Платформа симуляции атакующих техник

CTRLHACK

Общее описание

CTRLHACK – российский продукт класса Breach and Attack Simulation.

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.

Какие задачи решает?

CTRLHACK поможет определить реальный уровень защищенности инфраструктуры

Проведение симуляций атакующих действий хакеров на постоянной основе позволяет выявить и устранить проблемы в работе средств защиты и повысить эффективность SOC.

ПРОВЕРКА СРЕДСТВ ЗАЩИТЫ

Какие из атакующих действий блокируют средства защиты?
Как работают средства защиты в разных сегментах сети?

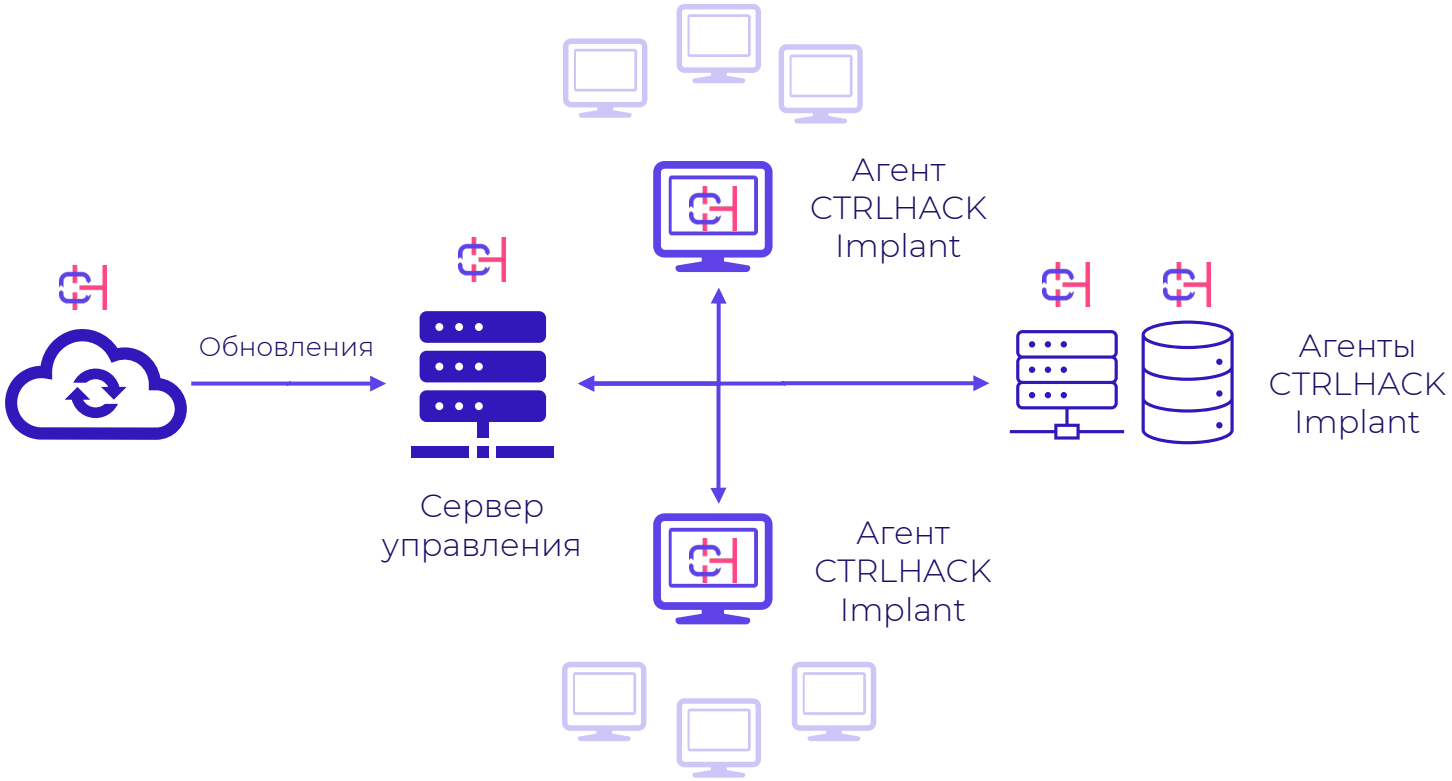
ДЕТЕКТИРОВАНИЕ ТЕХНИК

Какие атакующие техники не детектируются? Какие события для каждой атакующей техники есть в SOC, а каких не хватает?

РАЗВИТИЕ SOC

Формируются ли инциденты в SOC? Как команда реагирует на инциденты? Как быстро устраняются инциденты?

Состав платформы



Сервер управления

On-premise или облако

Агент

Windows, Linux, MacOS

Контейнеры

Бесконфликтность со средствами защиты

Автоматический запуск заданий по расписанию

Агенты

Для симуляций необходимы агенты

Агент получает с сервера управления задание со сценарием симуляции, выполняет задание и возвращает результаты на сервер управления.

- Дистрибутив агента скачивается непосредственно из интерфейса сервера управления
- Рекомендуется устанавливать агенты в каждом сегменте сети
- Агент должен иметь сетевой доступ к серверу управления

Для работы CTRLHACK не нужно вносить изменения в инфраструктуру

Группировка агентов по организационным подразделениям

Как это работает

Симуляция – заданная в скрипте последовательность действий

Безопасно

- Скриптовый язык для симуляции
- Можно создать сложные сценарии
- Подробный протокол активности в рамках симуляции
- Откат внесенных атакующей техникой изменений

Основные функции

Проверка средств защиты периметра и конечных точек

Модуль предназначен для проверки блокирования средствами защиты актуальных вредоносных файлов и попыток соединения с адресами из «черных» списков

Основной модуль – атакующие техники по стадиям матрицы MITRE

Модуль предназначен для проверки детектирования актуальных атакующих техник, применяемых хакерами после проникновения в сеть

Первичный доступ

Симуляция – работа с реальными вредоносными адресами и файлами

Без запуска. Только соединение, скачивание и выкладывание на диск

- Соединение с бот-серверами
- Скачивание через web вредоносных файлов
- Получение вредоносных файлов по e-mail

Постоянно обновляемая база адресов и экземпляров вредоносных файлов

ABUSE.ch

Первичный доступ

- Модуль позволяет проверить:
  - Работу периметровых средств защиты.
  - Работу средств защиты почтовых коммуникаций.
  - Работу средств защиты рабочих станций.
  - Фиксацию инцидентов в SOC.
- Результаты проверки помогут:
  - Определить проблемы в настройках средств защиты.
  - Обнаружить отличия в политиках в разных сегментах сети.
  - Проверить готовность средств защиты к отражению актуальных атак.

Базовые атакующие техники

Симуляция – действия в ОС, специфичные для атакующих техник

ФАЙЛЫ | РЕЕСТР | ПРОЦЕССЫ | СЕТЬ

Симуляция техник по разным стадиям атаки

MITRE | ATT&CK®

- Более 200 реализаций техник
- Техники для ОС Windows, Linux, MacOS
- Атомарные техники и сценарии

Постоянно обновляемая база атакующих техник

Базовые атакующие техники

Пользователь всегда может:

- Посмотреть исходный код скрипта симуляции.
- Внести необходимые изменения.
- Создать свои собственные скрипты симуляций.

Исходный код скрипта
erase_eventlog_undetect_wevtutil для техники T1070.001.

Описание

```
{
  "labels": [
    "platform/windows",
    "react/block",
    "threat/high",
    "tactic/defense_evasion"
  ],
  "short_description": "Удаление событий windows eventlog посредством изменения файла логгирования
10 может не работать",
  "mitre": "T1070.001",
  "name": "erase_eventlog_undetect_wevtutil"
}
```

Параметры

```
{
}
```

Исходный код

```
load('lib://std/process/v1', 'process')
load('lib://std/file/v1', 'file')
load('lib://std/tool/v1', 'tool')

get_log         = "cmd.exe /c wevtutil gl Security"
set_log         = "cmd.exe /c wevtutil sl Security /lfn:\"{f}\""
clean_log       = "cmd.exe /c wevtutil cl Security"
del_logfile     = "cmd.exe /c del /f /q {f}"
stop_eventlog   = "cmd.exe /c net stop eventlog /Y"
start_eventlog  = "cmd.exe /c net start eventlog"

def log_parse(log):
    t = ""
    for l in log.splitlines():
        if l.find("logFileName") != -1:
            t = ":".join(l.split(":")[1:]).strip()
            break

    return t
```

Базовые атакующие техники

По результатам выполнения симуляции формируется детальный отчет.

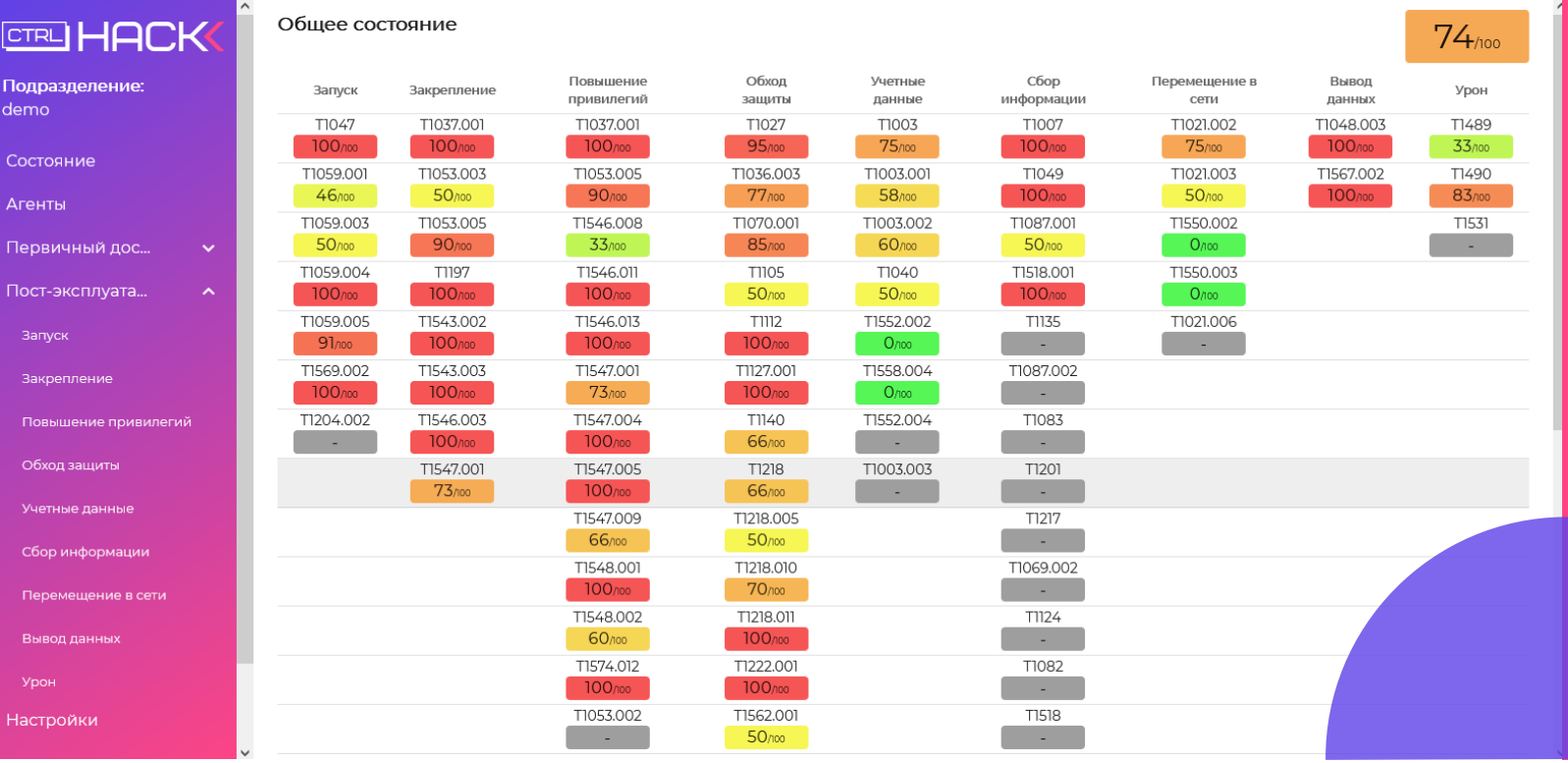
В отчете указаны:

- Адреса узлов.
- Полная информация о всех действиях во время симуляции (команды с указанием параметров, файлы, ключи реестра, сетевые соединения и т.д.).
- Полная информация о всех действиях по время процедуры «отката».

IP Хоста	Техника	Тип	Данные
10.0.0.6	certutil_download_urlcache_obfuscated (T1105)	check_point	{ "args": { "args": [], "cmd": "cmd.exe /c certutil -[illegible]urlc[illegible]ache -s[illegible]lit http://live.sysinternals.com /psversion.txt tempfile.txt", "env": [], "wait": true }, "fn_name": "process.run" }
10.0.0.6	certutil_download_urlcache_obfuscated (T1105)	check_point	{ "fn_name": "process.run", "result": { "exit_code": 0, "log": "**** Online ****\r\ 0000 ...\r\n 0027\r\nCertUtil: -URLCache command completed successfully.\r\n", "message": "", "pid": 4504, "result": true } }
10.0.0.6	certutil_download_urlcache_obfuscated (T1105)	check_point	{ "args": { "path": "tempfile.txt" }, "fn_name": "file.delete" }
			{ "fn_name": "file.delete",

Базовые атакующие техники

- Модуль позволяет проверить:
  - Работу средств защиты рабочих станций.
  - Полноту сбора событий с рабочих станций и серверов.
  - Правила детектирования техник в SIEM.
  - Формируются ли инциденты в SOC.
  - Как проводится реагирование на инцидент.
- Результаты проверки помогут:
  - Определить все ли необходимые события поступают в SIEM.
  - Корректно ли работают правила детектирования.
  - Разработать новые правила детектирования.

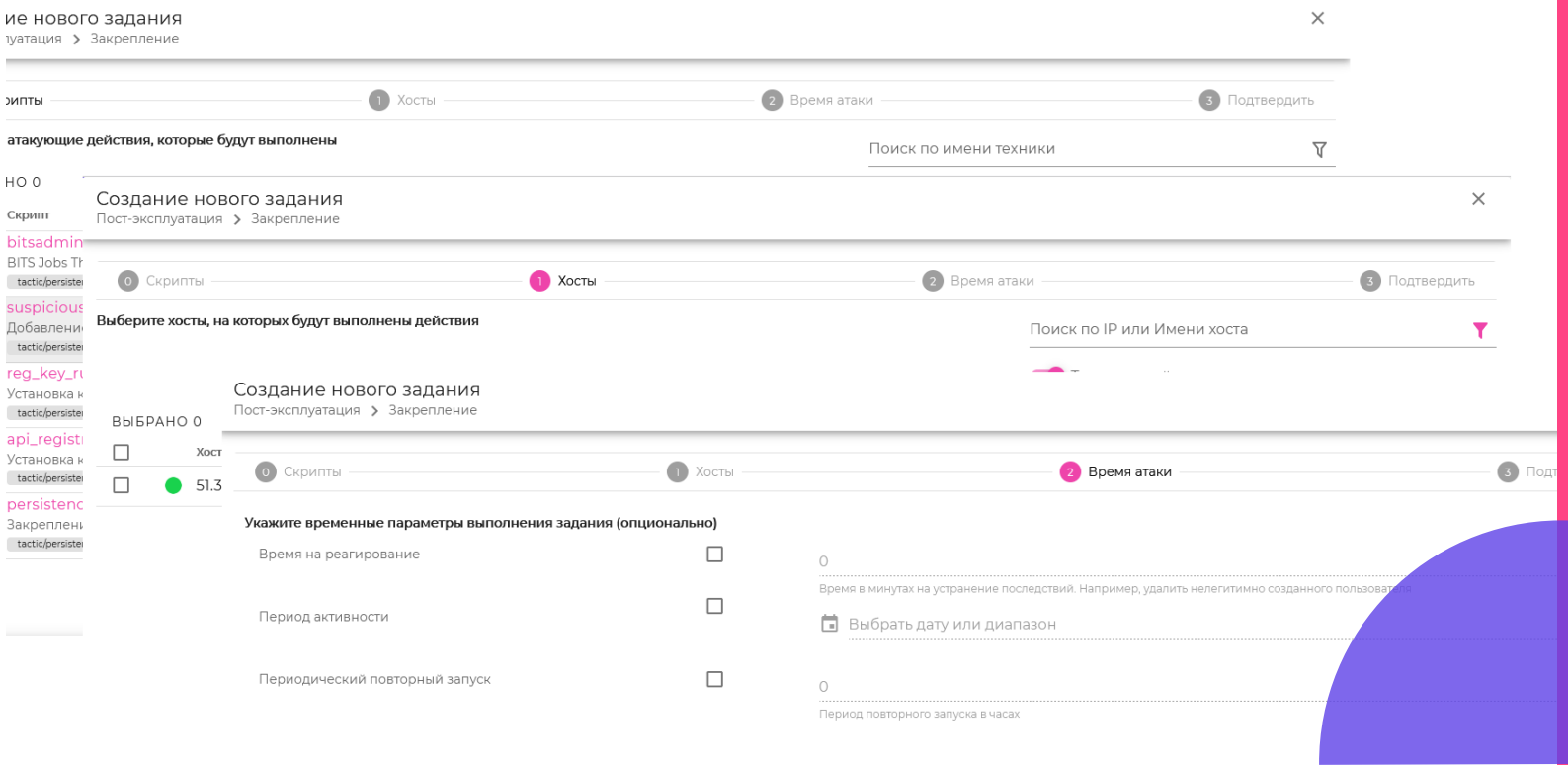


Управление платформой запуск симуляций и анализ результатов проводится в удобном и понятном интерфейсе

ИНТЕРФЕЙС

Результаты выполнения симуляций и оценка рисков для каждой стадии проведения атаки отображаются в графическом виде.

Можно получить как сводную оценку текущего состояния киберзащиты, так и детальный отчет по каждой атакующей технике.



Формирование заданий и их запуск производится с использованием пошагового конструктора

ЗАДАНИЯ

Для каждого задания можно выбрать набор узлов для симуляции, скрипты атакующих техник, а также задать параметры запуска.

Для задания можно задать расписание запуска, а также время на реагирование команды защиты.