**Центр безопасности Azure** — это служба мониторинга, позволяющая наблюдать за состоянием безопасности во всех ваших службах, как в Azure, так и в локальной среде. Термин "состояние безопасности" относится к элементам управления и политикам кибербезопасности, а также к тому, насколько хорошо вы можете прогнозировать угрозы безопасности, предотвращать их и реагировать на них.

*Возможности центра безопасности:*

-Мониторинг параметров безопасности для локальных и облачных рабочих нагрузок.

-Автоматическое применение необходимых настроек безопасности к новым ресурсам по мере их появления в сети.

-Предоставление рекомендаций по обеспечению безопасности на основе текущих конфигураций, ресурсов и сетей.

-Непрерывное отслеживание ваших ресурсов и выполнение автоматических оценок безопасности для определения потенциальных уязвимостей до того, как ими смогут воспользоваться злоумышленники.

-Использование машинного обучения для обнаружения и блокировки установки вредоносных программ на виртуальных машинах и других ресурсах. Можно с помощью адаптивных элементов управления приложениями определять правила, в которых перечислены разрешенные приложения, чтобы могли запускаться только приложения, которые вы разрешили.

-Обнаружение и анализ потенциальных входящих атак, а также исследование угроз и любых действий после нарушений, которые могут произойти.

-Обеспечение оперативного управления доступом к сетевым портам. Таким образом, сеть будет разрешать только необходимый трафик и тогда, когда он необходим, что позволяет сократить количество направлений атак.

В разделе **Гигиена безопасности ресурсов** можно увидеть состояние своих ресурсов с точки зрения безопасности. Рекомендации разделены на категории важности "низкая", "средняя" и "высокая", чтобы упростить назначение приоритетов действиям по исправлению. Пример приведен ниже.



**Оценка безопасности** — это показатель состояния безопасности организации. Оценка безопасности выполняется с помощью элементов управления безопасностью или групп связанных рекомендаций по безопасности. Ваша оценка — это процентная доля элементов управления безопасностью, которым вы соответствуете.

Возможности для защиты от угроз:

-JIT-доступ к виртуальной машине

Можно настроить JIT-доступ к виртуальным машинам. Он блокирует трафик в конкретных сетевых портах виртуальных машин, но разрешает его в течение определенного времени, когда он запрашивается и утверждается администратором.

-Адаптивные элементы управления приложениями

Можно контролировать, каким приложениям разрешено запускаться на ее виртуальных машинах. В фоновом режиме Центр безопасности использует машинное обучение для просмотра процессов, выполняемых на виртуальной машине. Он создает правила исключений для каждой группы ресурсов, в которой находятся виртуальные машины, и предоставляет рекомендации. Этот процесс обеспечивает отправку предупреждений, которые информируют компанию о неавторизованных приложениях, запущенных на ее виртуальных машинах.

-Адаптивная защита сети

Центр безопасности может отслеживать шаблоны интернет-трафика виртуальных машин и сравнивать эти шаблоны с текущими параметрами группы безопасности сети (NSG) компании. Исходя из этого, Центр безопасности может давать рекомендации, следует ли дальше блокировать группы безопасности сети, и предоставить рекомендации по исправлению.

-Мониторинг целостности файлов

Tailwind Traders также может настроить мониторинг изменений, важных файлов Windows и Linux, настроек реестра, приложений и других аспектов, которые могут свидетельствовать об атаке на систему безопасности.

**Azure Sentinel** — это облачная система управления информационной безопасностью и событиями безопасности Майкрософт (SIEM). Он использует интеллектуальную аналитику безопасности и анализ угроз.

*Azure Sentinel позволяет выполнять следующие задачи.*

-Сбор облачных данных в большом масштабе.

Собирайте данные по всем пользователям, устройствам, приложениям и инфраструктуре как локально, так и из нескольких облаков.

-Обнаружение ранее необнаруженных угроз.

Сведите к минимуму количество ложноположительных результатов с помощью комплексной аналитики и аналитики угроз Майкрософт.

-Исследование угроз с помощью искусственного интеллекта.

Изучайте подозрительные действия в большом масштабе, опираясь на многолетний опыт Майкрософт в области кибербезопасности.

-Быстрое реагирование на инциденты.

Используйте встроенную оркестрацию и автоматизацию распространенных задач.

*Какие источники данных подключаются:*

-Подключение решений Майкрософт.

-Подключение других служб и решений.

-Подключение стандартных отраслевых источников данных.

**Способы обнаружения угроз:**

Во встроенной аналитике используются шаблоны, разработанные экспертами по безопасности и аналитиками Майкрософт на основе известных угроз, распространенных векторов атак и цепочек эскалации подозрительной активности. Эти шаблоны можно настраивать, а затем искать в среде любые действия, которые выглядят подозрительно. В некоторых шаблонах используется функциональная аналитика машинного обучения, основанная на собственных алгоритмах Майкрософт.

Настраиваемая аналитика — это правила, которые вы создаете для поиска определенных критериев в вашей среде. Вы можете предварительно просматривать количество результатов, которые выдаст запрос (на основе прошлых событий журнала), и устанавливать расписание для выполнения запроса. Можно также установить порог предупреждения.

**Исследование и реагирование**

Когда Azure Sentinel обнаруживает подозрительные события, Tailwind Traders может исследовать определенные предупреждения или инциденты (группу связанных предупреждений). С помощью графа исследования компания может проверять информацию от сущностей, напрямую связанных с предупреждением, а также просматривать общие запросы исследования, что помогает в проведении исследования.

Компания также будет использовать сборники схем Azure Monitor для автоматизации реагирования на угрозы. Например, она может задать предупреждение, которое будет искать вредоносные IP-адреса, пытающиеся получить доступ к сети, и создать книгу, которая выполняет следующие действия.

1.Когда срабатывает предупреждение, открывает запрос в системе отправки ИТ-запросов.

2.Отправляет сообщение в канал службы безопасности в Microsoft Teams или Slack, чтобы аналитики по вопросам безопасности знали об инциденте.

3.Отправьте всю информацию в оповещении своему старшему сетевому администратору и администратору безопасности. Сообщение электронной почты содержит две пользовательские кнопки: Блокировать и Игнорировать.

**Azure Key Vault** — это облачная служба для хранения секретов приложений в одном центральном месте. Она обеспечивает безопасный доступ к конфиденциальной информации, предоставляя возможности управления доступом и ведения журнала.

**Azure Key Vault предоставляет следующие возможности:**

-Управление секретами

Azure Key Vault можно использовать для безопасного хранения токенов, паролей, сертификатов, ключей API и других секретов со строгим контролем доступа к ним.

-Управление ключами шифрования.

Azure Key Vault можно использовать как решение для управления ключами. Эта служба позволяет легко создавать и контролировать ключи шифрования, используемые для шифрования данных.

-Управление сертификатами SSL/TLS.

С помощью службы Azure Key Vault можно подготавливать, администрировать и развертывать общедоступные и закрытые сертификаты SSL и TLS для ресурсов Azure и внутренних ресурсов.

-Хранение секретов с помощью аппаратных модулей безопасности (HSM).

Секреты и ключи могут быть защищены программными средствами или с помощью HSM проверки на соответствие стандарту FIPS 140-2 уровня 2.

**Ниже перечислены основные преимущества использования Key Vault:**

-Централизация секретов приложений.

Централизованное хранение секретов приложений позволяет управлять их распространением и снижает вероятность случайной утечки.

-Безопасное хранение секретов и ключей.

Azure использует стандартные отраслевые алгоритмы, длины ключей и модули HSM. Для доступа к Azure Key Vault требуется соответствующая проверка подлинности и авторизация.

-Мониторинг доступа и управление доступом.

С помощью Azure Key Vault вы можете отслеживать доступ к секретам приложений и управлять им.

-Упрощенное администрирование секретов приложений

Key Vault упрощает регистрацию и обновление сертификатов из общедоступных центров сертификации (ЦС). Вы также можете масштабировать и реплицировать содержимое в пределах регионов и использовать стандартные инструменты управления сертификатами.

-Интеграция с другими службами Azure

Key Vault можно интегрировать с учетными записями хранения, реестрами контейнеров, концентраторами событий и многими другими службами Azure. Затем эти службы могут безопасно ссылаться на секреты, хранящиеся в Azure Key Vault.

Некоторые организации обязаны соблюдать нормативные требования, согласно которым они должны быть единственным клиентом, использующим физическую машину, на которой размещены их виртуальные машины. **Выделенный узел Azure** предоставляет выделенные физические серверы для размещения ваших виртуальных машин Azure с ОС Windows и Linux.

**Выделенный узел Azure:**

предоставляет возможности обзора и контроля серверной инфраструктуры, в которой работают ваши виртуальные машины Azure;

помогает удовлетворить требования соответствия благодаря развертыванию рабочих нагрузок на изолированном сервере;

позволяет выбирать количество процессоров, возможности сервера, серию и размеры виртуальных машин в рамках одного узла.

**Брандмауэр** — это устройство сетевой безопасности, которое отслеживает входящий и исходящий сетевой трафик и решает, блокировать или разрешить определенный трафик, на основе заданного набора правил безопасности. Вы можете создавать правила брандмауэра, определяющие диапазоны IP-адресов. Доступ к целевому серверу разрешается только клиентам, которым предоставлены IP-адреса из этих диапазонов. Правила брандмауэра также могут включать сведения о конкретных сетевых протоколах и портах.

**Брандмауэр Azure** — это управляемая облачная служба сетевой безопасности, которая помогает защищать ресурсы в ваших виртуальных сетях Azure. Брандмауэр Azure — это брандмауэр с отслеживанием состояния. Он анализирует весь контекст сетевого подключения, а не только отдельный пакет сетевого трафика. Брандмауэр Azure обеспечивает высокую доступность и неограниченную облачную масштабируемость.

**Брандмауэр Azure предоставляет множество функциональных возможностей, в том числе:**

-высокий уровень доступности;

-неограниченную облачную масштабируемость;

-правила фильтрации входящего и исходящего трафика;

-поддержку внутреннего преобразования сетевых адресов назначения (DNAT).

-ведение журнала Azure Monitor.

**Брандмауэр Azure позволяет настроить:**

-Правила приложений, определяющие полные доменные имена (FQDN), к которым можно получить доступ из подсети.

-Правила сети, определяющие адрес источника, протокол, порт назначения и адрес назначения.

-Правила преобразования сетевых адресов (NAT), которые определяют IP-адреса и порты назначения для преобразования входящих запросов.

**Шлюз приложений Azure** также предоставляет брандмауэр, который называется брандмауэром веб-приложения (WAF). WAF обеспечивает централизованную внутреннюю защиту ваших веб-приложений от распространенных эксплойтов и уязвимостей. Служба Azure Front Door и сеть доставки содержимого также предоставляют службы WAF.

**Распределенная атака типа "отказ в обслуживании" (DDoS)** пытается перегрузить и исчерпать ресурсы приложения, чтобы оно замедлилось или перестало отвечать на запросы законных пользователей. Атаки DDoS могут быть нацелены на любой общедоступный в Интернете ресурс, в том числе на веб-сайты.

**Служба "Защита от атак DDoS Azure" предоставляет следующие уровни обслуживания.**

Основной

Стандартный

**Уровень обслуживания "Стандартный" помогает предотвратить следующие виды атак.**

-Объемные атаки.

Они нацелены на то, чтобы заполнить сетевой уровень значительным объемом сетевого трафика, который очень похож на обычный.

-Протокольные атаки.

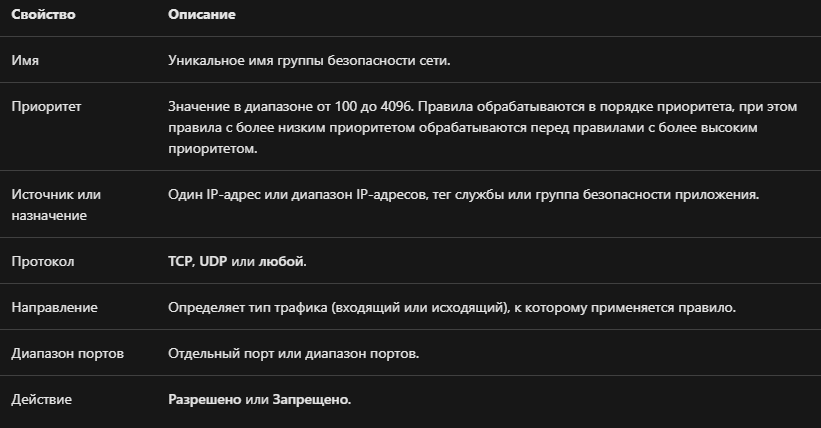
Эти атаки пытаются ухудшить доступность целевого объекта, используя уязвимости в стеке протоколов уровней 3 и 4.

-Атаки на уровне ресурсов (приложений) (только с брандмауэром веб-приложений).

Они направлены на пакеты веб-приложения и стремятся нарушить передачу данных между узлами. Для защиты от атак L7 необходим брандмауэр веб-приложений (WAF). Защита от атак DDoS Azure стандартного уровня защищает WAF от объемных и протокольных атак.

**Группа безопасности сети** позволяет фильтровать входящий и исходящий сетевой трафик ресурсов Azure в виртуальной сети Azure. Группы безопасности сети можно считать внутренним брандмауэром. NSG может содержать несколько правил безопасности относительно входящего и исходящего трафика к ресурсам и от ресурсов для его фильтрации по исходному и конечному IP-адресу, порту и протоколу.

Группа безопасности сети может содержать столько правил, сколько вам нужно, в пределах, установленных в подписке Azure. Каждое правило определяет следующие свойства.



**Защита уровня периметра**

-Используйте службу "Защита от атак DDoS Azure" для фильтрации крупномасштабных атак, прежде чем они приведут к отказу в обслуживании для пользователей.

-Используйте брандмауэры периметра с Брандмауэром Azure для выявления вредоносных атак на вашу сеть и предупреждения о них.

**Защита сетевого уровня**

-Ограничьте обмен данными между ресурсами, сегментировав сеть и настроив управление доступом.

-Настройте запрет по умолчанию.

-Ограничьте входящий и исходящий интернет-трафик, где это необходимо.

-Реализуйте безопасное подключение к локальным сетям.

**Объединение служб**

Вы можете объединять службы безопасности и сетевые службы Azure для управления сетевой безопасностью и обеспечения повышенной многоуровневой защиты. Ниже приводятся два способа объединения служб.

-Группы безопасности сети и Брандмауэр Azure

-Брандмауэр веб-приложения Шлюза приложений Azure и Брандмауэр Azure