ITD GROUP

Платформа симуляции кибератакующих техник

CTRLHACK

Ландшафт угроз

1

Сложность и разнообразие кибератак растет , и при этом растет финансовая мотивация проведения атак. В арсенале хакеров всегда есть инструменты, позволяющие обойти средства защиты от проникновения.

2

Атаки – это многоходовые операции. После проникновения все только начинается. Хакеры преследуют вполне конкретные цели. В ходе выполнения действий в сети они используют различные техники и инструменты.

3

Защите от атакующих техник внутри корпоративной сети должно уделяться не меньше внимания, чем защите периметра. При этом в большинстве случаев действия в сети обнаружить и заблокировать даже проще, чем защититься от проникновения.

4

Таким образом, на первый план выходит задача развития компетенций выявления присутствия хакеров в сети и быстрого реагирования на их действия. Это позволит останавливать атаку на ранних стадиях.

Что делать?

Подготовиться к кибератакам и получить актуальную картину реальной защищенности корпоративной сети можно только выполняя действия, аналогичные действиям хакеров. Для решения задачи непрерывной оценки готовности организации к отражению кибератак в реальном времени необходимо использовать средства автоматической симуляции кибератак.

Предлагаемое решение

CtrlHack позволяет автоматически выполнять симуляции техник, используемых хакерами. Действия атакующих имитируются для того, чтобы определить, как на них реагируют средства защиты, и насколько эффективен процесс реагирования.

1 Все выполняемые во время симуляций действия безопасны

2 В состав включено более 200 атакующих техник для всех стадий выполнения атаки

3 Отдельные действия могут объединяться в сценарии

4 Сценарии могут запускаться по расписанию, а также комбинироваться

По результатам симуляций можно определить:

- Корректно ли работают средства защиты во всей инфраструктуре
- Как команда реагирует на инциденты
- Формируются ли инциденты в SOC
- Какие события для каждой атакующей техники есть в SOC, а какие отсутствуют
- Какие атакующие техники не детектируются
- Как быстро устраняются инциденты

Как это работает

Сервер управления разворачивается в сети организации или в облаке.

Для проведения симуляций в сети устанавливаются Агенты (ОС Windows, Linux, MacOS).

Сценарии симуляции открыты, их можно изменить в любой момент, а также создать свои сценарии симуляций.

01

Пользователь формирует задание с набором атакующих техник и запускает симуляцию на выбранных узлах в сети организации.

02

Задание автоматически запускается на выполнение на выбранных узлах.

03

После завершения симуляции пользователь получает подробный отчет обо всех выполненных действиях.

Для кого?

Решение рассчитано на крупные компании и корпорации, которые:

- Имеют команду мониторинга и реагирования (SOC) или пользуются услугами сервис-провайдера
- Обеспокоены тем, что атаки на организацию могут остаться незамеченными
- Хотят понять, какие атакующие техники команда мониторинга и реагирования не детектирует
- Стремятся повысить качество и полноту набора правил детектирования атакующих техник
- Стремятся повысить квалификацию своей команды мониторинга и реагирования

Выгоды от применения

Получение реальной информации о работе системы киберзащиты

Возможность проверки готовности персонала к выявлению кибератак

Повышение эффективности выявления кибератак без внедрения новых средств защиты

Оптимизация существующих процессов реагирования на инциденты

Определение необходимости во внедрении новых средств защиты и проведение их тестирования

Применение CtrlHack позволит:

- Иметь объективную оценку защищенности в любой момент времени и без необходимости привлечения внешних команд
- Трезво оценивать и снижать риски для бизнес-процессов компании
- Осуществлять стратегическое планирование развития системы киберзащиты, опираясь на данные о реальной защищенности
- Эффективно управлять бюджетом на поддержание и развитие системы киберзащиты

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