АВТОМАТИЧЕСКАЯ СИМУЛЯЦИЯ КИБЕРАТАК

в комплексной системе защиты компании

CTRLHACK

Breach and Attack Simulation

- **Симуляция** различных действий хакеров
  - Выполнение операций в инфраструктуре, а не моделирование
- Проверка работы средств защиты
  - Различные средства защиты и SOC
- Проверка процессов
- Автоматический или полуавтоматический режим

Не замена пентестам

Существующие процессы

- Процесс управления уязвимостями

  Наиболее качественный процесс. Но совсем не работает с TTP

- Процесс Threat Intelligence

  Работа только с конкретными экземплярами. В продвинутых случаях ручная работа по TTP

- Пентесты (возможно red team)

  Работа только по отдельным векторам и части инфраструктуры. Эпизодическая работа

- Киберучения

  Не на своей инфраструктуре. Только тренировка персонала

Нет полной картины

Нет постоянной работы

Примеры атак

2021

E-mail, Word, macro

Cobalt Strike DLL

rclone.exe

ntdsAudit.exe

cmd:
ping, ipconfig, tasklist, systeminfo, nltest, net group, net user

SolarWinds

powershell

auditpol

scheduled task

удаленная остановка сервисов безопасности

облачный диск

2022

E-mail, Word, macro

Cobalt Strike DLL

Zerologon

powershell

cmd:
ping, nslookup nltest, net group

Sodinokibi (aka REvil)

сбор данных из общих папок

BloodHound

BITSAdmin

powershell

scheduled task

GPO для блокирования Windows Defender

Сканер уязвимостей нам не поможет

Даже с запуском эксплойтов

Симуляция действий хакеров

Проверено во время пентеста (red team):

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Phishing	User Execution	Browser Extensions	Process Injection	Modify Registry	Brute Force	Account Discovery	Exploitation of Remote Services	Data from Local System	Encrypted Channel	Exfiltration Over Web Service	Data Encrypted for Impact
				Process Injection	Network Sniffing	Network Share Discovery		Data from Network Shared Drive			
						Network Sniffing					

Используемые хакерами техники:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 техник	10 техник	17 техник	12 техник	32 техники	14 техник	22 техники	9 техник	15 техник	16 техник	8 техник	13 техник

Что делает BAS (часть 1)

- Позволяет запустить и проверить то, что не может сканер уязвимостей

  А это большая часть выполняемых хакером действий

- Позволяет проверить сразу много разных кибератакующих техник

  Руками это сделать невозможно

- Позволяет покрыть всю инфраструктуру практически за один запуск

  Это позволит выявить проблемы и отличия в разных сегментах сети

Все это автоматически

Не нужны глубокие знания хакерских техник

Блокирование кибератак

Проблемы блокирования кибератак

СЗИ

1. Большое количество техник не блокируется СЗИ
2. Нет понимания что реально блокируется, а что нет
3. Использование легитимных утилит
4. Использование инструментов ОС

SIEM

1. Большое количество «фолсов» для техник «из коробки»
2. Сбор событий. Покрытие всей сети
3. Развитие правил. SIEM не «черный ящик»

Детектирование техник. Реальность

5 из 14 топ техник MITRE детектируются

80% техник MITRE не покрываются правилами, поставляемыми вендорами SIEM

15% правил, поставляемыми вендорами SIEM не работают корректно в реальной инфраструктуре

190+ описаний различных техник в матрице MITRE

Отчет компании Cardinalops «2022 The state of SIEM detection risk»

Детектирование техник. Реальность

Результаты применения CtrlHack

01 30-70% техник не блокируется

02 Для Linux до 90% техник не блокируется и не детектируется

03 Для 30% техник нет событий в SIEM

04 Различия в настройках СЗИ в разных сегментах сети

05 Отличия в полноте сбора событий в разных сегментах сети

Что делает BAS (часть 2)

- Даст картину по работе разных средств защиты
- Позволяет понять какие из кибератакующих техник не будут заблокированы в вашей сети
- Даст всю информацию для развития правил детектирования
- Позволит проверить как работают процессы реагирования
- Дополнительно. Даст возможность оценить работу «внешнего» SOC

Все это автоматически

Не нужны глубокие знания хакерских техник

CTRLHACK

симуляция кибератакующих техник

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 эффективны процессы детектирования и реагирования.

Минцифры России

В реестре Российского ПО

Как это работает

Для симуляций необходимы агенты

- Дистрибутив агента скачивается из интерфейса управления
- Windows, Linux, MacOS

Симуляция – заданная в скрипте последовательность действий

- Скриптовый язык для симуляции
- Подробный протокол активности в рамках симуляции
- Откат внесенных атакующей техникой изменений

Для работы CTRLHACK не нужно вносить изменения в инфраструктуру

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

- Посещение «вредоносных» сайтов
- Скачивание через web вредоносных файлов
- Получение вредоносных файлов по e-mail

Постоянно обновляемая база адресов и экземпляров вредоносных файлов

ABUSE.ch

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

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

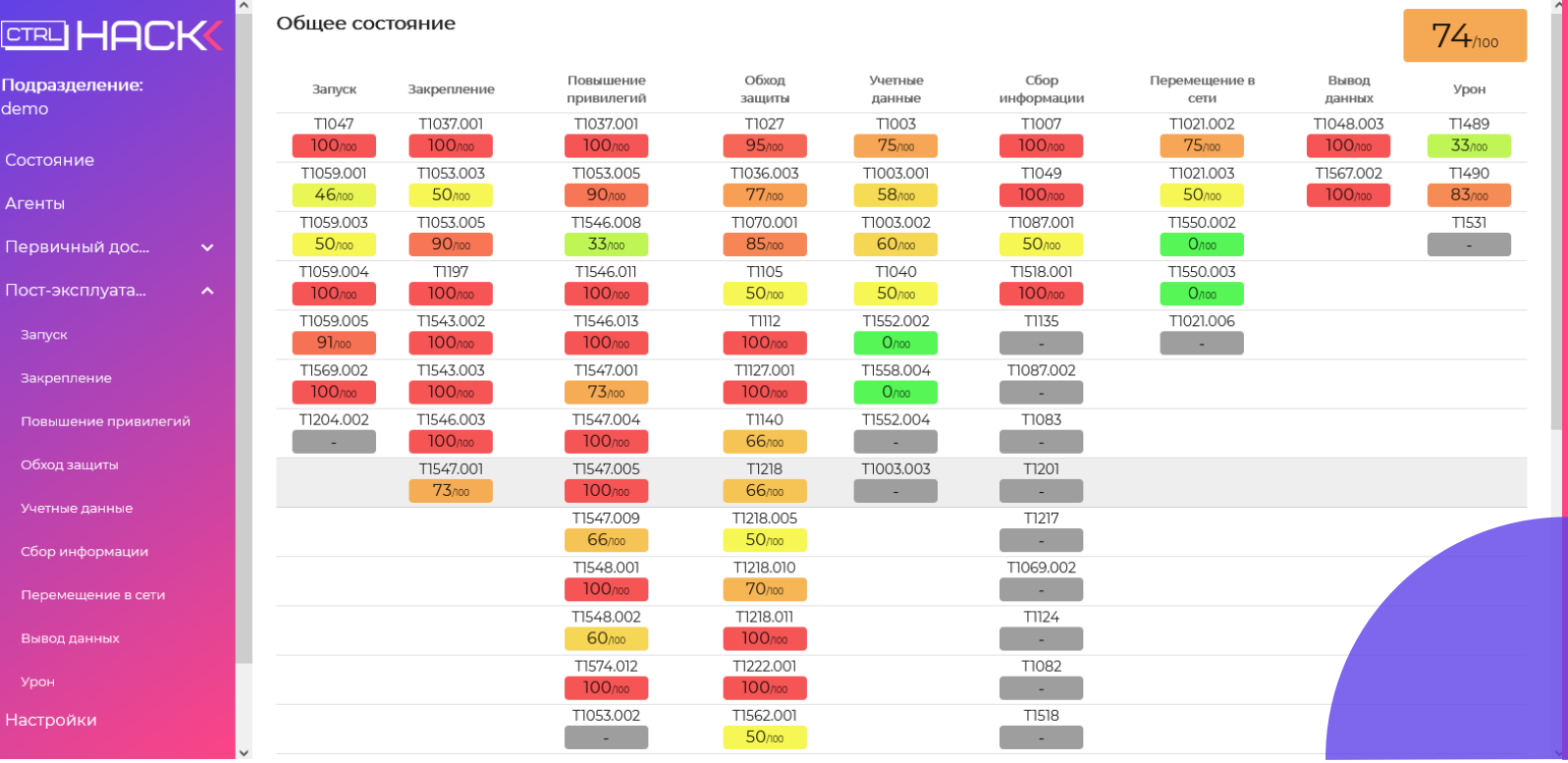
Какие из атакующих действий блокируют средства защиты?
Как работают средства защиты в разных сегментах сети?

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?



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.

WWW.CTRLHACK.RU

СПАСИБО!

ООО «КонтролХак»

127299, г. Москва, ул. Космонавта Волкова, д.20

+7 495 789-72-97

info@ctrlhack.ru