F.A.C.C.T.

ОБЗОР ПРОДУКТА

ATTACK SURFACE MANAGEMENT

Управление поверхностью атаки
с помощью данных киберразведки

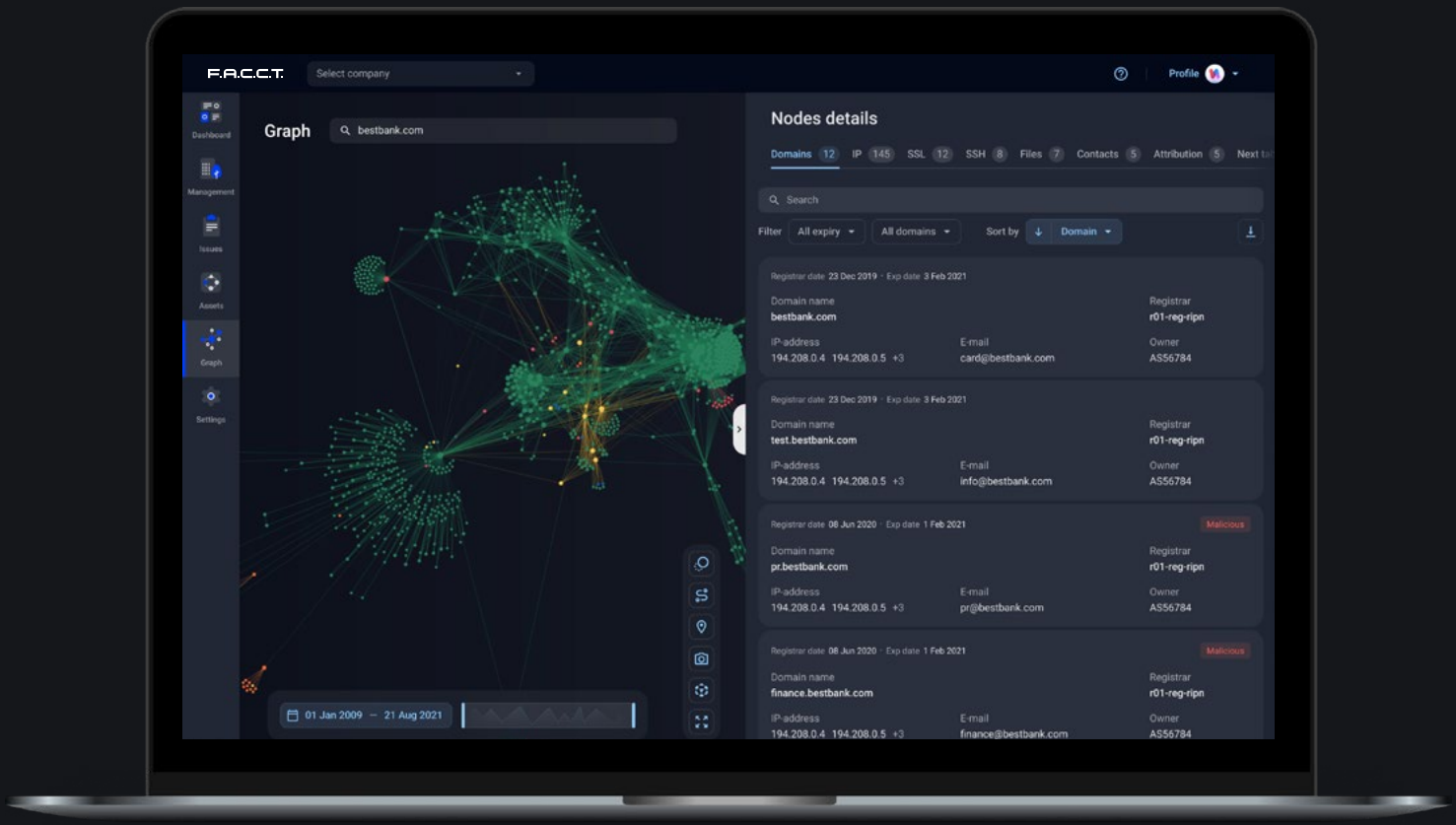
FACCT.RU

Полная картина внешней поверхности атаки

и уникальные данные для повышения уровня защищенности

Как правило, проникновения в корпоративные сети не связаны с эксплуатацией уязвимостей нулевого дня или использованием сложных инструментов. Большинство взломов происходит из-за многочисленных неотслеживаемых уязвимостей периметра, таких как непропатченные серверы, некорректные конфигурации баз данных и неконтролируемые теневые ИТ.

Attack Surface Management – это комплексное и основанное на данных кибербразведки SaaS-решение, позволяющее организациям оценивать поверхность атаки и управлять ею. Решение обеспечивает полную инвентаризацию всех интернет-ресурсов организации, выявляет уязвимости и приоритизирует критические риски для принятия должных мер.



Функционал и преимущества решения

Полная прозрачность

Не ограничиваясь сканированием пространства IPv4, Attack Surface Management выявляет и индексирует все ресурсы организации, включая теневые ИТ.

Максимальное покрытие

Attack Surface Management отслеживает все доступные извне ресурсы организации, включая локальные, облачные и гибридные решения.

Надежная защита

Управление внешней поверхностью атаки позволяет предотвратить необязательные риски и повысить уровень защищенности организации.

Обогащение контекстом

Всем проиндексированным ресурсам присваивается уровень риска, позволяющий приоритизировать действия по устранению уязвимостей.

Данные из уникальных источников

Attack Surface Management – единственное решение для управления внешней поверхностью атаки, которое обогащается данными из ботнетов, исследований вредоносных программ и дарквеба.

Быстрое начало работы

Attack Surface Management представляет собой безагентное облачное SaaS-решение, которое не требует установки ПО для начала работы.

Обнаружение критических рисков

в режиме реального времени для предотвращения угроз

Ежедневный мониторинг всех изменений внешней поверхности атаки

Выявление теневых ИТ и некорректных конфигураций

Оценка уровня защищенности с помощью уникальной информации из дарквеба

Проверенные актуальные данные для повышения уровня защищенности

Attack Surface Management выходит за рамки стандартных услуг и продуктов

Attack Surface Management превосходит существующие решения для управления внешней поверхностью атаки благодаря запатентованным технологиям и данным киберразведки.

Обогащение контекстом

Уникальные данные из признанной международными агентствами системы F.A.C.C.T. Threat Intelligence, распределенные по 8 категориям

Значимая информация

Оповещения о потенциальных проблемах, отслеживание изменений и отчеты, позволяющие предпринять эффективные действия

Непрерывный мониторинг

Постоянно обновляемые данные дают полный контроль над поверхностью атаки и ее уязвимостями

Устранение слепых зон инфраструктуры

Индексация ресурсов

Комплексный подход к мониторингу ресурсов организации

Выявление угроз

Исчерпывающий список уязвимостей с разбивкой по категориям ресурсов и уровню риска

Управление рисками и устранение недостатков

Количественная оценка рисков для приоритизации задач по повышению защищенности

Уникальные возможности

Запатентованные технологии F.A.C.C.T., лежащие в основе Attack Surface Management

- Web & Internet snapshot generator
- Network graph analysis
- Malware config extractor
- Malware protocol emulator
- Phishing predictor
- Botnet data extractor
- Dark Web scraping engine
- Vulnerability detector

Описание компании

F.A.C.C.T. — один из ведущих мировых разработчиков решений для обнаружения и предотвращения кибератак, выявления мошенничества и защиты интеллектуальной собственности в сети.

1 300+
успешных исследований по всему миру

550+
enterprise-клиентов

120+
патентов и заявок

№1
первый поставщик услуги Incident Response в России

20 млрд +
сохраняют наши технологии в бюджете клиентов ежегодно

20 лет
практики и уникальной экспертизы на рынке РФ

Технологии и инновации

Кибербезопасность

- Threat Intelligence
- Управление поверхностью атаки
- Защита электронной почты
- Анализ сетевого трафика
- Детонация ВПО
- Защита конечных станций (EDR)
- XDR

Противодействие мошенничеству

- Противодействие мошенничеству client-side
- Адаптивная аутентификация
- Защита от ботов
- Выявление платежного мошенничества
- Поведенческий анализ

Защита бренда

- Антифишинг
- Антипиратство
- Антимошенничество
- Антиконтрафакт
- Выявление утечек данных
- Защита VIP-персон

Портфолио услуг

Аудит и консалтинг	• Анализ защищенности • Тестирование на проникновение • Red Teaming • Оценка соответствия и консалтинг	• Выявление следов компрометации • Проверка готовности к реагированию на инциденты
Обучающие программы	• Для технических специалистов • Для широкой аудитории	• Мастер-классы для детей
Реагирование на инциденты и цифровая криминалистика	• Реагирование на инциденты • Реагирование на инциденты по подписке	• Цифровая криминалистика • eDiscovery
Managed Services	• Managed Detection • Managed Threat Hunting	• Managed Response
Исследование высокотехнологичных преступлений	• Исследование киберпреступлений	

Предотвращаем и исследуем киберпреступления с 2003 года