Cloud Advisor

CSPM нового поколения с анализом контекста

Автор: Cloud Advisor

Тип документа: Whitepaper

Содержание

Безопасность облака и CSPM 2

Проблемы CSPM 2

Решение – расстановка приоритетов алертам 3

CSPM нового поколения с анализом контекста 4

Вывод 4

Безопасность облака и CSPM

Облачная модель потребления услуг продолжает набирать обороты. Одни компании увеличивают свое присутствие в облаке, повышая количество ресурсов в нем, другие только открывают для себя новые возможности. Облако – это динамичная структура, где объекты постоянно создаются, изменяются и удаляются. На площадках облачных провайдеров разворачивается большое количество объектов со сложными взаимосвязями. При этом далеко не всегда доступ к использованию облака получают сотрудники, обладающие достаточными знаниями в области безопасности. Между тем, цена ошибки при конфигурации публичного облака – утечка, а порой и потеря данных.

Из-за ошибки конфигурации облачных ресурсов в публичном доступе оказались **более 123 миллионов записей** о клиентах и сотрудниках компании Decathlon – французской сети спортивных гипермаркетов для всей семьи. Среди утекшей информации были незашифрованные электронные письма и пароли клиентов, журналы вызовов API, личные данные сотрудников (сведения о трудовых договорах, даты рождения, номера свидетельств социального страхования и пр.).

В ответ на подобные угрозы появился класс программных продуктов Cloud Security Posture Management (CSPM) - средства управления состоянием облачной безопасности. Эти решения позволяют получать данные о конфигурации объектов, расположенных в облачной инфраструктуре, и в автоматическом режиме проверять их на соответствие политике безопасности, сигнализируя пользователю о ее возможных нарушениях и потенциальных угрозах.

Проблемы CSPM

Учитывая количество объектов и динамическую природу облака, продукт CSPM генерирует большое количество алертов о нарушениях политик безопасности. В некоторых средах их число может достигать нескольких сотен в день. Это приводит к ряду серьезных негативных последствий:

- Увеличение времени реагирования на критический инцидент. Инженер может разбираться с менее приоритетными алертами, в то время как критически важные события остаются без внимания.

- Пропуск важного алерта из-за усталости от оповещений. Среагировать на одно оповещение несложно, на десятки и сотни - на порядок сложнее. И чем больше их становится, тем выше риск того, что сотрудник упустит нечто важное.

- Повышение расходов, связанных с разбором алертов, которые являются ложными срабатываниями. Многие из алертов требуют длительного расследования с привлечением специалистов из других отделов.

- Эмоциональное выгорание инженеров. Постоянный поток оповещений и монотонная работа по их разбору приводит к выгоранию сотрудников, повышению текучести кадров, снижению удовлетворенности работой и производительности.

Решение - расстановка приоритетов алертам

Единственный способ бороться с огромным количеством алертов - их правильная приоритизация. Рассмотрим расстановку приоритетов на одном примере: представим, что у нас есть неверно настроенная группа безопасности, в которой разрешены все входящие соединения со всех IP-адресов.

Традиционная CSPM считает данные об объекте Security Group, выдаст алерт о том, что ее конфигурация не верна и предложит способ как это исправить. Какой приоритет имеет эта проблема? А если таких Security Group несколько - на какую следует обратить внимание в первую очередь?

Разберем возможные варианты, исходя из контекста:

- Группа безопасности может быть не привязана к виртуальной машине или привязана к ВМ, не имеющей публичного доступа. В этом случае приоритет данной проблемы Низкий. Заняться этой проблемой можно когда все первоочередные алерты обработаны.

- Группа безопасности привязана к публичной ВМ. Злоумышленник может подключиться к этой ВМ в случае наличия уязвимостей ПО или наличия ранее похищенных реквизитов доступа. Эту проблему нужно решать решать быстро и приоритет ее Высокий.

- Группа безопасности привязана к публичной ВМ, которая имеет права администратора на все остальное облако (через service account в случае Yandex Cloud или agency для Huawei Cloud). В этом случае злоумышленник может не только проникнуть на машину, но и получить контроль над всем облаком. Эта проблема имеет Критический приоритет и решать ее необходимо немедленно.

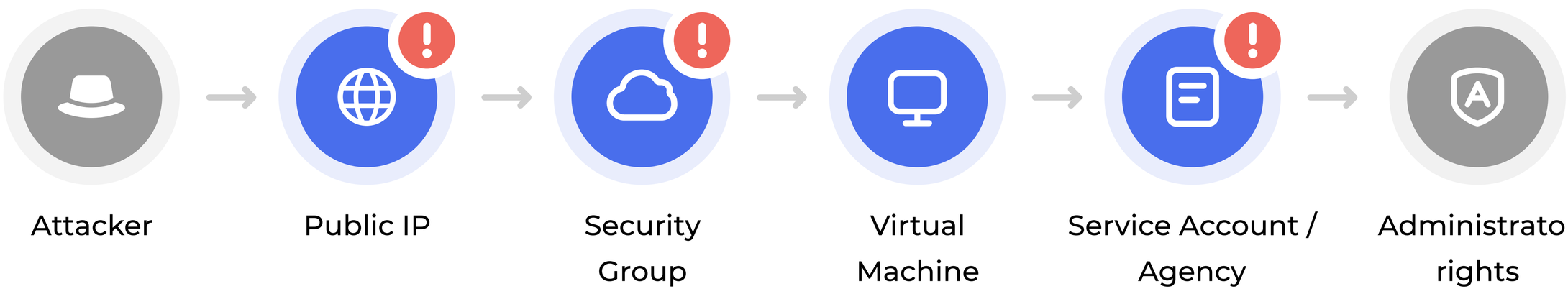
Однако, традиционные CSPM не анализируют подобный контекст и не видят различий в важности и опасности описанных вариантов. Более того, традиционные CSPM видят все три ситуации – ошибка в конфигурации группы безопасности, публичный IP-адрес у ВМ и наличие у ВМ высоких привилегий – как три отдельных, невзаимосвязанных алерта с одинаковым уровнем опасности – Средний.

CSPM нового поколения с анализом контекста

CSPM нового поколения не только анализирует каждый облачный ресурс как отдельный объект, но и рассматривает его сетевые соединения с другими облачными объектами и права, которые ресурс имеет в облаке. Таким образом, CSPM нового поколения видит не отдельные алерты, а их токсичные комбинации, которые формируют реальный вектор атаки.

> Защитники мыслят списками.
> Атакующие мыслят графами.
> Пока это так, атакующие побеждают.
>
> Джон Ламберт, Центр анализа угроз Майкрософт

В данном случае мы имеем следующий вектор атаки:



Случай с группами безопасности приведен в качестве примера, все остальные проверки облака на безопасность также должны учитывать контекст.

Вывод

Командам, отвечающим за безопасность в публичном облаке, необходимо использовать средства управления состоянием облачной безопасности (CSPM). Выбор стоит делать в сторону средств нового поколения с приоритизацией алертов на основе сетевой связности и анализа прав в облаке. Подобные решения позволяют повысить скорость и качество обработки инцидентов безопасности и снизить стоимость и трудоемкость данного процесса.

Одним из таких решений является Cloud Advisor, обеспечивающий защиту облачных инфраструктур, развернутых в Яндекс.Облаке, SberCloud.Advanced или Huawei Cloud. Дополнительная информация о продукте доступна по адресу www.cloudadvisor.app