HARDENING GUIDE · СМ «ПУЛЬТ»

Руководство по безопасной настройке системы мониторинга ИТ-инфраструктуры Пульт

ООО «Лаборатория Числитель» · версия продукта **2.3.0**

Документ для администраторов установки и сопровождения

Обзор

Настоящее руководство описывает меры безопасной настройки системы мониторинга ИТ-инфраструктуры Пульт (далее — СМ «ПУЛЬТ») версии 2.3.0. Документ предназначен для администраторов, которые устанавливают и сопровождают продукт в контуре организации.

Имена параметров конфигурации приведены в том виде, в котором они используются в поставке, например DenyKey, EnableGlobalScripts и TLSConnect. Имена файлов конфигурации в конкретной установке могут отличаться, в том числе иметь вид zabbix_*.conf или pult_*.conf, поэтому администратор ориентируется на фактические пути в развёрнутой среде.

Руководство охватывает настройки агента, агента 2, сервера, прокси, веб-интерфейса, ролей доступа, шифрования каналов связи, скриптов, макросов и аудита.

1. Состав мер безопасной настройки

Меры настоящего руководства уменьшают поверхность атаки и снижают последствия возможной компрометации. Они не являются обязательным условием работоспособности мониторинга, однако их применение повышает защищённость установки.

Меры с уровнем профиля L1 администратор применяет в первую очередь как базовый набор. Меры уровня L2 усиливают защиту в более требовательных контурах. Для каждой меры в последующих разделах приведены описание, обоснование, порядок настройки и проверка. Отступления от рекомендаций администратор оформляет исключением с указанием обоснования, ответственного лица, срока действия и компенсирующих мер.

В таблице ниже перечислены проверки, которые рассматриваются в настоящем руководстве. По таблице администратор оценивает состав и критичность мер, выбирает нужный раздел и переходит к расшифровке меры. После расшифровки мер приведён раздел о типовых инцидентах информационной безопасности и способах их обнаружения в СМ «ПУЛЬТ». В конце документа — сводный перечень для отметки выполнения.

Группа	Компонент	№	Мера	Критичность	Назначение
Ограничение исполнения кода на агентах	Агент и Агент 2	2.1	Запрет произвольного выполнения ключа system.run[*] на агентах	Критическая	Администратор обеспечивает запрет произвольного выполнения ключа system.run[*] на всех агентах.
Ограничение исполнения кода на агентах	Агент и Агент 2	2.2	Ограничение удалённых команд конкретными ключами и командами	Критическая	Если удалённые команды необходимы, администратор разрешает только конкретный ключ и конкретную команду.

Группа	Компонент	№	Мера	Критичность	Назначение
Ограничение исполнения кода на агентах	Агент и Агент 2	2.3	Соблюдение порядка правил AllowKey и DenyKey	Высокая	Соблюдать порядок AllowKey/DenyKey и исключить перекрывающие шаблоны.
Ограничение исполнения кода на агентах	Агент и Агент 2	2.4	Исключение system.run из параметров HostnameItem, HostMetadataItem и HostInterfaceItem	Критическая	Не использовать system.run в HostnameItem, HostMetadataItem и HostInterfaceItem.
Ограничение исполнения кода на агентах	Агент и Агент 2	2.5	Отключение UnsafeUserParameters и ограничение UserParameter	Высокая	Оставить UnsafeUserParameters=0 и запретить гибкие UserParameter с невалидируемым вводом.
Ограничение исполнения кода на агентах	Агент и Агент 2	2.6	Защита конфиги, Include-файлы, плагины и wrapper-скрипты от записи пользователями без админских прав	Высокая	Защитить конфиги, Include-файлы, плагины и wrapper-скрипты от записи пользователями без админских прав.
Ограничение исполнения кода на агентах	Агент и Агент 2	2.7	Логировать выполнение удалённые команды при наличии разрешённых исключений	Высокая	Логировать выполнение удалённые команды при наличии разрешённых исключений.
Минимальные привилегии процессов	Linux Agent	3.1	Запуск классический агент не от root; AllowRoot=0	Критическая	Запускать классический агент не от root; AllowRoot=0.
Минимальные привилегии процессов	Агент 2 и systemd	3.2	Явно задать непривилегированного пользователя службы Агент 2	Критическая	Явно задать непривилегированного пользователя службы Агент 2.
Минимальные привилегии процессов	Server / Proxy / Agent	3.3	На хостах сервер СМ «ПУЛЬТ»/Proxy запускать агент под отдельной учётной записью	Высокая	На хостах сервер СМ «ПУЛЬТ»/Proxy запускать агент под отдельной учётной записью.
Минимальные привилегии процессов	Linux sudo	3.4	Запрет zabbix ALL=(ALL) ALL/NOPASSWD:ALL и членство в административных группах	Критическая	Администратор обеспечивает запрет zabbix ALL=(ALL) ALL/NOPASSWD:ALL и членство в административных группах.
Минимальные привилегии процессов	Linux sudo	3.5	Если sudo необходим, разрешать только root-owned wrapper без произвольных аргументов	Высокая	Если sudo необходим, разрешать только root-owned wrapper без произвольных аргументов.
Минимальные привилегии процессов	Windows Agent	3.6	Не запускать агент от LocalSystem/локального администратора	Критическая	Не запускать агент от LocalSystem/локального администратора.
Минимальные привилегии процессов	Windows Agent	3.7	Выдача права мониторинга точечно через встроенные группы/ACL	Средняя	Выдавать права мониторинга точечно через встроенные группы/ACL.
Минимальные привилегии процессов	Linux / Windows	3.8	Формализация исключения по повышенным правам	Высокая	Формализовать исключения по повышенным правам.
Минимальные привилегии	Windows network access	3.9	Ограничение доступ агента к UNC/SMB и исходящий SMB	Высокая	Ограничить доступ агента к UNC/SMB и исходящий SMB.

Группа	Компонент	№	Мера	Критичность	Назначение
процессов					
Минимальные привилегии процессов	Агент и Агент 2 (Windows)	3.10	Установка агента Windows по путям установщика по умолчанию	Средняя	Путь установки по умолчанию сопровождается корректными правами доступа к файлам агента.
Сетевой доступ и шифрование	Active agent	4.1	Для active agents включить TLS PSK или сертификаты и отключить unencrypted	Критическая	Для active agents включить TLS PSK или сертификаты и отключить unencrypted.
Сетевой доступ и шифрование	Passive agent	4.2	Для passive checks принимать только TLS PSK/certificate	Критическая	Для passive checks принимать только TLS PSK/certificate.
Сетевой доступ и шифрование	PSK lifecycle	4.3	Использование уникальный криптографически стойкий PSK на хост/группу риска и защищать файл ключа	Высокая	Использовать уникальный криптографически стойкий PSK на хост/группу риска и защищать файл ключа.
Сетевой доступ и шифрование	Server ↔ Proxy	4.4	Шифрование и взаимно аутентифицировать связь Server–Proxy	Критическая	Шифровать и взаимно аутентифицировать связь Server–Proxy.
Сетевой доступ и шифрование	TCP/10051	4.5	Ограничение вход на сервер или прокси TCP/10051 доверенными сетями агентов/ прокси	Критическая	Ограничить вход на сервер или прокси TCP/10051 доверенными сетями агентов/ прокси.
Сетевой доступ и шифрование	TCP/10050	4.6	Ограничение passive agent TCP/10050 адресами назначенного сервер или прокси	Высокая	Ограничить passive agent TCP/10050 адресами назначенного сервер или прокси.
Сетевой доступ и шифрование	Active-only agent	4.7	При отсутствии passive checks установить StartAgents=0	Средняя	При отсутствии passive checks установить StartAgents=0.
Сетевой доступ и шифрование	Agent source перечень разрешённых значений	4.8	Параметр Server= должен содержать только конкретные сервер или прокси, а не широкие сети	Высокая	Параметр Server= должен содержать только конкретные сервер или прокси, а не широкие сети.
Сетевой доступ и шифрование	Autoregistration	4.9	Защита active-agent autoregistration PSK и ограничить действия авторегистрации	Критическая	Защитить active-agent autoregistration PSK и ограничить действия авторегистрации.
Сетевой доступ и шифрование	Trapper items	4.10	Для каждого trapper item задать Allowed hosts и не принимать данные от произвольных источников	Высокая	Для каждого trapper item задать Allowed hosts и не принимать данные от произвольных источников.
Сетевой доступ и шифрование	Веб-интерфейс и сервер	4.11	Шифрование соединения между веб-интерфейсом и сервером	Высокая	Параметры TLSFrontendAccept и связанные с ними настройки защищают служебный канал между веб-интерфейсом и сервером.
Сервер, прокси и удалённые действия	Сервер СМ «ПУЛЬТ»	5.1	Отключение global scripts на сервере, если не нужны: EnableGlobalScripts=0	Критическая	Отключить global scripts на сервере, если не нужны: EnableGlobalScripts=0.
Сервер, прокси и удалённые	Прокси СМ «ПУЛЬТ»	5.2	Сохранение параметра EnableRemoteCommands=0 на	Критическая	Оставить EnableRemoteCommands=0 на

Группа	Компонент	№	Мера	Критичность	Назначение
действия			Proxy, если выполнение не требуется		Proxy, если выполнение не требуется.
Сервер, прокси и удалённые действия	Scripts / Actions / Items	5.3	Инвентаризация все пути выполнения команд	Критическая	Инвентаризировать все пути выполнения команд.
Сервер, прокси и удалённые действия	Скрипты	5.4	Экранирование макросов в пользовательских глобальных скриптах	Высокая	Значения простых макросов в глобальных скриптах не экранируются автоматически.
Доступ и роли	User roles	6.1	Право Execute scripts выдавать отдельной минимальной роли	Критическая	Право Execute scripts выдавать отдельной минимальной роли.
Доступ и роли	Scripts administration	6.2	Разделение право запуска и право создания/изменения скриптов	Критическая	Разделить право запуска и право создания/изменения скриптов.
Доступ и роли	Frontend accounts	6.3	Минимизация Super admin/Admin, запретить общие учётные записи и отключить неиспользуемых пользователей	Высокая	Минимизировать Super admin/Admin, запретить общие учётные записи и отключить неиспользуемых пользователей.
Доступ и роли	Frontend authentication	6.4	Требование MFA для привилегированных и внешне доступных учётных записей	Высокая	Требовать MFA для привилегированных и внешне доступных учётных записей.
Доступ и роли	API	6.5	Ограничение доступные API-методы по ролям и сетевому источнику	Высокая	Ограничить доступные API-методы по ролям и сетевому источнику.
Доступ и роли	API tokens	6.6	API-токены должны иметь владельца, срок действия, минимальную роль и ротацию	Высокая	API-токены должны иметь владельца, срок действия, минимальную роль и ротацию.
Доступ и роли	Конфигурация веб-интерфейса	6.7	Отключение HTTP-аутентификации веб-интерфейса при отсутствии необходимости	Высокая	Параметр ALLOW_HTTP_AUTH управляет допуском HTTP-аутентификации пользователей веб-интерфейса.
Защита данных и расширений	Macros / scripts / media types	7.1	Не хранить секреты открытым текстом в командах, скриптах и обычных макросах	Высокая	Не хранить секреты открытым текстом в командах, скриптах и обычных макросах.
Защита данных и расширений	Templates / modules / widgets	7.2	Импорт шаблоны, модули и виджеты только из доверенного источника с review	Высокая	Импортировать шаблоны, модули и виджеты только из доверенного источника с review.
Защита данных и расширений	Webhooks / media types	7.3	Ограничение исходящие назначения и секреты webhooks/media types	Высокая	Ограничить исходящие назначения и секреты webhooks/media types.
Обновления компонентов	Все компоненты	8.1	Использование поддерживаемую ветку и устанавливать актуальные security releases в установленный SLA	Критическая	Использовать поддерживаемую ветку и устанавливать актуальные security releases в установленный SLA.

Группа	Компонент	№	Мера	Критичность	Назначение
Веб-интерфейс	Web server / TLS	9.1	Публикация frontend только по HTTPS; HTTP перенаправлять на HTTPS	Высокая	Публиковать frontend только по HTTPS; HTTP перенаправлять на HTTPS.
Веб-интерфейс	Network access	9.2	Ограничение frontend доверенными админскими сетями/VPN/reverse proxy	Высокая	Ограничить frontend доверенными админскими сетями/VPN/reverse proxy.
Веб-интерфейс	HTTP security	9.3	Включение безопасные cookie и anti-framing/CSP headers	Средняя	Включить безопасные cookie и anti-framing/CSP headers.
Веб-интерфейс	Web server hygiene	9.4	Скрытие сигнатуры сервера/PHP и удалить default/test/debug pages	Средняя	Скрыть сигнатуры сервера/PHP и удалить default/test/debug pages.
Веб-интерфейс	HTML notifications/widgets	9.5	Кодирование макрозначения при вставке в HTML-контекст	Высокая	Кодировать макрозначения при вставке в HTML-контекст.
Веб-интерфейс	Все компоненты	9.6	Использование кодировки UTF-8	Высокая	СМ «ПУЛЬТ» поддерживает кодировку UTF-8 как штатный вариант представления текстовых данных.
Веб-интерфейс	Веб-сервер и данные веб-интерфейса	9.7	Закрытие сетевого доступа к файлу списка распространённых паролей	Средняя	Файл со списком распространённых паролей используется политикой паролей и не должен быть доступен клиентам по протоколу HTTP.
Веб-интерфейс	Администрирование веб-интерфейса	9.8	Сохранение параметров X-Frame-Options и изоляции iframe	Средняя	По умолчанию параметр Use X-Frame-Options имеет значение SAMEORIGIN, а изоляция iframe включена.
Аудит и обнаружение отклонений	Audit log	10.1	Не отключать журнал аудита СМ «ПУЛЬТ» и включить запись системных действий	Высокая	Не отключать журнал аудита СМ «ПУЛЬТ» и включить запись системных действий.
Аудит и обнаружение отклонений	Retention / SIEM	10.2	Установка корпоративную retention аудита и экспортировать критичные журналы во внешнюю систему	Высокая	Установить корпоративную retention аудита и экспортировать критичные журналы во внешнюю систему.
Аудит и обнаружение отклонений	Critical objects	10.3	Оповещение об изменении изменения users, roles, tokens, scripts, media types, actions, items, proxies, hosts и encryption settings	Высокая	Алертить изменения users, roles, tokens, scripts, media types, actions, items, proxies, hosts и encryption settings.
Аудит и обнаружение отклонений	Configuration drift	10.4	Периодически сканировать агенты на AllowKey/DenyKey, UserParameter, privilege и TLS drift	Высокая	Периодически сканировать агенты на AllowKey/DenyKey, UserParameter, privilege и TLS drift.
Аудит и обнаружение отклонений	Network telemetry	10.5	Сохранение source IP и аномалии подключений к 10050/10051 во внешних сетевых логах	Высокая	Сохранять source IP и аномалии подключений к 10050/10051 во внешних сетевых логах.
Аудит и обнаружение	Time synchronization	10.6	Синхронизация время Server, Proxy, Agents, DB, frontend и	Средняя	Синхронизировать время Server, Proxy, Agents, DB,

Группа	Компонент	№	Мера	Критичность	Назначение
отклонений			сетевых средств		frontend и сетевых средств.

2. Ограничение исполнения кода на агентах

2.1 Запрет произвольного выполнения ключа system.run[*] на агентах

№: 2.1 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Агент и Агент 2

Описание

Мера применяется к компоненту «агент и Агент 2» и устанавливает следующее требование. Администратор обеспечивает запрет произвольного выполнения ключа system.run[*] на всех агентах. Данная мера ограничивает выполнение команд ОС через ключ агента system.run. Параметр DenyKey запрещает совпавшие вызовы, при этом данный запрет не блокирует автоматически другие механизмы исполнения кода в СМ «ПУЛЬТ».

Обоснование

Мера снижает риск небезопасной конфигурации компонента «агент и Агент 2». Компрометация СМ «ПУЛЬТ» или учётной записи с правом запуска скриптов приводит к удалённому выполнению команд на узле.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору не следует разрешать широкий шаблон подстановки. Администратору рекомендуется зафиксировать итоговое правило DenyKey=system.run[*]. Исключения администратор оформляет точечными правилами AllowKey, размещёнными выше общего запрета.

Проверка

После применения настройки администратор выполняет проверку соответствия. Команда zabbix_agentd -t 'system.run[id]' возвращает значение ZBX_NOTSUPPORTED. Затем администратор проверяет действующую конфигурацию агента и выполняет отрицательный контрольный запрос с сервера. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> В актуальных версиях продукта system.run[*] уже не разрешён по умолчанию. Отсутствие явной строки само по себе не означает уязвимость.

2.2 Ограничение удалённых команд конкретными ключами и командами

№: 2.2 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Агент и Агент 2

Описание

Мера применяется к компоненту «агент и Агент 2» и устанавливает следующее требование. Если удалённые команды необходимы, администратор разрешает только конкретный ключ и конкретную команду. Данная мера задаёт узкие исключения из запрета system.run: какие конкретно команды агенту разрешено выполнять. Чем шире шаблон команды и аргументов, тем больше возможностей получает вызывающая сторона.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «агент и Агент 2». Шаблон AllowKey=system.run[*] снимает основную границу безопасности агента.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». В качестве примера администратор задаёт AllowKey=system.run[/usr/local/sbin/zbx-check-backup,*], затем DenyKey=system.run[*]. Администратору не следует разрешать shell-интерпретаторы и произвольные аргументы.

Проверка

После применения настройки администратор выполняет проверку соответствия. В конфигурации отсутствует правило AllowKey=system.run[*]. Каждый разрешённый вызов сопоставлен с владельцем и подтверждённой необходимостью. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Для каждого исключения требуется отдельная оценка инъекций аргументов.

2.3 Соблюдение порядка правил AllowKey и DenyKey

№: 2.3 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Агент и Агент 2

Описание

Мера применяется к компоненту «агент и Агент 2» и устанавливает следующее требование. Соблюдать порядок AllowKey/DenyKey и исключить перекрывающие шаблоны. Данная мера определяет результат проверки ключа по правилам AllowKey/DenyKey: применяется первое совпадение. Порядок нужен, чтобы точечное разрешение работало, а остальные вызовы попадали под общий запрет.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «агент и Агент 2». Первое совпавшее правило применяется. Ошибочный порядок делает запрет неэффективным или ломает мониторинг.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется размещать узкие AllowKey до общего DenyKey. Администратору рекомендуется проверять каждое правило тестовыми разрешёнными и запрещёнными ключами.

Проверка

После применения настройки администратор выполняет проверку соответствия. Автотест подтверждает: разрешён только утверждённый вызов, варианты команды и аргументов блокируются. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Применимо ко всем платформам.

2.4 Исключение system.run из параметров HostnameItem, HostMetadataItem и HostInterfaceItem

№: 2.4 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Агент и Агент 2

Описание

Мера применяется к компоненту «агент и Агент 2» и устанавливает следующее требование. Не использовать system.run в HostnameItem, HostMetadataItem и HostInterfaceItem. HostnameItem, HostMetadataItem и HostInterfaceItem получают имя, метаданные и сведения об интерфейсе узла из ключей агента. Исключение system.run из этих параметров убирает отдельный путь запуска команд при формировании этих сведений.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «агент и Агент 2». Администратору рекомендуется эти параметры могут выполнять system.run независимо от AllowKey/DenyKey и образуют скрытый обход запрета.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется использовать статические значения либо безопасные встроенные ключи без shell. Администратору рекомендуется проверить включаемые конфиги.

Проверка

После применения настройки администратор выполняет проверку соответствия. Поиск system.run во всех основных и Include-конфигах. Значения параметров не вызывают команды. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Особенно важно при active checks и авторегистрации.

2.5 Отключение UnsafeUserParameters и ограничение UserParameter

№: 2.5 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Агент и Агент 2

Описание

Мера применяется к компоненту «агент и Агент 2» и устанавливает следующее требование. Оставить UnsafeUserParameters=0 и запретить гибкие UserParameter с невалидируемым вводом. UnsafeUserParameters управляет допуском опасных символов в аргументах пользовательских проверок. Проверка аргументов в UserParameter и wrapper ограничивает подстановку недоверенного ввода в shell. Значение 0 не заменяет безопасное написание скрипта.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «агент и Агент 2». Подстановка внешних параметров в shell-команду может привести к инъекция команд.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется использовать фиксированные UserParameter или wrapper с перечень разрешённых значений входов. Администратору не следует передавать ввод в sh/cmd/PowerShell.

Проверка

После применения настройки администратор выполняет проверку соответствия. Конфиг показывает UnsafeUserParameters=0. Негативные тесты со спецсимволами не исполняют команды. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Для legacy-исключений — документированный компенсирующая мера.

2.6 Защита конфиги, Include-файлы, плагины и wrapper-скрипты от записи пользователями без админских прав

№: 2.6 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Агент и Агент 2

Описание

Мера применяется к компоненту «агент и Агент 2» и устанавливает следующее требование. Защитить конфиги, Include-файлы, плагины и wrapper-скрипты от записи пользователями без админских прав. Файловые права определяют, кто может менять конфигурацию агента и исполняемые им скрипты или плагины. Защита от записи препятствует подмене разрешённой команды и снятию ограничений через изменение конфигурации.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «агент и Агент 2». Подмена разрешённого wrapper или правила AllowKey превращает узкое исключение в RCE.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Root/Administrator владеет файлами. Сервисный пользователь имеет только чтение. Администратору рекомендуется запретить исполнение из временных и пользовательских каталогов.

Проверка

После применения настройки администратор выполняет проверку соответствия. Проверка ACL/owner/mode и контроль целостности. Сервисный пользователь не может изменить файл. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Linux и Windows.

2.7 Логировать выполнение удалённые команды при наличии разрешённых исключений

№: 2.7 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Агент и Агент 2

Описание

Мера применяется к компоненту «агент и Агент 2» и устанавливает следующее требование. Логировать выполнение удалённые команды при наличии разрешённых исключений. LogRemoteCommands включает журналирование поддерживаемых запусков удалённых команд агентом. Помогает расследовать их использование, но само по себе не запрещает команды и не заменяет аудит процессов ОС.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «агент и Агент 2». Без журналирования сложно выявить злоупотребление и восстановить цепочку атаки.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется включить LogRemoteCommands=1, централизовать логи, создать правила на неожиданные команды/узлы.

Проверка

После применения настройки администратор выполняет проверку соответствия. Тестовый разрешённый запуск появляется в agent log и SIEM с host, временем и командой. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Если удалённые команды полностью запрещены — мера может быть Н/П.

3. Минимальные привилегии процессов

3.1 Запуск классический агент не от root; AllowRoot=0

№: 3.1 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Linux Agent

Описание

Мера применяется к компоненту «Linux Agent» и устанавливает следующее требование. Запускать классический агент не от root; AllowRoot=0. Данная мера определяет права классического агента в Linux. AllowRoot управляет допуском запуска от root, User задаёт пользователя при предусмотренном агентом снижении привилегий. Фактические права также зависят от настройки службы.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Linux Agent». RCE через агент получает права root и полный контроль над ОС.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется оставить AllowRoot=0 и User=zabbix/отдельного непривилегированного пользователя. Администратору рекомендуется выдать только необходимые права на чтение.

Проверка

После применения настройки администратор выполняет проверку соответствия. Процесс и systemd unit работают от выделенного пользователя. Id не показывает uid=0. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Исключение — только с утверждённым обоснованием и компенсирующими мерами.

3.2 Явно задать непривилегированного пользователя службы Агент 2

№: 3.2 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Агент 2 и systemd

Описание

Мера применяется к компоненту «Агент 2 и systemd» и устанавливает следующее требование. Явно задать непривилегированного пользователя службы Агент 2. Данная мера определяет учётную запись и полномочия процесса Агент 2 на уровне службы ОС. В конфигурации Агент 2 нет параметра User. Права задаются менеджером служб, например systemd или службой Windows.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Агент 2 и systemd». У Агент 2 нет параметра User. Ошибка unit/service может незаметно дать root/SYSTEM.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется настроить User= и Group= в systemd unit/drop-in либо отдельную service account в Windows.

Проверка

После применения настройки администратор выполняет проверку соответствия. Systemctl show ... -p User,Group и фактический владелец процесса соответствуют baseline. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Для Агент 2 проверка выполняется на уровне менеджера служб.

3.3 На хостах сервер СМ «ПУЛЬТ»/Proxy запускать агент под отдельной учётной записью

№: 3.3 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Server / Proxy / Agent

Описание

Мера применяется к компоненту «Server / Proxy / Agent» и устанавливает следующее требование. На хостах сервер СМ «ПУЛЬТ»/Proxy запускать агент под отдельной учётной записью. Разделяет права агента и сервер или прокси на одной машине. Разные учётные записи и файловые ACL ограничивают возможность агента читать секреты и изменять данные центральных компонентов.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Server / Proxy / Agent». Общая учётная запись связывает компрометацию агента с данными/секретами Server или Proxy.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется разделить пользователей и файловые права для server, proxy и agent. Закрыть чтение конфигов с секретами.

Проверка

После применения настройки администратор выполняет проверку соответствия. UID/SID процессов различаются. Агент не читает server/proxy config и TLS secrets. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Требование прямо отражено в СМ «ПУЛЬТ» Security Best Practices.

3.4 Запрет zabbix ALL=(ALL) ALL/NOPASSWD:ALL и членство в административных группах

№: 3.4 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Linux sudo

Описание

Мера применяется к компоненту «Linux sudo» и устанавливает следующее требование. Администратор обеспечивает запрет zabbix ALL=(ALL) ALL/NOPASSWD:ALL и членство в административных группах. Данная мера ограничивает повышение привилегий сервисной учётной записи через sudo и административные группы. Даже агент без root получает административный эквивалент, если его УЗ разрешены любые привилегированные команды.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Linux sudo». Любая команда агента становится локальной эскалацией до root.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется удалить общие sudo-права и членство wheel/sudo/docker/lxd. Администратору рекомендуется заменить на точечный wrapper.

Проверка

После применения настройки администратор выполняет проверку соответствия. Sudo -l -U zabbix не содержит широкий шаблон подстановки/ALL. Группы пользователя не дают админский эквивалент. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Docker/lxd фактически эквивалентны root-доступу.

3.5 Если sudo необходим, разрешать только root-owned wrapper без произвольных аргументов

№: 3.5 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Linux sudo

Описание

Мера применяется к компоненту «Linux sudo» и устанавливает следующее требование. Если sudo необходим, разрешать только root-owned wrapper без произвольных аргументов. Данная мера ограничивает перечень операций, которые агент может выполнить с повышенными правами. Wrapper — вспомогательный скрипт с фиксированной логикой и проверкой аргументов. Его защита от записи предотвращает подмену разрешённой операции.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Linux sudo». Разрешение shell, редактора, package manager, systemctl с произвольным unit или аргументами позволяет обход.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Sudoers: точный абсолютный путь, фиксированные аргументы, NOEXEC где применимо. Wrapper валидирует перечень разрешённых значений и не пишет во временные пути.

Проверка

После применения настройки администратор выполняет проверку соответствия. Негативные тесты с дополнительными аргументами и подменой PATH отказаны. Wrapper недоступен на запись. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Каждое исключение имеет владельца и срок пересмотра.

3.6 Не запускать агент от LocalSystem/локального администратора

№: 3.6 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Windows Agent

Описание

Мера применяется к компоненту «Windows Agent» и устанавливает следующее требование. Не запускать агент от LocalSystem/локального администратора. Данная мера определяет полномочия Windows-агента и запускаемых им команд. LocalSystem даёт высокие системные права. Отдельная ограниченная сервисная УЗ уменьшает последствия выполнения кода от имени агента.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Windows Agent». RCE получает NT AUTHORITY\SYSTEM и полный контроль конечного устройства.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется создать отдельную service account без интерактивного входа и локальных админских групп. Администратору рекомендуется выдать только Log on as a service и необходимые ACL.

Проверка

После применения настройки администратор выполняет проверку соответствия. Whoami процесса показывает выделенную учётную запись. Она не состоит в Administrators и не имеет лишних user rights. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Для DC и критичных серверов — отдельная оценка прав.

3.7 Выдача права мониторинга точечно через встроенные группы/ACL

№: 3.7 **Профиль:** L1 (рекомендуемая базовая мера) **Критичность:** средняя **Компонент:** Windows Agent

Описание

Мера применяется к компоненту «Windows Agent» и устанавливает следующее требование. Выдавать права мониторинга точечно через встроенные группы/ACL. Группы и ACL Windows дают доступ к конкретным источникам метрик: журналам событий, счётчикам, файлам и службам. Позволяют предоставить необходимые права мониторинга без общего членства в Administrators.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Windows Agent». Избыточные локальные права увеличивают последствия компрометации.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Для требуемых метрик использовать Performance Monitor Users, Event Log Readers и точечные WMI/SCM/файловые ACL.

Проверка

После применения настройки администратор выполняет проверку соответствия. Матрица метрика→право подтверждает отсутствие Administrators. Сбор метрик работает. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Набор прав зависит от используемых items.

3.8 Формализация исключения по повышенным правам

№: 3.8 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Linux / Windows

Описание

Мера применяется к компоненту «Linux / Windows» и устанавливает следующее требование. Формализовать исключения по повышенным правам. Организационная мера: фиксирует обоснование повышенных прав, владельца, срок, согласование и компенсирующие меры. Помогает пересматривать исключения, но сама технически права не ограничивает.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Linux / Windows». Временные исключения становятся постоянными и не пересматриваются.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Для каждого исключения: обоснование, владелец, срок, конкретная команда/право, компенсирующие меры и периодический review.

Проверка

После применения настройки администратор выполняет проверку соответствия. Реестр исключений полон. Просроченных исключений нет. Права совпадают с записью. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Организационная мера.

3.9 Ограничение доступ агента к UNC/SMB и исходящий SMB

№: 3.9 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Windows network access

Описание

Мера применяется к компоненту «Windows network access» и устанавливает следующее требование. Ограничить доступ агента к UNC/SMB и исходящий SMB. Данная мера ограничивает обращения агента к сетевым файловым ресурсам Windows и исходящие SMB-соединения. Данная мера уменьшает вероятность передачи NTLM-аутентификации на недоверенный сервер при обращении к UNC-пути.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Windows network access». Обращение к контролируемому UNC может раскрыть NTLM-аутентификацию/хэш учётной записи службы.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется запретить ненужный исходящий TCP/445, блокировать UNC в разрешённых командах/параметрах, использовать локальные пути.

Проверка

После применения настройки администратор выполняет проверку соответствия. Негативный тест к недоверенному SMB заблокирован. В конфиге/скриптах нет UNC. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Актуально прежде всего для Windows.

3.10 Установка агента Windows по путям установщика по умолчанию

№: 3.10 **Профиль:** L1 (рекомендуемая базовая мера) **Критичность:** средняя

Компонент: Агент и Агент 2 (Windows)

Описание

Путь установки по умолчанию сопровождается корректными правами доступа к файлам агента. Произвольный каталог без надлежащих ограничений ослабляет защиту файлов установки.

Обоснование

Мера снижает риск небезопасной конфигурации указанного компонента. Непривилегированный пользователь может изменить файлы установки и тем самым обойти ограничения конфигурации.

Порядок настройки

Администратору рекомендуется использовать пути установщика MSI по умолчанию. При выборе иного каталога администратор назначает права доступа, сопоставимые со штатной установкой, и запрещает запись пользователям без административных полномочий.

Проверка

После применения настройки администратор выполняет проверку соответствия. Администратор убеждается в том, что каталог установки недоступен на запись обычным пользователям, а служба агента запускается от выделенной сервисной учётной записи. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

4. Сетевой доступ и шифрование

4.1 Для active agents включить TLS PSK или сертификаты и отключить unencrypted

№: 4.1 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Active agent

Описание

Мера применяется к компоненту «Active agent» и устанавливает следующее требование. Для active agents включить TLS PSK или сертификаты и отключить unencrypted. TLSConnect выбирает защиту исходящих соединений active agent с сервер или прокси. PSK или сертификат обеспечивают аутентификацию и шифрование. На принимающей стороне также нужно запретить незашифрованный режим для соответствующего узла.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Active agent». Без аутентифицированного TLS возможны подмена/перехват данных и неавторизованная отправка значений.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». TLSConnect=psk или cert. Уникальная identity. TLS-поля синхронизировать на host/proxy/server.

Проверка

После применения настройки администратор выполняет проверку соответствия. Соединение устанавливается только в выбранном TLS-режиме. Незашифрованный тест отклоняется. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> PSK приемлем, сертификаты удобнее при зрелой PKI.

4.2 Для passive checks принимать только TLS PSK/certificate

№: 4.2 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Passive agent

Описание

Мера применяется к компоненту «Passive agent» и устанавливает следующее требование. Для passive checks принимать только TLS PSK/certificate. TLSAccept определяет, какие типы входящих соединений принимает агент для passive checks. Разрешение только PSK/certificate исключает незашифрованный доступ. Сервер или прокси должен использовать согласованный TLS-режим.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Passive agent». Незашифрованный listener допускает перехват и увеличивает риск неавторизованных запросов.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». TLSAccept=psk/cert без unencrypted. Администратору рекомендуется настроить соответствующую encryption policy у host.

Проверка

После применения настройки администратор выполняет проверку соответствия. Подключение без TLS на 10050 отклоняется. Штатные checks успешны. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Если StartAgents=0 — Н/П.

4.3 Использование уникальный криптографически стойкий PSK на хост/группу риска и защищать файл ключа

№: 4.3 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** PSK lifecycle

Описание

Мера применяется к компоненту «PSK lifecycle» и устанавливает следующее требование. Использовать уникальный криптографически стойкий PSK на хост/группу риска и защищать файл ключа. Данная мера управляет общими секретами TLS PSK: генерацией, разграничением, хранением и ротацией. Раздельные ключи уменьшают число узлов, затрагиваемых утечкой одного ключа. Файловые ACL ограничивают его чтение.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «PSK lifecycle». Общий или доступный на чтение PSK расширяет blast radius компрометации.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется генерировать случайный PSK, хранить с минимальными ACL, не передавать в тикетах/логах, регулярно ротировать.

Проверка

После применения настройки администратор выполняет проверку соответствия. Нет повторно используемых PSK. Файл читается только сервисом/root. Процесс ротации протестирован. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Частоту ротации установить внутренним стандартом.

4.4 Шифрование и взаимно аутентифицировать связь Server–Proxy

№: 4.4 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Server ↔ Proxy

Описание

Мера применяется к компоненту «Server ↔ Proxy» и устанавливает следующее требование. Шифровать и взаимно аутентифицировать связь Server–Proxy. Защищает канал передачи данных между сервер СМ «ПУЛЬТ» и Proxy от перехвата и подмены. TLS с корректной проверкой PSK или сертификата позволяет аутентифицировать участников соединения.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Server ↔ Proxy». Компрометация канала proxy позволяет подменять данные и расширяет доступ к сегментам.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется настроить PSK/certificates для proxy и server, запретить unencrypted, проверить identity/issuer/subject.

Проверка

После применения настройки администратор выполняет проверку соответствия. Незашифрованная и неверно аутентифицированная proxy-сессия отклоняется. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Для всех active/passive proxies.

4.5 Ограничение вход на сервер или прокси TCP/10051 доверенными сетями агентов/прокси

№: 4.5 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** TCP/10051

Описание

Мера применяется к компоненту «TCP/10051» и устанавливает следующее требование. Ограничить вход на сервер или прокси TCP/10051 доверенными сетями агентов/прокси. Сетевая фильтрация определяет, с каких адресов разрешено подключаться к TCP/10051 на сервер или прокси. Данная мера ограничивает доступ посторонних источников к приёмному сервису, но не заменяет TLS и прикладную проверку отправителя.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «TCP/10051». Публичная или широкая доступность увеличивает поверхность атак и возможность неавторизованных submissions.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Firewall/ACL/security groups: перечень разрешённых значений адресов прокси/агентских подсетей. Deny by default. Для roaming — VPN/private overlay.

Проверка

После применения настройки администратор выполняет проверку соответствия. Скан из недоверенной сети не достигает 10051. Правила сопоставлены с актуальным инвентарём. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> TLS не заменяет сетевую сегментацию.

4.6 Ограничение passive agent TCP/10050 адресами назначенного сервер или прокси

№: 4.6 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** TCP/10050

Описание

Мера применяется к компоненту «TCP/10050» и устанавливает следующее требование. Ограничить passive agent TCP/10050 адресами назначенного сервер или прокси. Firewall и список разрешённых источников агента ограничивают доступ к TCP/10050. Только назначенный сервер или прокси должен иметь возможность опрашивать passive agent. Шифрование задаётся отдельно.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «TCP/10050». Широкий listener раскрывает сервис и допускает запросы из лишних сегментов.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Host firewall перечень разрешённых значений + узкий Server=. Администратору не следует использовать 0.0.0.0/0 или ::/0.

Проверка

После применения настройки администратор выполняет проверку соответствия. 10050 доступен только с назначенных СМ «ПУЛЬТ» nodes. Запрос с другого адреса отклоняется. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Если passive checks не используются — закрыть порт полностью.

4.7 При отсутствии passive checks установить StartAgents=0

№: 4.7 **Профиль:** L1 (рекомендуемая базовая мера) **Критичность:** средняя **Компонент:** Active-only agent

Описание

Мера применяется к компоненту «Active-only agent» и устанавливает следующее требование. При отсутствии passive checks установить StartAgents=0. У классического агент СМ «ПУЛЬТ» StartAgents=0 отключает процессы passive checks и прослушивание их порта. Активные проверки могут продолжить работу. Параметр нельзя автоматически переносить на Агент 2: у него другой набор настроек.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Active-only agent». Ненужный listener увеличивает поверхность атаки.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется перевести items на active checks, задать StartAgents=0 и закрыть TCP/10050.

Проверка

После применения настройки администратор выполняет проверку соответствия. На узле нет LISTEN 10050. Active items получают данные. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Применимо только к active-only модели.

4.8 Параметр Server= должен содержать только конкретные сервер или прокси, а не широкие сети

№: 4.8 **Профиль:** L2 (усиленная мера) **Критичность:** высокая

Компонент: Agent source перечень разрешённых значений

Описание

Мера применяется к компоненту «Agent source перечень разрешённых значений» и устанавливает следующее требование. Параметр Server= должен содержать только конкретные сервер или прокси, а не широкие сети. Server задаёт допустимые источники входящих запросов к passive agent. Узкий перечень уменьшает круг систем, которые могут опрашивать агент. Этот параметр не задаёт адрес назначения active checks.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Agent source перечень разрешённых значений». Широкий список разрешённых источников ослабляет контроль passive checks.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется указать IP/DNS конкретных СМ «ПУЛЬТ» nodes. Администратору рекомендуется синхронизировать с host firewall.

Проверка

После применения настройки администратор выполняет проверку соответствия. Effective config не содержит широких CIDR. Проверка с постороннего IP отказана. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> DNS требует защиты и предсказуемого резолвинга.

4.9 Защита active-agent autoregistration PSK и ограничить действия авторегистрации

№: 4.9 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Autoregistration

Описание

Мера применяется к компоненту «Autoregistration» и устанавливает следующее требование. Защитить active-agent autoregistration PSK и ограничить действия авторегистрации. Данная мера контролирует автоматическую регистрацию active agents и связанные действия: назначение групп и шаблонов. Аутентификация регистрации и ограничения actions уменьшают риск добавления недоверенного узла. Это отдельный процесс от обычной передачи метрик.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Autoregistration». Неаутентифицированный агент может создать/изменить объект либо получить опасные шаблоны и действия.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется использовать PSK autoregistration, ограничить action conditions, host groups, templates и права. Администратору рекомендуется мониторить новые регистрации.

Проверка

После применения настройки администратор выполняет проверку соответствия. Агент без корректного PSK не регистрируется. Тестовый агент попадает только в карантинную группу. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Особенно важно в динамичных средах.

4.10 Для каждого trapper item задать Allowed hosts и не принимать данные от произвольных источников

№: 4.10 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Trapper items

Описание

Мера применяется к компоненту «Trapper items» и устанавливает следующее требование. Для каждого trapper item задать Allowed hosts и не принимать данные от произвольных источников. Allowed hosts ограничивает источники значений для конкретного trapper item. Это проверка отправителя по разрешённым адресам, а не шифрование и не универсальная настройка для всех active-agent items.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Trapper items». Sender/agent может инжектировать ложные значения в trapper item.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется заполнить Allowed hosts конкретными IP/DNS/CIDR, использовать TLS/сетевые ACL, убрать неиспользуемые trapper items.

Проверка

После применения настройки администратор выполняет проверку соответствия. zabbix_sender с неразрешённого IP отклоняется. Штатный источник принят. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Администратору не следует считать поле host криптографической идентификацией.

4.11 Шифрование соединения между веб-интерфейсом и сервером

№: 4.11 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Веб-интерфейс и сервер

Описание

Параметры TLSFrontendAccept и связанные с ними настройки защищают служебный канал между веб-интерфейсом и сервером. Данная мера дополняет HTTPS для доступа браузера к веб-серверу и TLS для агентов.

Обоснование

Мера снижает риск небезопасной конфигурации указанного компонента. При отсутствии шифрования возможен перехват служебного трафика между веб-интерфейсом и сервером.

Порядок настройки

На сервере администратор настраивает сертификаты и параметр TLSFrontendAccept=cert, а также согласовывает конфигурацию веб-интерфейса.

Проверка

После применения настройки администратор выполняет проверку соответствия. Незашифрованное подключение веб-интерфейса к серверу отклоняется, при этом штатная работа интерфейса сохраняется. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

5. Сервер, прокси и удалённые действия

5.1 Отключение global scripts на сервере, если не нужны: EnableGlobalScripts=0

№: 5.1 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Сервер СМ «ПУЛЬТ»

Описание

Мера применяется к компоненту «сервер СМ «ПУЛЬТ»» и устанавливает следующее требование. Отключить global scripts на сервере, если не нужны: EnableGlobalScripts=0. EnableGlobalScripts управляет доступностью выполнения глобальных скриптов СМ «ПУЛЬТ». Это ограничение отдельного механизма удалённых действий, а не универсальный запрет всех способов выполнения кода в сервер или прокси/Agent.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «сервер СМ «ПУЛЬТ»». Компрометация привилегированной учётной записи позволяет исполнять команды на сервер или прокси/Agent.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется установить EnableGlobalScripts=0. Администратору рекомендуется удалить /disable неиспользуемые scripts и actions.

Проверка

После применения настройки администратор выполняет проверку соответствия. Effective server config показывает 0. Попытка запуска server-side script невозможна. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> В новых установках 7.0+ sample/config может уже содержать 0, но нужно проверить.

5.2 Сохранение параметра EnableRemoteCommands=0 на Proxy, если выполнение не требуется

№: 5.2 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Прокси СМ «ПУЛЬТ»

Описание

Мера применяется к компоненту «прокси СМ «ПУЛЬТ»» и устанавливает следующее требование. Оставить EnableRemoteCommands=0 на Proxy, если выполнение не требуется. EnableRemoteCommands в конфигурации Proxy управляет разрешением выполнения удалённых команд самим Proxy. Не заменяет отдельные ограничения агента и настройки global scripts на Server.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «прокси СМ «ПУЛЬТ»». Proxy часто имеет доступ в изолированные сегменты. RCE на нём расширяет компрометацию.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется проверить proxy config, отключить удалённые команды и ограничить права операционной системы-пользователя proxy.

Проверка

После применения настройки администратор выполняет проверку соответствия. Effective config показывает 0. Proxy не выполняет тестовую remote command. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Исключение — только точечно и с журналированием.

5.3 Инвентаризация все пути выполнения команд

№: 5.3 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Scripts / Actions / Items

Описание

Мера применяется к компоненту «Scripts / Actions / Items» и устанавливает следующее требование. Инвентаризировать все пути выполнения команд. Проверка выявляет объекты и механизмы, через которые могут выполняться команды. Реестр нужен для удаления лишних путей исполнения, согласования исключений и назначения владельцев. Сама инвентаризация ничего не блокирует.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Scripts / Actions / Items». Опасный вызов может находиться не только в global script, но и в action operation, item, UserParameter или media type.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется вести реестр scripts, actions, remote command operations, system.run items, UserParameters, SSH/Telnet checks, webhooks и внешних scripts.

Проверка

После применения настройки администратор выполняет проверку соответствия. Экспорт/API-инвентарь сопоставлен с утверждённым реестром. Неизвестных объектов нет. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Администратору рекомендуется проверять после импортов шаблонов и обновлений.

5.4 Экранирование макросов в пользовательских глобальных скриптах

№: 5.4 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Скрипты

Описание

Значения простых макросов в глобальных скриптах не экранируются автоматически. Администратор применяет функции макросов, чтобы исключить небезопасную подстановку значений.

Обоснование

Мера снижает риск небезопасной конфигурации указанного компонента. Подстановка недоверенного значения может нарушить границу команды или привести к инъекции.

Порядок настройки

В текстах скриптов администратор применяет функции макросов вместо неэкранированных макросов. Администратору не следует передавать значения макросов в оболочку командной строки без проверки.

Проверка

После применения настройки администратор выполняет проверку соответствия. Просмотр глобальных скриптов подтверждает отсутствие неэкранированных макросов в командной строке. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

6. Доступ и роли

6.1 Право Execute scripts выдавать отдельной минимальной роли

№: 6.1 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** User roles

Описание

Мера применяется к компоненту «User roles» и устанавливает следующее требование. Право Execute scripts выдавать отдельной минимальной роли. Право Execute scripts определяет, кому разрешён запуск скриптов через соответствующие функции СМ «ПУЛЬТ» и API. Ограничение этого права не уменьшает полномочия ОС, с которыми будет выполнен разрешённый скрипт.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «User roles». Избыточная роль позволяет перейти от доступа к UI/API к RCE.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется создать роли оператор/админ без Execute scripts. Администратору рекомендуется оставить право только ограниченной группе. Администратору рекомендуется ограничить доступ к host groups.

Проверка

После применения настройки администратор выполняет проверку соответствия. Матрица ролей подтверждает минимальный круг. Script.execute API недоступен без права. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Снятие Execute scripts также ограничивает соответствующий API-метод.

6.2 Разделение право запуска и право создания/изменения скриптов

№: 6.2 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Scripts administration

Описание

Мера применяется к компоненту «Scripts administration» и устанавливает следующее требование. Разделить право запуска и право создания/изменения скриптов. Разделяет полномочия на создание или изменение команд и их запуск. Это модель доступа и согласования, направленная против бесконтрольного создания и исполнения произвольного скрипта одним пользователем, а не один параметр конфигурации.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Scripts administration». Пользователь, способный создать и запустить скрипт, получает универсальный RCE-путь.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется ограничить административные UI/API-права, ввести peer review для скриптов, контролировать scope и confirmation.

Проверка

После применения настройки администратор выполняет проверку соответствия. Тестовые роли не могут одновременно создать и выполнить новый опасный скрипт. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Реализация зависит от RBAC-процесса и версии Zabbix.

6.3 Минимизация Super admin/Admin, запретить общие учётные записи и отключить неиспользуемых пользователей

№: 6.3 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Frontend accounts

Описание

Мера применяется к компоненту «Frontend accounts» и устанавливает следующее требование. Минимизировать Super admin/Admin, запретить общие учётные записи и отключить неиспользуемых пользователей. Данная мера управляет числом привилегированных пользователей, персональной атрибуцией действий и отключением лишних УЗ. Уменьшает количество точек административного доступа и облегчает установление автора изменений.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Frontend accounts». Компрометация общей/избыточной учётной записи даёт трудноатрибутируемый широкий доступ.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Персональные accounts, регулярный recertification, disable Guest/default/unused, отдельная break-glass учётная запись.

Проверка

После применения настройки администратор выполняет проверку соответствия. Список пользователей сопоставлен с HR/IAM. Shared accounts отсутствуют. Guest не имеет доступа. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Периодичность review установить внутренним стандартом.

6.4 Требование MFA для привилегированных и внешне доступных учётных записей

№: 6.4 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Frontend authentication

Описание

Мера применяется к компоненту «Frontend authentication» и устанавливает следующее требование. Требовать MFA для привилегированных и внешне доступных учётных записей. MFA требует дополнительный фактор при входе, а не только пароль. Данная мера уменьшает риск захвата панели при утечке пароля. Не заменяет отдельную защиту API-токенов и действующих сессий.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Frontend authentication». Кража пароля приводит к захвату панели и потенциальному RCE.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется интегрировать SSO/IdP с MFA либо встроенную MFA версии. Исключения только для break-glass под контролем.

Проверка

После применения настройки администратор выполняет проверку соответствия. Политика MFA применяется к целевым ролям. Вход только с паролем отклоняется. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Администратору рекомендуется проверить поддержку в используемой версии/IdP.

6.5 Ограничение доступные API-методы по ролям и сетевому источнику

№: 6.5 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** API

Описание

Мера применяется к компоненту «API» и устанавливает следующее требование. Ограничить доступные API-методы по ролям и сетевому источнику. Ограничение API-методов задаёт, какие операции разрешены роли: чтение данных, изменение объектов или запуск скриптов. Сетевые ограничения отдельно определяют, откуда доступен API.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «API». Широкий API упрощает массовое изменение hosts/items/scripts/actions после кражи токена.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Для сервисных ролей оставить перечень разрешённых значений методов. Администратору рекомендуется запретить script.*, user.*, token.*, configuration.import и другие неиспользуемые методы.

Проверка

После применения настройки администратор выполняет проверку соответствия. Токен сервиса получает ожидаемый отказ на запрещённые методы. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Список методов зависит от интеграции.

6.6 API-токены должны иметь владельца, срок действия, минимальную роль и ротацию

№: 6.6 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** API tokens

Описание

Мера применяется к компоненту «API tokens» и устанавливает следующее требование. API-токены должны иметь владельца, срок действия, минимальную роль и ротацию. Данная мера контролирует выдачу, владельца, срок действия, отзыв, хранение и ротацию API-токенов. Полномочия токена связаны с учётной записью, поэтому ограничение её прав столь же важно, как защита самого секрета.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «API tokens». Бессрочный токен с широкими правами остаётся скрытым постоянным доступом.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется задать expiration, отдельного service user, минимальную роль. Администратору рекомендуется хранить в vault. Администратору рекомендуется отключать и регенерировать по процедуре.

Проверка

После применения настройки администратор выполняет проверку соответствия. Нет токенов без владельца/срока. Секреты не в конфиг-репозиториях. Ротация проверена. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Администратору не следует использовать персональные токены для сервисов.

6.7 Отключение HTTP-аутентификации веб-интерфейса при отсутствии необходимости

№: 6.7 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Конфигурация веб-интерфейса

Описание

Параметр ALLOW_HTTP_AUTH управляет допуском HTTP-аутентификации пользователей веб-интерфейса. Если механизм не используется в контуре, администратор его отключает.

Обоснование

Мера снижает риск небезопасной конфигурации указанного компонента. Ненужный механизм входа расширяет поверхность атаки на веб-интерфейс.

Порядок настройки

В файле конфигурации веб-интерфейса администратор задаёт значение $ALLOW_HTTP_AUTH = false. После повторного запуска процедуры первоначальной настройки администратор повторно проверяет сохранение параметра.

Проверка

После применения настройки администратор выполняет проверку соответствия. В файле конфигурации установлено значение false, а вход с использованием HTTP-аутентификации недоступен. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

7. Защита данных и расширений

7.1 Не хранить секреты открытым текстом в командах, скриптах и обычных макросах

№: 7.1 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Macros / scripts / media types

Описание

Мера применяется к компоненту «Macros / scripts / media types» и устанавливает следующее требование. Не хранить секреты открытым текстом в командах, скриптах и обычных макросах. Данная мера снижает риск раскрытия паролей и токенов в командах, макросах, экспорте и журналах. Защищённое хранилище и минимальные права доступа управляют использованием секретов. Маскировка в UI не равна шифрованию хранения.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Macros / scripts / media types». Секреты попадают в экспорт, UI, audit/logs или становятся доступны лишним ролям.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется использовать secret/vault macros, минимальные ACL и независимое получение секретов каждым сервер или прокси. Администратору не следует логировать значения.

Проверка

После применения настройки администратор выполняет проверку соответствия. Поиск по экспортам/БД/репозиториям не находит открытых секретов. Доступ к vault минимален. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Администратору рекомендуется проверить поддержку vault в выбранной архитектуре.

7.2 Импорт шаблоны, модули и виджеты только из доверенного источника с review

№: 7.2 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Templates / modules / widgets

Описание

Мера применяется к компоненту «Templates / modules / widgets» и устанавливает следующее требование. Импортировать шаблоны, модули и виджеты только из доверенного источника с review. Данная мера контролирует происхождение и содержимое импортируемых шаблонов и расширений. Проверка изменений позволяет выявить добавляемые команды, интеграции и исполняемый код до их использования в рабочей среде.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Templates / modules / widgets». Импорт может добавить опасные items, scripts, webhooks или код frontend-модуля.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется проверять подпись/хэш, diff объектов, system.run/UserParameter/webhooks. Администратору рекомендуется тестировать в изолированной среде.

Проверка

После применения настройки администратор выполняет проверку соответствия. Для каждого импорта есть источник, review и diff. Неизвестных расширений нет. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Особенно важно для сторонних/community пакетов.

7.3 Ограничение исходящие назначения и секреты webhooks/media types

№: 7.3 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Webhooks / media types

Описание

Мера применяется к компоненту «Webhooks / media types» и устанавливает следующее требование. Ограничить исходящие назначения и секреты webhooks/media types. Данная мера ограничивает адреса, к которым webhooks и каналы уведомлений могут обращаться, и доступные им секреты. Данная мера снижает возможность отправки данных на неутверждённые адреса и нежелательных запросов к внутренним сервисам.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Webhooks / media types». SSRF или эксфильтрация возможны через изменённый webhook и пользовательские параметры.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Egress перечень разрешённых значений/proxy, fixed endpoints, secret macros, review JavaScript и запрет произвольных URL.

Проверка

После применения настройки администратор выполняет проверку соответствия. Webhook не достигает internal metadata/RFC1918 вне перечень разрешённых значений. Изменения отслеживаются. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Набор разрешённых направлений определяется интеграциями.

8. Обновления компонентов

8.1 Использование поддерживаемую ветку и устанавливать актуальные security releases в установленный SLA

№: 8.1 **Профиль:** L1 (базовая обязательная мера) **Критичность:** критическая **Компонент:** Все компоненты

Описание

Мера применяется к компоненту «Все компоненты» и устанавливает следующее требование. Использовать поддерживаемую ветку и устанавливать актуальные security releases в установленный SLA. Управление обновлениями устраняет известные программные уязвимости и поддерживает компоненты на обслуживаемых версиях. SLA задаёт срок установки исправления. Это процесс эксплуатации, а не одна настройка Zabbix.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Все компоненты». Известные уязвимости frontend/server/agent могут обходить локальный меры защиты.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется отслеживать advisories, тестировать и обновлять сервер или прокси/Frontend/Agents. Администратору рекомендуется определить SLA по критичности.

Проверка

После применения настройки администратор выполняет проверку соответствия. Версии сверены с advisories и матрицей поддержки. Просроченных security updates нет. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Обновление не следует откладывать до завершения проекта TLS/сегментации.

9. Веб-интерфейс

9.1 Публикация frontend только по HTTPS; HTTP перенаправлять на HTTPS

№: 9.1 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Web server / TLS

Описание

Мера применяется к компоненту «Web server / TLS» и устанавливает следующее требование. Публиковать frontend только по HTTPS; HTTP перенаправлять на HTTPS. HTTPS шифрует обмен браузера с frontend и позволяет проверить серверный сертификат. Перенаправление HTTP переводит пользователя на HTTPS, а HSTS закрепляет использование HTTPS в поддерживающем браузере.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Web server / TLS». Перехват сессии/ учётных данных и downgrade при незащищённом доступе.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется настроить современный TLS, валидный сертификат, redirect и HSTS после проверки полного HTTPS.

Проверка

После применения настройки администратор выполняет проверку соответствия. HTTP даёт redirect. TLS scanner не находит слабых протоколов. HSTS присутствует. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Для внутреннего контура также требуется HTTPS.

9.2 Ограничение frontend доверенными админскими сетями/VPN/reverse proxy

№: 9.2 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Network access

Описание

Мера применяется к компоненту «Network access» и устанавливает следующее требование. Ограничить frontend доверенными админскими сетями/VPN/reverse proxy. Сетевая изоляция, VPN или контролируемый reverse proxy ограничивают круг пользователей и систем, способных достигнуть веб-интерфейса. Это внешний рубеж доступа, не замена ролям и аутентификации Zabbix.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Network access». Интернет-доступ существенно увеличивает риск credential attacks и эксплуатации frontend.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Firewall/WAF/ACL перечень разрешённых значений, VPN/ZTNA, отдельный management сегмент.

Проверка

После применения настройки администратор выполняет проверку соответствия. Из недоверенной сети frontend недоступен. Допустимые пути документированы. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Если необходим внешний доступ — MFA, WAF и усиленный мониторинг обязательны.

9.3 Включение безопасные cookie и anti-framing/CSP headers

№: 9.3 **Профиль:** L1 (рекомендуемая базовая мера) **Критичность:** средняя **Компонент:** HTTP security

Описание

Мера применяется к компоненту «HTTP security» и устанавливает следующее требование. Включить безопасные cookie и anti-framing/CSP headers. Secure ограничивает передачу cookie HTTPS-соединениями. HttpOnly закрывает чтение cookie скриптами. SameSite ограничивает межсайтовую отправку. CSP и anti-framing задают браузеру ограничения содержимого и встраивания страницы.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «HTTP security». Ослабленные cookie и отсутствие headers повышают риск кражи сессии, clickjacking и XSS impact.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Secure, HttpOnly, подходящий SameSite. CSP. Frame-ancestors/X-Frame-Options. HSTS.

Проверка

После применения настройки администратор выполняет проверку соответствия. Проверка response headers и cookies в браузере/сканере соответствует baseline. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> CSP внедрять после теста совместимости виджетов.

9.4 Скрытие сигнатуры сервера/PHP и удалить default/test/debug pages

№: 9.4 **Профиль:** L1 (рекомендуемая базовая мера) **Критичность:** средняя **Компонент:** Web server hygiene

Описание

Мера применяется к компоненту «Web server hygiene» и устанавливает следующее требование. Скрыть сигнатуры сервера/PHP и удалить default/test/debug pages. Данная мера уменьшает раскрытие версий и технической информации через HTTP-заголовки и тестовые страницы. Удаление phpinfo, debug и default content исключает ненужные диагностические точки доступа, но не заменяет обновления.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Web server hygiene». Раскрытие версий и тестовые страницы облегчают разведку и могут раскрывать конфигурацию.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Server_tokens/ServerSignature off, expose_php off. Администратору рекомендуется удалить samples, phpinfo, default vhost. Debug выключен.

Проверка

После применения настройки администратор выполняет проверку соответствия. Headers/ошибки не раскрывают версии. Типовые test paths возвращают 404/403. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Настройки зависят от NGINX/Apache/PHP-FPM.

9.5 Кодирование макрозначения при вставке в HTML-контекст

№: 9.5 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** HTML notifications/widgets

Описание

Мера применяется к компоненту «HTML notifications/widgets» и устанавливает следующее требование. Кодировать макрозначения при вставке в HTML-контекст. Кодирование не даёт недоверенному значению интерпретироваться как HTML-разметке вместо текста. Способ зависит от места отображения: обработка шаблона уведомлений не исправляет автоматически сторонний виджет или все возможные XSS-контексты.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «HTML notifications/widgets». Непроверенное значение history/macro может привести к stored HTML/XSS в совместимом контексте.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется использовать htmlencode macro function. Администратору не следует рендерить недоверенные значения как raw HTML. Администратору рекомендуется тестировать виджеты/шаблоны.

Проверка

После применения настройки администратор выполняет проверку соответствия. Контрольный payload отображается текстом и не исполняется в UI/email. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

9.6 Использование кодировки UTF-8

№: 9.6 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Все компоненты

Описание

СМ «ПУЛЬТ» поддерживает кодировку UTF-8 как штатный вариант представления текстовых данных. Данная мера исключает применение альтернативных кодировок, для которых известны проблемы безопасности.

Обоснование

Мера снижает риск небезопасной конфигурации указанного компонента. Применение иной кодировки может привести к известным проблемам безопасности при обработке данных.

Порядок настройки

Администратору рекомендуется использовать UTF-8 во всех компонентах и клиентских соединениях. Администратору не следует переключать кодировки базы данных и веб-интерфейса на альтернативные варианты ради совместимости с устаревшими скриптами.

Проверка

После применения настройки администратор выполняет проверку соответствия. Администратор убеждается в том, что кодировка базы данных, веб-интерфейса и локалей процессов СМ «ПУЛЬТ» соответствует UTF-8. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

9.7 Закрытие сетевого доступа к файлу списка распространённых паролей

№: 9.7 **Профиль:** L1 (рекомендуемая базовая мера) **Критичность:** средняя

Компонент: Веб-сервер и данные веб-интерфейса

Описание

Файл со списком распространённых паролей используется политикой паролей и не должен быть доступен клиентам по протоколу HTTP.

Обоснование

Мера снижает риск небезопасной конфигурации указанного компонента. Утечка словаря упрощает подбор паролей к учётным записям веб-интерфейса.

Порядок настройки

В конфигурации Apache или Nginx администратор запрещает выдачу файла ui/data/top_passwords.txt либо актуального пути в поставке.

Проверка

После применения настройки администратор выполняет проверку соответствия. HTTP-запрос к указанному файлу возвращает код 403 или 404. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

9.8 Сохранение параметров X-Frame-Options и изоляции iframe

№: 9.8 **Профиль:** L1 (рекомендуемая базовая мера) **Критичность:** средняя

Компонент: Администрирование веб-интерфейса

Описание

По умолчанию параметр Use X-Frame-Options имеет значение SAMEORIGIN, а изоляция iframe включена. Администратор сохраняет эти значения, если нет обоснованной необходимости в ином режиме.

Обоснование

Мера снижает риск небезопасной конфигурации указанного компонента. Отключение параметров снижает защиту от clickjacking и атак через встраивание содержимого.

Порядок настройки

Администратору рекомендуется сохранять значения по умолчанию. Изменение допускается только при необходимости отображения внешних виджетов и после оценки риска.

Проверка

После применения настройки администратор выполняет проверку соответствия. В разделе администрирования параметры не отключены без оформленного исключения. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

10. Аудит и обнаружение отклонений

10.1 Не отключать журнал аудита СМ «ПУЛЬТ» и включить запись системных действий

№: 10.1 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Audit log

Описание

Мера применяется к компоненту «Audit log» и устанавливает следующее требование. Не отключать журнал аудита СМ «ПУЛЬТ» и включить запись системных действий. Встроенный аудит фиксирует поддерживаемые действия и изменения объектов СМ «ПУЛЬТ». Запись системных действий расширяет видимость автоматических изменений. Это отдельный журнал, не равнозначный техническим логам сервер или прокси.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Audit log». Без аудита невозможно надёжно расследовать изменения scripts/actions/users/tokens.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». AuditLogEnabled=1. AuditLogMode включает нужные действия. Администратору рекомендуется ограничить доступ к Administration → Audit log.

Проверка

После применения настройки администратор выполняет проверку соответствия. Тестовое изменение объекта появляется с пользователем, временем, IP и деталями. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Параметры и поля зависят от версии.

10.2 Установка корпоративную retention аудита и экспортировать критичные журналы во внешнюю систему

№: 10.2 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Retention / SIEM

Описание

Мера применяется к компоненту «Retention / SIEM» и устанавливает следующее требование. Установить корпоративную retention аудита и экспортировать критичные журналы во внешнюю систему. Retention определяет срок доступности событий, а внешний архив или SIEM сохраняет их вне самого Zabbix. Retention аудита и retention метрик history различаются. Конкретный срок задаётся внутренней политикой.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Retention / SIEM». Локальная housekeeping может удалить доказательства. Атакующий с админ-доступом влияет на локальные данные.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется определить 180/365 дней по политике либо немедленный SIEM/archive. Администратору рекомендуется защитить от изменения и синхронизировать время.

Проверка

После применения настройки администратор выполняет проверку соответствия. Поиск события за контрольный период успешен. Внешняя копия доступна и неизменяема. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Встроенное значение по умолчанию не считать достаточным для расследований.

10.3 Оповещение об изменении изменения users, roles, tokens, scripts, media types, actions, items, proxies, hosts и encryption settings

№: 10.3 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Critical objects

Описание

Мера применяется к компоненту «Critical objects» и устанавливает следующее требование. Алертить изменения users, roles, tokens, scripts, media types, actions, items, proxies, hosts и encryption settings. Правила мониторинга формируют оповещения при изменении критичных объектов и настроек. Наличие записи в audit log само по себе не гарантирует уведомления или реакции ИБ.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Critical objects». Администратору рекомендуется эти объекты образуют основные пути персистентности, RCE и подмены данных.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Правила SIEM на create/update/delete/enable. Baseline допустимых администраторов и change windows.

Проверка

После применения настройки администратор выполняет проверку соответствия. Контрольное изменение создаёт alert с объектом, субъектом и source IP. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

10.4 Периодически сканировать агенты на AllowKey/DenyKey, UserParameter, privilege и TLS drift

№: 10.4 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Configuration drift

Описание

Мера применяется к компоненту «Configuration drift» и устанавливает следующее требование. Периодически сканировать агенты на AllowKey/DenyKey, UserParameter, privilege и TLS drift. Периодически сравнивает фактические настройки, права и TLS с утверждённым baseline. Выявляет повторное появление опасных разрешений и другие отклонения после локальных изменений, обновлений или импорта конфигурации.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Configuration drift». Локальные отклонения возвращают system.run, sudo или unencrypted mode после исправления.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Policy-as-code/Ansible/EDR query: действующая конфигурацияs, service user, sudoers/groups, ports, TLS. Исключения из реестра.

Проверка

После применения настройки администратор выполняет проверку соответствия. Отчёт покрывает 100% управляемых агентов и выделяет только утверждённые исключения. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Администратору рекомендуется проверять Include-файлы, а не только основной конфиг.

10.5 Сохранение source IP и аномалии подключений к 10050/10051 во внешних сетевых логах

№: 10.5 **Профиль:** L2 (усиленная мера) **Критичность:** высокая **Компонент:** Network telemetry

Описание

Мера применяется к компоненту «Network telemetry» и устанавливает следующее требование. Сохранять source IP и аномалии подключений к 10050/10051 во внешних сетевых логах. Сохраняет источник, назначение и время сетевых соединений для сопоставления с событиями Zabbix. Помогает расследовать подозрительную передачу значений. Не гарантирует однозначную привязку каждой history-записи к IP, особенно при NAT или Proxy.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Network telemetry». History row может не содержать надёжный source IP. Без firewall/NDR/NetFlow hunt ограничен.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Администратору рекомендуется логировать firewall/load balancer/NDR/NetFlow. Администратору рекомендуется коррелировать host/key/time. Администратору рекомендуется алертить новые источники и всплески submissions.

Проверка

После применения настройки администратор выполняет проверку соответствия. Тестовое соединение видно с реальным source IP и коррелируется с СМ «ПУЛЬТ» timestamp. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Администратору не следует утверждать , что source IP всегда хранится в history table.

10.6 Синхронизация время Server, Proxy, Agents, DB, frontend и сетевых средств

№: 10.6 **Профиль:** L1 (рекомендуемая базовая мера) **Критичность:** средняя **Компонент:** Time synchronization

Описание

Мера применяется к компоненту «Time synchronization» и устанавливает следующее требование. Синхронизировать время Server, Proxy, Agents, DB, frontend и сетевых средств. Синхронизирует часы компонентов и средств защиты. Обеспечивает сопоставимость временных меток при расследовании, корректность расписаний и проверок сроков действия сертификатов.

Обоснование

Мера снижает риск небезопасной конфигурации компонента «Time synchronization». Несогласованное время мешает корреляции и может влиять на TLS/сертификаты.

Порядок настройки

Администратор выполняет настройку в конфигурации соответствующего компонента СМ «ПУЛЬТ». Защищённый корпоративный NTP/chrony, мониторинг offset и отказов синхронизации.

Проверка

После применения настройки администратор выполняет проверку соответствия. Offset всех узлов в установленном допуске. Событие коррелируется между источниками. Ожидаемый результат состоит в том, что критерий проверки выполняется без отклонений.

Примечание

> Допуск определить внутренним стандартом.

11. Работа с типовыми инцидентами информационной безопасности

В настоящем разделе приведены типовые инциденты информационной безопасности, которые могут возникнуть при эксплуатации СМ «ПУЛЬТ». Администратор использует перечень для сопоставления наблюдаемых событий с угрозами, настройки обнаружения по метрикам и триггерам и организации оповещения. Рекомендуется периодически возвращаться к перечню при изменении контура мониторинга и состава узлов.

Для каждого инцидента указаны категория, характерное событие или цепочка событий, идентификатор и наименование угрозы по базе угроз, наблюдаемые параметры, а также действия администратора в СМ «ПУЛЬТ» по обнаружению и реагированию. Настройку порогов триггеров администратор выполняет в соответствии с руководством пользователя СМ «ПУЛЬТ» и моделью здоровья объектов мониторинга. Оповещения направляют по каналам, принятым в организации, в том числе по электронной почте, в SIEM-систему, по SMS или в мессенджеры.

11.1 Отказ в обслуживании при росте нагрузки на критичный узел (УБИ-1.1)

Категория потенциального инцидента — отказ в обслуживании. Характерные события: значительное увеличение потребляемых ресурсов на критичном узле и недоступность узла или системы. Угроза по базе угроз — УБИ-1.1 «Угроза попытки осуществления деструктивных воздействий на ИТ-инфраструктуру и защищаемые активы». Наблюдаемые параметры: высокая нагрузка на CPU, память или сетевой трафик на критичном узле.

Администратор отслеживает утилизацию CPU, памяти, дисков и сетевого трафика. При превышении заданных порогов администратор настраивает триггеры и уведомления.

11.2 Заражение вредоносным ПО при запуске нетиповой службы (УБИ-2.2)

Категория потенциального инцидента — заражение вредоносным ПО. Характерное событие: запуск нетиповой службы на узле. Угроза по базе угроз — УБИ-2.2 «Угроза внесения ошибок и уязвимостей на этапах установки, настройки и эксплуатации защищаемых компонентов ИТ-инфраструктуры». Наблюдаемые параметры: аномальные операции или активность в системах управления и критичных сервисах.

Администратор контролирует версии пакетов, состояние конфигурационных файлов и соответствие настроек шаблонам. При несогласованных версиях или изменениях конфигурации администратор настраивает триггеры и уведомления.

11.3 Недоступность узла или системы (УБИ-2.6)

Категория потенциального инцидента — отказ в обслуживании. Характерное событие: недоступность узла или системы. Угроза по базе угроз — УБИ-2.6 «Угроза потери оборудования, устройств, носителей информации и документов». Наблюдаемые параметры: отключение устройств и отсутствие данных от SNMP-агентов на определённом диапазоне.

Администратор настраивает проверку доступности по протоколам ICMP, SNMP и через агенты, а также пользовательские проверки UserParameter при необходимости. Если узел недоступен дольше заданного интервала, срабатывают триггеры и уведомления.

11.4 Недоступность трёх и более узлов одной системы (УБИ-2.6)

Категория потенциального инцидента — отказ в обслуживании. Характерное событие: недоступность трёх и более узлов одной системы. Угроза по базе угроз — УБИ-2.6 «Угроза потери оборудования, устройств, носителей информации и документов». Наблюдаемые параметры: отключение устройств и отсутствие данных от SNMP-агентов на определённом диапазоне.

Администратор настраивает проверку доступности по протоколам ICMP, SNMP и через агенты, а также пользовательские проверки UserParameter при необходимости. Если несколько узлов одной системы недоступны дольше заданного интервала, срабатывают триггеры и уведомления.

11.5 Недоступность площадки (УБИ-2.6)

Категория потенциального инцидента — отказ в обслуживании. Характерное событие: недоступность площадки, когда недоступны более пятидесяти узлов в одной геолокации. Угроза по базе угроз — УБИ-2.6 «Угроза потери оборудования, устройств, носителей информации и документов». Наблюдаемые параметры: отключение устройств и отсутствие данных от SNMP-агентов на определённом диапазоне.

Администратор настраивает проверку доступности по протоколам ICMP, SNMP и через агенты, а также пользовательские проверки UserParameter при необходимости. При массовой недоступности узлов одной геолокации срабатывают триггеры и уведомления.

11.6 Несоблюдение требований безопасности персоналом (УБИ-2.9)

Категория потенциального инцидента — нарушение политик безопасности. Характерное событие: несоблюдение требований безопасности персоналом. Угроза по базе угроз — УБИ-2.9 «Угрозы несоблюдения персоналом установленных требований безопасности». Наблюдаемые параметры: попытки доступа к защищённым системам и несанкционированные операции.

Администратор обеспечивает журналирование аутентификаций и операций доступа, а также контроль активности пользователей и попыток входа. При несанкционированных входах или превышении числа неудачных попыток администратор настраивает триггеры и уведомления.

11.7 Отказ вспомогательных систем при атаке типа «отказ в обслуживании» (УБИ-4.2)

Категория потенциального инцидента — отказ в обслуживании. Характерные события: значительное увеличение потребляемых ресурсов на критичном узле, недоступность узла или системы, выявление сетевой атаки типа «отказ в обслуживании». Угроза по базе угроз — УБИ-4.2 «Угроза отказа или некорректного функционирования вспомогательных систем, поддерживающих функционирование информационных систем». Наблюдаемые параметры: недоступность систем резервирования и служб мониторинга.

Администратор отслеживает состояние служб, статус задач и сообщения об ошибках в журналах. При изменении статуса, ошибках в журналах или отсутствии ответов вспомогательных систем администратор настраивает триггеры и уведомления.

11.8 Недоступность инфраструктурных сервисов из-за высокой загрузки (УБИ-4.3)

Категория потенциального инцидента — отказ в обслуживании. Характерные события: значительное увеличение потребляемых ресурсов на критичном узле, недоступность узла или системы, выявление сетевой атаки типа «отказ в обслуживании». Угроза по базе угроз — УБИ-4.3 «Угроза недоступности инфраструктурных сервисов из-за большой загрузки сетей связи и вычислительных ресурсов». Наблюдаемые параметры: высокая нагрузка на CPU, память или сетевой трафик на критичном узле.

Администратор отслеживает утилизацию CPU, памяти, дисков и сетевого трафика. При превышении заданных порогов администратор настраивает триггеры и уведомления.

11.9 Появление нового узла в инфраструктуре (УБИ-5.1)

Категория потенциального инцидента — нарушение политик безопасности. Характерное событие: появление нового узла в инфраструктуре. Угроза по базе угроз — УБИ-5.1 «Угроза перехвата, модификации и подмены данных, передаваемых по каналам связи». Наблюдаемые параметры: обнаружение появления новых узлов в сети.

Администратор обеспечивает автоматическое отслеживание и журналирование добавления новых объектов мониторинга, в том числе по IP-адресам. При необходимости администратор настраивает интеграцию с SIEM-системой для детектирования инцидентов информационной безопасности.

11.10 Обнаружение подозрительного ПО на узле (УБИ-6.5)

Категория потенциального инцидента — нарушение политик безопасности. Характерное событие: обнаружение подозрительного программного обеспечения на узле. Угроза по базе угроз — УБИ-6.5 «Угрозы компрометации учётных записей пользователей и администраторов». Наблюдаемые параметры: аномальные входы и высокая нагрузка на аутентификацию.

Администратор обеспечивает журналирование попыток входа и статистику по активным сессиям. При превышении порога неудачных попыток или появлении сессий от неизвестных пользователей администратор настраивает триггеры и уведомления.

11.11 Нарушение доступности вычислительных ресурсов (УБИ-6.6)

Категория потенциального инцидента — нарушение политик безопасности. Характерные события: значительное увеличение потребляемых ресурсов на критичном узле, недоступность узла или системы, выявление сетевой атаки типа «отказ в обслуживании». Угроза по базе угроз — УБИ-6.6 «Угрозы нарушения доступности вычислительных ресурсов». Наблюдаемые параметры: высокая нагрузка на CPU, память или сетевой трафик на критичном узле.

Администратор отслеживает утилизацию CPU, памяти, дисков и сетевого трафика. При превышении заданных порогов администратор настраивает триггеры и уведомления.

11.12 Внедрение и эксплуатация вредоносного ПО (УБИ-6.7)

Категория потенциального инцидента — нарушение политик безопасности. Характерные события: изменение состава программного обеспечения на узле, запуск нетипичных процессов, нетипичная сетевая активность, запуск запрещённого программного обеспечения. Угроза по базе угроз — УБИ-6.7 «Угрозы внедрения и эксплуатации вредоносного ПО». Наблюдаемые параметры: запуск вредоносных процессов и изменение системных файлов.

Администратор контролирует процессы, выявляет новые или неизвестные процессы и проверяет целостность системных файлов. При появлении вредоносных или нетипичных процессов администратор настраивает триггеры и уведомления.

11.13 Несанкционированная передача данных (УБИ-6.11)

Категория потенциального инцидента — утечка данных. Характерное событие: аномалия по передаваемому объёму данных на внешние адреса или по внутренней сети. Угроза по базе угроз — УБИ-6.11 «Угроза несанкционированной передачи данных». Наблюдаемые параметры: аномальные исходящие соединения.

Администратор анализирует журналы сетевых устройств и фильтрует соединения по портам для выявления несанкционированных подключений. При превышении порога отправленных данных или обращении к необычным адресам администратор настраивает триггеры и уведомления.

11.14 Несанкционированная подмена или внедрение объекта сети (УБИ-6.15)

Категория потенциального инцидента — нарушение политик безопасности. Характерное событие: появление нового узла в инфраструктуре. Угроза по базе угроз — УБИ-6.15 «Угроза несанкционированной подмены или внедрения объекта сети». Наблюдаемые параметры: обнаружение появления новых узлов в сети.

Администратор обеспечивает автоматическое отслеживание и журналирование добавления новых объектов мониторинга, в том числе по IP-адресам. При необходимости администратор настраивает интеграцию с SIEM-системой для детектирования инцидентов информационной безопасности.

11.15 Недоступность ресурсов виртуальной инфраструктуры (УБИ-8.3)

Категория потенциального инцидента — отказ в обслуживании. Характерные события: значительное увеличение потребляемых ресурсов на критичном узле и недоступность узла или системы. Угроза по базе угроз — УБИ-8.3 «Угроза недоступности вычислительных ресурсов виртуальной инфраструктуры». Наблюдаемые параметры: недоступность или сбои виртуальных машин и гипервизора.

Администратор отслеживает состояние гипервизора и статус виртуальных машин. При недоступности или высокой нагрузке администратор настраивает триггеры и уведомления.

12. Сводный перечень мер

В таблице приведён перечень мер настоящего руководства для отметки выполнения после настройки.

№	Критичность	Мера	Выполнено
2.1	критическая	Запрет произвольного выполнения ключа system.run[*] на агентах	
2.2	критическая	Ограничение удалённых команд конкретными ключами и командами	
2.3	высокая	Соблюдение порядка правил AllowKey и DenyKey	
2.4	критическая	Исключение system.run из параметров HostnameItem, HostMetadataItem и HostInterfaceItem	
2.5	высокая	Отключение UnsafeUserParameters и ограничение UserParameter	
2.6	высокая	Защита конфиги, Include-файлы, плагины и wrapper-скрипты от записи пользователями без админских прав	
2.7	высокая	Логировать выполнение удалённые команды при наличии разрешённых исключений	
3.1	критическая	Запуск классический агент не от root; AllowRoot=0	

№	Критичность	Мера	Выполнено
3.2	критическая	Явно задать непривилегированного пользователя службы Агент 2	
3.3	высокая	На хостах сервер СМ «ПУЛЬТ»/Proxy запускать агент под отдельной учётной записью	
3.4	критическая	Запрет zabbix ALL=(ALL) ALL/NOPASSWD:ALL и членство в административных группах	
3.5	высокая	Если sudo необходим, разрешать только root-owned wrapper без произвольных аргументов	
3.6	критическая	Не запускать агент от LocalSystem/локального администратора	
3.7	средняя	Выдача права мониторинга точечно через встроенные группы/ACL	
3.8	высокая	Формализация исключения по повышенным правам	
3.9	высокая	Ограничение доступ агента к UNC/SMB и исходящий SMB	
3.10	средняя	Установка агента Windows по путям установщика по умолчанию	
4.1	критическая	Для active agents включить TLS PSK или сертификаты и отключить unencrypted	
4.2	критическая	Для passive checks принимать только TLS PSK/certificate	
4.3	высокая	Использование уникальный криптографически стойкий PSK на хост/группу риска и защищать файл ключа	
4.4	критическая	Шифрование и взаимно аутентифицировать связь Server–Proxy	
4.5	критическая	Ограничение вход на сервер или прокси TCP/10051 доверенными сетями агентов/прокси	
4.6	высокая	Ограничение passive agent TCP/10050 адресами назначенного сервер или прокси	
4.7	средняя	При отсутствии passive checks установить StartAgents=0	
4.8	высокая	Параметр Server= должен содержать только конкретные сервер или прокси, а не широкие сети	
4.9	критическая	Защита active-agent autoregistration PSK и ограничить действия авторегистрации	
4.10	высокая	Для каждого trapper item задать Allowed hosts и не принимать данные от произвольных источников	
4.11	высокая	Шифрование соединения между веб-интерфейсом и сервером	
5.1	критическая	Отключение global scripts на сервере, если не нужны: EnableGlobalScripts=0	
5.2	критическая	Сохранение параметра EnableRemoteCommands=0 на Proxy, если выполнение не требуется	
5.3	критическая	Инвентаризация все пути выполнения команд	
5.4	высокая	Экранирование макросов в пользовательских глобальных скриптах	
6.1	критическая	Право Execute scripts выдавать отдельной минимальной роли	
6.2	критическая	Разделение право запуска и право создания/изменения скриптов	
6.3	высокая	Минимизация Super admin/Admin, запретить общие учётные записи и отключить неиспользуемых пользователей	
6.4	высокая	Требование MFA для привилегированных и внешне доступных учётных записей	
6.5	высокая	Ограничение доступные API-методы по ролям и сетевому источнику	
6.6	высокая	API-токены должны иметь владельца, срок действия, минимальную роль и ротацию	
6.7	высокая	Отключение HTTP-аутентификации веб-интерфейса при отсутствии необходимости	
7.1	высокая	Не хранить секреты открытым текстом в командах, скриптах и обычных макросах	

№	Критичность	Мера	Выполнено
7.2	высокая	Импорт шаблоны, модули и виджеты только из доверенного источника с review	
7.3	высокая	Ограничение исходящие назначения и секреты webhooks/media types	
8.1	критическая	Использование поддерживаемую ветку и устанавливать актуальные security releases в установленный SLA	
9.1	высокая	Публикация frontend только по HTTPS; HTTP перенаправлять на HTTPS	
9.2	высокая	Ограничение frontend доверенными админскими сетями/VPN/reverse proxy	
9.3	средняя	Включение безопасные cookie и anti-framing/CSP headers	
9.4	средняя	Скрытие сигнатуры сервера/PHP и удалить default/test/debug pages	
9.5	высокая	Кодирование макрозначения при вставке в HTML-контекст	
9.6	высокая	Использование кодировки UTF-8	
9.7	средняя	Закрытие сетевого доступа к файлу списка распространённых паролей	
9.8	средняя	Сохранение параметров X-Frame-Options и изоляции iframe	
10.1	высокая	Не отключать журнал аудита СМ «ПУЛЬТ» и включить запись системных действий	
10.2	высокая	Установка корпоративную retention аудита и экспортировать критичные журналы во внешнюю систему	
10.3	высокая	Оповещение об изменении изменения users, roles, tokens, scripts, media types, actions, items, proxies, hosts и encryption settings	
10.4	высокая	Периодически сканировать агенты на AllowKey/DenyKey, UserParameter, privilege и TLS drift	
10.5	высокая	Сохранение source IP и аномалии подключений к 10050/10051 во внешних сетевых логах	
10.6	средняя	Синхронизация время Server, Proxy, Agents, DB, frontend и сетевых средств	