ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ПЛАТФОРМЫ СИМУЛЯЦИИ КИБЕРАТАК CTRLHACK ДЛЯ АНАЛИЗА УРОВНЯ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИИ

ПЯТАКОВ МАКСИМ

Сооснователь CTRLHACK

СОЛОВЬЕВ ВЛАДИМИР

Руководитель направления внедрения средств защиты отдела технических решений

Breach and Attack Simulation BAS

Симуляция хакерских техник в инфраструктуре компании

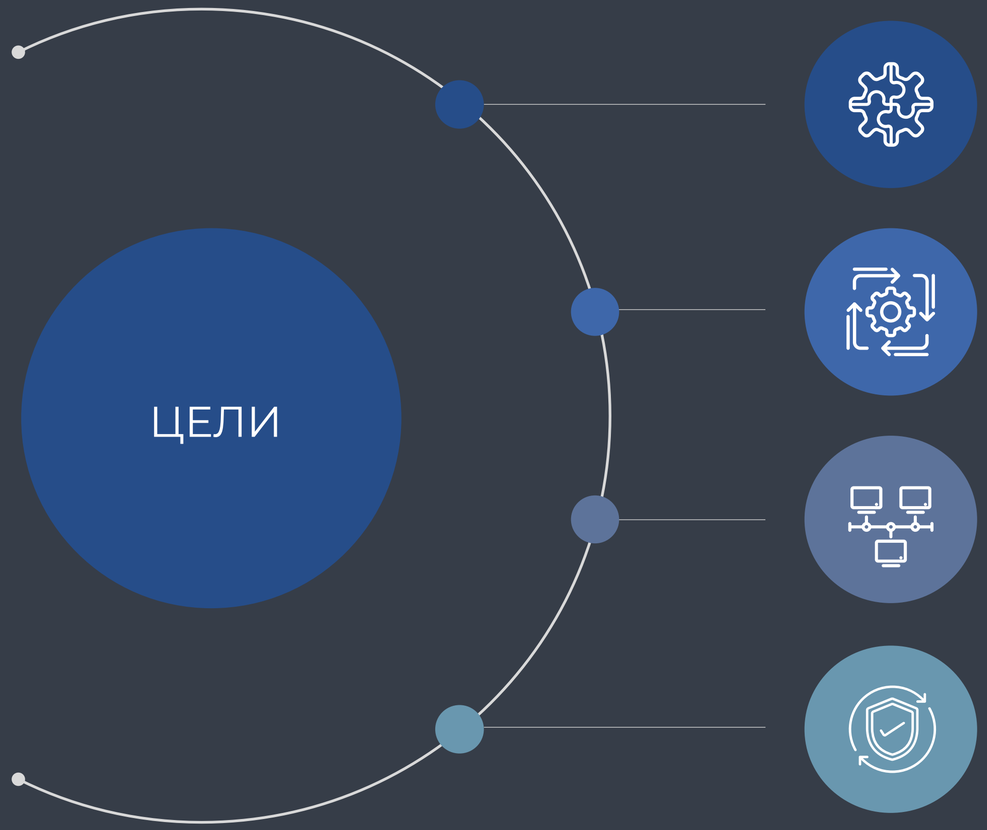
Имитируют действия хакеров в автоматическом режиме

Нацелены на проверку внутренней инфраструктуры

Позволяют построить процесс непрерывной оценки системы защиты

Системы класса BAS

Симуляция хакерских техник в инфраструктуре компании



Проверка работы средств защиты

Проверка покрытия правилами детектирования

Проверка всей инфраструктуры

Повышение эффективности детектирования

ВОЗМОЖНОСТИ

CTRLHACK

Для работы не требуется вносить изменения в инфраструктуру и отключать средства защиты информации

БАЗА ЗНАНИЙ

Более 250 техник

База постоянно обновляется

ЗАПУСК СИМУЛЯЦИЙ

Симуляции запускаются непосредственно в инфраструктуре

ПРОЦЕСС

Автоматическое выполнение, в т.ч. по расписанию

ОТЧЕТЫ

Детальный технический отчет

Отчеты для руководства

Какие задачи решает?

CTRLHACK

Проверка средств защиты

Какие из хакерских техник блокируют СЗИ, корректно ли они настроены?

Детектирование техник

Какие из хакерских техник детектируются в SIEM, достаточно ли событий для детектирования техник?

Развитие SOC

Формируются ли инциденты в SOC, как команда реагирует на инциденты?

КАК ЭТО РАБОТАЕТ

Симуляции представляют собой набор действий на рабочих станциях и серверах. По итогам выполнения симуляций формируется детальный отчет о всех выполненных действиях.

01 **Агенты**

На рабочие станции и сервера устанавливаются агенты

02 **Симуляция**

На агентах выполняются действия, имитирующие действия хакеров

03 **Реакция**

СЗИ должны реагировать, в SIEM должны отправляться события

МОДУЛИ СИСТЕМЫ

Первичный доступ

Соединение с адресами из «черных списков».
Скачивание вредоносных файлов через Web.
Сохранение вредоносных файлов на диск.
Письма с вредоносными вложениями.

Пост-эксплуатация

Отдельные техники по всем стадиям атаки после получения первичного доступа.
Техники для ОС Windows, Linux, MacOS.
Привязка к MITRE.

Проверка работы NGFW, песочницы, почтового антивируса, антивируса на PC и серверах

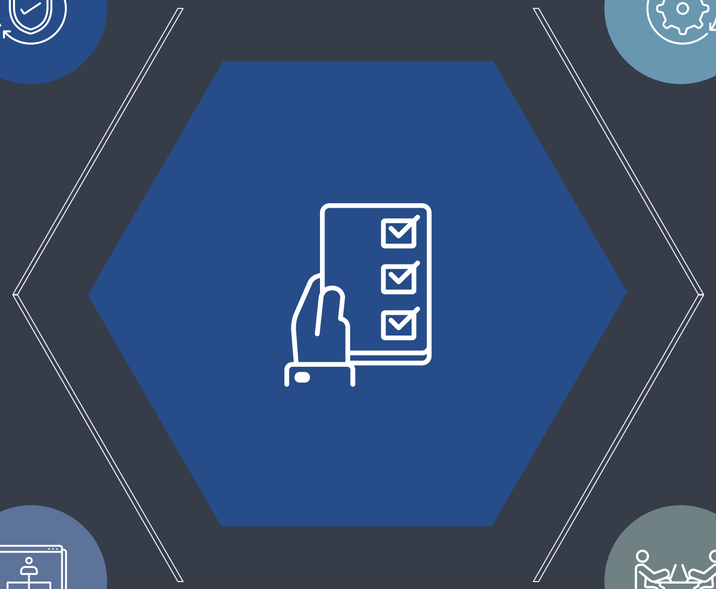
Проверка работы SIEM, антивируса на PC и серверах, EDR/XDR

Опыт использования

Валидация и развитие функций детектирования атакующих действий злоумышленника на уровне SOC

Проверка корректности работы внедренных СЗИ

Оценка фактического уровня риска ИБ для дочерних организаций



Валидация процессов реагирования

Обоснованный выбор и модернизация СЗИ

Проведение киберучений

ПЛАН ПОКАЗА

Почтовый вектор

Проверка антивируса для почтового сервера

Web-ссылки

Проверка NGFW

Вредоносные файлы

Проверка антивируса на PC

Техники MITRE

Проверка XDR

ООО «КОНТРОЛХАК»
+7 (495) 789 72 97
info@ctrlhack.ru

СПАСИБО!

ВСЕГДА РАДЫ СОТРУДНИЧЕСТВУ