Политика KES 12.2 для Linux Servers

Название политики:

Политика KES 12.2 Linux - Сервера (Linux)

Применение:

- Группа устройств: Сервера (Linix)
- Тип ОС: Linux
- Применение политики: Принудительно с наследованием параметров

Для кого эта политика:

- Серверная часть

Компоненты

Kaspersky Security Network	**Включен**	Проверка по облачной базе Kaspersky
Защита от файловых угроз	**Включен**	Проверка файловой системы
Защита от веб-угроз	**Включен**	Зашита от веб-угроз, как бы это не звучало.
Защита от сетевых угроз	**Включен**	Firewall
Защита от шифрования	**Включен**	Защита файлов в локальных директориях с сетевым доступом по протоколам SMB/NFS от удаленного вредоносного шифрования
Поведенческий анализ	**Включен**	Анализ поведения
Detection and Response (KATA)	**Выключен**	EDR, MDR
Контроль приложений	**Выключен**	Контроль запускаемых приложений (черный и белый списки)
Контроль целостности системы	**Включен**	Контроль изменений файлов в системе, реестра и подключения к компьютеру внешних устройств

Контроль устройств	**Выключен**	Контроль подключенных и внешних устройств
Веб-контроль	**Включен**	Контроль доступа к веб-ресурсам
Проверка контейнеров	**Включен**	Проверка пространств имен и контейнеров в реальном времени
Интеграция с KUMA	**Выключен**	Интеграция с SIEM системой
Легкий агент	**Выключен**	Серверный вариант использования, с выносом активных компонентов на SVM сервер

Общие

- Активная политика - **включить**
- Наследовать параметры родительской политики - **выключить**
- Обеспечить принудительное наследование параметров для дочерних политик - **выключить**

Настройка событий

Настройка событий

- Регистрация событий
  - Хранить в базе данных Сервера администрирования в течении (сут) - **до 60**
  - **Экспортировать в SIEM-систему по протоколу Syslog**
- События, которые стоит отправлять в SIEM

Тип события	Время хранения на KSC	Отправка в SIEM
:drop_of_blood: Критические события		Да :tick: / Нет :cross:
Нарушено лицензионное соглашение	30 дней	

Защита от файловых угроз

- Включить защиту от файловых угроз - **включить**
- Режим защиты - **Интеллектуальный режим**
- Проверка областей:
    - Основная область **"/"**

- Параметры проверки
    - Проверять архивы - **включить**
    - Проверять почтовые базы - выключить
    - Проверять файлы почтовых форматов - выключить
    - Пропускать текстовые файлы - выключить
    - Пропускать файл, если его проверка длится более (сек) - **60**
    - Пропускать файл, если его размер более (МБ) - **200**
    - Сообщать о незараженных объектах - выключить
    - Сообщать о необработанных объектах - выключить
    - Сообщать об упакованных объектах - выключить
    - Использовать технологию iChecker - включить
    - Использовать эвристический анализ - включить (Рекомендованный)

- Действия при обнаружении угрозы
    - Первое - **Выполнять рекомендованное действие**
    - Второе действие - **Блокировать**

Выполнять рекомендованное действие над объектом на основе данных об уровне опасности угрозы, обнаруженной в файле, и возможности его лечения

Исключения защиты от файловых угроз

- Директории\Файлы

Название области исключения	Путь	Комментарий

Данные PG	/var/lib/postgresql/**/main/	
WAL-файлы	/var/lib/postgresql/**/main/pg_wal/	
Исполняемые файлы PG	/usr/lib/postgresql/**/bin/	
Данные MySQL	/var/lib/mysql/	
Сокет MySQL	/var/run/mysqld/mysql.sock	
Сокет PG	/var/run/postgresql/.s.PGSQL.*	
Данные Redis	/var/lib/redis/	
RDB-файлы Redis	/var/lib/redis/dump.rdb	
AOF-файлы Redis	/var/lib/redis/appendonly.aof	
Сокет Redis	/var/run/redis/redis.sock	
Данные RabbitMQ	/var/lib/rabbitmq/	
Сокет RabbitMQ	/var/run/rabbitmq/	
Данные Kafka	/var/lib/kafka/	

- Включить управление сетевым экраном - выключить

На серверах используется ufw, нет смысла дублировать его работу в Касперском

Защита от веб-угроз

- Включить защиту от веб-угроз - **включить**
- Действие при обнаружении угрозы - **Блокировать**
- Доверенные веб-адреса - ***.serbsky.ru, *.serbsky.lan.**
- Параметры защиты от веб-угроз
  - Использовать эвристический анализ для обнаружения фишинговых ссылок - **включить**
    - Обнаруживать вредоносные объекты - **включить**
    - Обнаруживать фишинговые ссылки - **включить**
    - Обнаруживать рекламные приложения - **выключить**
    - Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным - **выключить**

Защита от сетевых угроз

- Включить защиту от сетевых угроз - **включить**
- Действие при обнаружении угрозы - **Блокировать**
- Блокировать атакующие устройства - **включить**
- Блокировать атакующее устройство на (мин) - **60**
- Исключения
    - Scaner -**RedCHeck**

Продвинутая защита

Kaspersky Security Network

- Включить облачный режим - **включить**
    - **Расширенный режим KSN**

- Использовать серверы KSN, если прокси-сервер KSN недоступен - **включить**

Защита от шифрования

- Включить защиту от шифрования - **включить**
- Области защиты - **Все общие директории**
- Параметры защиты
    - Действие при обнаружении шифрования - **Блокировать**
    - Блокировать недоверенное устройство на (мин) - **30**

- Исключения - **Пока нет**
- Исключения по маске - **Пока нет**

Анализ поведения

- Включить анализ поведения - **включить**
- Действие при обнаружении вредоносной активности - **Информировать**
- Исключения по процессам - **Пока нет**

Detection and Response

Managed Detection and Response

- Нет лицензии

Endpoint Detection and Response (KATA)

- Нет лицензии

Network Detection and Response (KATA)

- Нет лицензии

Контроль безопасности

Контроль приложений

- Включить контроль приложений - **выключить**

Контроль Целостности системы

- Включить контроль целостности системы - **включить**

- Области мониторинга
  - **/opt/kaspersky/kesl**
  - **/etc/ssh/sshd_config**
  - **/etc/passwd**
  - **/etc/shadow**
  - **/etc/sudoers**
  - **/boot**
  - **/etc/redis/redis.conf**
  - **/etc/rabbitmq/rabbitmq.conf**
  - **/etc/kafka/servcer.properties**
  - **/etc/postgresql/**/pg_hba.conf**
  - **/etc/postgresql/**/postgresql.conf**

- Исключения по маске - **Пока нет**

Контроль устройств

- Включить контроль устройств - **выключить**

Веб-Контроль

- Включить Веб-контроль - **включить**
- Правила Веб-контроля
  - **Торренты**
  - **Криптовалюты, майнинг**
    - Блокировка по категориям
    - Фильтровать адреса - **Любой адрес**
    - Применять к пользователям - **Ко всем пользователям**
    - Расписание работы правила - **Всегда**
    - Действие правила - **Запретить**

- Правило по умолчанию - **Разрешить**

Локальные задачи

Управление задачами

- Разрешить пользователям просмотр и управление локальными задачами - **выключить**
- Разрешить пользователям просмотр и управление задачами, созданными через KSC - **выключит**

Проверка съемных дисков

- Включить проверку съемных дисков при подключении к устройству - **выключить**
- Блокировать доступ к съемному диску во время проверки - **выключить**

Общие параметры

Параметры прокси-сервера

- Параметры подключения - **Не использовать прокси-сервер**
- Использовать Kaspersky Security Center в качестве прокси-сервера для активации приложения - **выключить**

Параметры приложения

- Обнаруживать легальные приложения, которые злоумышленники могут использовать для нанесения вреда устройствам или данным - выключить
- Показывать всплывающие уведомления в графическом пользовательском интерфейсе - выключить
- Производительность
    - Ограничить потребление ресурсов процессора для задач проверки (%) - **80**
    - Ограничение на использование памяти для задач проверки (МБ) - **2048**
    - Максимальное количество задач выборочной проверки: **5**

- Параметры запуска приложения
    - Максимальное количество неудачных последовательных попыток запуска приложения - **5**
    - Максимальное время ожидания запуска приложения (мин) - **3**

- Параметры трассировки

    - Путь к директории трассировки - **/var/log/kaspersky/kesl**
    - Максимальный размер файла трассировки (МБ) - **500**
    - Максимальное количество файлов трассировки - **10**
    - Создавать файл дампа при сбое в работе приложения - **выключить**

- Дополнительные параметры приложения
    - Включить мониторинг стабильности работы приложения - **выключить**
    - Использование памяти приложением - **Ограничивается автоматически**

- Режим перехвата файловых операций
    - Блокировать доступ к файлам во время проверки - **включить**

Параметры проверки контейнеров

- Включить проверку пространств имен и контейнеров - включить
- Действие с контейнером при обнаружении угрозы - Остановить, если не удалось вылечить
- Параметры проверки контейнеров
    - Использовать Docker **/var/run/docker.sock**
    - Использовать CRI-O - **выключить**
    - Использовать Podman - **выключить**
    - Использовать runc - **выключить**

Параметры сети

- Включить проверку защищенных соединений - **включить**
- Переход на домен с недоверенным сертификатом - **Разрешать**
- Переход на домен с ошибкой проверки защищенных соединений - **Добавлять домен в исключения**
- Политика проверки сертификатов - **Полная проверка**
- Доверенные домены
    - ***.serbsky.ru**
    - ***.serbsky.lan**

- Доверенные корневые сертификаты - **Пока нет**
- Параметры сетевых портов
    - **80**

    - **81**
    - **82**
    - **83**
    - **443**
    - **868**
    - **1080**
    - **3128**
    - **5000**
    - **7900**
    - **8000**
    - **8080**
    - **8088**
    - **8888**
    - **11523**
        - Контролировать только выбранные сетевые порты

Глобальные исключения

- Пока нет исключенных точек монтирования

Исключение памяти процессов

- Пока нет процессов для исключения

Параметры хранилищ

- Хранить объекты не более (дней) - **60**
- Ограничить размер резервного хранилища до (МБ) - **выключить**
- Ограничить размер карантина до (МБ) - **200**
- Уведомлять при заполнении карантина на (%) - **90**
- Передача данных на Сервер администрирования
    - Информировать о файлах карантина - **включить**
    - Информировать о файлах резервного хранилища - **включить**
    - Информировать о необработанных файлах - **включить**
    - Информировать об установленных устройствах - **включить**

Интеграция с KUMA

- Включить интеграцию с KUMA - **выключить**
- Использовать защищенное соединение - **выключить**
    - Сервер: **нет**
- Параметры подключения к серверам KUMA
    - Максимальное время ожидания соединения с сервером (сек) - **10**
    - Использовать двустороннюю аутентификацию - **выключить**
- Параметры передачи данных - Максимальная задержка отправки событий (сек) - **30**

Режим легкого агента

- Не используется

Профили политик

- Пока не используется

Revision #2
Created 18 June 2025 18:48:08 by admin_mf
Updated 18 June 2025 18:50:57 by admin_mf