Платформа симуляции
кибератакующих техник

01 | Описание платформы

CTRLHACK

Единственный российский продукт класса Breach and Attack Simulation

Выполнение симуляций непосредственно в инфраструктуре организации

Автоматическое выполнение симуляций, в т.ч. по заданному расписанию

Определение реального уровня защищенности инфраструктуры и повышение эффективности детектирования хакерских действий

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

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 **Симуляция**

Реальное выполнение действий, имитирующих действия хакеров.

02 **Реакция**

СЗИ должны реагировать, в SIEM должны отправляться события.

03 **Сценарии**

Все сценарии симуляций открыты. Можно изменять и создавать свои сценарии.

Состав системы

Сервер управления

- Варианты установки: в облаке CTRLHACK;
  в сети компании, в т.ч. в изолированных сетях
- Возможна многосерверная установка для сложных распределенных сетей

Запуск на агентах

- Устанавливаются на рабочие станции и сервера (ОС Windows, Linux, MacOS)
- Необходимо покрыть 10% инфраструктуры

Запуск без агентов

- Для запуска симуляций необходимы данные для доступа
- Выполнение симуляций для ОС Windows и Linux

Модули системы

Первичный доступ

Имитируются действия корпоративного пользователя при доступе к сети Интернет. В результате таких действий хакер может получить доступ в инфраструктуру компании.

Пост-эксплуатация

Имитируются действия хакеров в сети после получения первичного доступа в инфраструктуру компании.

Модуль
Первичный доступ

Соединение с адресами из «черных списков».

Скачивание вредоносных файлов через Web.

Сохранение вредоносных файлов на диск.

Письма с вредоносными вложениями.

01

Симуляции с использованием реальных вредоносных объектов и адресов из «черных» списков.

02

Безопасная работа. Без запуска. Только соединение, скачивание и сохранение на диск.

03

Постоянно обновляемая база адресов и экземпляров вредоносных файлов. Данные из ABUSE.ch.

04

Период обновления настраивается. Возможны ежедневные обновления.

Модуль
Первичный доступ

Проверка работы:

NGFW,

песочницы и почтового антивируса,

антивируса на АРМ и серверах.

РАБОТА СЗИ

Проверяется готовность средств защиты к блокированию актуальных угроз.

НАСТРОЙКИ СЗИ

Выявляются проблемы в настройках средств защиты, а также отличия в настройках в разных сегментах сети.

ИНЦИДЕНТЫ

Проверяется фиксация инцидентов в SOC.

Модуль Пост-эксплуатация

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

01 В базе более 370 реализаций различных техник.
База постоянно обновляется.

02 В симуляциях реализована возможность работы с файлами, процессами, сетевыми соединениям, реестром (для Windows).

03 В техниках используются в т.ч. стандартные инструменты ОС, легитимные утилиты и инструменты администрирования.

04 Большинство техник не блокируются средствами защиты «по умолчанию». Необходимо их детектировать на уровне SIEM.

Модуль Пост-эксплуатация

Проверка работы:

SIEM, антивируса на АРМ и серверах, EDR/XDR и процессов в SOC.

БЛОКИРОВАНИЕ ТЕХНИК

Определяется какие из техник блокируются средствами защиты.

ДЕТЕКТИРОВАНИЕ ТЕХНИК

Определяется какие из техник детектируются правилами в SIEM.

СБОР СОБЫТИЙ

Симуляции позволяют определить насколько полно собираются события в SIEM.

РЕАГИРОВАНИЕ

Проверка процессов реагирования на инциденты.

Модуль
Пост-эксплуатация

Разработка правил детектирования

В результате симуляций предоставляются все необходимые данные для разработки правил.

Появляется возможность выстроить процесс автоматического аудита правил детектирования.

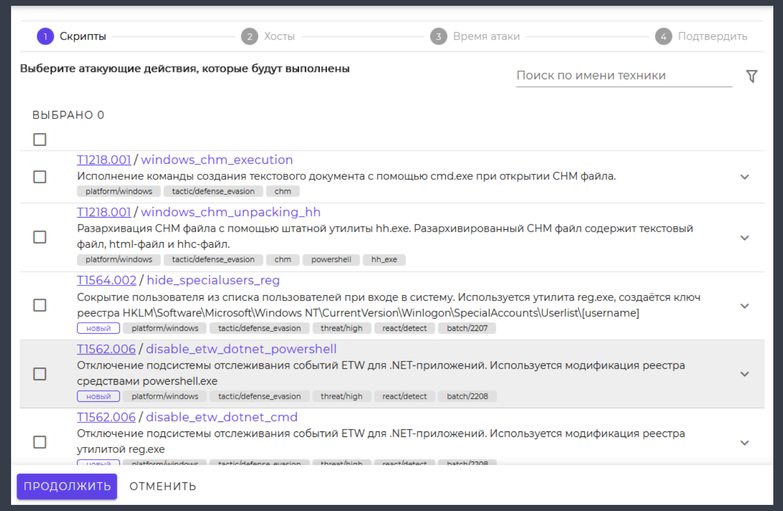
Интеграция с SIEM

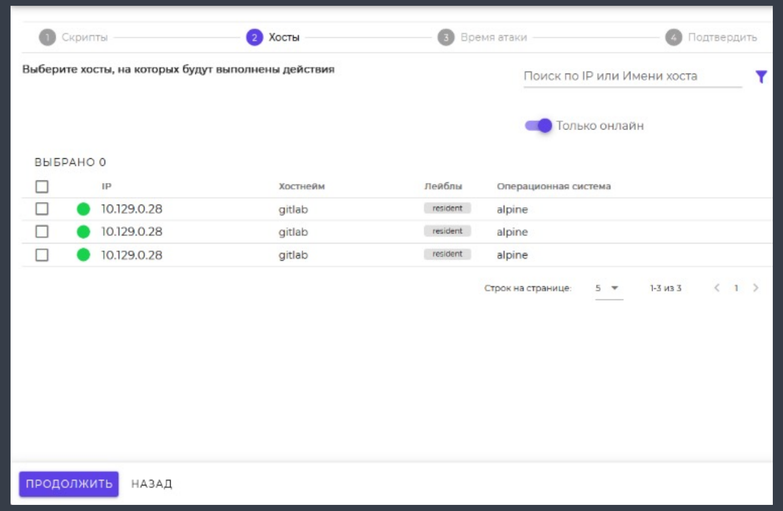
Получение данных

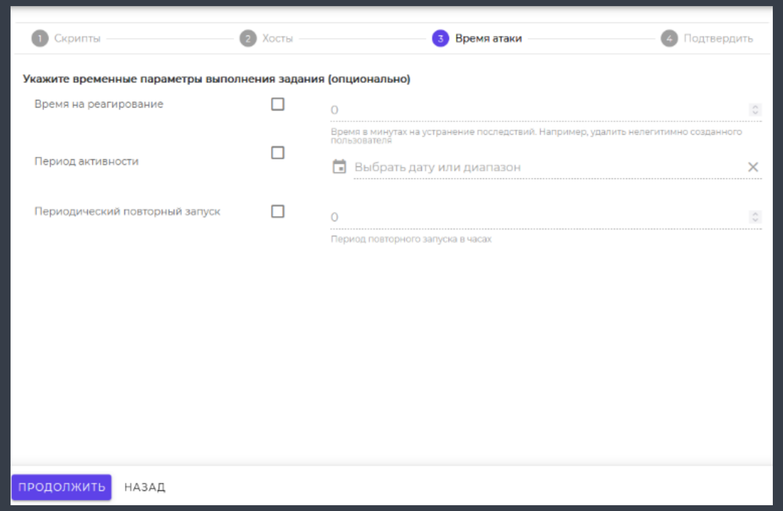
Получение из SIEM и отображение в интерфейсе CtrlHack информации о событиях, имеющих отношение к выполненной симуляции.

Отправка данных

Передача в SIEM данных о работе системы.







Запуск заданий

Запуск заданий с использованием простого пошагового конструктора.

Выбор действия

Выбираются вредоносные объекты или атакующие техники. Здесь можно посмотреть сам скрипт и описание техники.

Выбор узлов

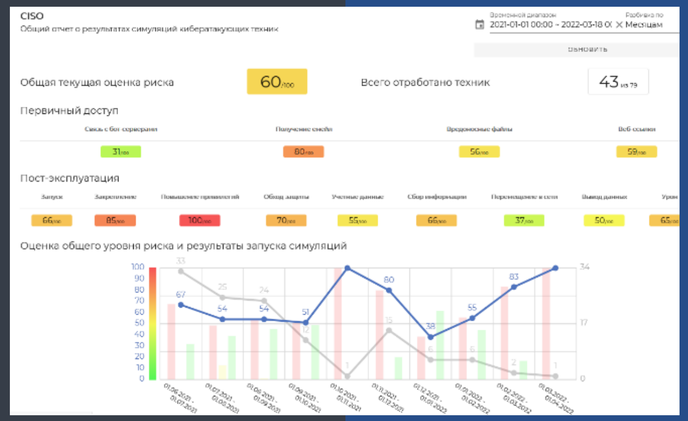
Выбираются агенты на которых будет выполняться симуляция.

Задание параметров

Можно задать время отложенного запуска или расписание для запуска.

Аналитика и отчеты

Несколько уровней отчетности: Dashboard, отчеты разной глубины, технический отчет о выполненном задании.



02 | Практическое применение

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.

Использование в сегменте АСУТП.

Примеры результатов симуляций

Первичный доступ | Проверка NGFW

№	URL	Хосты. Скачивание заблокировано	Хосты. Скачивание прошло успешно	Всего	Инцидент в SOC	События от NGFW
1	http://ballatstone.com/ballatstone.com/Dy0/	21	0	21	0	21
2	https://res.hjfile.cn/pt/jp/topics/pronounce/assets/hjpro50.exe	19	2	21	0	19

Для одного из URL на части узлов был успешно скачан вредоносный файл.
Для остальных узлов скачивание было заблокировано.

Примеры результатов симуляций

Первичный доступ | Проверка антивируса

№	Filename	Хосты Не удалось сохранить файл	Хосты Файл сохранен, но затем удален СЗИ	Хосты Файл сохранен и не удален	Всего	Инцидент в SOC	Антивирус События
1	Account Details for transfer.exe	5	15	1	21	20	20
2	FedEx Tracking _pdf.exe	5	16	0	21	20	21
3	Payment.swifT.exe	6	15	0	21	20	20

Один из вредоносных файлов на одном из узлов был успешно сохранен без удаления.
На остальных узлах антивирус обнаружил файл.
При этом антивирус работал по-разному на разных узлах.
Для другого файла, при наличии событий от одного из узлов, нет инцидента в SOC.

Примеры результатов симуляций

Пост-эксплуатация | Техники Windows

№	Техника	Стадия и код MITRE	Хосты Заблокировано	Хосты Выполнено	Инцидент в SOC	События в SIEM
1	dump_lsass_exe_memory_using_procdump	Credential, T1003.001	20	2	18	18
2	execute_a_command_as_a_service	Execution, T1569.002	0	22	0	17
3	masquerading_powershell_exe_running_as_taskhostw_exe	Evasion, T1036.003	22	0	0	17
4	persistence_via_wmi_event_subscription	Persistance, T1546.003	18	4	22	22
5	powershell_cmdlet_scheduled_task	Persistance, T1053.005	5	17	0	12
6	wmi_execute_local_process	Execution, T1047	0	22	0	22

Успешное выполнение техник. Отсутствие событий от некоторых узлов.
Отсутствие инцидентов в SOC при наличии событий.

Примеры результатов симуляций

Пост-эксплуатация | Техники Linux

№	Техника	Стадия и код MITRE	Выполнено	Заблокировано	События SOC	Инцидент SOC
1	cron_add_script_to_all_cron_subfolders	Persistance, T1053.003	✓		+	-
2	cron_add_script_to_var_spool_crontabs_folder	Persistance, T1053.003		✓	-	-
3	create_systemd_service	Persistance, T1543.002		✓	+	+
4	set_a_setuid_flag_on_file	Privileges, T1548.001	✓		+	-
5	create_hidden_folder_and_script	Evasion, T1564.001	✓		+	-
6	modify_file_timestamps_using_reference_file	Evasion, T1070.006	✓		+	-
7	copy_private_ssh_keys_with_cp	Credential, T1552.004	✓		+	-

Большинство техник успешно выполняются.

Практически полное отсутствие инцидентов в SOC при наличии событий.

03 | Лицензирование. Пилот

Лицензирование Пилот

Предлагаем провести пилотный проект для ознакомления в функциями и результатами работы CTRLHACK.

ЛИЦЕНЗИРОВАНИЕ

Ежегодная подписка (срочная лицензия на 1 год).

По количеству узлов симуляций.
Дополнительный модуль интеграции с SIEM.
Организационные подразделения.
Два уровня технической поддержки.

ПИЛОТ

Простой и быстрый пилот.
Небольшие требования к ресурсам.
Запуск пилота за 2 часа.
Практический результат на реальных симуляциях.

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

СПАСИБО!

ВСЕГДА РАДЫ СОТРУДНИЧЕСТВУ