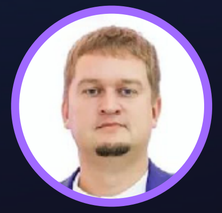
А как ваш бизнес выглядит из интернета?



Михаил Комиссаров

Региональный директор
по продажам

Findler

Что, если бы вы могли смотреть на свой бизнес глазами хакера?

- Забытые облачные хранилища
- Краденый пароль сотрудника
- Бреши в защите
- Публично доступный резервный файл
- Персональные данные «всплывшие» в даркнете

Современные киберугрозы

Киберугрозы, с которыми компании сталкиваются в реальной жизни.

- **Шифрование инфраструктуры**
- **Кража/слив персональных данных**
- **Финансовые убытки**
- **Репутационные потери**
- **Штрафы от регуляторов**

Почему киберразведка критична — с неё начинается большинство атак на компанию.

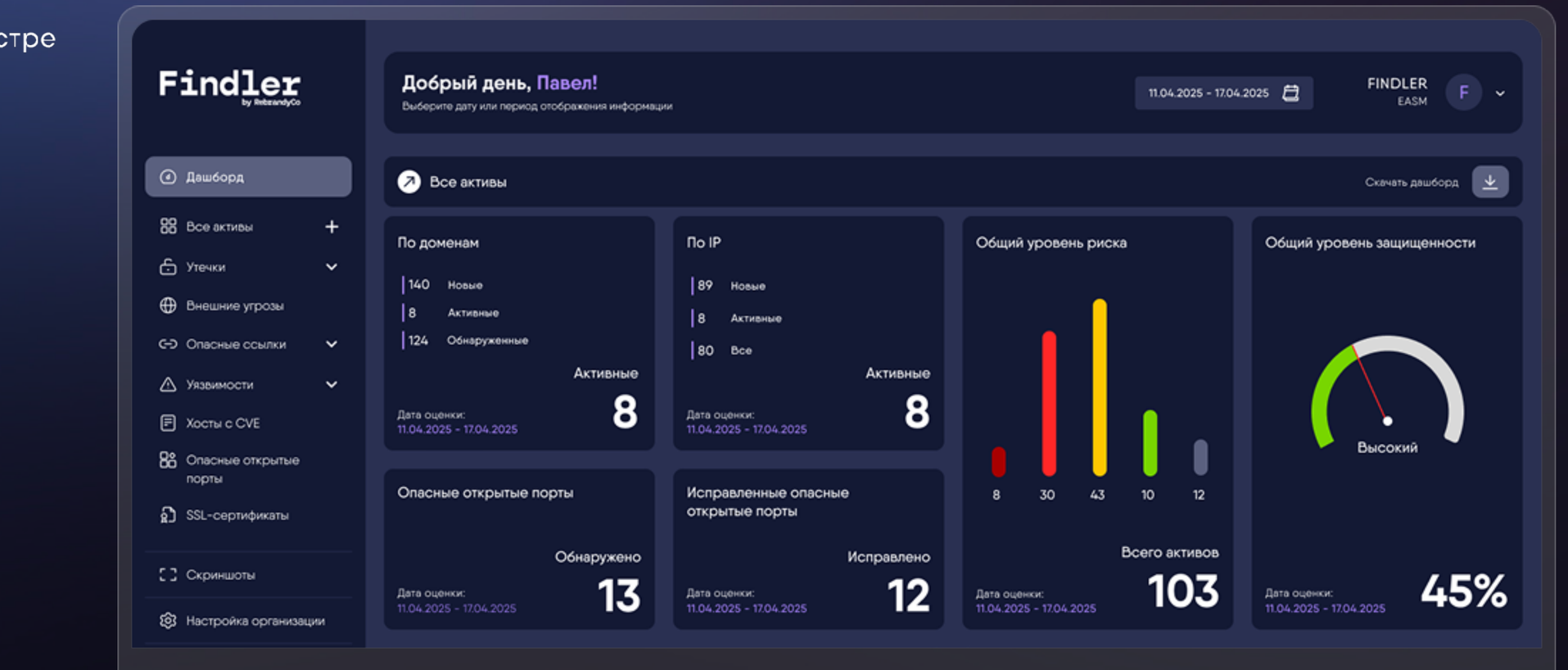
- Вся нужная информация доступна в открытых источниках.
- OSINT ≠ взлом, это про поиск данных.

Для кого?

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

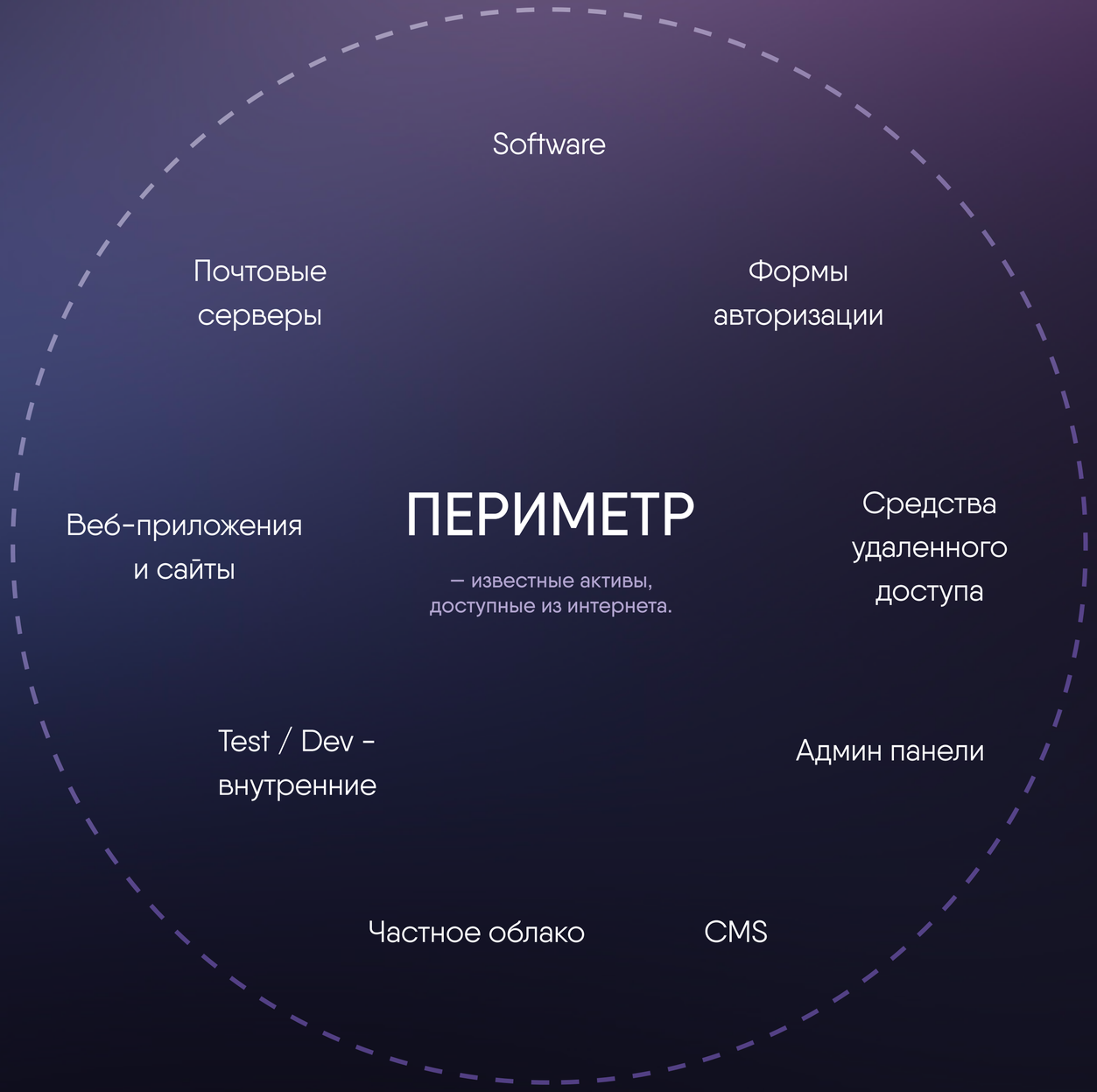
FINDLER находится в реестре российского ПО

Подробнее:

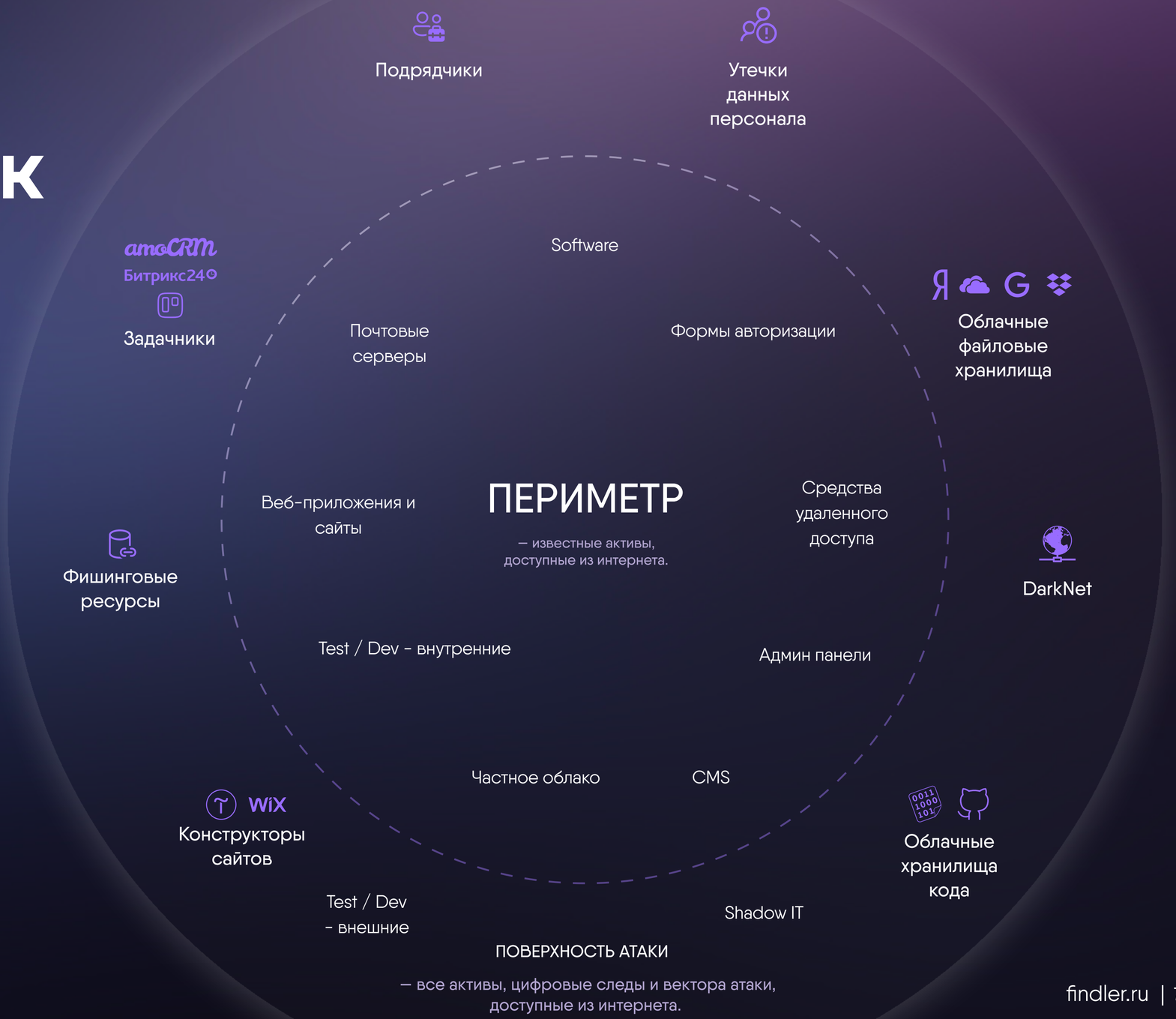


Что видите вы (периметр)

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



Что видит злоумышленник (поверхность атаки)



Преимущества для бизнеса

Выявляйте угрозы ДО инцидентов

- Слитые пароли
- Уязвимые публичные данные
- Следы подготовки атак
- Фишинговый сайты
- Аномалии на ваших страницах

Устраняйте риски БЫСТРЕЕ

- Автоматическая приоритизация: критичное vs шум
- Рекомендации по исправлению на русском языке
- Легко стыкуется с SOC/SIEM

Мониторинг периметра

Государственная организация

На старте:

10 Объектов мониторинга.

Найдено:

> 13000 Общее кол-во объектов, обнаруженных за время работы.

> 6000 Кол-во 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.

FINDLER

разрабатывают этичные хакеры для наших клиентов

RebrandyCo — это

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

Наши достижения:

- В ТОП-3 рейтинга 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 СКЗИ);
- Сертифицированные специалисты OSCP и OSEP.

Наши услуги

Тестирование
web-ресурсов
на проникновение

Анализ
защищенности
мобильных
приложений

Тестирование
на проникновение
в корпоративную
инфраструктуру

Анализ
защищенности
Wi-Fi и LAN сетей

Нагрузочное
тестирование

Обратная
разработка

Социальная
инженерия
и киберучения

FINDLER OSINT
современная
киберразведка

Демо кабинет

Давайте теперь посмотрим
личный кабинет и функционал
FINDLER OSINT

Демо кабинет доступен по ссылке:
demo.findler.ru

Findler