MaxPatrol SIEM

Пакет экспертизы. Атаки на Microsoft Active Directory
Версия пакета 3.4

Дата редакции документа: 17.07.2024

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 MaxPatrol SIEM для сбора этих событий. В руководстве также дано описание событий ИБ, регистрируемых MaxPatrol SIEM по правилам корреляции, входящим в состав пакета.

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

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

Комплект документации 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 — 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 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 MaxPatrol SIEM.
- PDQL-запросы для анализа активов — содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в MaxPatrol SIEM.
- Руководство разработчика — содержит рекомендации по созданию правил нормализации, обогащения, агрегации и корреляции событий, описание утилит MaxPatrol SIEM SDK для их отладки, а также информацию о доступных в MaxPatrol SIEM функциях сервиса REST API.

В этом разделе

Условные обозначения (см. раздел 1.1)

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

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	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 **OK**	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 MaxPatrol SIEM

Вы можете найти дополнительную информацию о MaxPatrol SIEM на портале технической поддержки.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки.

2. О пакете экспертизы

В состав пакета включены правила корреляции MaxPatrol SIEM для регистрации событий информационной безопасности, связанных с подозрительной активностью в сети службы каталогов Microsoft Active Directory. Выявленные события могут свидетельствовать о развитии атак на IT-инфраструктуру организации.

Подготовка пакета экспертизы к использованию состоит из следующих этапов:

1. Установка пакета экспертизы в MaxPatrol SIEM. Выполняется автоматически при обновлении PT KB по инструкциям Руководства по внедрению.
2. Добавление объектов (правил корреляции, правил нормализации и табличных списков) в набор для установки. Выполняется по инструкциям из раздела «Работа с наборами для установки» Руководства оператора.

   Внимание! Необходимо добавлять в набор установки не только правила корреляции, но и объекты, необходимые для этих правил. Список таких объектов для каждого правила приведен в приложении «Зависимости».
3. Установка набора в конвейеры обработки событий. Выполняется по инструкции из раздела «Установка объектов в конвейеры обработки событий» Руководства оператора.

Таблица 2. Регистрируемые события ИБ[1]

Событие ИБ	Тактика	Техника
Abuse_Kerberos_RC4 — обнаружена возможная эксплуатация уязвимости CVE-2022-33679 в Kerberos. Злоумышленник предпринял попытку восстановить сеансовый ключ одного из пользователей, чтобы получить аутентифицированный сеанс от его имени. Злоумышленник может получить учетные данные других пользователей и развить атаку	Credential Access	Steal or Forge Kerberos Tickets
Active_Directory_Snapshot — обнаружено создание снапшота структуры Active Directory с помощью AdExplorer.exe	Discovery	Permission Groups Discovery: Domain Groups
ActiveDirectory_Data_Collection — обнаружено выполнение LDAP-запроса для сбора информации о домене с помощью утилиты AD Explorer или SharpHound	Discovery	Domain Trust Discovery, Account Discovery: Domain Account, Permission Groups Discovery:

1 Тактики и техники атак приводятся по классификации MITRE ATT&CK.

Событие ИБ	Тактика	Техника
		Domain Groups, Remote System Discovery
ADCS_Certify_Coerce — обнаружен перехват хеша протокола сетевой аутентификации Microsoft Windows (NTLM) или билета TGT учетной записи сервера центра сертификации в результате принудительной аутентификации на удаленном узле. Злоумышленник может скомпрометировать сервер центра сертификации и развить атаку	Credential Access	Forced Authentication
ADCS_CRL_Abusing — обнаружена подозрительная активность на сервере центра сертификации с использованием списка отозванных сертификатов (CRL). Злоумышленник может вынудить сервер центра сертификации пройти аутентификацию на удаленном сервере или получить возможность удаленно запустить вредоносный код на сервере центра сертификации	Credential Access	Forced Authentication
ADCS_Recon — обнаружено выполнение LDAP-запроса на поиск серверов сертификации в сети	Discovery	Network Service Discovery
ADCSync_Attack — обнаружена попытка получения хешей NTLM учетных записей пользователей Active Directory с помощью службы сертификатов Active Directory (AD CS)	Lateral Movement	Use Alternate Authentication Material
AdminSDHolder_Modification_Attack — обнаружено добавление значения в свойства контейнера AdminSDHolder. Злоумышленник может закрепиться в системе или повысить свои привилегии	Persistence	Account Manipulation
Bulk_Certs_Allowed_to_One_User — обнаружена выдача большого количества сертификатов центра сертификации одному пользователю	Credential Access	Steal or Forge Authentication Certificates
CA_Cert_Export — обнаружен экспорт сертификата центра сертификации, который может быть использован для выпуска сертификата любого пользователя без знания пароля	Credential Access	Steal or Forge Authentication Certificates

Событие ИБ	Тактика	Техника
Cert_Allowed_Alt_SAN — обнаружен запрос сертификата, который позволяет задать альтернативный SubjectAccountName	Lateral Movement	Use Alternate Authentication Material
Cert_Request_and_Approved_with_Alt_SAN — обнаружен запрос сертификата с альтернативным именем для учетной записи	Credential Access	Steal or Forge Authentication Certificates
Computer_Delegation_Configured — обнаружено изменение параметров делегирования в домене	Persistence	Modify Authentication Process: Domain Controller Authentication
Copy_Mimikatz_To_Share — обнаружено копирование утилиты Mimikatz в общую папку на удаленном узле. Злоумышленник может удаленно использовать эту утилиту	Lateral Movement	Lateral Tool Transfer
DACL_Resolver_Aced — обнаружена выгрузка списка избирательного управления доступом (DACL) для объектов Active Directory с помощью утилиты Aced	Discovery	Permission Groups Discovery: Domain Groups
DC_Auth_with_Pfx — обнаружен запрос билета TGT с помощью сертификата или смарт-карты	Lateral Movement	Use Alternate Authentication Material
DCShadow_Attack — обнаружена возможная атака DCShadow, которая позволяет создать поддельный контроллер домена Active Directory для внесения вредоносных изменений и закрепления в инфраструктуре, избегая обнаружения	Defense Evasion	Rogue Domain Controller
DCSync_Attack — обнаружена атака DCSync. Злоумышленник может получить учетные данные пользователей домена	Credential Access	DCsync
DCSync_Privileges_Given — обнаружена выдача привилегий, которые необходимы для проведения атаки DCSync. Злоумышленник может получить учетные данные пользователей домена	Credential Access	DCsync
DNS_Zone_Transfer_To_Untrusted_Host — обнаружен TCP-запрос AXFR от DNS-сервера, не указанного в табличном списке	Discovery	Domain Trust Discovery

Событие ИБ	Тактика	Техника
Trusted_DNS_servers. Злоумышленник может узнать больше о структуре атакуемой сети при помощи дампа зоны DNS		
Enable_SAN_Flag_CA_Policy — обнаружена установка флага EDITF_ATTRIBUTESUBJECTALTNAME2, который позволяет задавать альтернативный SubjectAccountName для всех выпущенных сертификатов	Persistence	Modify Authentication Process: Domain Controller Authentication
Failed_Network_Access_with_Unknown_User — обнаружена неудачная попытка входа от имени отключенной или несуществующей учетной записи	Credential Access	Brute Force
gMSA_Password_Access — злоумышленник получил доступ к атрибутам LDAP, где хранятся данные, позволяющие генерировать пароли для групповых учетных записей служб (gMSA)	Credential Access	Credentials from Password Stores
Golden_Cert — обнаружен запрос билетов TGT по скомпрометированному ранее сертификату центра сертификации. Злоумышленник может использовать полученные билеты, чтобы восстановить хеш-суммы паролей пользователей	Credential Access	Steal or Forge Authentication Certificates
GPO_Created_Or_Modified — обнаружено создание или изменение объекта групповой политики	Privilege Escalation	Domain or Tenant Policy Modification: Group Policy Modification
Groups_And_Users_Enumeration — обнаружена выгрузка списка доменных (локальных) пользователей или групп пользователей. Злоумышленник получил список пользователей и (или) групп пользователей в домене	Discovery	Account Discovery
Kerberoasting — обнаружен запрос билетов TGS с определенными типами шифрования	Credential Access	Steal or Forge Kerberos Tickets: Kerberoasting
Kerberos_Silver_Ticket — обнаружена атака Silver Ticket. Злоумышленник выпустил поддельный билет TGS для учетной записи, чтобы получить доступ на один из узлов	Credential Access	Steal or Forge Kerberos Tickets: Silver Ticket

Событие ИБ	Тактика	Техника
KrbRelay_Usage — обнаружены признаки одного из вариантов использования утилит KrbRelay или DavRelayUp. Злоумышленник из-за отсутствия подписи LDAP-запроса может использовать ретрансляцию процесса аутентификации для повышения привилегий до локального администратора, чтобы выполнить вредоносный код на скомпрометированном узле	Privilege Escalation	Exploitation for Privilege Escalation
Machine_Account_Quota_Access — обнаружено получение доступа к атрибуту MS-DS-Machine-Account-Quota, где хранятся данные о количестве машинных учетных записей, которые непривилегированный пользователь может создать в домене	Discovery	Account Discovery: Domain Account
Machine_Account_Quota_Changes — обнаружено изменение атрибута MS-DS-Machine-Account-Quota, где хранятся данные о количестве машинных учетных записей, которые непривилегированный пользователь может создать в домене	Persistence	Account Manipulation
Potential_domain_groups_and_users_enumeration_handle — обнаружена попытка выгрузки с контроллера домена списка пользователей или списка групп пользователей (запрос дескриптора объекта SAM_DOMAIN). Злоумышленник может получить список пользователей и (или) групп пользователей в домене	Discovery	Account Discovery
Potential_localgroups_and_administrators_enumeration_handle — обнаружена попытка выгрузки списка пользователей группы локальных администраторов или списка групп пользователей. Злоумышленник может получить список пользователей и (или) групп пользователей в домене	Discovery	Account Discovery
Potential_session_enumeration_process — обнаружен запуск утилиты для выгрузки списка активных пользовательских сеансов. Злоумышленник может получить учетные данные привилегированных пользователей	Discovery	Account Discovery

Событие ИБ	Тактика	Техника
Potential_Users_Or_Groups_Enumeration_Process — обнаружена попытка выгрузки с контроллера домена списка пользователей или групп пользователей с использованием процесса net.exe (net1.exe). Злоумышленник может получить список пользователей и (или) групп пользователей в домене	Discovery	Account Discovery
PowerViewPy_RBCD_Attack — обнаружено, что в домене настроено ограниченное делегирование на основе ресурсов	Persistence	Account Manipulation
Remote_Actions_With_Domain_Objects — обнаружено использование скриптов из инструмента PowerView	Persistence	Account Manipulation
Replication_to_unauthorized_DRA — обнаружена репликация Active Directory с источником, не указанным в табличном списке Directory_Replication_Agent. Создав поддельный контроллер домена, злоумышленник может изменить объекты в Active Directory	Discovery	Account Discovery
Session_enumeration_smb — обнаружена выгрузка списка активных пользовательских сеансов. Злоумышленник может получить учетные данные привилегированных пользователей	Discovery	Account Discovery
SAM_Account_Name_Spoofing — обнаружено одно из событий: — смена логина учетной записи (объекта в Active Directory) на логин, не содержащий символа $ в конце; — запрос TGT от имени учетной записи, логин которой совпадает с именем контроллера домена, но не содержит $ в конце	Privilege Escalation	sAMAccountName Spoofing
ShadowCred_Used — обнаружен один из признаков использования техники Shadow Credentials: — изменение атрибута msds-keycredentiallink объекта службы каталога; — использование механизма аутентификации без пароля для получения билета TGT системной учетной записи	Privilege Escalation, Defense Evasion	Exploitation for Privilege Escalation, Abuse Elevation Control Mechanism: Bypass User Account Control

Событие ИБ	Тактика	Техника
SIDHistory_Modification_Attack — обнаружено, что учетной записи добавлен атрибут SIDHistory. Злоумышленник может повысить свои привилегии в домене	Privilege Escalation	SID-History Injection
Subrule_PowerView_Objects_Actions — обнаружено удаленное изменение доменных объектов (доменных пользователей и групп, машинных учетных записей) с помощью инструмента PowerView (PowerViewPy)	Persistence	Account Manipulation
Subrule_Tickets_Requested — обнаружен запрос сеансовых билетов для получения доступа к службам	Credential Access	Steal or Forge Kerberos Tickets: Kerberoasting
TGS_request_by_non_existent_user — обнаружена попытка получения билета TGS для несуществующего пользователя	Credential Access	Steal or Forge Kerberos Tickets
Untrusted_Terminal_Server_Activity — обнаружен подозрительный запрос от недоверенного терминального сервера	Discovery	System Information Discovery
Zerologon_Attack — обнаружена возможная эксплуатация уязвимости CVE-2020-1472 в Active Directory, которая позволяет сменить пароль к учетной записи контроллера домена	Privilege Escalation	Exploitation for Privilege Escalation

3. Настройка источников

Источниками событий для правил корреляции пакета экспертизы могут служить серверы, рабочие станции и контроллеры домена в сети службы каталогов Microsoft Active Directory для Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016. Также источником событий может служить служба Microsoft Sysmon. События источников сохраняются в журнале событий Windows.

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

> **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 10 Collector. 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)).

Для получения событий службы Microsoft Sysmon ее нужно установить на рабочих станциях, серверах и контроллерах домена. Если служба установлена, необходимо изменить параметры конфигурации службы.

Для настройки других источников событий на контроллере домена нужно:

1. Настроить журналирование LDAP-запросов в реестре Windows.
2. Для серверов и рабочих станций — настроить аудит создания процессов из командной строки Windows с помощью групповой политики.
3. Для контроллеров домена, серверов и рабочих станций — настроить расширенную политику аудита (AAP) Windows с помощью групповой политики.
4. Создать и настроить доменную учетную запись для сбора событий MP 10 Collector из журнала событий Windows согласно инструкциям в Руководстве по настройке источников.

   > **Примечание.** Для сбора событий MP 10 Collector вместо доменной учетной записи на всех контроллерах домена, 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 MaxPatrol SIEM нужно добавить одну учетную запись с общими для всех записей учетными данными.

В этом разделе

Настройка расширенной политики аудита с помощью групповой политики (см. раздел 3.3)

Настройка службы Microsoft Sysmon (см. раздел 3.4)

3.1. Выбор источников событий

Для регистрации события ИБ по правилам корреляции пакета необходимо настроить журналирование определенных событий на источниках, указанных в таблице ниже.

Внимание! Для каждого события ИБ нужно настроить все доступные источники.

Для аудита Windows в таблице указаны идентификаторы событий системы безопасности Windows (например, 4688 — событие «A new process has been created»), для Sysmon — идентификаторы типов событий, указанные в конфигурационном файле Sysmon (например, 1 — события «Process Creation»). Настройка журналирования событий описана в соответствующих разделах далее.

Таблица 3. Источники и идентификаторы событий, необходимых для регистрации событий ИБ

Событие ИБ	**Источник события**	
	Расширенный аудит Windows	**Служба Sysmon**
Abuse_Kerberos_RC4	4768, 4769, 4771	—
Active_Directory_Snapshot [2]	1644	—
ActiveDirectory_Data_Collection [2]	1644	—
ADCS_CRL_Abusing	4871, 4872	11
ADCS_Certify_Coerce	4624, 5156, 5140	3
ADCS_Recon [2]	1644	—
ADCSync_Attack	4887, 4888, 4898	—
AdminSDHolder_Modification_Attack	5136	—
Bulk_Certs_Allowed_to_One_User	4887	—
CA_Cert_Export	4688, 5059, 5145	—
Cert_Allowed_Alt_SAN	4887, 4888, 4898	—
Cert_Request_and_Approved_with_Alt_SAN	4886, 4887	—
Computer_Delegation_Configured	5136	—
Copy_Mimikatz_To_Share	5145	—

2 Необходимо настроить журналирование LDAP-запросов (см. раздел 3.2). Для каждого запроса регистрируется событие с идентификатором 1644.

Событие ИБ	Источник события	
	Расширенный аудит Windows	Служба Sysmon
DACL_Resolver_Aced [2]	1644	—
DC_Auth_with_Pfx	4768	—
DCShadow_Attack	4624, 4742	—
DCSync_Attack	4624, 4662	—
DCSync_Privileges_Given	5136	—
DNS_Zone_Transfer_To_Untrusted_Host	6001, 6525	—
Enable_SAN_Flag_CA_Policy	—	13
Failed_Network_Access_with_Unknown_User	4625	—
gMSA_Password_Access	4662	—
GPO_Created_Or_Modified	5136, 5137	—
Golden_Cert	4688, 4768, 5059, 5145	—
Groups_And_Users_Enumeration	4624, 4661	—
Kerberoasting [2]	1644, 4769	—
Kerberos_Silver_Ticket	4624	—
KrbRelay_Usage	4624, 5156	3
Machine_Account_Quota_Access [2]	1644, 4662	—
Machine_Account_Quota_Changes [2]	1644, 5136	—
Potential_domain_groups_and_users_enumeration_handle	4624, 4661	—
Potential_localgroups_and_administrators_enumeration_handle	4624, 4661	—
Potential_session_enumeration_process	4688	1
Potential_Users_Or_Groups_Enumeration_Process	4688	1
PowerViewPy_RBCD_Attack [2]	1644, 5136	—
Remote_Actions_With_Domain_Objects [2]	1644, 4720, 4724, 4726, 4728, 4729, 4732, 4733, 4738, 4741, 4742, 4743, 5136	—
Replication_to_unauthorized_DRA	4928, 4929	—

Событие ИБ	Источник события	
	Расширенный аудит Windows	Служба Sysmon
SAM_Account_Name_Spoofing	4742, 4768	—
Session_enumeration_smb	4624, 5145	—
ShadowCred_Used [2]	1644, 4768, 5136	—
SIDHistory_Modification_Attack	4738, 5136	—
Subrule_PowerView_Objects_Actions [2]	1644	—
Subrule_Tickets_Requested	4769	—
TGS_request_by_non_existent_user	4769	—
Untrusted_Terminal_Server_Activity	5145	—
Zerologon_Attack	4742, 5723, 5805, 5823	—

3.2. Настройка журналирования LDAP-запросов

Для регистрации событий безопасности Windows с идентификатором 1644 с помощью редактора реестра нужно настроить журналирование LDAP-запросов.

► Чтобы настроить журналирование LDAP-запросов:

1. Выберите **Пуск** → **Выполнить**.
2. В поле **Открыть** введите `regedit` и нажмите кнопку **ОК**.

   Откроется окно **Редактор реестра**.
3. В левой части окна выберите узел `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics`.
4. Выберите параметр **15 Field Engineering**.

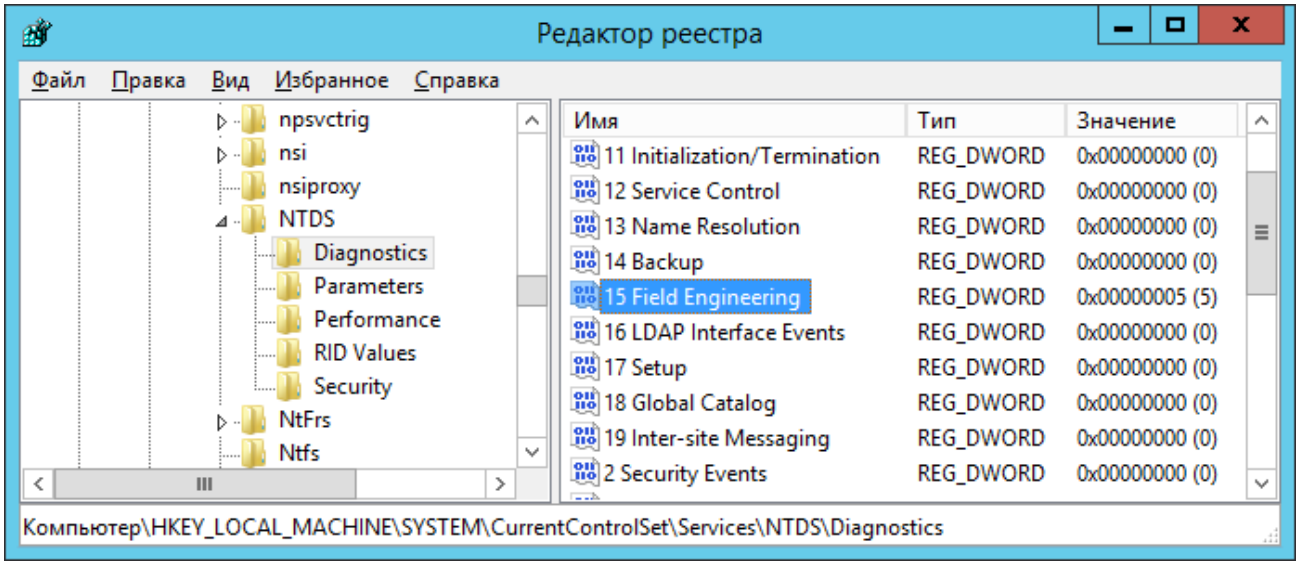

Рисунок 1. Выбор параметра 15 Field Engineering

5. В главном меню в разделе **Правка** выберите пункт **Изменить**.
6. В блоке параметров **Система исчисления** выберите вариант **Десятичная**.
7. В поле **Значение** введите `5` и нажмите кнопку **ОК**.

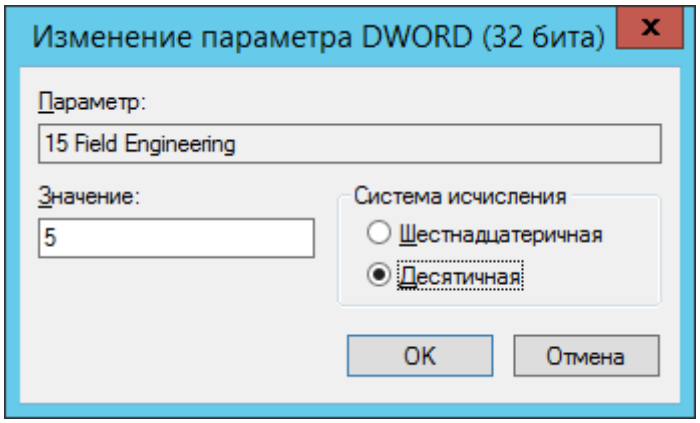

Рисунок 2. Настройка параметра 15 Field Engineering

8. В левой части окна выберите узел `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters`.
9. В главном меню выберите **Правка** → **Создать** → **Параметр DWORD**.
10. Введите имя созданного параметра `Expensive Search Results Threshold`.
11. В главном меню в разделе **Правка** выберите пункт **Изменить**.
12. В блоке параметров **Система исчисления** выберите вариант **Десятичная**.
13. В поле **Значение** введите `1` и нажмите кнопку **ОК**.

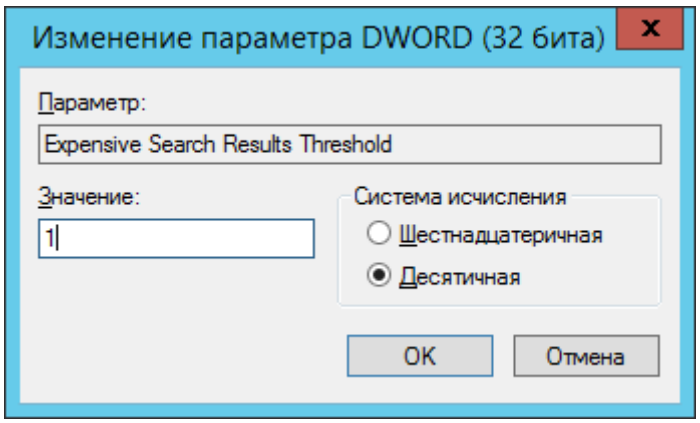

Рисунок 3. Настройка параметра Expensive Search Results Threshold

14. В главном меню выберите **Правка** → **Создать** → **Параметр DWORD**.
15. Введите имя созданного параметра `Inefficient Search Results Threshold`.
16. В главном меню в разделе **Правка** выберите пункт **Изменить**.
17. В блоке параметров **Система исчисления** выберите вариант **Десятичная**.
18. В поле **Значение** введите `1` и нажмите кнопку **ОК**.

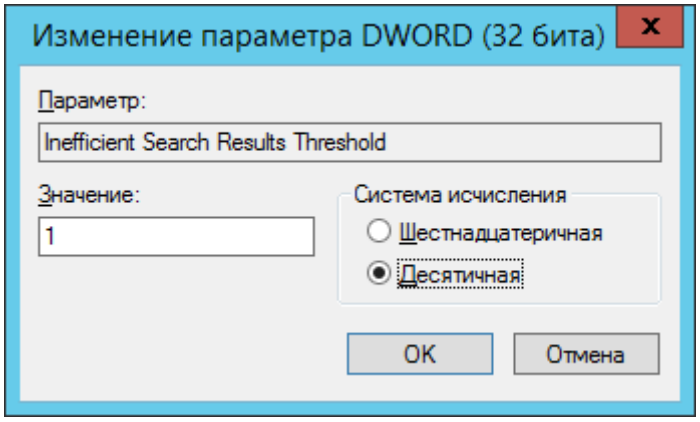

Рисунок 4. Настройка параметра Inefficient Search Results Threshold

Журналирование LDAP-запросов настроено.

3.3. 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

Идентификатор события	Категория	Подкатегория	Тип аудита
4624	Вход/выход	Аудит входа в систему	Успех
4625	Вход/выход	Аудит входа в систему	Отказ
4661	Доступ к объектам; Служба каталогов	Аудит объектов ядра, Аудит диспетчера учетных записей безопасности; Аудит доступа к службе каталогов	Успех
4662	Служба каталогов	Аудит доступа к службе каталогов	Успех
4688[3]	Подробное отслеживание	Аудит создания процессов	Успех
4720, 4724, 4726	Управление учетными записями	Аудит управления учетными записями пользователей	Успех
4728, 4729, 4732, 4733	Управление учетными записями	Аудит управления группами безопасности	Успех
4738	Управление учетными записями	Аудит управления учетными записями пользователей	Успех
4741, 4743	Управление учетными записями	Аудит управления учетными записями компьютеров	Успех
4742	Управление учетными записями	Аудит управления учетными записями компьютеров	Успех
4768	Вход учетной записи	Аудит службы проверки подлинности Kerberos	Успех, Отказ
4769	Вход учетной записи	Аудит операций с билетами службы Kerberos	Успех, Отказ
4771	Вход учетной записи	Аудит службы проверки подлинности Kerberos	Отказ
4871, 4872, 4886, 4887	Доступ к объектам	Аудит служб сертификации	Успех
4888	Доступ к объектам	Аудит служб сертификации	Отказ

3 Для регистрации события необходимо также с помощью групповой политики настроить включение командной строки в события создания процессов.

Идентификатор события	Категория	Подкатегория	Тип аудита
4898	Доступ к объектам	Аудит служб сертификации	Успех
4928	Служба каталогов	Аудит репликации службы каталогов	Успех
4929	Служба каталогов	Аудит подробной репликации службы каталогов	Успех
5059	Система	Аудит других системных событий	Успех
5136, 5137	Служба каталогов	Аудит изменения службы каталогов	Успех
5140	Доступ к объектам	Аудит общего файлового ресурса	Успех
5145	Доступ к объектам	Аудит сведений об общем файловом ресурсе	Успех, Отказ
5156	Доступ к объектам	Аудит подключения платформы фильтрации	Успех
5723, 5805	Вход учетной записи	Аудит других событий входа и выхода	Отказ
5823	Управление учетными записями	Аудит управления учетными записями компьютеров	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 политики **Управление групповой политикой** → **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.

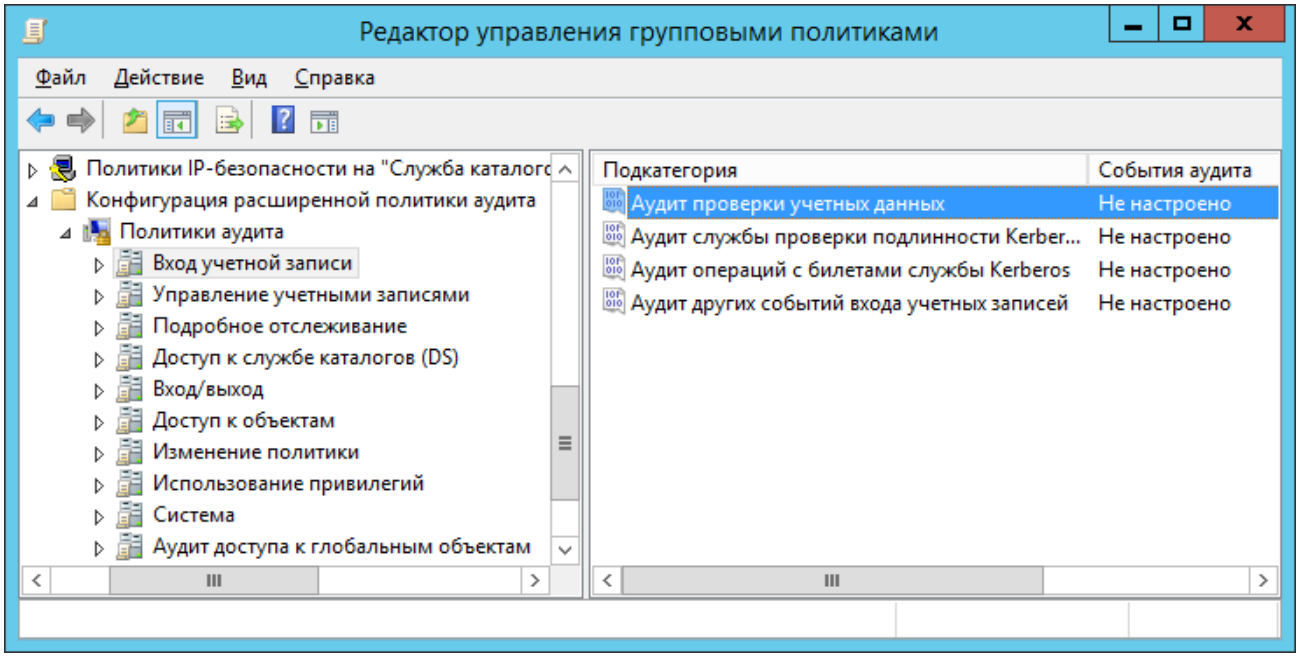

Рисунок 5. Выбор подкатегории политики аудита

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

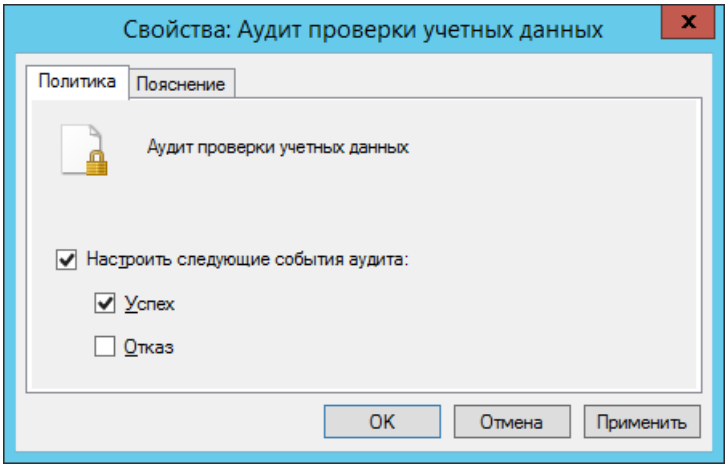

Рисунок 6. Настройка подкатегории политики аудита

11. Нажмите кнопку **OK**.

Расширенная политика аудита настроена.

3.4. Настройка службы Microsoft Sysmon

На активе необходимо установить службу Microsoft Sysmon или, если служба установлена, изменить ее конфигурацию. Конфигурационные файлы службы доступны на странице с описанием пакета в Knowledge Base. Вы также можете скачать конфигурационные файлы:

— для контроллеров домена — с сайта storage.ptsecurity.com;

— для рабочих станций — с сайта storage.ptsecurity.com;

— для серверов — с сайта storage.ptsecurity.com.

Примечание. Файлы конфигурации актуальны для Microsoft Sysmon версии 13.34 (со схемой конфигурации 4.81) или выше.

Установка Microsoft Sysmon

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

► Чтобы установить службу Microsoft Sysmon:

1. Откройте интерфейс командной строки Windows от имени администратора.
2. Запустите установочный файл:
   ```
   sysmon.exe -i <Путь к конфигурационному файлу>
   ```
3. В открывшемся окне нажмите кнопку **Agree**.

Служба установлена.

Изменение конфигурации Microsoft Sysmon

► Чтобы изменить конфигурацию службы Microsoft Sysmon:

1. В конфигурационный файл службы Microsoft Sysmon в секцию `EventFiltering` добавьте фильтры событий, указанные в скачанном конфигурационном файле.
2. Откройте интерфейс командной строки Windows от имени администратора.
3. Запустите установочный файл:
   ```
   sysmon.exe -c <Путь к конфигурационному файлу>
   ```

Конфигурация службы изменена.

4. Настройка MaxPatrol SIEM

Для сбора событий источников с актива в MaxPatrol SIEM нужно:

1. Добавить учетную запись ОС для доступа на актив.
2. Создать и запустить задачу с профилем WinEventLogMSAD на сбор событий из журнала Windows.
3. Создать и запустить задачу с профилем WinEventLogSysmon на сбор событий службы Microsoft Sysmon.

В этом разделе

Добавление учетной записи ОС (см. раздел 4.1)

Создание и запуск задачи на сбор событий (см. раздел 4.2)

Создание и запуск задачи на сбор событий службы Microsoft Sysmon (см. раздел 4.3)

4.1. Добавление учетной записи ОС

- Чтобы добавить в 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.
  4. В раскрывающемся списке **Метки** установите флажок **WindowsLogs**.
  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 и запуск задачи на сбор событий

- Чтобы создать и запустить 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 на сбор данных**.

  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **WinEventLogMSAD**.
  5. В раскрывающемся списке **Учетная запись** выберите учетную запись для доступа к источнику.
  6. Если требуется, в раскрывающемся списке **Агент** выберите MP 10 Collector для сбора событий.
  7. В панели **Цели сбора данных** на вкладке **Включить** в поле **Сетевые адреса** введите IP-адрес источника событий.

     Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи.

  8. Нажмите кнопку **Сохранить и запустить**.

  Задача на сбор событий с источника создана и запущена.

4.3. Создание и запуск задачи на сбор событий службы Microsoft Sysmon

- Чтобы создать и запустить 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 на сбор данных**.

  3. В поле **Название** введите название задачи.
  4. В раскрывающемся списке **Профиль** выберите **WinEventLogSysmon**.
  5. В раскрывающемся списке **Учетная запись** выберите учетную запись пользователя ОС.

6. Если требуется, в раскрывающемся списке **Агент** выберите MP 10 Collector для сбора событий.
7. В панели **Цели сбора данных** на вкладке **Включить** в поле **Сетевые адреса** введите IP-адрес источника событий.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи.
8. Нажмите кнопку **Сохранить и запустить**.

Задача на сбор событий с источника создана и запущена.

5. Расследование инцидента

В расследовании инцидента помогает анализ связанного с ним события ИБ. По значениям полей события вы можете определить:

— `dst.ip`, `dst.fqdn` или `dst.host` — IP-адрес и полное доменное имя (FQDN) узла, на который направлена атака (`dst.port` — порт подключения);

— `event_src.ip`, `event_src.fqdn` или `event_src.host` — IP-адрес и полное доменное имя (FQDN) узла, на котором зарегистрирован инцидент;

— `src.ip`, `src.fqdn` или `src.host` — IP-адрес и полное доменное имя (FQDN) узла, с которым связана подозрительная активность;

— `subject.account.id`, `subject.account.name`, `subject.account.domain` — идентификатор, логин 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 узлом, на котором была обнаружена подозрительная активность.

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 необходимо настроить механизм обработки ложных срабатываний. Для этого данные связанного с инцидентом события ИБ необходимо внести в табличный список для исключений.

Вы можете использовать белые списки Common_whitelist_value, Common_whitelist_regex и черные списки Common_blacklist_value, Common_blacklist_regex. Табличные списки с постфиксом value вы можете заполнять по ссылке из сводки о событии ИБ в интерфейсе MaxPatrol SIEM или вручную, табличные списки с постфиксом regex — только вручную. Исключения, указанные в черных списках, обладают более высоким приоритетом по сравнению с исключениями в белых списках.

При ручном заполнении табличных списков в колонках нужно указать:

— **rule** — имя правила корреляции, по которому зарегистрировано событие (указано в поле события `correlation_name`).

Примечание. Буквы во все колонки табличного списка, кроме колонки **rule**, 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.

— **host** — имя узла, на котором зарегистрировано событие (указано в поле `event_src.host`).

— **user_id** — идентификатор учетной записи, с которой связана подозрительная активность (указан в поле `subject.account.id`).

— **specific_value** — дополнительную информацию о событии (указана в поле `alert.key`).

— **specific_regex** — регулярное выражения (PCRE) для дополнительной информации о событии (составляется на основе данных, указанных в поле `alert.key`).

— **user_name** — логин учетной записи, с которой связана подозрительная активность (указано в поле `subject.account.name`).

Примечание. Значения в колонках **user_name** и **user_domain** вводятся только для сведения, фильтрация событий по ним не выполняется.

— **user_domain** — домен учетной записи, с которой связана подозрительная активность (указан в поле `subject.account.domain`).

— **comments** — любой текстовый комментарий.

— **exclude** — если требуется отключить регистрацию инцидентов и событий ИБ, в черных списках необходимо указать `yes`.

Примечание. Исключения, для которых в колонке **exclude** указано `yes`, обладают высоким приоритетом. Вы можете использовать это для указания частных случаев исключений, которые не должны попадать под более общие исключения в черных списках.

6. Техническая поддержка

Базовая техническая поддержка продуктов вида Standard включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продуктов

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продуктов в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках технической поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продуктов.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта обеспечены все аппаратные и программные требования, описанные в документации.

Устранение ошибок и дефектов в работе продуктов в рамках выпуска обновленных версий продукта

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к порталу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической поддержки необходимо оставить заявку на портале технической поддержки и предоставить специалисту технической поддержки следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и наборы диагностических данных, которые требуются для анализа;

— снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг технической поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по технической поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет

за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 5. Время реакции на заявку

Уровень значимости заявки	Критерии значимости заявки	Время реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист технической поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— о планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

— предоставлено решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, не подпадающими под гарантийные обязательства по продукту Positive Technologies;

— заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Приложение. Зависимости

В набор для установки нужно добавлять как сами правила корреляции, так и объекты базы данных PT KB, которые необходимы для работы этих правил. Перечень таких объектов для каждого правила указан ниже.

> **Примечание.** Вы можете выбрать из пакета экспертизы те правила корреляции, которые хотите использовать, и добавить в набор для установки только их и те объекты базы данных PT KB, которые необходимы для работы этих правил.

Abuse_Kerberos_RC4

Правила нормализации:

- PT-NF-1904: PT_Microsoft_Windows_eventlog_4768_A_Kerberos_authentication_ticket_was_requested;
- PT-NF-1907: PT_Microsoft_Windows_eventlog_4771_Kerberos_pre_authentication_failed;
- PT-NF-2611: PT_Microsoft_Windows_wmi_4771_Kerberos_pre_authentication_failed.

Active_Directory_Snapshot

Правило нормализации: PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

ActiveDirectory_Data_Collection

Правило нормализации: PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

ADCS_Certify_Coerce

Правила нормализации:

- PT-NF-1820: PT_Microsoft_Windows_eventlog_4624_An_account_was_successfully_logged_on;
- PT-NF-1968: PT_Microsoft_Windows_eventlog_5140_A_network_share_object_was_accessed;
- PT-NF-1976: PT_Microsoft_Windows_eventlog_5156_WFP_has_permitted_connection;
- PT-NF-2367: PT_Microsoft_Windows_eventlog_Sysmon_3_Network_connection.

Табличные списки:

- PT-TL-285: List_Servers;
- PT-TL-415: AssetGrid_Servers.

ADCS_CRL_Abusing

Правила нормализации:

— PT-NF-1527: PT_Microsoft_Certification_Authority_eventlog_4871_Admin_resend_certificate_stoplist;

— PT-NF-1528: PT_Microsoft_Certification_Authority_eventlog_4872_Publish_certificate_revocation_list;

— PT-NF-2364: PT_Microsoft_Windows_eventlog_Sysmon_11_File_create.

Табличные списки:

— PT-TL-204: Script_Extensions;

— PT-TL-477: CRL_Publication_Time.

ADCS_Recon

Правило нормализации: PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

AdminSDHolder_Modification_Attack

Правило нормализации: PT-NF-1964: PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified.

ADCSync_Attack

Правила корреляции:

— PT-CR-2101: Bulk_Certs_Allowed_to_One_User;

— PT-CR-830: Cert_Allowed_Alt_SAN.

Bulk_Certs_Allowed_to_One_User

Правило нормализации: PT-NF-1540: PT_Microsoft_Certification_Authority_eventlog_4887_Certificate_Services_approved_certificate_request.

CA_Cert_Export

Правила нормализации:

— PT-NF-1841: PT_Microsoft_Windows_eventlog_4688_A_new_process_has_been_created;

— PT-NF-1962: PT_Microsoft_Windows_eventlog_5059_Key_migration_operation;

— PT-NF-2657: PT_Microsoft_Windows_wmi_5059_Key_migration_operation.

Cert_Allowed_Alt_SAN

Правила нормализации:

— PT-NF-1540: PT_Microsoft_Certification_Authority_eventlog_4887_Certificate_Services_approved_certificate_request;

— PT-NF-1541: PT_Microsoft_Certification_Authority_eventlog_4888_Certificate_Services_denied_certificate_request;

— PT-NF-1549: PT_Microsoft_Certification_Authority_eventlog_4898_Certificate_Services_loaded_template.

Cert_Request_and_Approved_with_Alt_SAN

Правила нормализации:

— PT-NF-1539: PT_Microsoft_Certification_Authority_eventlog_4886_Certificate_Services_received_certificate_request;

— PT-NF-1540: PT_Microsoft_Certification_Authority_eventlog_4887_Certificate_Services_approved_certificate_request.

Computer_Delegation_Configured

Правило нормализации: PT-NF-1964: PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified.

Copy_Mimikatz_To_Share

Правило нормализации: PT-NF-1973: PT_Microsoft_Windows_eventlog_5145_A_network_share_object_was_checked.

DACL_Resolver_Aced

Правило нормализации: PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

Табличный список: PT-TL-122: Significant_Windows_groups.

DC_Auth_with_Pfx

Правило нормализации: PT-NF-1904: PT_Microsoft_Windows_eventlog_4768_A_Kerberos_authentication_ticket_was_requested.

DCShadow_Attack

Правило нормализации: PT-NF-1880:
PT_Microsoft_Windows_eventlog_4742_A_computer_account_was_changed.

Табличные списки:

— PT-TL-285: List_Servers;

— PT-TL-415: AssetGrid_Servers.

DCSync_Attack

Правило нормализации: PT-NF-1833:
PT_Microsoft_Windows_eventlog_4662_An_operation_was_performed_on_an_object.

Табличные списки:

— PT-TL-285: List_Servers;

— PT-TL-415: AssetGrid_Servers.

DCSync_Privileges_Given

Правило нормализации: PT-NF-1964:
PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified.

DNS_Zone_Transfer_To_Untrusted_Host

Правила нормализации:

— PT-NF-2282:
PT_Microsoft_Windows_eventlog_6001_dns_server_successfully_completed_transfer_of_zone_version;

— PT-NF-2287:
PT_Microsoft_Windows_eventlog_6525_zone_transfer_request_for_secondary_zone_was_refused_by_master;

— PT-NF-2853:
PT_Microsoft_Windows_wmi_6001_dns_server_successfully_completed_transfer_of_zone_version;

— PT-NF-2858:
PT_Microsoft_Windows_wmi_6525_zone_transfer_request_for_secondary_zone_was_refused_by_master;

— PT-NF-3139: PT_Opensource_NSD_syslog_zone_stored;

— PT-NF-5149: PT_Opensource_BIND_syslog_zone_transfer_master_start.

Табличный список: PT-TL-22: Trusted_DNS_servers.

Enable_SAN_Flag_CA_Policy

Правило нормализации: PT-NF-2365:
PT_Microsoft_Windows_eventlog_Sysmon_13_Registry_value_changed.

Failed_Network_Access_with_Unknown_User

Правило нормализации: PT-NF-1821:
PT_Microsoft_Windows_eventlog_4625_An_account_failed_to_log_on.

gMSA_Password_Access

Правило нормализации: PT-NF-1833:
PT_Microsoft_Windows_eventlog_4662_An_operation_was_performed_on_an_object.

Правило корреляции: PT-CR-2295: Subrule_gMSA_LDAP_Query.

GPO_Created_Or_Modified

Правила нормализации:

- PT-NF-1964: PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified;
- PT-NF-1965: PT_Microsoft_Windows_eventlog_5137_A_directory_service_object_was_created.

Golden_Cert

Правило нормализации: PT-NF-1904:
PT_Microsoft_Windows_eventlog_4768_A_Kerberos_authentication_ticket_was_requested.

Правило корреляции: PT-CR-1215: CA_Cert_Export.

Groups_And_Users_Enumeration

Правила корреляции:

- PT-CR-79: Potential_domain_groups_and_users_enumeration_handle;
- PT-CR-81: Potential_Users_Or_Groups_Enumeration_Process;
- PT-CR-82: Potential_localgroups_and_administrators_enumeration_handle.

Kerberoasting

Правило нормализации: PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

Правило корреляции: PT-CR-878: Subrule_Tickets_Requested.

Kerberos_Silver_Ticket

Правила нормализации:

— PT-NF-1820: PT_Microsoft_Windows_eventlog_4624_An_account_was_successfully_logged_on;

— PT-NF-2527: PT_Microsoft_Windows_wmi_4624_An_account_was_successfully_logged_on.

Табличный список: PT-TL-208: Known_Windows_Accounts.

KrbRelay_Usage

Правило нормализации: PT-NF-1820:
PT_Microsoft_Windows_eventlog_4624_An_account_was_successfully_logged_on.

Правило корреляции: PT-CR-859: Subrule_IMarshal_Interface.

Табличные списки:

— PT-TL-285: List_Servers;

— PT-TL-415: AssetGrid_Servers.

Machine_Account_Quota_Access

Правила нормализации:

— PT-NF-1833:
PT_Microsoft_Windows_eventlog_4662_An_operation_was_performed_on_an_object;

— PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

Machine_Account_Quota_Changes

Правила нормализации:

— PT-NF-1964: PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified;

— PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

Potential_domain_groups_and_users_enumeration_handle

Правила нормализации:

— PT-NF-1820: PT_Microsoft_Windows_eventlog_4624_An_account_was_successfully_logged_on;

— PT-NF-1832: PT_Microsoft_Windows_eventlog_4661_The_handle_to_an_object_was_requested;

— PT-NF-2463: PT_Microsoft_Windows_wmi_528_A_user_successfully_logged_on_to_a_computer;

— PT-NF-2475: PT_Microsoft_Windows_wmi_540_Logon_success;

— PT-NF-2527: PT_Microsoft_Windows_wmi_4624_An_account_was_successfully_logged_on;

— PT-NF-2537: PT_Microsoft_Windows_wmi_4661_The_handle_to_an_object_was_requested.

Potential_localgroups_and_administrators_enumeration_handle

Правила нормализации:

- PT-NF-1820: PT_Microsoft_Windows_eventlog_4624_An_account_was_successfully_logged_on;
- PT-NF-2463: PT_Microsoft_Windows_wmi_528_A_user_successfully_logged_on_to_a_computer;
- PT-NF-2475: PT_Microsoft_Windows_wmi_540_Logon_success;
- PT-NF-2527: PT_Microsoft_Windows_wmi_4624_An_account_was_successfully_logged_on.

Potential_session_enumeration_process

Правило нормализации: PT-NF-1841: PT_Microsoft_Windows_eventlog_4688_A_new_process_has_been_created.

Табличный список: PT-TL-24: Potential_session_enumeration_process_Names.

Potential_Users_Or_Groups_Enumeration_Process

Правило нормализации: PT-NF-1841: PT_Microsoft_Windows_eventlog_4688_A_new_process_has_been_created.

PowerViewPy_RBCD_Attack

Правила нормализации:

- PT-NF-1964: PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified;
- PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

Remote_Actions_With_Domain_Objects

Правила нормализации:

- PT-NF-1860: PT_Microsoft_Windows_eventlog_4720_A_user_account_was_created;
- PT-NF-1863: PT_Microsoft_Windows_eventlog_4724_An_attempt_was_made_to_reset_an_account_s_password;
- PT-NF-1865: PT_Microsoft_Windows_eventlog_4726_A_user_account_was_deleted;
- PT-NF-1867: PT_Microsoft_Windows_eventlog_4728_A_member_was_added_to_a_security_enabled_global_group;
- PT-NF-1868: PT_Microsoft_Windows_eventlog_4729_A_member_was_removed_from_a_security_enabled_global_group;

- PT-NF-1871: PT_Microsoft_Windows_eventlog_4732_A_member_was_added_to_a_security_enabled_local_group;
- PT-NF-1872: PT_Microsoft_Windows_eventlog_4733_A_member_was_removed_from_a_security_enabled_local_group;
- PT-NF-1876: PT_Microsoft_Windows_eventlog_4738_A_user_account_was_changed;
- PT-NF-1879: PT_Microsoft_Windows_eventlog_4741_A_computer_account_was_created;
- PT-NF-1880: PT_Microsoft_Windows_eventlog_4742_A_computer_account_was_changed;
- PT-NF-1881: PT_Microsoft_Windows_eventlog_4743_A_computer_account_was_deleted;
- PT-NF-1964: PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified;
- PT-NF-2564: PT_Microsoft_Windows_wmi_4720_A_user_account_was_created;
- PT-NF-2567: PT_Microsoft_Windows_wmi_4724_An_attempt_was_made_to_reset_an_account_s_password;
- PT-NF-2569: PT_Microsoft_Windows_wmi_4726_A_user_account_was_deleted;
- PT-NF-2571: PT_Microsoft_Windows_wmi_4728_A_member_was_added_to_a_security_enabled_global_group;
- PT-NF-2572: PT_Microsoft_Windows_wmi_4729_A_member_was_removed_from_a_security_enabled_global_group;
- PT-NF-2575: PT_Microsoft_Windows_wmi_4732_A_member_was_added_to_a_security_enabled_local_group;
- PT-NF-2576: PT_Microsoft_Windows_wmi_4733_A_member_was_removed_from_a_security_enabled_local_group;
- PT-NF-2580: PT_Microsoft_Windows_wmi_4738_A_user_account_was_changed;
- PT-NF-2583: PT_Microsoft_Windows_wmi_4741_A_computer_account_was_created;
- PT-NF-2584: PT_Microsoft_Windows_wmi_4742_A_computer_account_was_changed;
- PT-NF-2585: PT_Microsoft_Windows_wmi_4743_A_computer_account_was_deleted;
- PT-NF-2659: PT_Microsoft_Windows_wmi_5136_A_directory_service_object_was_modified.

Правило корреляции: PT-CR-1342: Subrule_PowerView_Objects_Actions.

Replication_to_unauthorized_DRA

Правила нормализации:

— PT-NF-1944: PT_Microsoft_Windows_eventlog_4928_Active_Directory_replica_source_naming_context_established;

— PT-NF-1945: PT_Microsoft_Windows_eventlog_4929_Active_Directory_replica_source_naming_context_removed;

— PT-NF-2639: PT_Microsoft_Windows_wmi_4928_Active_Directory_replica_source_naming_context_established;

— PT-NF-2640: PT_Microsoft_Windows_wmi_4929_Active_Directory_replica_source_naming_context_removed.

Табличный список: PT-TL-26: Directory_Replication_Agent.

Session_enumeration_smb

Правила нормализации:

— PT-NF-1820: PT_Microsoft_Windows_eventlog_4624_An_account_was_successfully_logged_on;

— PT-NF-1973: PT_Microsoft_Windows_eventlog_5145_A_network_share_object_was_checked;

— PT-NF-2463: PT_Microsoft_Windows_wmi_528_A_user_successfully_logged_on_to_a_computer;

— PT-NF-2475: PT_Microsoft_Windows_wmi_540_Logon_success;

— PT-NF-2527: PT_Microsoft_Windows_wmi_4624_An_account_was_successfully_logged_on.

Правило корреляции: PT-CR-84: Potential_session_enumeration_process.

Табличный список: PT-TL-23: Session_enumeration_smb_IPC_White_list_SID.

SAM_Account_Name_Spoofing

Правила нормализации:

— PT-NF-1880: PT_Microsoft_Windows_eventlog_4742_A_computer_account_was_changed;

— PT-NF-1904: PT_Microsoft_Windows_eventlog_4768_A_Kerberos_authentication_ticket_was_requested.

Табличные списки:

— PT-TL-285: List_Servers;

— PT-TL-415: AssetGrid_Servers.

ShadowCred_Used

Правила нормализации:

— PT-NF-1904: PT_Microsoft_Windows_eventlog_4768_A_Kerberos_authentication_ticket_was_requested;

— PT-NF-1964: PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified.

SIDHistory_Modification_Attack

Правила нормализации:

— PT-NF-1876: PT_Microsoft_Windows_eventlog_4738_A_user_account_was_changed;

— PT-NF-1964: PT_Microsoft_Windows_eventlog_5136_A_directory_service_object_was_modified.

Subrule_PowerView_Objects_Actions

Правило нормализации: PT-NF-2110: PT_Microsoft_Windows_eventlog_1644_ldap_query.

Subrule_Tickets_Requested

Правило нормализации: PT-NF-1905: PT_Microsoft_Windows_eventlog_4769_Kerberos_service_ticket_requested.

TGS_request_by_non_existent_user

Правило нормализации: PT-NF-1905: PT_Microsoft_Windows_eventlog_4769_Kerberos_service_ticket_requested.

Untrusted_Terminal_Server_Activity

Правило нормализации: PT-NF-1973: PT_Microsoft_Windows_eventlog_5145_A_network_share_object_was_checked.

Табличные списки:

— PT-TL-285: List_Servers;

— PT-TL-415: AssetGrid_Servers.

Zerologon_Attack

Правила нормализации:

— PT-NF-10262: PT_Microsoft_Windows_eventlog_5823_dc_change_password;

— PT-NF-10548: PT_Microsoft_Windows_eventlog_5723_session_setup_from_computer_failed;

— PT-NF-10549: PT_Microsoft_Windows_eventlog_5805_account_failed_authenticate;
— PT-NF-1880: PT_Microsoft_Windows_eventlog_4742_A_computer_account_was_changed.