Модуль 3

- 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.
- Некоторые политики должны быть созданы с нуля, некоторые могут быть сделаны путём модификации существующих в системе.
- Для некоторых политик необходима работа с разными разделами консоли управления ТМ: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.
- При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, участник должен самостоятельно задать уровень угрозы при разработке политики).
- 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 как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.
- **Внимание! Необходимо называть политики/объекты/категории и прочие объекты в соответствии с номером и названием задания, например «Задание 1», «Политика 4», «Политика 10», «Объект 1». Без верно названных объектов проверка вашего задания может стать невозможной. При выполнении задания учитывайте, что совместно с созданными могут срабатывать стандартные политики, что необходимо предотвратить.**
- В комплексных заданиях необходимо пользоваться объектами защиты.

- Задания можно выполнять в любом порядке.
- Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.
- Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.
- Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.
- Все скриншоты необходимо сохранить на рабочем столе RDP машины в папке «Модуль 3».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: **CP-1.jpg**

где CP – сокращение от англ. creating a policy,
1 – номер задания

Пример 2 для сохранения скриншота работающей политики: **PW-1.jpg**

где PW – сокращение от англ. policy work,
1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:
PW-1-2.jpg

где PW – сокращение от англ. policy work,
1 – номер задания;
2 – номер скриншота для задания 1.

! ***При проверке политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга (для проверки сработки политик). Необходимо учитывать данное условие при разработке и проверке политик.***

Задание 1

Создайте локальную группу пользователей «Пристальное наблюдение» в Traffic Monitor. Добавьте в нее пользователя домена виртуальной клиентской машины.
Подтвердите выполнение задания скриншотами.

Задание 2

Для работы системы необходимо настроить периметр компании:

- Почтовый домен: demo.lab.
- Список веб ресурсов (необходимо создать новый список ресурсов, назвав его «Доверенные домены»): worldskills.moscow, worldskills.ru, mezhvuz.ru.
  Необходимо создать новый список ресурсов, назвав его «Доверенные домены».
- Группа персон: пользователи домена.
- Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 3

Для недавно нанятого аудитора компании необходимо создать пользователя системы IWTM с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей.
Логин: auditor, пароль: xxXX1234
Подтвердите выполнение задания скриншотами настройки прав пользователя.

Политика 4

В связи с постоянными проблемами при организации очередного чемпионата WorldSkills (Корпоративный Чемпионат), совет директоров решил контролировать передачу информации о WorldSkills и межвузовском чемпионате за пределы компании. В связи с этим необходимо создать политику в InfoWatch Traffic Monitor на правило передачи текстовых данных за пределы компании (на адрес вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills», «МежВуз» и «MezhVuz».
Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять или не стоять пробел между словами, например:

«Ворлд Skills», «Меж Vuz». Ложных срабатываний быть не должно (например, просто на Меж или Skills).

Вердикт: разрешить √ Уровень нарушения: низкий • Тег: Политика 4

Политика 5

Для мониторинга движения анкет необходимо вести наблюдение за анкетами с печатью компании за пределы компании, запрещая любую внешнюю передачу документов, содержащих печать компании в пустых и заполненных бланках «анкета участника.docx», при этом бланки без печати или просто печать не контролировать.
Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.

Печать + бланк:
Вердикт: запретить × Уровень нарушения: средний • Тег: Политика 5

Политика 6

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа (шаблон — «Договор компании.doc») за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 30%.
Пустой документ:
Вердикт: разрешить √ Уровень нарушения: низкий • Тег: Политика 6

Документ с фамилией генерального директора:
Вердикт: разрешить √ Уровень нарушения: средний • Тег: Политика 6

Документ с фамилией генерального директора и печатью компании:
Вердикт: запретить × Уровень нарушения: высокий • Тег: Политика 6

Политика 7

В честь юбилея компании была запущена акция с промокодами на скидку в 50% на перевозки для постоянных клиентов. По условиям акции промокод выдается только по запросу постоянного клиента. Есть вероятность утечки промокодов, в связи с этим необходимо контролировать защитить утечку текстового документа, содержащего промокоды («промокоды.docx»).
Стоит учесть, что передаваться может не целый файл, а **один или несколько** купонов.

Отдел продаж может пересылать данную информацию совершенно свободно.

Вердикт: запретить × Уровень нарушения: средний • Тег: Политика 7

Политика 8

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика (до ≈50%) как внутри компании, так и за ее пределы. Фотография котика есть в дополнительных данных.

Вердикт: запретить × Уровень нарушения: низкий • Тег: Политика 8

Политика 9

Дочерняя компания «ООО Повозка» занимается транспортировкой грузов в разные города. Каждому рейсу присваивается уникальный идентификационный номер по следующему шаблону «4 буквы (латиница, любой регистр) - (знак дефиса) номер груза (от 0 до 1000, исключая несчастливые номера: 666 и 13) . (точка) 2 буквы (кириллица, верхний регистр)
Например: jDat-123.УЛ , kdSU-665.ЪЩ
Не должно быть срабатывания на несчастливые номера грузов (например: kTdO-666.Д или jfUd-13.ЮШ).
Необходимо контролировать передачу, а также копирование на съемные носители вышеуказанных данных всем, кроме отдела договоров.
Вердикт: разрешить √ Уровень нарушения: средний • Тег: политика 9

Политика 10

Всем сотрудникам кроме сотрудников и руководителей отдела кадров запрещено отправлять паспортные данные РФ в любом виде (текст, сканы, фото), данные СНИЛС и ИНН за пределы компании.

Вердикт: запретить × Уровень нарушения: средний • Тег: Политика 10

Политика 11

В последнее время сотрудники стали чаще обсуждать популярные сериалы, вышедшие или снятые в 2020 году в мессенджерах и социальных сетях, из-за

чего упала общая производительность на 8%. Было решено отследить, кто больше всего занимается не рабочей деятельностью, для чего необходимо создать политику для отслеживания 5 популярных на данный момент сериалов при передаче через веб-сообщения и почту.

Список сериалов по рейтингу по версии кинопоиск:
1. Рик и Морти
2. Доктор Кто
3. Голяк
4. Бесстыжие
5. Ход Королевы

Вердикт: разрешить √ Уровень нарушения: средний • Тег: Политика 11

Политика 12

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: (содержащей urn (хеш) файла). Ложных срабатываний просто на слово magnet (в т.ч. с двоеточием) быть не должно.
Также необходимо установить контроль за видео файлами (mp4, avi и т.д.) при попытке передачи через браузер и почту.
Вышеуказанными данными сотрудники могут обмениваться не только внутри компании.
Для торрент-файлов и ссылок:
Вердикт: запретить × Уровень нарушения: средний • Тег: политика 12
Для видеофайлов:
Вердикт: разрешить √ Уровень нарушения: средний • Тег: политика 12

Политика 13

Сотрудники отдела ИТ заподозрены в сливе баз данных клиентов.
Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из отдела информатизации. Критичными данными в выгрузке являются телефоны, ИНН, ОКПО, ОКФС, ОКОГУ и ОКОПФ и в 1 документе присутствует 3 или более

компаний. Для настройки используйте файл «Выгрузка из БД.csv».

Вердикт: разрешить √ Уровень нарушения: высокий • Тег: Политика 13

Политика 14

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить потенциальную утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты доменов компании: demo и demolab, демо, демолаб.

Возможные домены первого уровня: ru, su, org, lab, рф.

Детектирование только частей адресов (например @demo.ru) недопустимо.

Пример формата адресов: e-mail@demolab.ru , mail+tag@demo.lab , мой.меил@демолаб.рф , элепочта@демо.рф и т. п.

Разрешенные спецсимволы в корпоративной почте: **_ . - +**

Вердикт: разрешить √ Уровень нарушения: средний • Тег: Политика 14

Политика 15

Сотрудники и партнеры компании стали получать большое количество различных рекламных сообщений на мобильные номера, в связи с чем возникло подозрение о том, что кто-то производит «слив» номеров из баз данных компании путем передачи информации за пределы компании через браузер, почту или флешки.

Необходимо контролировать передачу как минимум 3 мобильных номеров в 1 сообщении, т.к. передача всего одного номера не является потенциальным сливом данных (может быть просто контактной информацией).

Мобильные номера могут быть только операторов РФ (код страны 7, код оператора начинается с 9), в различных форматах, например:

+7 (987) 123-45-67, +79871234567, +7 987 123 4567, 8-987 123-4567 и т.д.

Необходимо учесть все варианты, в т.ч. без кода страны, кода выхода на городскую телефонную сеть, комбинации пробелов, скобок, дефисов.

Вердикт: разрешить √ Уровень нарушения: высокий • Тег: Политика 15

Политика 16

Необходимо поставить на мониторинг все зашифрованные и запароленные архивы, так как попытки передачи таких данных несут потенциальную

опасность утечки.

Вердикт: разрешить √ Уровень нарушения: низкий • Тег: Политика 16