интенсив
Архипелаг
2121

АГЕНТСТВО СТРАТЕГИЧЕСКИХ ИНИЦИАТИВ
20.35 УНИВЕРСИТЕТ
ПЛАТФОРМА НТИ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

CTRLHACK

Платформа симуляции кибератак в инфраструктуре организации

https://pt.2035.university/project/ctrlhack-platforma-simulacii-kiberatak-v-infrastrukture-organizacii

Проблема

30 – 70% атакующих техник хакеров не детектируются

1. Как в реальности работают средства защиты?
2. Какие именно техники не детектируются?
3. Все ли необходимые данные собираются в сети?

Как получать эту информацию постоянно?

Решение

Симуляция кибератакующих техник в инфраструктуре компании

По результатам симуляций команда киберзащиты сможет определить:

1

СРЕДСТВА ЗАЩИТЫ

корректно ли работают средства защиты

2

ТЕХНИКИ

какие атакующие техники не детектируются

3

SOC

формируются ли инциденты в SOC

4

СОБЫТИЯ

какие события есть в SIEM, а каких не хватает

Продукт

CtrlHack – платформа симуляции кибератак в инфраструктуре организации

01 Выполняются действия, имитирующие действия хакеров

02 Более 200 атакующих техник

03 Отдельные техники могут объединяться в сценарии

04 Проверка работы средств защиты

05 Оценка достаточности событий в SIEM

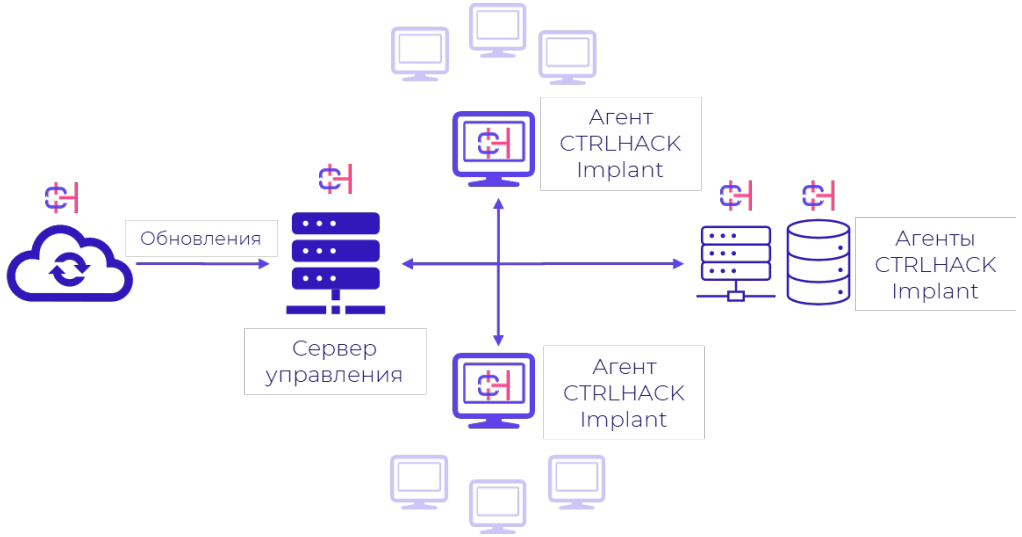
06 Проверка корректности правил детектирования в SOC

В результате детектируется на 30-50% больше атакующих техник

Продукт

CtrlHack – платформа симуляции кибератак в инфраструктуре организации

- Сервер управления on-prem или в облаке
- Подробный отчет о выполненных действиях
- Для работы нужны агенты
- Автоматическое выполнение Запуск по расписанию



Конкуренты

Аналогичных российских разработок нет.

Пока...

В России представлены Cymulate и Pentera

На зарубежных рынках около 10 вендоров. SafeBreach, AttackIQ, и др.

ПРЕИМУЩЕСТВА CTRLHACK

Безопасные симуляции.
Без запуска вредоносных файлов

Открытые сценарии симуляций.
Все действия - в скриптах..

Не нужно изменять инфраструктуру и отключать средства защиты

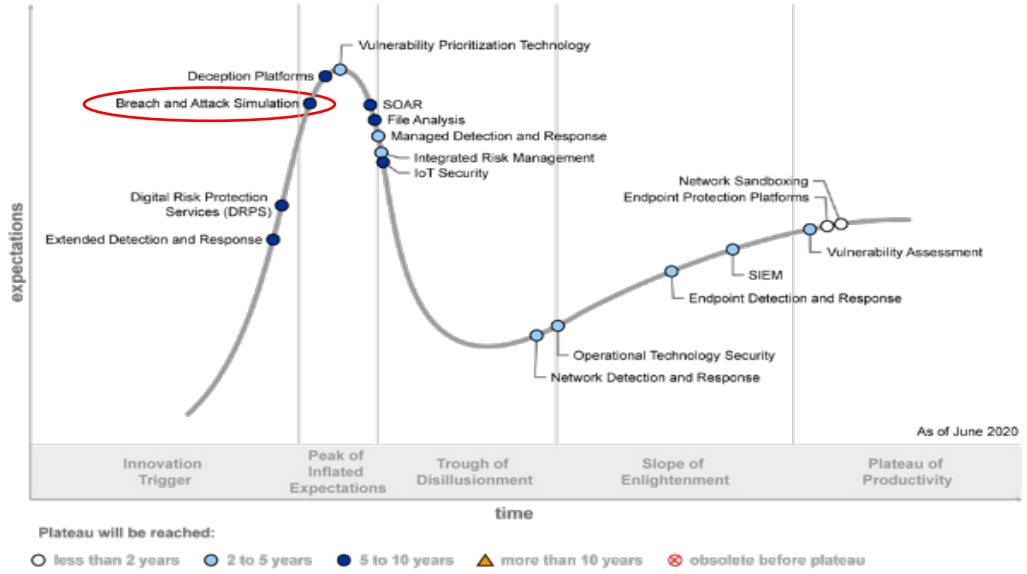
Рынок

CTRLHACK относится к решениям класса Breach and Attack Simulation (BAS)

- Показатель проникновения на рынок - от 1% до 5% целевой аудитории.
- Рост глобального рынка до 1 млрд. 416 млн. $ в год к 2025 г.
  CAGR - 32.47%
- Объем российского рынка к 2025 г. – 2 млрд. руб.
  До 300 покупателей.

Планируем занять 30% рынка

Hype Cycle for Security Operations, 2020



Source: Gartner
ID: 467096

Бизнес-модель

ЛИЦЕНЗИИ

Ежегодная подписка

Стоимость зависит от набора функциональных модулей и размера сети

СЕРВИС

Совместные с партнерами сервисы

- Оценка рисков
- Непрерывный контроль защищенности
- Совершенствование SOC

ПАРТНЕРЫ

Продажи через партнеров

Системные интеграторы

ИБ интеграторы

Планируемая выручка в 2023 году – 185 млн. руб.

Расходы в 2023 году 67 млн. руб.

Динамика развития

12 пилотных проектов

Организации с гос. участием, телеком, банки, энергетика

Результат успешного пилота

Государственная компания

- Выявлены и устранены проблемы в процессах обновления и настроек антивируса
- Выявлены и устранены проблемы с получение событий безопасности
- На 30% увеличено покрытие детектами в SOC атакующих техник

2019

Старт разработки

Сентябрь 2020

Отработка MVP

Первые общения с клиентами, CustDev, первое пилотное внедрение

Январь 2021

Выход на рынок

Активное общение с клиентами, пилотные проекты, маркетинговые активности.

Планы развития

2022

- Интеграция со средствами защиты информации
- Создание исследовательской лаборатории для поиска новых уязвимостей и разработке уникальных методов проведения тестов на проникновение
- Выпуск собственных отчетов об атаках и уязвимостях, участие в 2 конференциях, внедрение не менее чем в 7 новых клиентах

2023

- Исследования по созданию модуля построения векторов атак на базе методов искусственного интеллекта
- Получение патента на технологию безопасной имитации атак
- Внедрение не менее чем в 15 новых клиентах

Предложение для Партнёра

Пилотные проекты для корпоративных клиентов:

Крупные компании (Топ 300 компаний России):

- Банки
- Страховые компании
- Нефтегаз
- Ретейл
- Промышленность
- и др.

Уже по итогам пилотного проекта повышается эффективность детектирования атакующих техник

Команда

Куприн Сергей

Сооснователь, CEO

Общее руководство и тех. развитие проекта

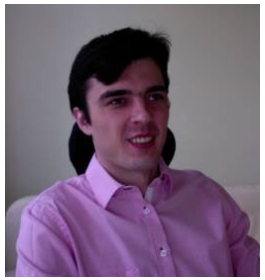
ОПЫТ: Руководство НИОКР и командой из 50 чел. Продажи проектов с бюджетом более 100 млн. руб. Развитие компетенции по исследованиям в области ИБ.

Пятаков Максим

Сооснователь, CMO

Продажи, продвижение продукта

ОПЫТ: Создал «с нуля» подразделение с оборотом более 250 млн. руб. Руководил НИОКР и проектами по построению систем киберзащиты. Стартап Академия МШУ Сколково



Бачурин Егор

CTO

Руководство разработкой продукта

ОПЫТ: Более 10 лет в области разработки ПО. Опыт в разработке распределенных высоконагруженных систем

Команда 10 человек

14 лет опыта в разработке средств защиты и имитаций взлома корпоративных сетей

интенсив
Архипелаг
2121

АГЕНТСТВО СТРАТЕГИЧЕСКИХ ИНИЦИАТИВ

20.35 УНИВЕРСИТЕТ

ПЛАТФОРМА НТИ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Контакты

Сайт	CTRLHACK.RU
Телефон	+7 (903) 589-72-97
email	m.pyatakov@ctrlhack.ru