ITD GROUP

Применение CtrlHack для повышения эффективности SOC

CTRLHACK

CTRLHACK

CtrlHack – российская платформа симуляции кибератакующих техник непосредственно в инфраструктуре организации.

CtrlHack позволяет в автоматическом режиме запускать более 200 симуляций различных кибератакующих техник на агентах, развернутых в сети организации. Симуляции полностью повторяют техники, используемые хакерами, при этом не несут угрозы инфраструктуре организации, в которой они эксплуатируются. Все симуляции описаны в открытых скриптах. В базе знаний CtrlHack есть симуляции техник для всех стадий выполнения атаки и этот набор постоянно обновляется и расширяется.

По результатам симуляций в системе формируются необходимые отчеты. Для каждой симуляции выдается детальная техническая информация обо всех выполненных действиях и их результатах. Данная информация может использоваться сотрудниками для написания правил детектирования кибератакующих техник.

ITD GROUP

ДЛЯ ТОГО, ЧТОБЫ ЭФФЕКТИВНО ОБНАРУЖИВАТЬ ТЕХНИКИ ЗЛОУМЫШЛЕННИКОВ, НЕОБХОДИМО ПОСТОЯННО РАЗВИВАТЬ НАБОР ПРАВИЛ ДЕТЕКТИРОВАНИЯ В SIEM.

CtrlHack позволяет в автоматическом режиме (в том числе по заранее заданному расписанию) проводить проверки:

- работы средств защиты информации;
- качества детектирования техник на уровне центра мониторинга;
- качества работы и соблюдения параметров работы для внешних сервисов кибербезопасности.

А также выявлять проблемы и отличия в настройках средств защиты и операционных систем в разных сегментах сети для территориально-распределенных инфраструктур.

В состав CtrlHack входят два модуля проверок:

Модуль «Первичный доступ»

Позволяет проводить симуляции, направленные на проверку работы периметровых средств защиты (IPS, NGFW), средств защиты электронной почты («песочница», почтовые антивирусы), средств за-щиты конечных точек (антивирусы, EDR).

Модуль «Пост-эксплуатация»

Позволяет проводить симуляции различных техник злоумышленников на разных шагах выполнения атаки в соответствии с матрицей MITRE. Данные симуляции направлены на проверку работы правил детектирования в решениях класса SIEM, повышение эффективности разработки данных правил, а также на проверку процесса обработки инцидентов на уровне SOC.

- Нужно анализировать новые и постоянно развивающиеся техники злоумышленников.
- Проверить, как эти техники работают в конкретной инфраструктуре и достаточно ли событий поступает в SIEM-систему для обнаружения злоумышленника.

Уже на основе анализа этих данных следует разрабатывать правила детектирования.

На последнем этапе необходимо проверить, как это правило работает во всей инфраструктуре.

Эффективно разрабатывать правила детектирования для максимального покрытия разных техник для всех стадий выполнения кибератаки можно только используя средства, позволяющие автоматически проводить симуляции таких техник во всей инфраструктуре.

CtrlHack является таким средством и позволяет решить эти проблемы.

- Платформа несет с собой необходимую экспертизу и знания по новым атакующим техникам злоумышленников.
- Платформа позволяет провести автоматическую симуляцию этих техник.

ITD GROUP

Результаты симуляций позволяют определить:

- насколько полно собираются все необходимые события,
- как работают правила детектирования в SIEM
- насколько полно обнаруживаются разные стадии выполнения атак.

Детальная техническая информация о выполненных в рамках симуляций действиях позволит аналитикам SOC легко разрабатывать новые правила детектирования (или модифицировать имеющиеся) и в дальнейшем тестировать работу этих правил. Кроме того, появляется возможность определить реальное время выявления инцидентов и реагирования на них.

Таким образом, CtrlHack позволяет

1 Существенно облегчить написание правил, предоставляя для этого готовые данные.

2 Снизить требования к квалификации сотрудников, сняв задачу глубоко разбираться в хакерских тех-никах, без снижения качества.

3 Покрыть всю инфраструктуру без исключений, т.е. быстро проверить, как определенное правило работает в каждом её сегменте.

4 Сделать процесс написания – тестирования – корректировки непрерывным за счет автоматизации.

Кроме того, для корректности работы правил детектирования нужно обеспечить сбор необходимых событий безопасности с узлов сети из всей инфраструктуры. И при этом нужно быть уверенным, что в какой-то момент (например, из-за действий сотрудников ИТ-подразделений) не перестали поступать определенные события из какого-либо сегмента территориально-распределенной сети. Проводить мониторинг полноты сбора событий для всей инфраструктуры руками невозможно. Симуляция же кибератакующих техник на постоянной основе по всей инфраструктуре оперативно покажет из какого сегмента и какие именно события перестали поступать.

Также применение CtrlHack позволит оценить, как быстро фиксируются инциденты в SOC, какие действия выполняют сотрудники после фиксации инцидента и в рамках реагирования на инцидент.

НА ОСНОВЕ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ АНАЛИТИКИ SOC СМОГУТ РАЗРАБОТАТЬ НЕОБХОДИМЫЕ ПРАВИЛА КОРРЕЛЯЦИИ И ДАЛЕЕ АВТОМАТИЧЕСКИ ПЕРЕЗАПУСТИТЬ СИМУЛЯЦИИ ДЛЯ ПРОВЕРКИ КОРРЕКТНОСТИ ИХ РАБОТЫ.

CTRLHACK

Непрерывная объективная оценка
уровня защищенности и повышение
эффективности системы защиты

ITD GROUP

Эксклюзивный дистрибьютор – компания ITD Group

123557, Москва, Большой Тишинский переулок, д. 19, стр. 3

+7 (499) 502-13-75
info@iitdgroup.ru