

Региональный этап чемпионата по
профессиональному мастерству «Профессионалы» и
чемпионата высоких технологий Республики
Башкортостан

по компетенции:

F7 «Корпоративная защита от внутренних угроз
информационной безопасности»

Конкурсное задание

День 1

Модуль А. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Описание

Вы работаете инженером в центре информационной безопасности (департамент проектирования и внедрения) интегратора DEMO Lab.

Вам поручили собрать демонстрационный стенд в отдельной «песочнице» и развернуть DLP-систему на отдельном сегменте сети.

В «песочнице» развернут контроллер домена (с каталогом AD), с которым необходимо будет осуществить интеграцию DLP-системы. До установки системы необходимо подготовить доменных пользователей.

В качестве виртуальной инфраструктуры для пилотного проекта используется среда виртуализации VMware Workstation.

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM). Необходимо развернуть компоненты уровня сети (network) и хоста (endpoint). Вам необходимо установить и настроить компоненты DLP-системы в соответствии с выданным заданием.

Необходимо использовать следующие виртуальные машины:

- ☐ **AD-Demo.lab** (контроллер домена demo.lab)
- ☐ **Astra TM** (предустановленный, необходимо настроить)
- ☐ **WSRV-IWDM** (Windows Server для IWDM)
- ☐ **W10-agent-1** (ПК первого нарушителя)
- ☐ **AstraClient** (ПК второго нарушителя)

Сетевые настройки вирт. машин указаны в *дополнительной карточке заданий*.

Сетевые адаптеры на виртуальных машинах необходимо настроить самостоятельно!

Основными каналами потенциальной утечки данных являются носители информации, электронная почта и различные интернет-ресурсы.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах.

Если в задании необходимо сделать скриншот, необходимо называть его по номеру задания, согласно примера: Задание_5_копирование.jpg.

Задание 1: Подготовка Active Directory (AD)

Для дальнейших работ в AD необходимо создать подразделение организации (Organization Unit) под названием «**RCOffice**», добавить в него новые каталоги пользователей и компьютеров (Users и Computers). В каталог Users требуется добавить следующих пользователей:

- **iwdm-ad** (права доменного администратора), пользователь для машины IWDM-NODE и консоли IWDM
- **dbadmin** (права доменного администратора, для WSRV-IWDM и консоли IWDM)
- **user1** (1 машина W10, права пользователя домена, W10-cli)
- **user2** (2 машина Astra, права пользователя домена, Astra-Cli)
- **user-ldapsync** (права пользователя домена), пользователь для осуществления LDAP-синхронизации
- **tmoff** (права пользователя домена), пользователь для входа в веб-консоль IWTM

Допускается создание дополнительных подразделений внутри указанных для удобства работы (например, для групповых политик).

Для всех пользователей необходимо задать пароль ххХХ1243

Стоит учесть, что после ввода в домен, компьютеры необходимо переносить в ранее созданный каталог Computers (внутри OU «RCOffice»)

В соответствии с политикой компании для обеспечения безопасности компьютеров брандмауэр должен быть активен. Для установки компонентов системы необходимо настроить правила брандмауэра с помощью групповых политик домена.

Ввести в домен все вышеуказанные серверные и пользовательские машины (в т. ч. **Astra-Cli**).

Задание 2: Настройка IWTM

1. Настройте LDAP-синхронизацию для IWTM с помощью пользователя **user-ldapsync**.
2. Для работы с консолью IWTM настройте дополнительного доменного пользователя **tmoff** (задать все встроенные роли (officer и administrator) и все области видимости), но управление продолжить от пользователя **officer**.

Задание 3: Развертывание DLP уровня хоста. InfoWatch Device Monitor

В соответствии с Вашей частью пилотного проекта на отдельном сегменте сети «песочницы» Заказчика необходимо развернуть следующие компоненты InfoWatch Device Monitor (IWDM):

1. БД PostgreSQL;
2. Основной Сервер и Консоль управления.
3. Агенты IWDM на машины «нарушителей»

Ваша задача — установить указанные компоненты IWDM на виртуальные машины. Вход в систему необходимо осуществить от ранее созданных (см. задание №1)

доменных пользователей.

- ☐ Установить базу данных PostgreSQL на машину **WSRV-IWDM**.
- ☐ Установить Device Monitor Server и консоль управления на машину **WSRV-**

IWDM. Сервер необходимо подключить к ранее установленной базе данных. Управление сервером осуществляется с локальной консоли Device Monitor.

- ☐ Установить дополнительную консоль управления на машину **AD-Demo.lab**.
- ☐ Установить **InfoWatch Device Monitor Client** на ПК пользователей путем:

о удаленного распространения через задачи в Device Monitor на виртуальную машину AstraClient,

о групповых политик на виртуальную машину W10-agent-1.

Осуществите интеграцию сервера безопасности IWDM с Active Directory от пользователя **user-ldapsync**, созданного ранее. Необходимо синхронизировать каталог компьютеров и пользователей.

При работе IWDM брандмауэр должен быть активен. Выключение брандмауэра приводит к снижению оценки.

Задание 4: Развертывание InfoWatch Crawler

Для контроля общих сетевых ресурсов в организации необходимо развернуть следующие сетевые компоненты InfoWatch Traffic Monitor на машину WSRV-IWDM: Crawler Server и Crawler Scanner

После установки InfoWatch Crawler необходимо создать задачу на ежедневное сканирование сетевых ресурсов. Предварительно требуется создать общую сетевую папку на виртуальной машине WSRV-IWDM: «RC_share_iwdm» с правами чтения и записи

для всех пользователей домена

Зафиксировать скриншотом работоспособность краулера и задач, проверить сработку на любой файл и любую политику.

Задание 5: Базовая проверочная политика

Необходимо создать новую или использовать имеющуюся политику на проверку установленной системы. Наименование политики «Чемпионат1» Политику необходимо проверить!

Политика должна работать на все возможные события: Правило передачи, копирования, буфера обмена (или работы в приложениях), а также хранения.

В качестве объекта защиты необходимо контролировать передачу текста: **Первая настройка системы произведена успешно!** Установить низкий уровень угрозы для всех событий, добавить тег «Чемпионат». Все объекты, технологии и т. п., связанные с данной политикой, называйте «Чемпионат, Чемпионат 1» и т. д. Необходимо создать запрос, выводящий информацию только о четырех событиях разных типов (передача, копирование, хранение и буфер обмена), по одному событию на каждый тип

Важно учитывать морфологию и возможную замену букв на латинский алфавит.

Модуль Д. Технологии агентского мониторинга

Задание 1. Групповые политики:

Зафиксируйте все этапы настройки, создания и выполнения (срабатывание, где возможно) всех групповых политик скриншотами!

Групповая политика 1:

- ☐ Минимальная длина пароля должна составлять 9 символов;
- ☐ Срок жизни пароля должен составлять 10 дней.
- ☐ Количество сохраненных паролей: 1

Выполнение заданий подтвердить скриншотами.

Групповая политика 2:

- ☐ Отключить возможность локального входа для пользователей **tmoff** и **user-ldapsync** с помощью групповых политик;

Выполнение задания подтвердить скриншотами.

Следующие политики необходимо применить **только для Windows 10 клиентов** для OU «RCOffice»:

Групповая политика 3:

С помощью редактора групповой политики запретить доступ к редактору реестра и диспетчеру задач. Выполнение задания подтвердить скриншотами.

Групповая политика 4:

Создайте групповую политику для отображения текстового сообщения пользователям после входа в Windows с содержанием «**РЧ 2023!**»

Групповая политика 5:

В связи с удаленной работой сотрудников, подключающихся по RDP и случайно выключающих компьютер, необходимо запретить выключение, спящий режим и перезагрузку компьютера из интерфейса Windows.

Групповая политика 6:

Задать Обязательный (Mandatory) профиль для пользователя **user-cli2**. Эталонный профиль можно сформировать с любого пользователя.

Групповая политика 7:

Установить фон рабочего стола с логотипом «RC2023» на всех клиентских машинах домена с помощью групповых политик. Фон необходимо разработать самостоятельно.

Групповая политика 8:

Для упрощения коммуникации между отделами требуется осуществить добавление сетевого диска (папки, созданной ранее для краулера) общего доступа с помощью групповых политик Windows в AD с автоматическим подключением при загрузке системы.

Задание 2, политики AstraLinux:

Зафиксируйте все этапы настройки, создания и выполнения (срабатывание, где возможно) всех политик скриншотами!

Политика 1:

Создать локальную политику паролей для AstraClient графическими средствами fly-admin для локальных пользователей:

- ☐ Минимальная длина пароля должна составлять 9 символов;
- ☐ Срок жизни пароля должен составлять 10 дней.
- ☐ Максимальное количество неудачных попыток входа: 3.

Политика 2

Разрешить использовать только доверенный USB-носитель.

Выполнение зафиксировать скриншотом.

Политика 3

Разрешить выключать компьютер локально и удалённо только администратору.

Выполнение и реализацию зафиксировать скриншотом

Политика 4

Создать пользователя **astraKiosk**. Настроить режим графического киоска сопредельным приложением (ХСА) для определенной группы пользователя.

Выполнение зафиксировать скриншотом

Задание 3, настройка IWDM

- Используйте для входа в консоль IWDM доменного пользователя *iwdm-ad*, в т. ч. для входа в консоль без пароля (галочкой). Задать максимальные права данного пользователя на работу в консоли IWDM.

Проверить работоспособность, зафиксировать настройку и выполнение

скриншотом запущенной консоли.

- Необходимо создать и выполнить задачу IWDM создания пароля для деинсталляции для машин, к которым это применимо. Пароль: xxXX1122

Задание 4, политики IWDM

Необходимо создать новые политики IWDM:

Политика 1:

Название: «Отдел 1», группа компьютеров: машина пользователя **user-cli1**

Политика 2:

Название: «Отдел 2», группа компьютеров: машина пользователя **user-cli2**

Правила для Отдела 1:

Правило 1

Необходимо запретить создание снимков экрана в граф. редакторах (Paint3D и Paint) и калькуляторе для предотвращения утечки данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них. ***Проверить работоспособность и зафиксировать выполнение скриншотом.***

Правило 3

С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.

Проверить работоспособность и зафиксировать настройку скриншотами.

Правило 4

Исключить приложение calc, cmd и powershell из перехвата Device Monitor. Необходимо учесть разные версии для различных архитектур.

Зафиксировать выполнение скриншотом (окно настройки).

Правило 5

1. Заблокируйте доступ к CD/DVD для сотрудников.

2. Сотруднику из отдела 2 понадобилось воспользоваться CD/DVD, передача информации согласована с руководством и теперь вам необходимо осуществить выдачу временного доступа (на 120 минут) клиенту на использование привода. Временный доступ должен быть получен с помощью «телефона». ***Зафиксировать скриншотами выдачу доступа.***

Правило 6

Необходимо поставить на контроль буфер обмена в текстовых процессорах (Word или Writer или Wordpad).

Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики.

Правило 7

На виртуальной машине необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность попыткой копирования текста из сеанса RDP и зафиксировать выполнение скриншотом. Для работы RDP может потребоваться дополнительная настройка.

Правило 8

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера Firefox и Chrome путем создания снимков экрана каждые 60 секунд или при переходе в другое окно.

Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в консоли IWTM. Подтвердить выполнение задания скриншотами свойств пользователя со снимками экрана в IWTM.

Правило 9

Создать политику по блокировке копирования исполняемых exe-файлов на USB-накопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик IWTM.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 11

Для предотвращения неэффективного расхода рабочего времени сотрудников отслеживать движение видео контента (*.avi, *.mov, *.mp4) в общих папках компании. Контролировать файлы больше 8 Мбайт и меньше 500 Мбайт. (1 Мбайт = 1024 Кбайт) **средствами IWDМ.**

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 12

Необходимо запретить пользоваться Microsoft Paint, а также Paint 3D (при наличии), так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом

Правила для Отдела 2:

Правило 13

В связи с небезопасностью ftp-серверов разрешить только скачивание по протоколу ftp, загрузку файлов на сервер запретить.

Проверить работоспособность на любом доступном файловом сервере и зафиксировать выполнение скриншотом.

Правило 14

Необходимо запретить использовать облачные хранилища dropbox и google drive, разрешить только скачивание с Yandex disk, остальные сервисы оставить открытыми. ***Проверить работоспособность запрета.***

Правило 15

1. Необходимо отслеживать копирование всех файлов на USB-накопители.
2. Запретить копирование файлов в ранее созданную общую папку краулера

Проверить работоспособность с помощью любой политики IWTМ и зафиксировать выполнение скриншотами.

Модуль В: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Создайте в системе InfoWatch Traffic Monitor политики безопасности согласно нижеперечисленным заданиям.

- Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.
- Для некоторых политик необходима работа с разными разделами консоли управления ТМ: категориями и терминами, технологиями, объектами защиты и т. п.
- При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием.
- Списки сотрудников, занимаемые позиции и отделы сотрудников (HR, Accounting и др.) представлены в разделе «Персоны» Infowatch Traffic Monitor по результатам LDAP-синхронизации с AD-сервером компании
- После создания всех политик будет запущен автоматический «генератор трафика», который передаст на InfoWatch Traffic Monitor поток данных, содержащих как утечки, так и легальную информацию.
- При правильной настройке политики InfoWatch Traffic Monitor должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний, т. к. легальные события не должны маркироваться. Должны быть выявлены все инциденты безопасности.
- Необходимо пользоваться объектами защиты.

ВНИМАНИЕ! Необходимо называть политики/объекты/категории/тэги и т. п. ТОЛЬКО в соответствии с номером и названием задания:

Политики — Политика XX, например «Политика 5». Для комбинированных политик формат: **Политика 5.1, Политика 5.2 и т. д.**
Объект защиты — Объект и XX, например «Объект 11».

Ошибки в названиях приводят к снижению баллов или даже к невозможности проверки. При выполнении задания учитывайте, что совместно с созданными могут срабатывать стандартные политики, что необходимо предотвратить.

ВНИМАНИЕ! ВСЕ политики «по-умолчанию», находящиеся в IWTM на момент старта соревнований, должны быть отключены или удалены.

Список тегов для политик: Политика 1, Политика 2, ..., Политика 17

Задание 1

Необходимо настроить доступ к системе пользователя auditor с правами просмотра отчетов и созданных политик, без возможности что-то изменять. Пароль задать xxXX1234.

Задание 2

Необходимо активировать и настроить технологию OCR Google Tesseract в системе как минимум на веб-сообщения и электронную почту. Некоторые политики могут проверяться с использованием данной технологии (указано отдельно).

Проверить работоспособность на любую политику — должен срабатывать перехватчик на изображение с текстом.

Задание 3

Создайте список веб-ресурсов и назовите его «Сайты партнеров». Туда необходимо включить следующие веб-ресурсы:

esim.firpo.ru, dp.firpo.ru, infotecs.ru

Задание 4

Для правильной работы системы необходимо настроить периметр компании: Домен: demo.lab.

Список веб ресурсов: Сайты партнеровГруппа

персон: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Политика 1

У генерального директора компании недавно появился пес и его фото утекло в сеть компании. Теперь сотрудники обмениваются испорченной картинкой внутри компании и выкладывают их в социальные сети. Директор решил, что его пес вызвал снижение качества работы сотрудников и хочет запретить обмен фотографией пса. Необходимо запретить обмен испорченной фотографией и немного измененной фотографией пса (до ≈50%) как внутри компании, так и за ее пределы. Фотография есть в дополнительных данных.

Вердикт: Заблокировать ×

Уровень нарушения: низкий •

Тег: Политика 1

Политика 2

В последнее время бюджет компании стал резко падать. Подозрения пали на начальника отдела кадров, директор подозревает его в проведении денежных средств «мимо кассы». В связи с этим необходимо отслеживать передачу всех номеров и сканов кредитных карт, отправляемых им.

Вердикт: Заблокировать ✕

Уровень нарушения: высокий •

Тег: Политика 2

Политика 3

В связи с санкциями и растущим курсом валют, компания ООО Demo Lab решила перейти на отечественные решения. Не все сотрудники поддерживают данное решение, поэтому необходимо перехватывать и запрещать отправку данных на сайты запрещенных в РФ организаций facebook.com, twitter.com, whatsapp.com; запретить отправку данных за пределы компании, содержащую информацию о «железе» и ПО — упоминания AMD, Intel, Байкал, Эльбрус, МСТ, Astra, Астра Linux, RedOS в любом регистре.

Проверку проводить при отправке на почтовые домены.

Вердикт: Заблокировать ✕

Уровень нарушения: высокий •

Тег: Политика 3

Политика 4

Дочерняя компания «ООО Повозка» занимается транспортировкой грузов в разные города. Каждому рейсу присваивается уникальный идентификационный номер по следующему шаблону «3-4 буквы (латиница, любой регистр) - (знак дефиса) номер груза (с ведущими нулями от 0000 до 1000, исключая следующие номера: 0777 и 0013) . (точка) от 1 до 3 букв (кириллица, верхний регистр) Например: jDRC-0003.Л, kSR-0665.ЪГА, jHy-0920.ЩЗ Не должно быть срабатывания на следующие номера грузов (например: kdO-0013.ю или jtfd-0777.ШАП). Необходимо контролировать передачу, а также

копирование на съемные носители и печать вышеуказанных данных. Проверить работоспособность. Учтите, что особо обобщенные регулярные выражения лучше разделить на несколько текстовых объектов для оптимизации поиска.

Вердикт: Разрешить **Ö** **Уровень**

нарушения: средний • **Тег:**

Политика 4

Политика 5

Необходимо создать политики для отслеживания документов (передача и копирование), содержащих договор компании (договор компании.doc).

Политики должны работать следующим образом (за периметр компании):

1. Если передается только договор компании (шаблон и заполненный шаблон, до 25% изменений) – разрешать, уровень низкий, тег «Политика 5.1».
2. Если передается договор компании, в котором присутствует фамилия генерального директора, а также нач. отдела кадров – разрешать, уровень средний, тег «Политика 5.2». Политика не должна срабатывать, если в документе только фамилия директора или только фамилия бухгалтера.
3. Если передается договор компании, в котором присутствует фамилия генерального директора, нач. отдела кадров, а также стоит печать компании (ООО Повозка) – разрешить, уровень высокий, тег «Политика 5.3».

Проверить работоспособность. Политики не должны срабатывать внутри компании, только при передаче за периметр.

Все политики, объекты и прочие элементы должны называться в соответствии с номерами (например Объект 5.1, Политика 5.2, Технология 5.3 и т. д.)

Вердикт 1: Разрешить **Ö** **Уровень**

нарушения 1: низкий • **Тег 1:**

Политика 5.1

Вердикт 2: Разрешить **Ö** **Уровень**

нарушения 2: средний • **Тег 2:**

Политика 5.2

Вердикт 3: Заблокировать **×** **Уровень**

нарушения 3: высокий • **Тег 3:**

Политика 5.3

Политика 6

Стало известно, что сотрудники отдела IT (IT) ООО «Повозка» за определенную сумму пропускают автомобили из близлежащих домов на служебную парковку. В связи с ужесточением корпоративной политики в компании, правом въезда на территорию обладает только генеральный директор.

Сотрудники охраны ведут журнал учета автомобилей в электронном виде и обмениваются между собой данными о припаркованных автомобилях.

Необходимо детектировать и блокировать номера всех автомобилей, которые незаконно парковались на частной территории компании ООО «Повозка», исключая номер автомобиля генерального директора K777OB15.

Буквы, используемые в автомобильных номерах:

А, В, Е, К, М, Н, О, Р, С, Т, У, Х (Верхний регистр) Цифры,

используемые в автомобильных номерах:

000 – 999

Регионы автомобильных номеров, подлежащие детектированию: 15, 02,

102, 74, 174, 66, 96, 196

Вердикт: заблокировать ✕

Уровень нарушения: Высокий •

Тег: Политика 6

Политика 7

В честь юбилея компании была запущена акция с промокодами на скидку в 70% на перевозки для постоянных клиентов. По условиям акции промокод выдается только по запросу постоянного клиента. Есть вероятность утечки промокодов из отдела продаж, в связи с этим необходимо контролировать защитить утечку текстового документа, содержащего промокоды («коды.docx»). Стоит учесть, что сотрудники могут слить не весь файл, а один или несколько купонов. Запретить передачу данных, содержащих информацию об этих купонах.

Проверить работоспособность на все купоны и на 1-2 купона.

Вердикт: заблокировать ✕ **Уровень**

нарушения: средний • **Тег:**

Политика 7

Политика 8

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела кадров отправлять документы, содержащие информацию о СНИЛС, ИНН, паспортных данных (в текстовом и графическом виде) за пределы компании.

Данная политика должна также работать на сканированные изображения, содержащие паспортные данные в текстовом виде (OCR).

Вердикт: заблокировать ✗ **Уровень**

нарушения: средний • **Тег:**

Политика 8

Политика 9

Два месяца назад в компании DemoLab заметили, что сотрудница отдела кадров расходует в три раза больше бумаги, чем прежде, хотя объем работ не был увеличен. Путем наблюдения за сотрудницей было установлено, что она, состоя в совете колледжа, регулярно собирает деньги с родителей за печать докладов и рефератов студентов групп, бесплатно распечатывая их в компании.

Необходимо создать политику безопасности, которая будет включать слова (с учетом морфологии): «файл», «доклад», «студент», «колледж», «куратор».

Проверку необходимо проверить путем отправки документа на печать и при помощи электронной почты.

Вердикт: Заблокировать ✗

Уровень нарушения: низкий •

Тег: Политика 9

Политика 10

В последнее время сотрудники стали чаще обсуждать популярные сериалы в мессенджерах и социальных сетях, из-за чего упала общая производительность на 10%. Было решено отследить, кто больше всего занимается не рабочей деятельностью, для чего необходимо создать политику для отслеживания 5 (пяти) популярных на данный момент сериалов при передаче через веб-сообщения и почту. Список: Wensday, Вампиры средней полосы, Клиника, Supernatural

Вердикт: разрешить ✓

Уровень нарушения: низкий •

Тег: Политика 10

Политика 11

Оказалось, что сотрудники не только обсуждают сериалы, а еще и обмениваются ссылками и torrent-файлами для их скачивания, после чего скачивают их, используя интернет-канал компании или обмениваются скачанным материалом внутри компании, что также нагружает сеть и заполняет ненужными данными локальные диски пользователей.

В связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов формата .torrent и ссылок формата magnet: (и содержащей urn (хеш) файла). Ложных срабатываний просто на слово Magnet (в т. ч. с двоеточием) быть не должно. Стоит учесть, что magnet-ссылки могут передаваться в том числе через буфер обмена в пределах браузера Google Chrome. Вышеуказанными данными сотрудники могут обмениваться не только внутри компании.

Для торрент-файлов:

Вердикт 1: Заблокировать ✖

Уровень нарушения 1: средний •

Тег 1: Политика 11.1

Для торрент-ссылок:

Вердикт 2: Разрешить ☐

Уровень нарушения 2: средний •

Тег 2: Политика 11.2

Политика 12

Компания-партнёр ООО «Рога» занимается разработкой технических чертежей. Необходимо запретить передачу за периметр компании

У каждого чертежа есть уникальный номер, состоящий из:

Первые 3 буквы латиница верхний регистр кроме E, D и F после идет “-“ номер от 0001 до 5000 после “+” 3 буквы кириллица или латиница верхний регистр. Если идут 3 буквы кириллица: “-“ и 3 цифры. Если латиница: “/” и 2 цифры.

Исключить серию номеров от 4 300 до 4 450 включительно. Должны срабатывать на ART-0096+ASD/66 VBN-1386+BAЧ-345 Не должны срабатывать на AET-0096+ASD/66 VBN-1386+BAЧ/34

Вердикт: Заблокировать ✖ **Уровень**

нарушения: средний • **Тег:**

Политика 12

Политика 13

У директора компании скоро юбилей и сотрудники решили его поздравить, сделав коллаж из его фотографий. Для того чтобы данное поздравление не попало к директору раньше срока, необходимо контролировать передачу фотографий директора, как внутри компании, так и за его пределами. Критичным является минимум 20% -ное совпадение передаваемого фото.

Вердикт: разрешить ✓ **Уровень**

нарушения: низкий • **Тег:**

Политика 13

Политика 14

Для мониторинга движения анкет необходимо вести наблюдение за заполненными анкетами с печатью компании за пределы компании, запрещая любую внешнюю передачу документов, содержащих печать компании в пустых и заполненных бланках «анкета участника.doc».

При этом пустые и заполненные анкеты без печати или просто печать не контролировать.

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.

Печать + бланк:

Вердикт: Заблокировать ✗ **Уровень**

нарушения: средний • **Тег:**

Политика 14

Политика 15

Ракетное вооружение для авиационных комплексов различного класса, в разработке которого участвует компания в интересах МО РФ, планируется к внедрению в эксплуатацию. Утечки по данному виду продукции в настоящее время недопустимы! Информация о технике может иметь конфиденциальный и секретный характер, хотя и не содержать гриф, в силу высокого темпа работ по проекту.

Необходимо блокировать любые попытки передачи данных об этих объектах на внешние адреса. Технические объекты задаются буквенно-цифровыми кодами на русском языке:

Р-Цифры-Буквы или РЦифрыБуква или Р-ЦифрыБуква

- Р – русская буква «Р»
- Цифры – не более 4-х подряд, например 27 или 5000 (может не быть цифр)
- Буквы – от 0 до 2-х подряд, например Р-27АЭ (управляемая ракета класса

«воздух-воздух» средней дальности)

При этом после Р или дефиса обязательно должна быть хотя бы одна цифра или одна буква (Т.е. не должно быть срабатываний на просто «Р» или «Р-»).

Вердикт: разрешить ✗

Уровень нарушения: Высокий •

Отправить уведомление: офицеру безопасности

Тег: Политика 15

Политика 16

При переезде в новый просторный офис, компанией ООО Demo Lab был расширен штат сотрудников – было решено взять несколько десятков выпускников технических вузов на стажировку. Для того, чтобы они работали более эффективно, директор компании предложил отслеживать доступ сотрудникам, работающим в отделе ИТ, доступ к основным социальным сетям и анонимным имиджбордам – vk.com, ok.ru, t.me, dobrochan.org, ii.yakuji.moe. Контроль для тестовых целей установить за электронными письмами в эти доменные зоны.

Вердикт: разрешить ✓ **Уровень**

нарушения: средний • **Тег:**

Политика 16

Политика 17

Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний. Критичными данными в выгрузке являются телефоны, ИНН, Регистрационный номер, ОКФС, ОКВЭД и ОКОПФ и в 1 документе присутствует более 5 компаний. Для настройки используйте файл stock_members_details_catch.csv.

Вердикт: разрешить ✓ **Уровень**

нарушения: низкий • **Тег:**

Политика 17

Политика 18

Необходимо поставить на мониторинг архивы (обычные и зашифрованные), так как попытки передачи таких данных несут потенциальную опасность компрометации сервисов компании.

Проверить работоспособность.

Вердикт: разрешить ✓ **Уровень**

нарушения: средний • **Тег:**

Политика 18