FINDLER OSINT

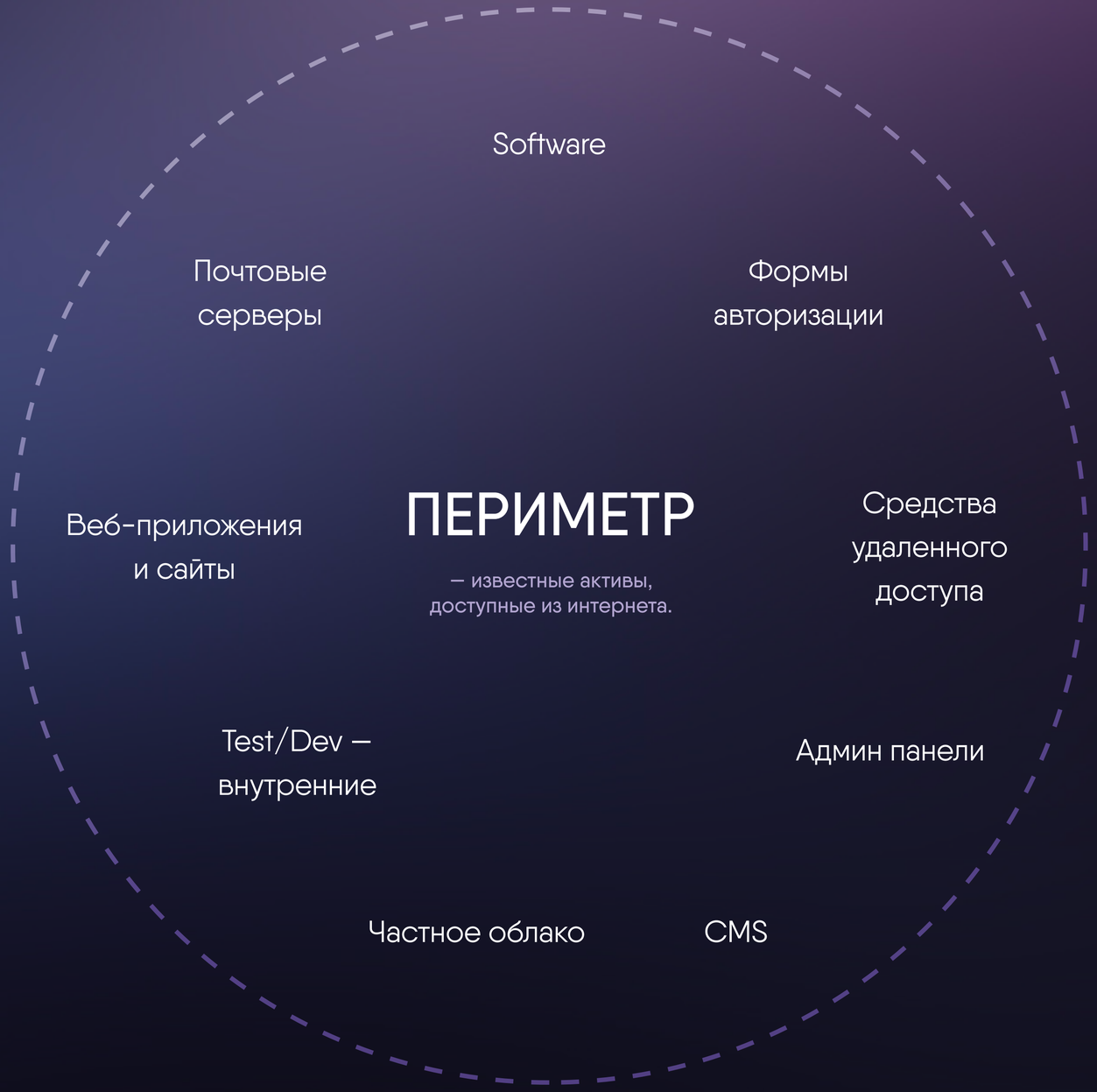
Findler

Почему киберразведка критична — с неё начинается большинство атак на компанию

- Вся нужная информация доступна в открытых источниках.
- OSINT ≠ взлом, это про поиск данных.

Что видит сотрудник

ПЕРИМЕТР — известные активы, доступные из интернета (IP, домены, мобильные приложения).



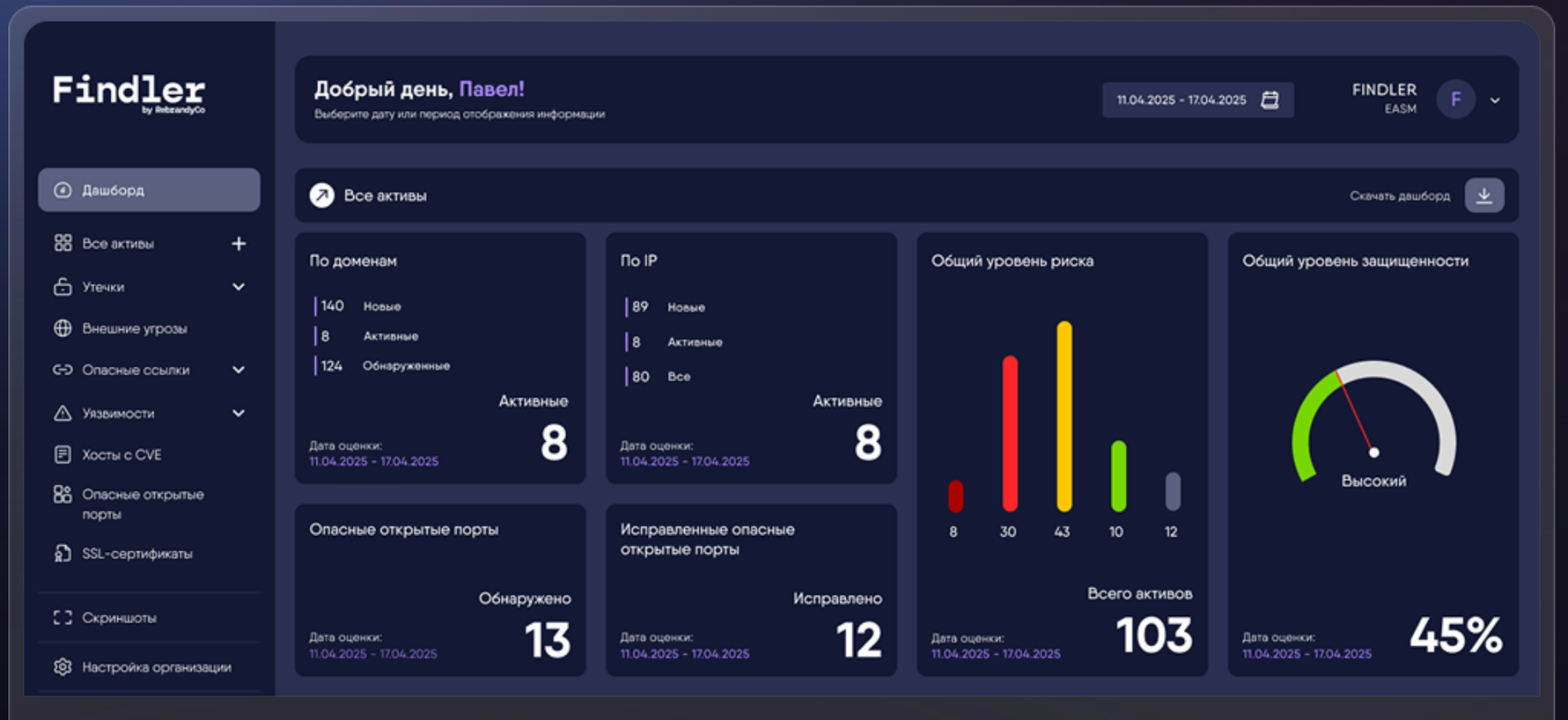
Что видит злоумышленник (поверхность атаки)

О решении

FINDLER OSINT – облачное решение для киберразведки, контроля цифровых активов и ранней идентификации киберугроз.

FINDLER находится в реестре российского ПО

Подробнее:



FINDLER OSINT в цифрах

200+ млрд.

Записей об утечках персональных данных.

> 20 000

Веб-приложений находятся на ежедневном мониторинге.

> 500 раз

Наша команда использовала FINDLER OSINT для проведения пентестов.

> 100 000

Активов обнаружено.

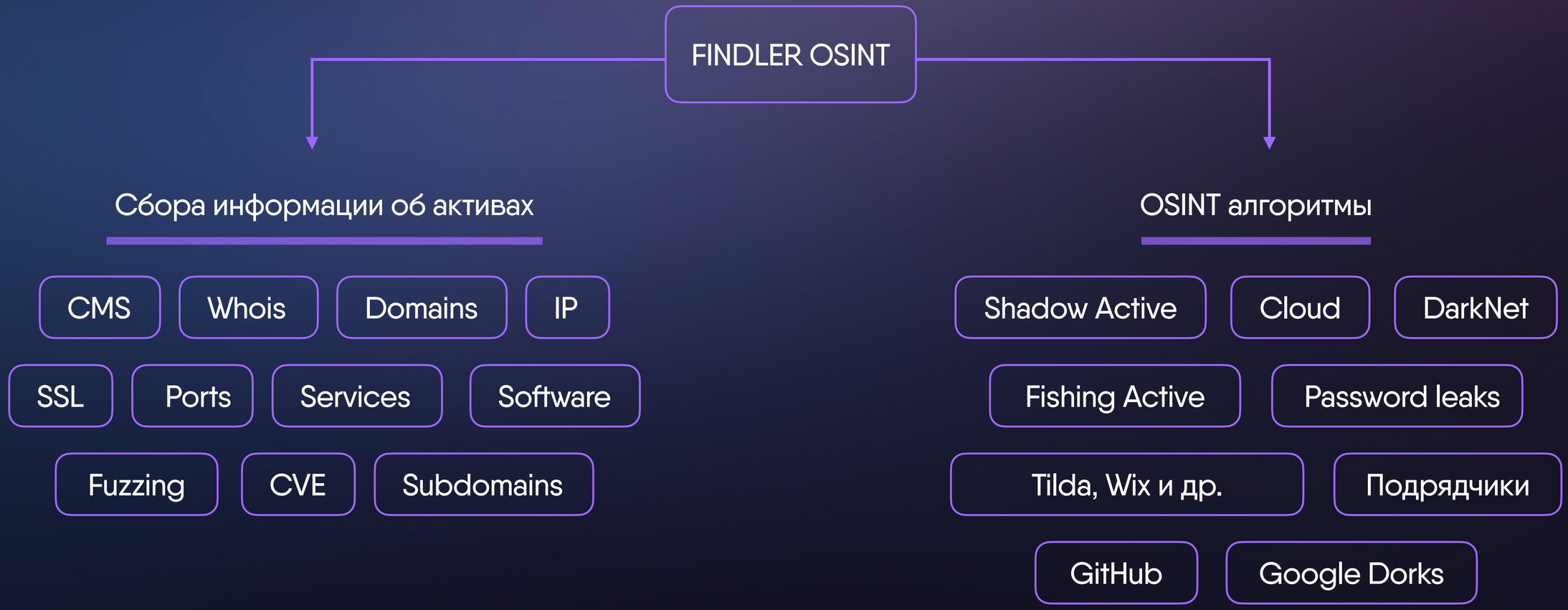
> 150 ТБ

Конфиденциальных данных обнаружено.

> 3 млн.

Подсетей используется для OSINT.

Модули продукта — из чего состоит



Алгоритм работы

1. Внесение первичных или новых данных в систему

2. Непрерывный процесс мониторинга:

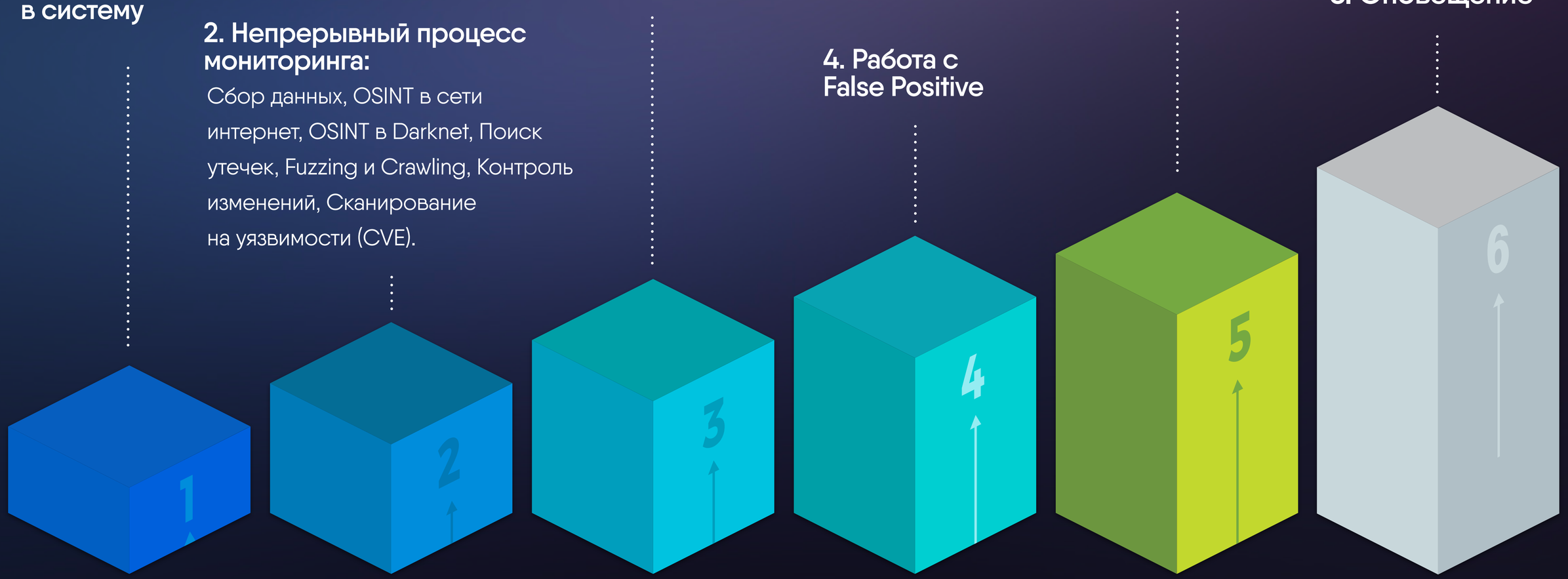
Сбор данных, OSINT в сети интернет, OSINT в Darknet, Поиск утечек, Fuzzing и Crawling, Контроль изменений, Сканирование на уязвимости (CVE).

3. Верификация и анализ уязвимостей

4. Работа с False Positive

5. Формирование отчета

6. Оповещение



Преимущества FINDLER OSINT

Продвинутая разведка

FINDLER проводит поиск утечек на GitHub, Pastebin, облачных хранилищах и в Telegram, расширяя поле разведки за пределы даркнета. Это обеспечивает **более раннее обнаружение скомпрометированных данных**, включая персональные и технические данные, появившиеся в открытых источниках.

Глубокий анализ

Система не ограничивается доменами — FINDLER проводит **fuzzing по IP-адресам и поддоменам**, выявляя технические директории, забытые dev/test-окружения, интерфейсы администрирования, которые часто упускаются другими EASM-системами. **Это устраняет слепые зоны на периметре компании.**

Высокая точность

Конверсия более 10% при выявлении утечек — **в 10 раз выше, чем у большинства решений.** Такой уровень точности п**озволяет оперативно обнаруживать реальную утечку,** а не шум, экономя время и ресурсы ИБ-команды.

Гибкая интеграция

Легко встраивается в ИБ-инфраструктуру и развивается с учётом кейсов заказчиков.

Адаптация под задачи клиента

FINDLER дорабатывает алгоритмы и сигнатуры по запросам заказчика, что позволяет учитывать специфику поверхности атаки и выявлять именно те угрозы, которые актуальны для конкретной компании.

ИИ-анализ уязвимостей с объяснениями на русском

FINDLER **предоставляет рекомендации по устранению уязвимости, на русском языке,** с использованием искусственного интеллекта.

Вы получите

- Мониторинг и выявление угроз 24/7
- Оповещения в реальном времени
- Контроль утечек данных
- Поиск и инвентаризацию цифровых активов компании
- Интеграцию с системами безопасности компании

FINDLER
разрабатывают этичные хакеры
для наших клиентов

RebrandyCo — это

команда экспертов, владеющая уникальными навыками и алгоритмами выявления уязвимостей в информационных системах.

Наши достижения:

- ТОП-3 в рейтинге исследователей по версии ФСТЭК России;
- В ТОП-10 по рейтингу Standoff 365 в России;
- В ТОП-10 в мире по версии Hackerone за всю историю площадки;
- Мы обладаем лицензиями ФСТЭК (ТЗКИ и СЗКИ);
- Сертифицированные специалисты OSCP и OSEP.

Findler

Нам доверяют

UNISENDER

Зенит 1925

LIFE

LEVEL TRAVEL

hh

ДИТ

inventive retail group

HOME CREDIT BANK

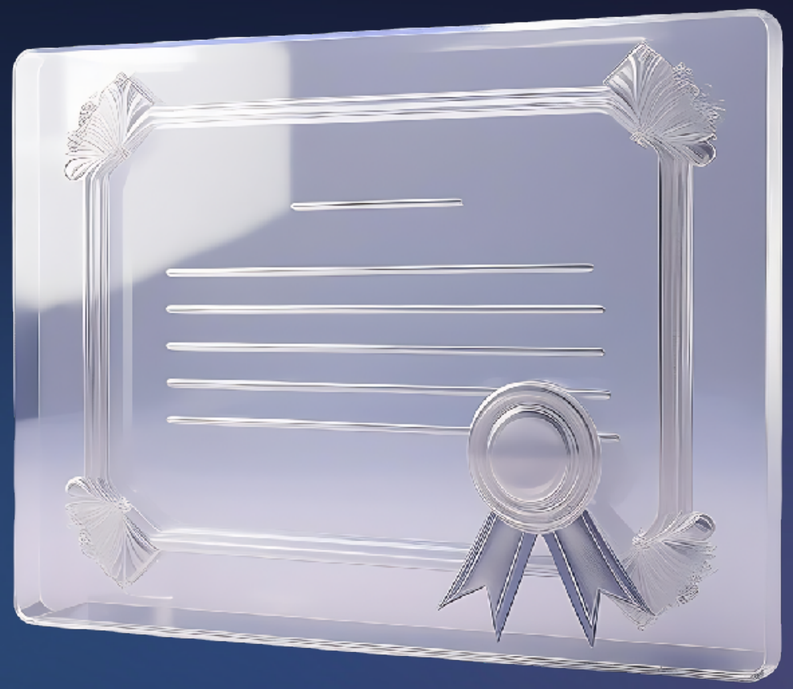
Шоколадница

inSales

МТС БАНК

re:Store

Лицензии и сертификаты

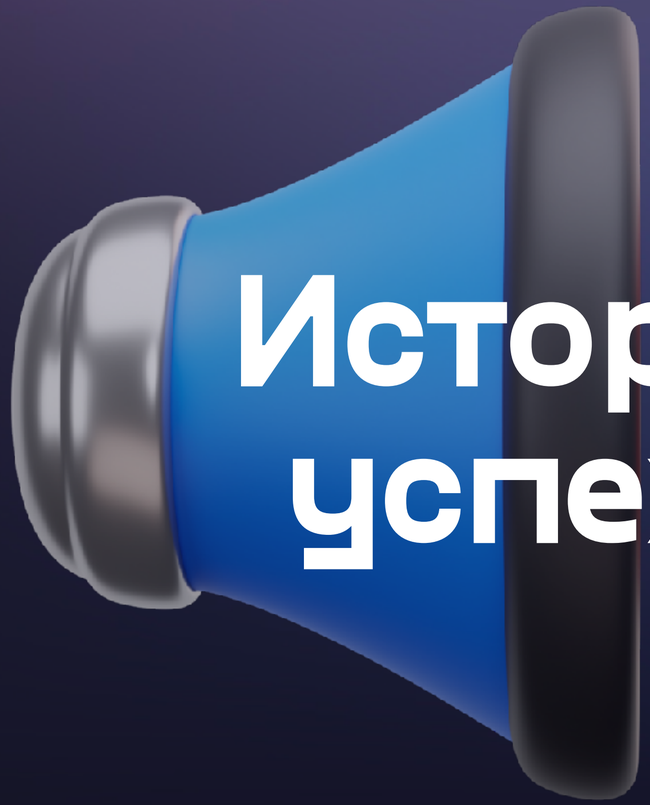


Лицензия ФСТЭК деятельность
по технической защите конфиденциальной
информации № Л024-00107-77/00667770

Лицензия ФСТЭК деятельность
по разработке и производству средств
защиты конфиденциальной информации
№ Л050-00107-77/00667771

Свидетельство о государственной
регистрации программы для ЭВМ

Реестровая запись №24273 от 04.10.2024
в реестре ПО Министерства Цифрового
Развития



Истории успеха

Мониторинг периметра

Государственная организация

На старте:

10 Объектов мониторинга.

Найдено:

> 13000 Общее количество объектов, обнаруженных за время работы.

> 6000 Количество объектов на постоянном мониторинге.

Результат:

- Предотвращена атака на Заказчика, организованная в DarkNet
- Пресечена утечка персональных данных.

10% Показатель релевантности утекших учетных записей:
10% — FINDLER
< 1% — аналогичное решение

FINDLER обнаружил:

- Множество открытых портов, CVE, опасных ссылок и IP.
- Конфиденциальную информацию в открытом доступе и планирование атак в Telegram каналах.

Контроль информации

Федеральный ритейлер

Задача:

Мониторинг и контроль утечки корпоративных данных компании.

Подготовка:

Разработка индивидуальной базы тегов и скриптов под потребности Заказчика.

Реализация:

Используя специально разработанные скрипты, FINDLER производит ежедневный мониторинг множества документов по файлообменникам, «теневым» ресурсам и другим каналам распространения информации.

Результат:

В ходе мониторинга FINDLER обнаружил документ в публичном облачном хранилище, содержащий данные активных бонусных карт с различными номиналами.

FINDLER разрабатывается этичными хакерами для клиентов

FINDLER обнаружил:

- Документ, содержащий актуальную информацию о бонусных картах клиента.
- Чувствительную информацию, относящуюся к сотрудникам клиента.

Кибеpразведка

Федеральный застройщик

Задача:

Реализация фишинговой атаки на Заказчика

Подготовка:

Имея доменное имя компании, FINDLER обнаружил неучтенный поддомен компании на одном из конструкторов сайтов и учетную запись топ-менеджера компании в базе утечек.

Реализация:

Завладев поддоменом, команда RebrandyCo создала фишинговую страницу и реализовала внутреннюю e-mail рассылку по всем сотрудникам компании от лица топ-менеджера.

Результат:

Успешная реализация фишинговой атаки на сотрудников компании, в ходе которой было собрано множество паролей, в том числе сотрудников ИТ отдела.

> 100 ТБ

Более 100 ТБ скомпрометированных данных обнаружил FINDLER.

FINDLER обнаружил:

- Множество неучтенных активов компании.
- Утечку данных учетных записей сотрудников.
- Критические сервисы в открытом доступе.

Остались вопросы?
С радостью
на них ответим

+7 (499) 673 00 75
+7 (3452) 58 50 29
info@rebrandy.co
www.rebrandy.co

FINDLER OSINT