domain \ Домен учетной записи	Домен учетной записи, которая пытается произвести вход
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведен запуск.
Logon Information \ Сведения о входе:	
Logon type \ Тип входа	**2 Интерактивный вход** Пользователь непосредственно вошел на компьютер **3 Сетевой вход** Пользователь подключился по сети к компьютеру **4 Пакетный вход** Используется при выполнении задач **5 Служба** Событие при запуске службы от имени пользователя. **7 Разблокировка рабочей станции** **8 Networkcleartext** Сетевой вход. Пароль пользователя был передан в нехешированной форме. **9 Newcredential** Пользователь клонировал свой текущий маркер и указал новые учетные записи. **10 remoteinteractive** Удаленный вход с использованием terminal services или remote desktop. **11 Кэшированный вход** Вход с использованием сетевых учетных данных хранящихся локально.
Process Information \ Информация о процессе:	
Process ID \ ИД процесса	Шестнадцатеричный ИД процесса, который запросил вход. По данному значению можно определить цепочку процессов за счет смежного поля Creator Process ID \ ИД процесса-создателя в событиях 4688, 4689.
Process Name \ Имя процесса	Полный путь и имя исполняемого файла
New Logon \ Новый вход:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, под которой был осуществлен вход. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, под которой осуществлен вход
Account Domain \ Домен учетной записи	Домен учетной записи, под которой осуществлен вход
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведен вход.
Network Information \ Сведения о сети:	
Workstation Name\ Имя рабочей станции	Имя рабочей станции, данное поле содержит имя станции, заполненное на основе содержащейся информация в пакете аутентификации.

Source Network Address \ Сетевой адрес	IP-адрес, с которого происходит вход.
Detailed Auth Info\ Детальные сведения:	
Logon Process \ Процесс входа	Имя доверенного процесса, который использовался для входа в систему.
Authentication Package \ Пакет проверки подлинности	Имя пакета проверки подлинности, который использовался для процесса проверки подлинности при входе.

4625 Событие неуспешного входа

Subject \ Субъект:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию входа. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, которая пытается произвести вход
Account Domain \ Домен учетной записи	Домен учетной записи, которая пытается произвести вход
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведен запуск.
Logon Information \ Сведения о входе:	
Logon type \ Тип входа	Тип входа **2 Интерактивный вход** Пользователь непосредственно вошел на компьютер **3 Сетевой вход** Пользователь подключился по сети к компьютеру **4 Пакетный вход** Используется при выполнении задач **5 Служба** Событие при запуске службы от имени пользователя. **7 Разблокировка рабочей станции** **8 Networkcleartext** Сетевой вход. Пароль пользователя был передан в нехешированной форме. **9 Newcredential** Пользователь клонировал свой текущий маркер и указал новые учетные записи. **10 remoteinteractive** Удаленный вход с использованием terminal services или remote desktop. **11 Кэшированный вход** Вход с использованием сетевых учетных данных хранящихся локально.
Failure Information \ Сведения об ошибке:	
Failure Reason \ Причина ошибки	Текстовое описание значения поля Status
Status \ Статус	Поле, содержит код, который содержит статус ошибки. **0XC000005E** В настоящее время нет доступных серверов входа для обслуживания запроса на вход. **0xC0000064** Вход пользователя с ошибками или учетной записью пользователя **0xC000006A** Вход пользователя в систему с ошибкой или неверным паролем **0XC000006D** Это может быть вызвано неверным именем пользователя или сведениями о проверке подлинности **0XC000006E** Неизвестное имя пользователя или неверный пароль. **0xC000006F** Вход пользователя за пределами авторизованного времени **0xC0000070** Вход пользователя с неавторизованной рабочей станции **0xC0000071** Вход пользователя с истекшим паролем

	0xC0000072 Вход пользователя в учетную запись отключена администратором **0XC00000DC** Сервер SAM находится в неправильном состоянии, чтобы выполнить требуемую операцию. **0XC0000133** Часы между контроллером домена и другим компьютером не синхронизованы **0XC000015B** Пользователь не предоставил запрошенный тип входа (правый вход) на этом компьютере. **0XC000018C** Не удалось выполнить запрос на вход, так как не удалось установить отношение доверия между основным доменом и доверенным доменом. **0XC0000192** Попытка входа в систему, но служба Netlogon не запущена. **0xC0000193** Вход пользователя с просроченной учетной записью **0XC0000224** Пользователь должен сменить пароль при следующем входе в систему **0XC0000225** Очевидно, что это ошибка в Windows, а не риск **0xC0000234** Вход пользователя с заблокированной учетной записью **0XC00002EE** Причина ошибки: при входе в систему произошла ошибка **0XC0000413** Вход невозможен: компьютер, на который осуществляется вход, защищен брандмауэром проверки подлинности. Для указанной учетной записи не разрешена проверка подлинности на компьютере. **0x0** Состояние ОК.
Process Information \ Информация о процессе:	
Process ID \ ИД процесса	Шестнадцатеричный ИД процесса, который запросил вход. По данному значению можно определить цепочку процессов за счет смежного поля Creator Process ID \ ИД процесса-создателя в событиях 4688, 4689.
Process Name \ Имя процесса	Полный путь и имя исполняемого файла
New Logon \ Новый вход:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, под которой был осуществлен вход. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, под которой осуществлен вход
Account Domain \ Домен учетной записи	Домен учетной записи, под которой осуществлен вход
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведен вход.
Network Information \ Сведения о сети:	
Workstation Name\ Имя рабочей станции	Имя рабочей станции, данное поле содержит имя станции, заполненное на основе содержащейся информация в пакете аутентификации.
Source Network Address \ Сетевой адрес	IP-адрес, с которого происходит вход.
Detailed Auth Info\ Детальные сведения:	
Logon Process \ Процесс входа	Имя доверенного процесса, который использовался для входа в систему.
Authentication Package \ Пакет проверки подлинности	Имя пакета проверки подлинности, который использовался для процесса проверки подлинности при входе.

4648 вход с явным использованием учетных данных

Subject \ Субъект:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию входа. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, которая пытается произвести вход
Account Domain \ Домен учетной записи	Домен учетной записи, которая пытается произвести вход
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведен запуск.
Account Whose Credentials Were Used:	
Account Name \ Имя учетной записи	Имя учетной записи, под которой осуществлен вход
Account Domain \ Домен учетной записи	Домен учетной записи, под которой осуществлен вход
Account Whose Credentials Were Used:	
Account Name \ Имя учетной записи	
Account Domain \ Домен учетной записи	
Process Information \ Информация о процессе:	
Process ID \ ИД процесса	Шестнадцатеричный ИД процесса, который запросил вход. По данному значению можно определить цепочку процессов за счет смежного поля Creator Process ID \ ИД процесса-создателя в событиях 4688, 4689.
Process Name \ Имя процесса	Полный путь и имя исполняемого файла
Target Server \ Целевой сервер:	
Target Server Name \ Имя целевого узла	Имя узла, на котором был запущен новый процесс
Additional Information \ Доп сведения	Дополнительные сведения по целевому узлу
Network Information \ Сведения о сети:	
Workstation Name\ Имя рабочей станции	
Source Network Address \ Сетевой адрес	

Event id 4725 Событие Отключения Учетной записи
Event id 4723 Событие Изменения пароля учетной записи
Event id 4724 Событие Сброса пароля учетной записи
Event id 4728 \ Event id 4732 Событие добавления в группу
Event id 4720 \ Event id 4726 Событие создания \ удаления Пользователя
В данном ряде событий есть поля, который помогают определить кто выполнил действия
Ниже представлен пример полей для события добавления в группу.

Subject \ Субъект:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, запросившей операцию входа. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, которая произвела действие
Account Domain \ Домен учетной записи	Домен учетной записи, которая произвела действие
Logon ID \ ИД входа	ИД входа, уникальное значение, позволяющее определить в рамках какой сессии был произведен запуск.

Member \ Член:	
Security ID \ ИД Безопасности	Идентификатор безопасности (SID) учетной записи, над которой выполнили действие. Средством просмотра автоматически пытается разрешиться в учетные данные.
Account Name \ Имя учетной записи	Имя учетной записи, над которой выполнили действие
Account Domain \ Домен учетной записи	Домен учетной записи, над которой выполнили действие

- Вход пользователя из нетипичной локации
- Брутфорс учетной записи
- Нетиповой сценарий входа для пользователя
- Несанкционированное использование учетной записи другим пользователем
- Нетипичное использование сервисов\ресурсов пользователем
- Наделение пользователя правами
- Несанкционированная смена паролей пользователей
- Создание и удаление пользователей в рамках проведения активностей
- Использование отключенных учетных записей