

Описание модуля Е: «Технологии защиты узла и агентского мониторинга»

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно).

При выполнении модуля Е ставятся следующие цели:

1. Настройка сервера агентского мониторинга для правильной работы системы.
2. Разработка политик и правил безопасности, предотвращающих утечки или попытку использования устройств и сервисов пользователями.
3. Разработка групповых политик домена для ограничения пользовательских действий.
4. Проверка работоспособности политик и правил безопасности.

Задача 1

Необходимо создать 2 новых группы компьютеров: «Test1» и «Test2», а также создать 2 новых политики: «Test1» и «Test2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Test1, а компьютер 2 — в Test2.

Зафиксировать выполнение скриншотом.

Задача 1: РЕШЕНИЕ

Задача выполняется на виртуальной машине IWDM. Перейдите к консоли управления Device Monitor. Для создания новой политики перейдите ко вкладке «Политики» и нажмите кнопку «Создать политики...» (зеленый плюсик в верхней левой части интерфейса), после чего впишите наименование по заданию, после чего сразу же сохраните политику. Повторите операцию для второй политики.

Затем, необходимо создать группу компьютеров, для этого перейдите ко вкладке «Группы компьютеров» и нажмите кнопку «Создать группу компьютеров...» (зеленый плюсик в верхней левой части интерфейса) установите наименование в соответствии с заданием, в поле «Политика» выберите соответствующую созданную политику. Теперь добавьте соответствующий компьютер в группу. Другие настройки не изменять.



Рисунок 1 – Создание группы компьютеров

Примените и сохраните настройки. Повторите действия для второго ПК.

Задача 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на другую машину для удаленного доступа к серверу агентского мониторинга.

Задача 2: РЕШЕНИЕ

Скопируйте установочный файл сервера Device Monitor в любое общедоступное сетевое хранилище (прим. <\\demolab\share>). Перейдите к виртуальной машине, на которую по заданию требуется установить дополнительную консоль. Откройте сетевое хранилище и скопируйте установочный файл в операционную систему VM.

Запустите установочный файл. Здесь необходимо повторить уже знакомую процедуру установки, за исключением некоторых особенностей. На шаге установки «Выборочная установка» у объекта «Сервер» выберите параметр «Этот компонент будет полностью недоступен». Затем нажмите установить.

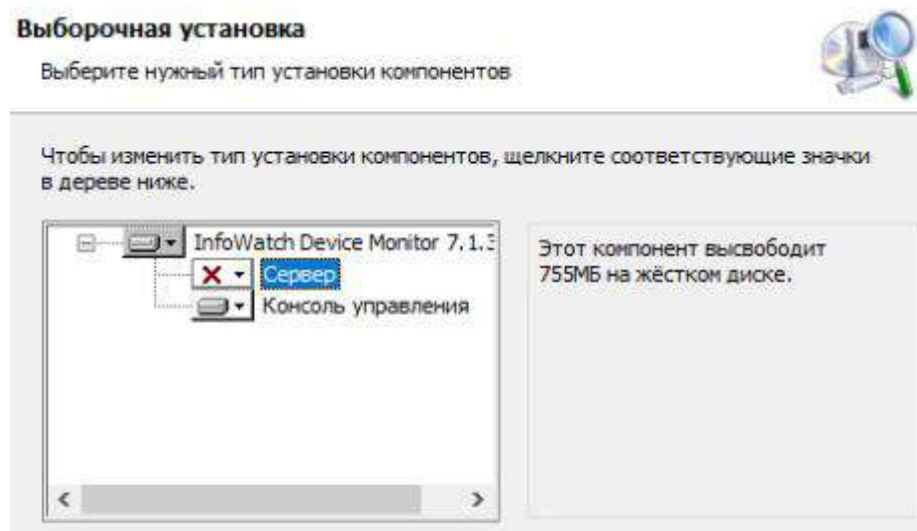


Рисунок 2 – Выборочная установка

Затем запустите установленное приложение и проверьте работоспособность подключившись к серверу IWDM.

Задача 3: разработать правила агентского мониторинга. Следующие правила создаются в **первой** политике.

Правило 1

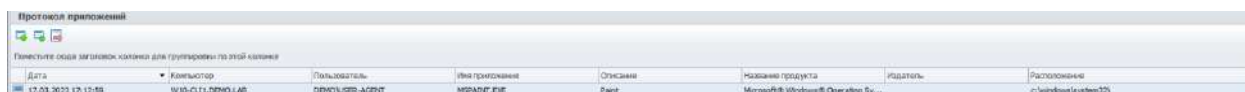
Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 1: РЕШЕНИЕ

Для того, чтобы запретить какое-либо приложение, его сначала **нужно открыть**. Поэтому, нужно перейти к виртуальной машине нарушителя (в соответствующей политике) и открыть приложение, в соответствии с заданием. В данном примере будет рассматриваться приложение mspaint.exe.

Переходим к машине нарушителя и открываем mspaint.exe. После открытия приложения на машине нарушителя **ЗАКРЫВАЕМ** его и возвращаемся к консоли управления сервером Device Monitor. Во вкладке «Приложения» нужно найти только что открытое приложение. Искать открытые приложения будет удобнее, если отсортировать список по дате.



Дата	Компьютер	Пользователь	Имя приложения	Описание	Название продукта	Издатель	Расположение
17.03.2023 17:12:59	W10-CLT1.DEMO-LAB	DEMO\USER-AGENT	MSPAINT.EXE	Paint	Microsoft Windows Operating System	c:\windows\system32	c:\windows\system32

Рисунок 3 – Появившееся приложение

После обнаружения приложения в списке, необходимо создать список приложений и добавить в него приложение. Для этого, выберите приложение, кликните на него ПКМ, затем нажмите «Добавить приложение в список вручную», затем нажмите «Создать новый...», назовите список «Правило 1» и выберите созданный список. В качестве атрибута соответствия приложения выбирайте «По подробной информации» или «По расположению».

Переходим к созданию правила. Для создания правила, необходимо перейти во вкладку «Политики», выбрать политику по заданию и нажать

кнопку «Создать правило...» (зеленый плюс, не перепутайте с «создать политику...»!). Теперь конфигурируйте правило: наименование установите по заданию («Правило 1»). В качестве перехватчика выберите «Application Monitor», поскольку правило создается на приложение. Теперь, необходимо конфигурировать правило: в зависимости от задания необходимо расставить галочки. В данном задании необходимо запретить открывать приложение mspaint.exe, ранее добавленное в список приложений. Для запрета открытия приложения активируйте галочку «Запретить запуск приложений с использованием списков», для запрета открытия приложения используйте «Черные списки». В качестве списка выберите только что созданный список. Сохраните правило.

Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2: РЕШЕНИЕ

Здесь также необходимо изначально открыть приложения табличных препроцессоров. В качестве табличных препроцессоров выступают Microsoft Excel и LibreOffice Calc. Какого-то из этих приложений может не оказаться на клиентской машине – не пугайтесь, такое может произойти.

Откройте приложения, закройте их, вернитесь к консоли управления, создайте список с приложениями, и создайте правило. Назовите правило «Task2», в качестве перехватчика выберите «ScreenShot Monitor», укажите список приложений. Сохраните правило.

Правило 3

Ограничить доступ к определенным облачным хранилищам (по вариантам).

Проверить работоспособность и зафиксировать выполнение

Правило 3: РЕШЕНИЕ

Для ограничения доступа к облачным хранилищам создайте правило «Правило 3», выберите перехватчик «Cloud Storage Monitor» и отметьте радиобокс «Доступ запрещен» у тех хранилищ, которые необходимо запретить.

Правило 4

Необходимо запретить печать на сетевых принтерах. Зафиксировать создание политики скриншотом.

Правило 4: РЕШЕНИЕ

Для запрета сетевой печати, создайте правило «Правило 4» и выберите перехватчик «Device Monitor», а в качестве типа устройства выберите «Сетевой принтер». Установите радиобокс «Использование запрещено». Сохраните правило.

Правило 5

Необходимо запретить запись файлов на определенные носители информации, при этом оставить возможность считывания информации. Проверить работоспособность и зафиксировать выполнение.

Правило 5: РЕШЕНИЕ

Для запрета записи файлов на определенные носители необходимо создать правило «Правило 5», в качестве перехватчика выбрать «Device Monitor», а в качестве типа устройства выбрать те устройства, которые необходимо ограничить по заданию. Радиобокс «доступ» - «только чтение».

Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

Правило 6: РЕШЕНИЕ

Прежде чем приступать к созданию правила, подключите доверенный носитель (флешка) к виртуальной машине, относящейся к заданию. Обязательно проверьте, что она подключилась – откройте ее в «Проводнике».

Теперь, найдите в панели задач иконку агента Device Monitor, нажмите ПКМ и перейдите к параметрам, после чего найдите вкладку «Список устройств» и распознайте записи, относящиеся к вашей флешке. Одно из устройств относится к виртуальным дискам VMWare, его легко распознать – в названии присутствует «VMware». Остальные два устройства относятся к флешке, это можно по описанию – в обеих записях. Запомните, какие устройства относятся к вашей флешке – доверенному носителю.

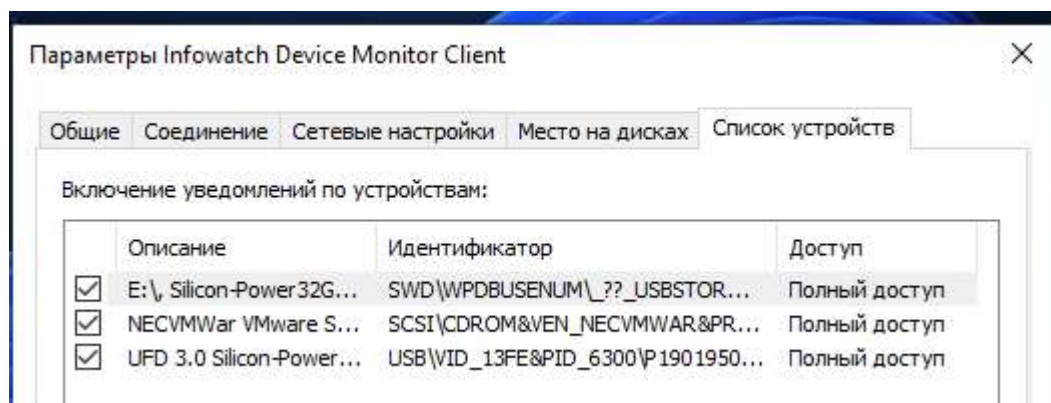


Рисунок 4 -Устройства, подключенные к ОС

Для создания такого рода правила необходимо перейти ко вкладке «Белые списки», после чего нажать кнопку «Создать белый список». В нижней части интерфейса выберите фильтр «группы компьютеров», а затем выберите ту группу компьютеров, к которой будет относиться правило, по заданию. Теперь нажмите кнопку «Найти...» в правой части интерфейса и выберите те устройства, которые относятся к вашему доверенному носителю.

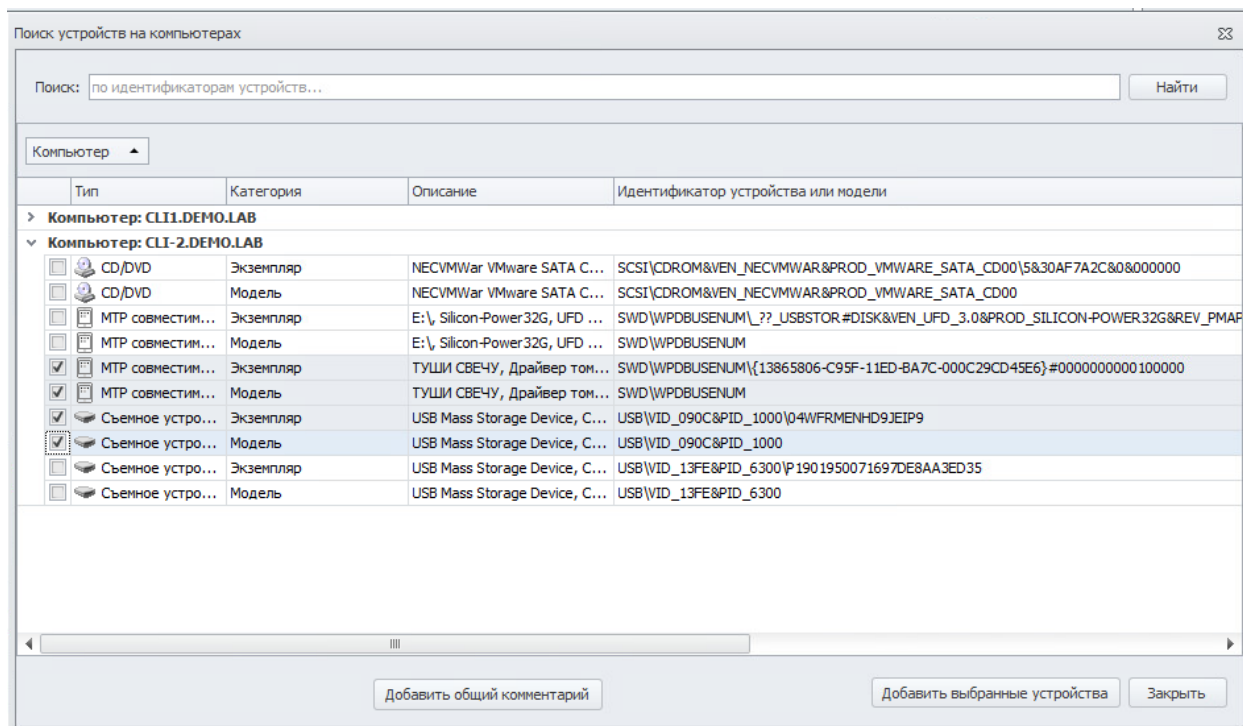


Рисунок 5 -Поиск устройств на ПК

После выбора устройств нажмите «Добавить выбранные устройства», после чего все должно выглядеть примерно так: как на рисунке 6.

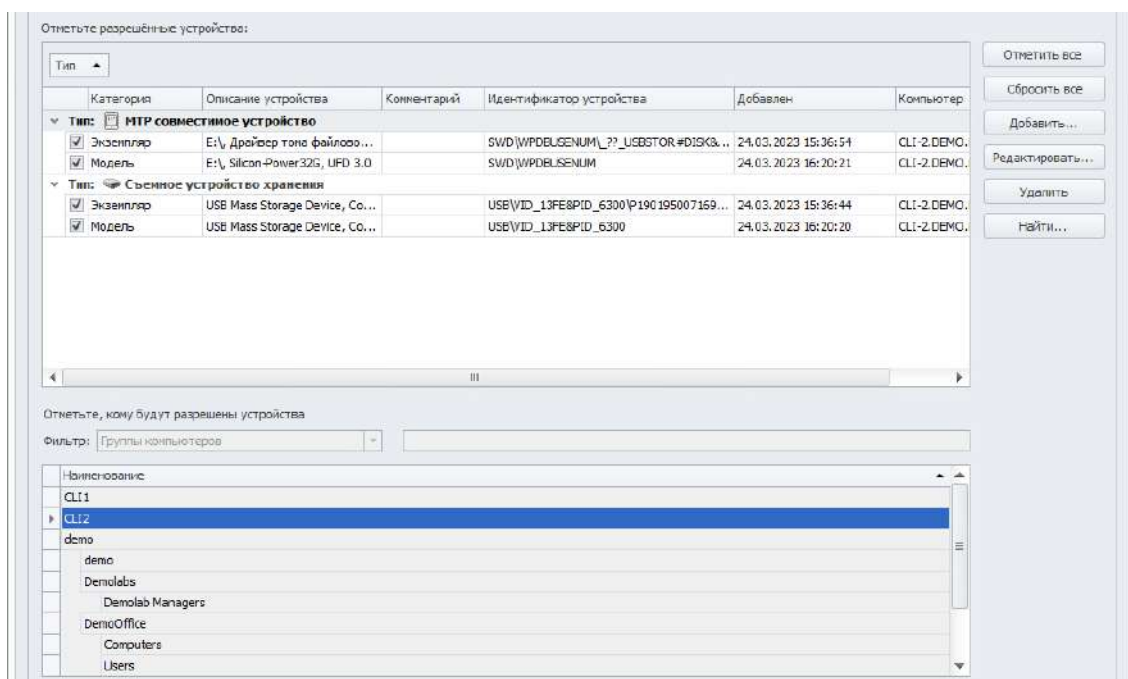


Рисунок 6 – Белый список

Теперь, можно считать, что правило применено и работоспособно.

Правило 7

Полностью запретить использование определенного устройства для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 7: РЕШЕНИЕ

Здесь правило аналогичное с предыдущим. Необходимо подключить «определенное устройство» к ПК по заданию, затем создать белый список, но в качестве фильтра выбрать «Сотрудники» и выбрать сотрудника, указанного по заданию. Затем продолжите действия, как в предыдущем правиле, следуя заданию. Сохраните белый список – правило применится.

Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для определенного устройства не определенное время для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Правило 8: РЕШЕНИЕ

С учетом ранее выполненного запрета, перейдите к виртуальной машине, относящейся к заданию, и найдите в панели задач, в трее, иконку агента Device Monitor. Перейдите ко вкладке «Список устройств», найдите устройство со статусом «заблокировано», выберите его и нажмите кнопку «Запросить доступ», которая располагается в нижнем левом углу.

Откроется окно «Временный доступ к устройству», выберите радиобокс «получение доступа к устройству по телефону».

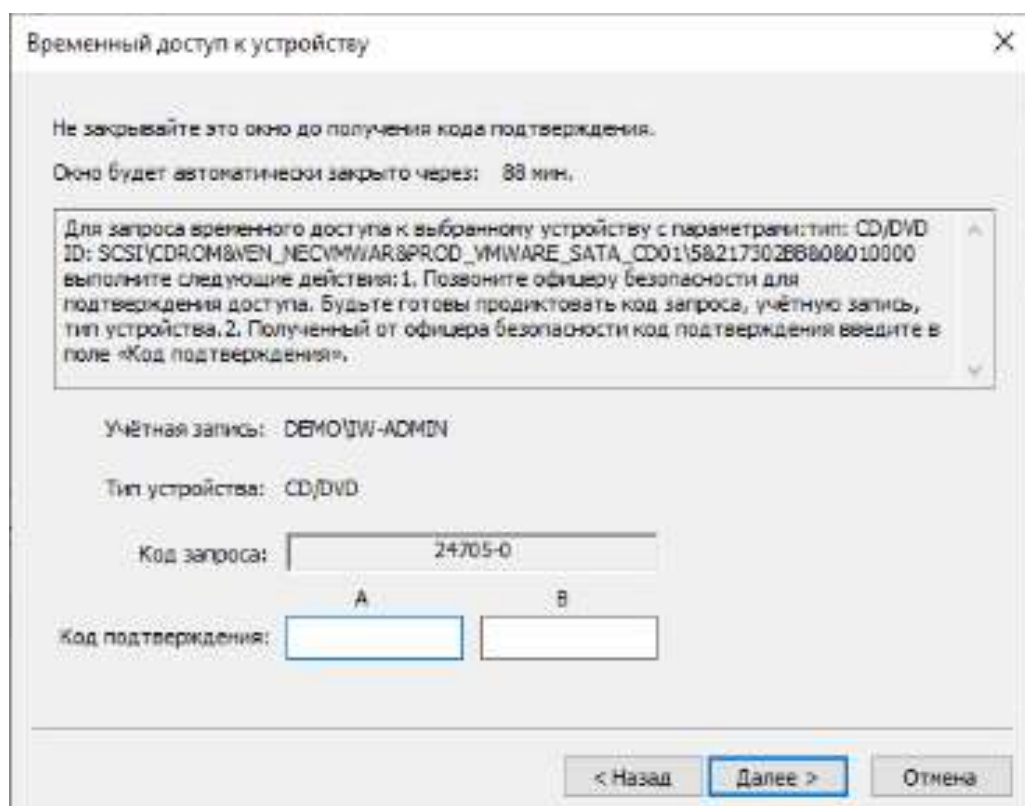


Рисунок 7 – Временный доступ к устройству

Запомните код запроса, затем перейдите к виртуальной машине IWDM, откройте консоль управления Device Monitor, перейдите ко вкладке «Инструменты» и нажмите «Временный доступ сотрудника».

Отметьте радиобокс «Продиктован по телефону (цифровой код запроса)», затем перейдите к следующему этапу. Доступ необходимо предоставить «к устройству». На следующем этапе введите параметры:

- учетную запись – по заданию;
- тип устройства – по заданию;
- код запроса необходимо ввести из окна, с которым вы взаимодействовали на виртуальной машине нарушителя. Пример кода представлен на рисунке 7;
- время доступа.



Рисунок 8 – Настройки временного доступа

Нажмите «Далее» и вы получите код подтверждения для сотрудника – его нужно ввести на виртуальной машине нарушителя.

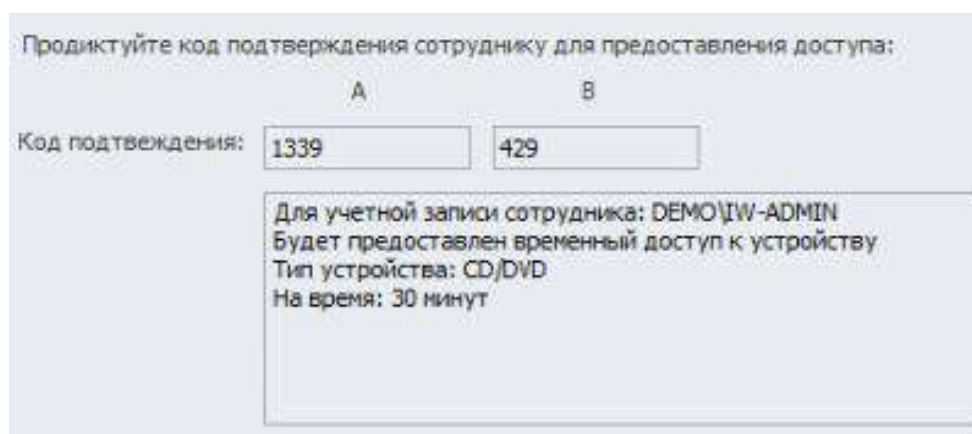


Рисунок 9 – Код подтверждения для сотрудника

На виртуальной машине нарушителя в поле «код подтверждения» введите полученный в консоли управления код

Временный доступ к устройству

Не закрывайте это окно до получения кода подтверждения.

Окно будет автоматически закрыто через: 70 мин.

Для запроса временного доступа к выбранному устройству с параметрами: тип: CD/DVD
ID: SCSI\CDROM\VEN_NECVMWARE&PROD_VMWARE_SATA_CD01\5&217302BB&0&010000
выполните следующие действия: 1. Позвоните офицеру безопасности для подтверждения доступа. Будьте готовы продиктовать код запроса, учётную запись, тип устройства. 2. Полученный от офицера безопасности код подтверждения введите в поле «Код подтверждения».

Учётная запись: DEMO\JW-ADMIN

Тип устройства: CD/DVD

Код запроса: 24705-0

Код подтверждения: A B
48662 380

Рисунок 10 – Подтверждение доступа к устройству

Если все сработает, вы получите следующее сообщение:

Вам предоставлен временный доступ к устройству:

Тип устройства: CD/DVD
ID устройства: SCSI\CDROM\VEN_NECVMWARE&PROD_VMWARE_SATA_CD01\5&217302BB&0&01
Период действия: 30 минут

Рисунок 11 – Сообщение об успешном разрешении

Вы выполнили задание.

Задача 4: разработать правила агентского мониторинга. Следующие правила создаются в политике «Test2».

Правило 9

Необходимо поставить на контроль буфер обмена в блокноте и notepad++. Проверить занесение нескольких событий в WEB-консоль. Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 9: РЕШЕНИЕ

Здесь необходимо сначала открыть приложение notepad++ на виртуальной машине нарушителя и занести его в список приложений. Создать правило «Правило 9» во второй политике, в качестве перехватчика выбирайте «Clipboard Monitor». В разделе «Перехватывать вставку из буфера обмена» выберите «В приложения кроме терминальных сессий», укажите только что созданный список.

Правило 10

Необходимо запретить использовать терминальные сессии для пользователя. Проверить работоспособность и зафиксировать выполнение

Правило 10:

Для открытия терминальных сессий используется приложение `mstsc.exe`. Используйте стандартный алгоритм запрета использования приложения. Открыть приложение, добавить в список, создать правило, запретить использование.

Правило 11

Необходимо установить контроль за компьютером потенциального нарушителя путем создания снимков экрана каждые 60 секунд или при смене окна.

Проверить работоспособность и зафиксировать выполнение

Правило 11: РЕШЕНИЕ

Нужно создать правило «Правило 11», установить перехватчик «ScreenShot Monitor». Настройки следующие: «Всегда», 60 сек.

Правило 12

Запретить передачу файлов определенного типа на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

Правило 12: РЕШЕНИЕ

Создать правило «Правило 12», перехватчик – «File Monitor». Тип приемника – в соответствии с заданием, в поле «маска файла» вписать маску указанных к запрету файлов.

Если сказано запретить исполняемые файлы, в качестве маски файлов указывается «*.exe,*.msi». Дополнительно стоит указать соответствующую категорию файлов в поле «Категория файла».

Задача 5: разработать и применить групповые политики домена.

Групповые применяются только на компьютер 2, должны быть созданы в домене. Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля, Минимальная длина пароля, Сложность пароля, Блокировка учетной записи при неверном вводе пароля.

Зафиксировать настройки политики скриншотами.

Групповая политика 1: РЕШЕНИЕ

Создайте групповую политику:

- Фильтры безопасности: «Пользователи домена» (Domain Users), «Компьютеры домена» (Domain Computers);
- Путь: «Конфигурация компьютера – Политики – Конфигурация Windows – Параметры безопасности – Политики учетных записей – Политика паролей»

Далее конфигурируйте политики, в соответствии с заданием.

Групповая политика 2

Запретить запуск приложений по списку (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами

Групповая политика 2: РЕШЕНИЕ

Создайте групповую политику:

- Фильтры безопасности: «Пользователи домена» (Domain Users), «Компьютеры домена» (Domain Computers);

Путь: «Конфигурация пользователя — Административные шаблоны — Система – Не запускать указанные приложения Windows»

Укажите те приложения, которые хотите ограничить.

Групповая политика 3

Запретить использование элементов системы стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3: РЕШЕНИЕ

Тут может попасться задание на запрет использования, например, панели управления.

Тут легче всего загуглить.

Вот, например, запрет использования панели управления:

<https://www.bezpk.ru/blog/item/kak-zapretit-dostup-k-paneli-upravleniya/>

Групповая политика 4

Запретить пользователю самостоятельно менять параметры системы (по вариантам задания). Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4: РЕШЕНИЕ

Тут тоже проще всего загуглить.

Групповая политика 5

Настроить дополнительные параметры системы, которые должны применяться для пользователя или компьютера (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5: РЕШЕНИЕ

Гуглите.