Positive Technologies MaxPatrol SIEM

Пакет экспертизы № 10. Выявление атак, использующих тактику "Закрепление" (по классификации MITRE ATT&CK)

POSITIVE TECHNOLOGIES

Дата редакции документа: 01.10.2019

Содержание

1. Об этом документе

Это руководство содержит информацию об установке пакета экспертизы, инструкции по настройке источника для журналирования событий, необходимых для работы пакета, и инструкции по настройке PT MaxPatrol SIEM для сбора этих событий. В руководстве также дано описание событий ИБ, регистрируемых PT MaxPatrol SIEM по правилам корреляции, входящих в состав пакет.

Руководство не содержит инструкций по установке, первоначальной настройке, администрированию и использованию основных функций PT MaxPatrol SIEM.

Руководство адресовано специалистам, выполняющим установку и интеграцию PT MaxPatrol SIEM в организации, и специалистам, ответственным за обеспечение информационной безопасности, контроль и расследование инцидентов.

Комплект документации PT MaxPatrol SIEM включает в себя следующие документы:

- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта.
- Руководство администратора — содержит справочную информацию и инструкции по установке, настройке и администрированию продукта.
- Руководство оператора безопасности — содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности.
- Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с PT MaxPatrol SIEM для сбора событий с источников и аудита активов.
- Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с PT MaxPatrol SIEM.
- PDQL-запросы для анализа активов — содержит информацию о системных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в PT MaxPatrol SIEM.
- Руководство разработчика — содержит рекомендации по созданию формул нормализации, правил корреляции, агрегации и обогащения событий и описание утилит PT MaxPatrol SIEM SDK для их отладки.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о PT MaxPatrol SIEM (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **ОК**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT MaxPatrol SIEM

Вы можете найти дополнительную информацию о PT MaxPatrol SIEM на ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 6).

2. О пакете экспертизы

В состав пакета включены правила корреляции PT MaxPatrol SIEM для выявления атак, использующих тактику "Закрепление" (Persistence), на Windows-системы. Для выделения тактик атак используется классификация из матрицы базы знаний MITRE ATT&CK.

Тактика "Закрепление" применяется злоумышленниками для того, чтобы обеспечить постоянный беспрепятственный доступ в скомпрометированную систему. Целью применения этой тактики может быть, например, обеспечение работоспособности бэкдора после перезагрузки системы. Сложность обнаружения действий злоумышленника, использующего тактику "Закрепление", зависит от полученных им прав доступа в системе: чем выше уровень доступа, тем больше у злоумышленника возможностей для маскировки своей активности.

Пакет экспертизы совместим с PT MaxPatrol SIEM версий 19.1 и выше. Установка пакета выполняется автоматически при обновлении Knowledge Base согласно инструкциям Руководства по внедрению.

При первоначальной настройке пакета в Knowledge Base нужно:

- выбрать инциденты, которые будут регистрироваться правилами корреляции пакета; для регистрации инцидента в табличном списке Rules_Operation_Mode в строке с его названием в колонке **mode** ввести `1` (если инцидент не указан в списке или в строке введен `0`, инцидент регистрироваться не будет);

  Внимание! Включение регистрации одновременно всех инцидентов значительно увеличивает нагрузку на MP SIEM Server. После включения регистрации нескольких инцидентов необходимо на основании полученных из них данных заполнить табличный список MITRE_ATTCK_whitelist (см. раздел 5) и лишь затем включать регистрацию остальных инцидентов.

- в табличном списке AD_Domain_Controllers указать IP-адреса и полные доменные имена (FQDN) контроллеров домена сети Microsoft Active Directory;

- в табличном списке AD_Security_Administrators нужно указать логины привилегированных учетных записей, IP-адреса и полные доменные имена (FQDN) узлов, с которых выполняется администрирование.

  Примечание. Буквы в табличные списки нужно вводить только в нижнем регистре. Кроме того, если данные в колонках могут принимать любые значения, необходимо ввести звездочку (*) в колонки с типом данных String и ноль в колонки с типом данных Number.

После установки и первоначальной настройки пакета экспертизы объекты базы данных Knowledge Base нужно установить в PT MaxPatrol SIEM.

Примечание. Для предотвращения повторной регистрации инцидентов в состав пакета входит табличный список Incidents, который содержит список инцидентов, зарегистрированных правилами корреляции пакета за последние сутки. Заполнение списка выполняется правилом обогащения Incidents_muting.

Таблица 2. Инциденты, регистрируемые для тактики "Закрепление"

Техника атаки[1]	Инцидент
Accessibility Features	Detect_Windows_Accessibility_StickyKey_modification — обнаружено изменение параметров запуска утилиты для специальных возможностей в Windows в разделе реестра Image File Execution Options. В команде запуска утилиты злоумышленник может указать вредоносное ПО в качестве приложения для отладки
Component Object Model Hijacking	Detect_possible_COM_object_persistence — обнаружено изменение ссылки на объект Component Object Model (COM) в реестре Windows. В команде запуска утилиты злоумышленник может указать вредоносное ПО в качестве dll-библиотеки
Create account	Detect_Account_created_on_local_system — обнаружено создание локальной учетной записи. Возможна компрометация узла
Create account	Detect_Fast_create_and_delete_account — обнаружены создание учетной записи и последующее ее удаление в течение короткого промежутка времени. Возможна компрометация узла
Create account	Detect_Possible_Add_new_user_in_commandline — обнаружено создание учетной записи, выполненное с использованием командного интерпретатора cmd.exe или powershell.exe
Image File Execution Options Injection	Detect_GlobalFlags_in_Image_File_Execution_Options — обнаружены изменения реестра Windows: изменены параметры запуска утилиты в разделе Image File Execution Options (в команде запуска утилиты злоумышленник может указать вредоносное ПО в качестве приложения для отладки); изменены параметры ReportingMode и MonitorProcess в разделе SilentProcessExit (злоумышленник может получить информацию об автоматическом завершении процессов)
New Service System Service Discovery	Detect_Windows_services_operations — обнаружено действие, выполненное с использованием командного интерпретатора cmd.exe или powershell.exe и связанное со службой Windows (просмотр, запуск, создание или удаление службы)
New Service	Windows_Malicious_service_registration — обнаружена установка службы в папку, не являющуюся системной папкой Windows (в любую папку, кроме `C:\windows\system32`, `C:\ProgramData`, `C:\Program Files`)
New Service	Windows_Service_Installed_From_NonSystem_Location — обнаружена установка службы из папки, не являющейся системной папкой Windows

[1] Для выделения техник атаки используется классификация из матрицы базы знаний MITRE ATT&CK.

Техника атаки[1]	Инцидент
Office Application Startup	Detect_Office_Normal_dotm_modification — обнаружено изменение стандартного шаблона документа Microsoft Office. Злоумышленник может встроить в шаблон макрос на языке Visual Basic for Applications для выполнения вредоносного сценария при запуске приложения Microsoft Office
Office Application Startup	Detect_Office_XLL_modification — обнаружено изменение параметров запуска надстроек Microsoft Word или Microsoft Excel в реестре Windows. Злоумышленник может встроить в файл надстройки вредоносный сценарий, который будет выполнятся при запуске приложения Microsoft Office
Registry Run Keys	Detect_Windows_Autorun_modify — обнаружено изменение параметров автоматического запуска программ при входе пользователей в Windows. Злоумышленник может настроить автоматический запуск вредоносного ПО или ПО для удаленного доступа
Screensaver	Detect_Windows_Screensaver_modification — обнаружено изменение параметров запуска экранной заставки Windows. Злоумышленник может настроить выполнение вредоносного сценария при ее запуске
Web Shell	Detect_Possible_Windows_Web_shell_created — обнаружены признаки установки сценария "веб-шелл" на веб-сервер Windows. Веб-шелл может использоваться злоумышленником для несанкционированного доступа на атакуемый узел или в качестве шлюза для удаленного доступа в атакуемую сеть
Windows Management Instrumentation Event Subscription	Detect_WMI_Subscriptions_modification — обнаружено создание WMI-подписки на события. Злоумышленник может использовать средства WMI для настройки выполнения вредоносного сценария при регистрации события
Winlogon Helper DLL	Detect_Registry_Winlogon_Helper — обнаружено изменение разделов реестра Windows, связанных с утилитой winlogon.exe. Эта утилита используется для входа и выхода пользователей из операционной системы

3. Настройка источников

Настройку источников на активе нужно выполнять от имени учетной записи, добавленной в группу Administrators на контроллере домена, в котором расположен актив.

> Внимание! При использовании в IT-инфраструктуре организации межсетевого экрана или других средств для контроля сетевого трафика требуется настроить в них правила, разрешающие трафик в обоих направлениях между узлом источника и узлом MP Agent. Используются системный TCP-порт 135 и динамические TCP-порты 49152—65535.
>
> Внимание! При использовании на узле источника межсетевого экрана Windows в нем нужно включить правила для входящих подключений "Удаленное управление журналом событий (именованные каналы - входящий)" (Remote Event Log Management (NP-In)), "Удаленное управление журналом событий (RPC)" (Remote Event Log Management (RPC)), "Удаленное управление журналом событий (RPC-EPMAP)" (Remote Event Log Management (RPC-EPMAP)).

Источниками событий для правил корреляции пакета экспертизы на активе служат операционная система Windows и служба Microsoft Sysmon. События обоих источников сохраняются в журнале событий Windows.

На активе нужно установить службу Microsoft Sysmon или, если служба установлена, изменить параметры конфигурации службы.

Для настройки Windows на контроллере домена актива нужно:

1. Настроить аудит Windows PowerShell с помощью групповой политики.

   Регистрация событий аудита Windows PowerShell доступна в клиентской ОС Windows 7, серверной ОС Windows Server 2008 R2 и в более поздних версиях.

   Внимание! Для работы правил корреляции пакета экспертизы на источнике должна быть установлена оболочка командной строки Windows PowerShell версии 5 или выше.

2. Настроить аудит создания процессов из командной строки Windows с помощью групповой политики.
3. Настроить расширенную политику аудита (ААР) Windows с помощью групповой политики.
4. Создать и настроить доменную учетную запись для сбора событий MP Agent из журнала событий Windows согласно инструкциям в Руководстве по настройке источников.

   Примечание. Для сбора событий MP Agent вместо доменной учетной записи на всех серверах и рабочих станциях вы можете создать учетные записи локальных пользователей ОС с одинаковыми учетными данными. Каждую учетную запись нужно добавить в локальную политику безопасности "Доступ к компьютеру из сети" и в локальную группу пользователей "Читатели журнала событий". В PT MaxPatrol SIEM нужно добавить одну учетную запись с общими для всех записей учетными данными.

В этом разделе

3.1. Выбор источников события для правил корреляции

События, необходимые для работы правил корреляции пакета, регистрируются различными источниками. Для каждого правила на источнике нужно настроить журналирование определенных событий. Для некоторых правил журналирование необходимых событий можно настроить одновременно на нескольких источниках.

Источники событий для правил корреляции пакета указаны в таблице, а настройка журналирования событий, необходимых для работы правил, описана в соответствующих разделах далее.

Таблица 3. Источники событий для правил корреляции пакета

Правило корреляции	Настройка источника событий		
	Аудит Windows PowerShell	Расширен-ный аудит Windows	Служба Sysmon
Detect_Account_created_on_local_system	—	Да	—
Detect_Fast_create_and_delete_account	—	Да	—
Detect_GlobalFlags_in_Image_File_Execution_Options	—	—	Да
Detect_Office_Normal_dotm_modification	—	—	Да
Detect_Office_XLL_modification	—	—	Да
Detect_Possible_Add_new_user_in_commandline[2]	Да	Да	Да
Detect_possible_COM_object_persistence	—	—	Да
Detect_Possible_Windows_Web_shell_created	—	—	Да
Detect_Registry_Winlogon_Helper	—	—	Да
Detect_Windows_Accessibility_StickyKey_modification	—	—	Да
Detect_Windows_Autorun_modify	—	—	Да
Detect_Windows_Screensaver_modification	—	—	Да
Detect_Windows_services_operations[2]	Да	Да	Да

[2] Для правила нужно настроить хотя бы один из источников событий.

Правило корреляции	Настройка источника событий		
	Аудит Windows PowerShell	Расширенный аудит Windows	Служба Sysmon
Detect_WMI_Subscriptions_modification	—	—	Да
Windows_Malicious_service_registration[3]	—	—	—
Windows_Service_Installed_From_NonSystem_Location[3]	—	—	—

3.2. Настройка аудита PowerShell с помощью групповой политики

► Чтобы настроить аудит PowerShell с помощью групповой политики:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление групповой политикой**.

   Запустится консоль управления групповыми политиками.

   Примечание. Вы можете запустить консоль управления групповыми политиками выполнив команду `gpmc.msc`.
3. В левой части окна выберите узел используемой групповой политики **Управление групповой политики** → **Лес: <Имя леса>** → **Домены** → **<Имя домена>** → **<Имя групповой политики серверов или рабочих станций>**.
4. В главном меню выберите **Действие** → **Изменить**.

   Откроется окно **Редактор управления групповыми политиками**.
5. В левой части окна выберите узел **Политика <Имя политики>** → **Конфигурация компьютера** → **Политики** → **Административные шаблоны** → **Компоненты Windows** → **Windows Powershell**.
6. Выберите **Включить ведение журнала модулей**.
7. В главном меню выберите **Действие** → **Изменить**.
8. В открывшемся окне выберите вариант **Включено**.
9. В панели **Параметры** нажмите кнопку **Показать**.
10. В открывшемся окне в поле **Значение** введите *.
11. Нажмите кнопку **ОК**.
12. В окне **Включить ведение журнала модулей** нажмите кнопку **ОК**.
13. Выберите **Включить регистрацию блоков сценариев PowerShell**.

[3] Для правила не требуется настраивать источник событий. Необходимые события регистрируются Windows по умолчанию.

14. В главном меню выберите **Действие** → **Изменить**.
15. В открывшемся окне выберите вариант **Включено**.
16. Нажмите кнопку **ОК**.

Аудит PowerShell настроен.

3.3. Настройка аудита создания процессов из командной строки с помощью групповой политики

► Чтобы настроить аудит создания процессов из командной строки Windows с помощью групповой политики:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление групповой политикой**.

   Запустится консоль управления групповыми политиками.

   Примечание. Вы можете запустить консоль управления групповыми политиками выполнив команду `gpmc.msc`.
3. В левой части окна выберите узел используемой групповой политики **Управление групповой политики** → **Лес: <Имя леса>** → **Домены** → **<Имя домена>** → **<Имя групповой политики серверов или рабочих станций>**.
4. В главном меню выберите **Действие** → **Изменить**.

   Откроется окно **Редактор управления групповыми политиками**.
5. В левой части окна выберите узел **Политика <Имя политики>** → **Конфигурация компьютера** → **Политики** → **Административные шаблоны** → **Система** → **Аудит создания процессов**.
6. Выберите **Включать командную строку в события создания процессов**.

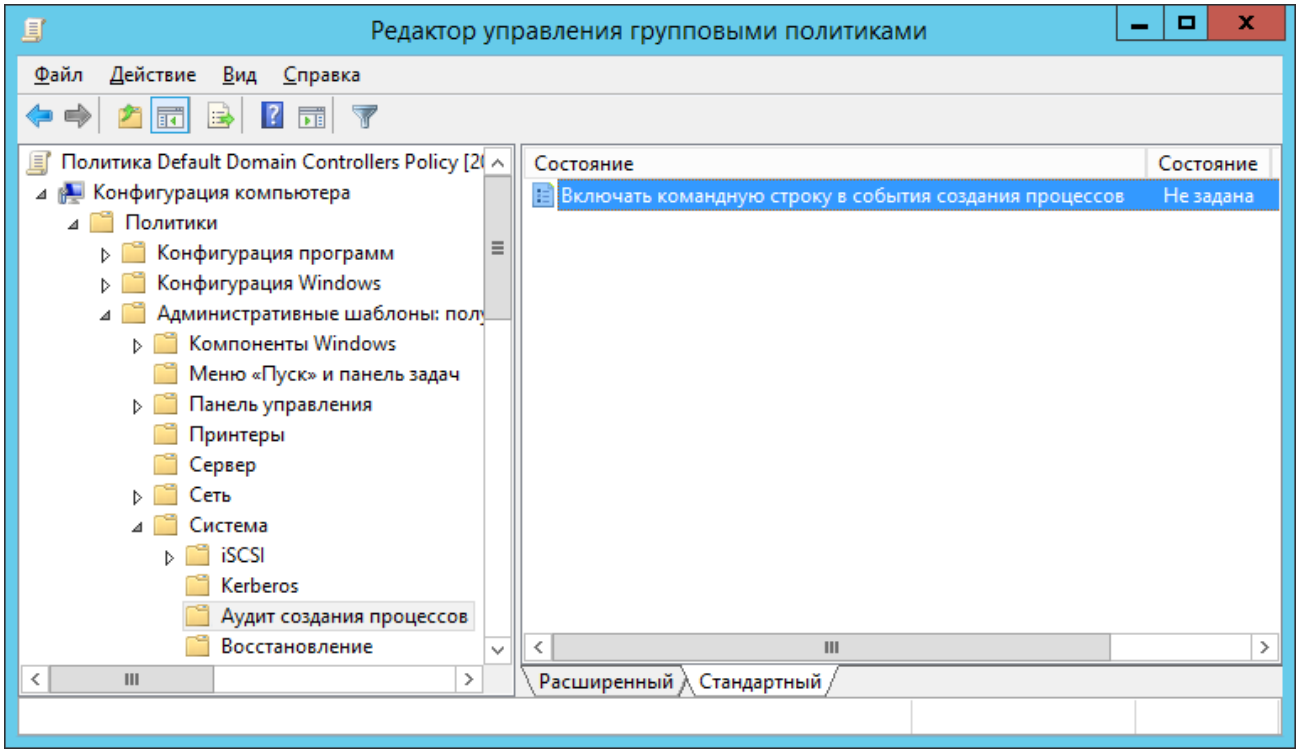

Рисунок 1. Выбор состояния "Включать командную строку в события создания процессов"

7. В главном меню выберите **Действие** → **Изменить**.
8. В открывшемся окне выберите вариант **Включено**.
9. Нажмите кнопку **ОК**.

Аудит создания процессов из командной строки Windows настроен.

3.4. Настройка расширенной политики аудита с помощью групповой политики

С помощью групповой политики на контроллере домена актива нужно настроить расширенную политику аудита в соответствии с таблицей.

Таблица 4. Настройка расширенной политики аудита

Категория	Подкатегория	Тип аудита
Подробное отслеживание	Аудит создания процессов[4]	Успех

[4] Включение аудита позволяет регистрировать событие 4688: A new process has been created (для регистрации события также нужно настроить групповую политику аудита создания процессов из командной строки). Событие необходимо для работы правил Detect_Possible_Add_new_user_in_commandline и Detect_Windows_services_operations.

Категория	Подкатегория	Тип аудита
Управление учетными записями	Аудит управления учетными записями пользователей[5]	Успех

- Чтобы настроить расширенную политику аудита с помощью групповой политики:

1. Откройте панель управления Windows.
2. Выберите **Администрирование** → **Управление групповой политикой**.

   Запустится консоль управления групповыми политиками.

   Примечание. Вы можете запустить консоль управления групповыми политиками выполнив команду `gpmc.msc`.
3. В левой части окна выберите узел используемой групповой политики **Управление групповой политики** → **Лес: <Имя леса>** → **Домены** → **<Имя домена>** → **<Имя групповой политики серверов или рабочих станций>**.
4. В главном меню выберите **Действие** → **Изменить**.

   Откроется окно **Редактор управления групповыми политиками**.
5. В левой части окна выберите узел **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Конфигурация расширенной политики аудита** → **Политики аудита** → **<Название категории>**.
6. Выберите подкатегорию политики аудита.

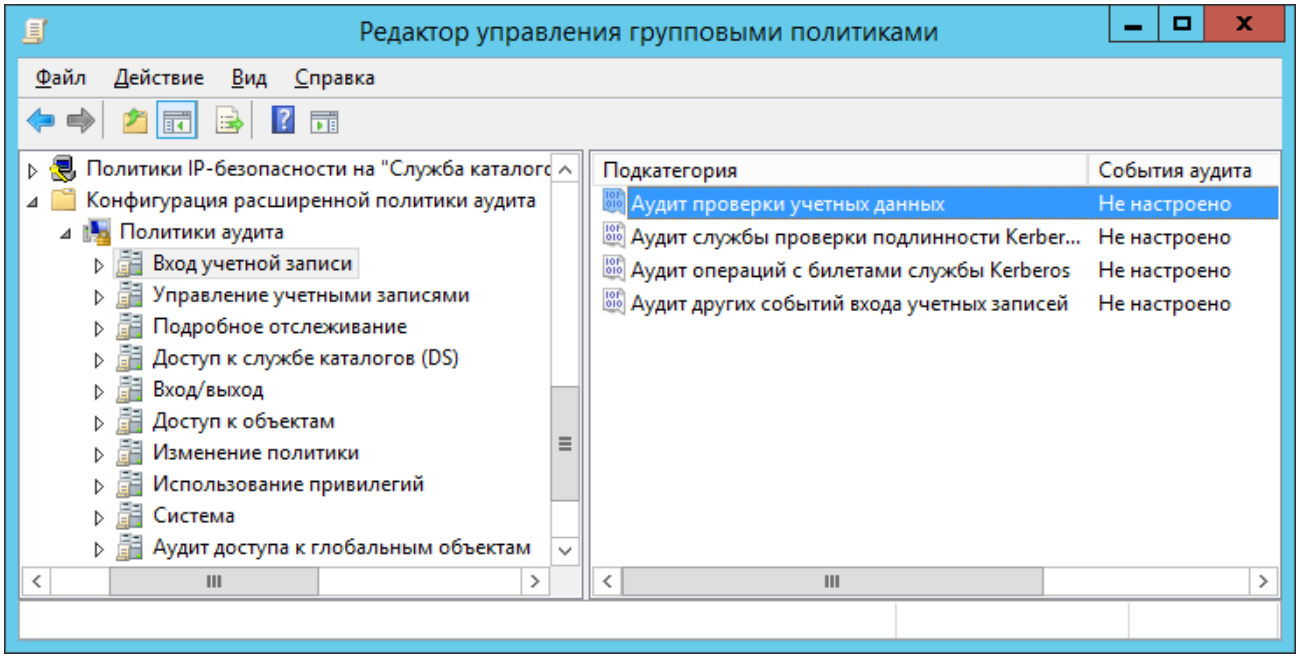

Рисунок 2. Выбор подкатегории политики аудита

[5] Включение аудита позволяет регистрировать события 4720: A user account was created, 4726 A user account was created, необходимые для работы правил Detect_Account_created_on_local_system и Detect_Fast_create_and_delete_account.

7. В главном меню выберите **Действие** → **Свойства**.
8. В открывшемся окне установите флажок **Настроить следующие события аудита**.
9. Если нужно включить аудит успехов, установите флажок **Успех**.
10. Если нужно включить аудит отказов, установите флажок **Отказ**.

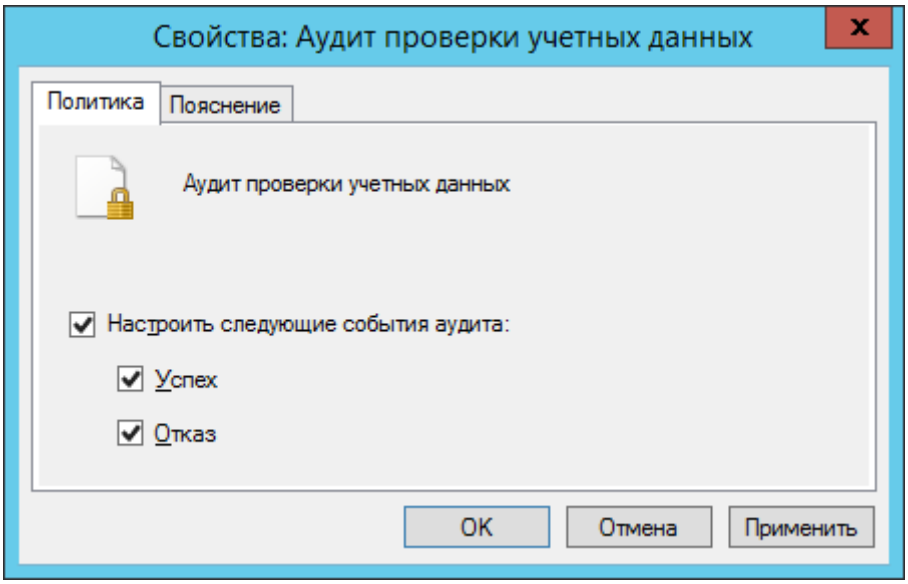

Рисунок 3. Настройка подкатегории политики аудита

11. Нажмите кнопку **ОК**.

Расширенная политика аудита настроена.

3.5. Настройка службы Microsoft Sysmon

Примечание. Эта инструкция разработана для службы Microsoft Sysmon версии 10.41.

На активе нужно установить службу Microsoft Sysmon или, если служба установлена, изменить параметры конфигурации службы.

Установка Microsoft Sysmon

Установочный файл службы Microsoft Sysmon вы можете скачать с сайта docs.microsoft.com.

- Чтобы установить службу Microsoft Sysmon:

1. Создайте конфигурационный файл (например, `SysmonConfig.xml`), вставьте в него параметры конфигурации, указанные ниже, и сохраните.
2. Откройте интерфейс командной строки Windows от имени администратора.

3. Запустите установочный файл:
   `sysmon.exe –i <Путь к конфигурационному файлу>`
4. В открывшемся окне нажмите кнопку **Agree**.

Служба установлена.

Изменение параметров конфигурации Microsoft Sysmon

- Чтобы изменить параметры конфигурации службу Microsoft Sysmon:

1. В конфигурационный файл службы Microsoft Sysmon в секцию `EventFiltering` добавьте фильтры событий, указанные в параметрах конфигурации ниже, и сохраните файл.
2. Откройте интерфейс командной строки Windows от имени администратора.
3. Запустите установочный файл:
   `sysmon.exe –c <Путь к конфигурационному файлу>`

Параметры конфигурации службы изменены.

Параметры конфигурационного файла

```
<Sysmon schemaversion="4.22">
  <HashAlgorithms>MD5</HashAlgorithms>
  <EventFiltering>
    <FileCreate onmatch="include">
      <!-- Для правила Detect_Office_XLL_modification -->
      <TargetFilename condition="end with">.wll</TargetFilename>
      <TargetFilename condition="end with">.xll</TargetFilename>
      <!-- Для правила Detect_Windows_Autorun_modify -->
      <TargetFilename condition="contains">\start menu\programs\startup\</
TargetFilename>
      <!-- Для правила Detect_Possible_Windows_Web_shell_created -->
      <!-- IIS -->
      <TargetFilename condition="contains">inetpub\wwwroot</TargetFilename>
      <TargetFilename condition="end with">.aspx</TargetFilename>
      <TargetFilename condition="end with">.asp</TargetFilename>
      <!-- Apache, Nginx -->
      <TargetFilename condition="end with">.php</TargetFilename>
      <TargetFilename condition="contains">\www\</TargetFilename>
      <TargetFilename condition="contains">\htdocs\</TargetFilename>
      <TargetFilename condition="contains">\html\</TargetFilename>
```

```
      <!-- Apache tomcat -->
      <TargetFilename condition="end with">.jsp</TargetFilename>
      <TargetFilename condition="end with">.jspx</TargetFilename>
      <TargetFilename condition="contains">\jsp\</TargetFilename>
      <!-- Для правила Detect_Office_Normal_dotm_modification -->
      <TargetFilename condition="contains">Normal.dotm</TargetFilename>
      <TargetFilename condition="contains">\appdata\roaming\microsoft\templates\</
TargetFilename>
    </FileCreate>
    <ProcessCreate onmatch="include">
      <!-- Для правила Detect_Possible_Add_new_user_in_commandline -->
      <Image condition="contains">\system32\net.exe</Image>
      <Image condition="contains">\system32\net1.exe</Image>
      <!-- Для правила Detect_Windows_services_operations -->
      <Image condition="contains">\system32\sc.exe</Image>
      <Image condition="contains">\wmic.exe</Image>
    </ProcessCreate>
    <RegistryEvent onmatch="include">
      <!-- Для правила Detect_GlobalFlags_in_Image_File_Execution_Options -->
      <TargetObject condition="contains">\Currentversion\Image File Execution Options
\</TargetObject>
      <TargetObject condition="contains">currentversion\silentprocessexit</
TargetObject>
      <!-- Для правила Detect_Office_XLL_modification -->
      <TargetObject condition="contains">\excel\options</TargetObject>
      <!-- Для правила Detect_Windows_Autorun_modify -->
      <TargetObject condition="contains">\CurrentVersion\Run</TargetObject>
      <TargetObject condition="contains">\Windows\Run</TargetObject>
      <!-- Для правила Detect_Windows_Screensaver_modification -->
      <TargetObject condition="contains">\Currentversion\Image File Execution Options
\</TargetObject>
      <TargetObject condition="contains">\control panel\desktop</TargetObject>
      <!-- Для правила Detect_Registry_Winlogon_Helper -->
      <TargetObject condition="contains">\currentversion\winlogon</TargetObject>
      <!-- Для правила Detect_Windows_Accessibility_StickyKey_modification -->
      <TargetObject condition="contains">\Currentversion\Image File Execution Options
\</TargetObject>
```

```
      <!-- Для правила Detect_possible_COM_object_persistence -->
      <TargetObject condition="contains"> classes\clsid\*\inprocserver32</
TargetObject>
    </RegistryEvent>
    <!-- Для правила Detect_WMI_Subscriptions_modification -->
    <WmiEvent onmatch="exclude">
    </WmiEvent>
  </EventFiltering>
</Sysmon>
```

4. Настройка PT MaxPatrol SIEM

Для сбора событий источников с актива в PT MaxPatrol SIEM нужно:

1. Добавить учетную запись ОС для доступа на актив.
2. На базе профиля WinEventLog создать профиль для сбора событий из журнала Windows.
3. Создать задачу на сбор событий из журнала Windows.
4. Создать задачу с профилем WinEventLogSysmon на сбор событий службы Microsoft Sysmon.
5. Запустить задачи на сбор событий.

В этом разделе

4.1. Добавление учетной записи

► Чтобы добавить в PT MaxPatrol SIEM учетную запись для доступа к источнику:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин-пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. В раскрывающемся списке **Транспорт** выберите **Windows logs**.
5. В поле **Логин** введите логин учетной записи.
6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.
7. Если для доступа к источнику используется доменная учетная запись, в поле **Домен** введите имя домена.
8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

4.2. Создание профиля для сбора событий

► Чтобы создать профиль для сбора событий:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.

   Откроется страница **Профили**.

2. В рабочей области выберите профиль **WinEventLog**.

3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **На базе выбранного профиля**.

   Откроется страница **Новый профиль**.

4. В поле **Название** введите название профиля.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

5. В блоке параметров транспорта в раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к источнику.

6. В блоке **Параметры** нажмите .

   Откроется страница **Настройка параметров профиля <Название профиля>**.

7. Выберите представление параметров в формате JSON.

8. Скопируйте текст с параметрами профиля из поля **Значения по умолчанию** в поле **Перекрытые значения**.

9. С помощью параметра `log_channels` укажите список каналов журнала и запросы:

```
"log_channels": [
    {
        "file": "System",
        "query": "*[System[(EventID=12 or (EventID &gt;= 19 and EventID &lt;= 23) or
EventID=104 or EventID=1074 or EventID=4826 or EventID=6009 or (EventID &gt;= 7000 and
EventID &lt;= 7045) )]]"
    },
    {
        "file": "Security",
        "query": "*"
    },
    {
        "file": "Microsoft-Windows-PowerShell/Operational",
        "query": "*[System[(EventID=4103 or EventID=4104)]]"
    }
]
```

10. Нажмите кнопку **Применить**.

11. Нажмите кнопку **Сохранить**.

Профиль для сбора событий создан.

4.3. Создание задачи на сбор событий

► Чтобы создать задачу на сбор событий с источника:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи**.

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите созданный ранее профиль для сбора событий.
5. В раскрывающемся списке **Агент** выберите MP Agent для сбора событий.
6. В блоке параметров **Цели** на вкладке **Включить в сканирование** в поле **Сетевые адреса** введите IP-адрес источника событий.

   Примечание. В блоке **Расписание** вы можете настроить регулярный автоматический запуск задачи.

7. Нажмите кнопку **Сохранить**.

Задача на сбор событий с источника создана.

4.4. Создание задачи на сбор событий службы Microsoft Sysmon

► Чтобы создать задачу на сбор событий с источника:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи**.

3. В поле **Название** введите название задачи.
4. В раскрывающемся списке **Профиль** выберите **WinEventLogSysmon**.

   Откроется блок параметров транспорта WindowsLogs.

5. В блоке параметров транспорта в раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к источнику.
6. В раскрывающемся списке **Агент** выберите MP Agent для сбора событий.

7. В блоке параметров **Цели** на вкладке **Включить в сканирование** в поле **Сетевые адреса** введите IP-адрес источника событий.

   Примечание. В блоке **Расписание** вы можете настроить регулярный автоматический запуск задачи.

8. Нажмите кнопку **Сохранить**.

Задача на сбор событий с источника создана.

5. Расследование инцидентов

В ходе расследования инцидента по значениям полей инцидента вы можете определить:

- `event_src.ip`, `event_src.fqdn` или `event_src.host` — IP-адрес и полное доменное имя (FQDN) узла, на который производилась атака;
- `src.ip`, `src.fqdn` или `src.host` — IP-адрес и полное доменное имя узла (FQDN), с которым связана подозрительная активность;
- `subject.id`, `subject.name`, `subject.domain` — идентификатор, имя и домен учетной записи, с которой связана подозрительная активность.

Примечание. Вы можете получить дополнительную информацию о действиях злоумышленника из анализа событий, связанных с его учетной записью и IP-адресом или полным доменным именем (FQDN) узла, с которого производилась атака.

Реагирование на инцидент

Если обнаруженная активность не является для учетной записи ожидаемой и легитимной, рекомендуется принять меры к блокировке учетной записи и (или) изоляции узла, с которого производилась атака.

При выявлении ложного срабатывания данные инцидента необходимо внести в табличный список MITRE_ATTCK_whitelist.

Примечание. Буквы в табличный список нужно вводить только в нижнем регистре. Кроме того, если данные в колонках могут принимать любые значения, необходимо ввести звездочку (*) в колонки с типом данных String и ноль в колонки с типом данных Number.

В колонках табличного списка нужно указать:

- **rule** — имя правила корреляции, по которому зарегистрирован инцидент (указано в поле инцидента `correlation_name`);
- **host** — имя узла, на котором зарегистрирован инцидент (указано в поле `event_src.host`);
- **user_id** — идентификатор учетной записи, с которой связана подозрительная активность (указан в поле `subject.id`);
- **specific_value** — дополнительную информацию о инциденте. Колонка заполняется данными из полей инцидентов, указанных в таблице ниже;

  Примечание. Значения, указываемые в колонках **user_name** и **user_domain**, являются информационными, фильтрация событий по ним не выполняется.
- **user_name** — имя учетной записи, с которой связана подозрительная активность (указано в поле `subject.name`);
- **user_domain** — домен учетной записи, с которой связана подозрительная активность (указано в поле `subject.domain`).

Таблица 5. Поля инцидентов для заполнения колонки specific_value табличного списка MITRE_ATTCK_whitelist

Инцидент	Поле инцидента[6]
Detect_Account_created_on_local_system	`object.domain`
Detect_Fast_create_and_delete_account	`object.name`
Detect_GlobalFlags_in_Image_File_Execution_Options	—
Detect_Office_Normal_dotm_modification	—
Detect_Office_XLL_modification	`object.name`
Detect_Possible_Add_new_user_in_commandline	`datafield5` или `object.value` или `object.path`
Detect_possible_COM_object_persistence	`object.value`
Detect_Possible_Windows_Web_shell_created	`object.path`
Detect_Registry_Winlogon_Helper	`object.value`
Detect_Windows_Accessibility_StickyKey_modification	`object.value`
Detect_Windows_Autorun_modify	`object.name`
Detect_Windows_Screensaver_modification	`object.value`
Detect_Windows_services_operations	`datafield5` или `object.value` или `object.path`
Detect_WMI_Subscriptions_modification	—
Windows_Malicious_system_like_process_started	`object.name`
Windows_Service_Installed_From_NonSystem_Location	`object.name`

[6] Если для инцидента не указано поле с данными для заполнения колонки specific_value, в колонку нужно ввести звездочку (*).

6. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Запросы на портале — основной способ обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

6.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Портал технической поддержки доступен на русском, английском, немецком и итальянском языках.

6.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по следующим телефонам:

- Великобритания +44 20 3769 3606
- Италия +39 06 9763 1532
- Казахстан +7 727 350 52 92
- Россия +7 495 744 01 44
- США +1 857 208 7273
- Чехия +420 530 510 700
- Южная Корея +82 2 6410 8582

Техническая поддержка по телефону предоставляется на русском и английском языке.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданному запросу.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте запрос на портале support.ptsecurity.com. Запрос на портале, созданный и обновляемый по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

6.3. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся запросам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

6.4. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

6.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

6.4.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

6.4.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 6).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 6. Время реакции на запрос и время его обработки

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта	До 24 часов	Не ограничено

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
	и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес		
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

6.4.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

- о диагностике проблемы и ее результатах;
- о поиске решения или возможности обойти причины возникновения проблемы;
- о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

- проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;
- проблема классифицирована как неподдерживаемая.

О компании

"Позитив Текнолоджиз" — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения "Позитив Текнолоджиз" для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты "Позитив Текнолоджиз" заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com