ITD GROUP

Кейсы применения CtrlHack

CTRLHACK

CTRLHACK

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

1 Валидация и развитие функций детектирования атакующих действий злоумышленника на уровне SOC

Для чего?

- Валидация правил детектирования атакующих техник.
- Контроль полноты сбора событий ИБ из всех сегментов сети.
- Возможность разработки и тестирования новых правил детектирования на базе информации о симуляциях реальных техник.

Каким образом?

Часть атакующих техник CtrlHack не блокируются средствами защиты и должны быть отработаны на уровне правил детектирования SIEM. Результаты выполнения симуляций позволяют определить:

- работают ли правила детектирования для определенных техник,
- достаточно ли событий поступает в SIEM из разных сегментов сети для работы правил,
- одинаковая ли полнота сбора событий из разных участков сети.

Если правила нет или оно некорректно работает, CtrlHack предоставляет всю техническую информацию по итогам симуляции. Этой информации достаточно для написания или модернизации правил детектирования аналитиками.

Кто уже так использует?

Например,

4 банка из ТОП-10
Девелоперская компания
Горно-металлургическая компания
Крупная государственная компания

2 Валидация процессов реагирования

Для чего?

- Проверка алгоритма работы сотрудников SOC в процессе реагирования.
- Проверка запуска и корректности работы сценариев в системах класса SOAR.
- Возможность полной автоматизации запуска симуляций и анализа их работы через SOAR

Каким образом?

CtrlHack позволяет проверить, удаляются ли артефакты, созданные во время выполнения техники через заданный промежуток времени. Также по итогам выполнения симуляции можно проверить время создания карточки инцидента и время работы персонала SOC по отработке данного инцидента.

Также имеется возможность запуска симуляций в автоматическом режиме из систем SOAR с последующей проверкой качества работы сценариев реагирования.

Кто уже так использует?

Например,

1 банк из ТОП-10
Девелоперская компания
Горно-металлургическая компания
Крупная государственная компания

3 Проверка корректности работы внедренных СЗИ

Для чего?

- Проверка корректности работы СЗИ.
- Выявление отличий в работе (настройках) СЗИ в разных сегментах сети.
- Проверка качества блокирования актуального вредоносного контента.

Каким образом?

В составе CtrlHack есть проверки, позволяющие оценить работу NGFW, систем защиты электронной почты (песочница, почтовый антивирус), антивирусов на конечных точках и систем класса EDR/XDR.

Запуск проверок в разных точках сети позволит оперативно выявлять изменения в настройках СЗИ или их отключение.

Кто уже так использует?

Например,

3 банка из ТОП-10
Девелоперская компания
Горно-металлургическая компания
Крупная государственная компания

4 Обоснованный выбор и модернизация СЗИ

Для чего?

Возможность выбора СЗИ на основе тестирования их функций в рамках запуска симуляций техник.

Каким образом?

Для тестирования разных классов решений формируются соответствующие наборы симуляций.

Решения разных вендоров проверяются в реальных условиях функционирования и на одних и тех же наборах симуляций.

Кто уже так использует?

Например,
Банк из ТОП-10, CtrlHack использован для тестирования решений класса XDR

5 Оценка фактического уровня риска ИБ для дочерних и аффилированных организаций с целью контроля реализации глобальной политики ИБ

Для чего?

Возможность проверки дочерних организаций из одного интерфейса без необходимости установки отдельных инстансов сервера управления.

Каким образом?

В интерфейсе CtrlHack можно создавать отдельные организационные подразделения и группировать в них агентов. В этом случае задания на симуляцию будут устанавливаться независимо для каждого такого подразделения, и для каждого подразделения будут формироваться отдельные отчеты. Также есть возможность разграничения прав доступа оператора системы для каждого подразделения.

Кто уже так использует?

Например,

Банк из ТОП-10

Девелоперская компания

CTRLHACK

Включен в Единый реестр российских программ для электронных вычислительных машин и баз данных. Запись в реестре №12299 от 21.12.2021.

ITD GROUP

Эксклюзивный дистрибьютор – компания ITD Group

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

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