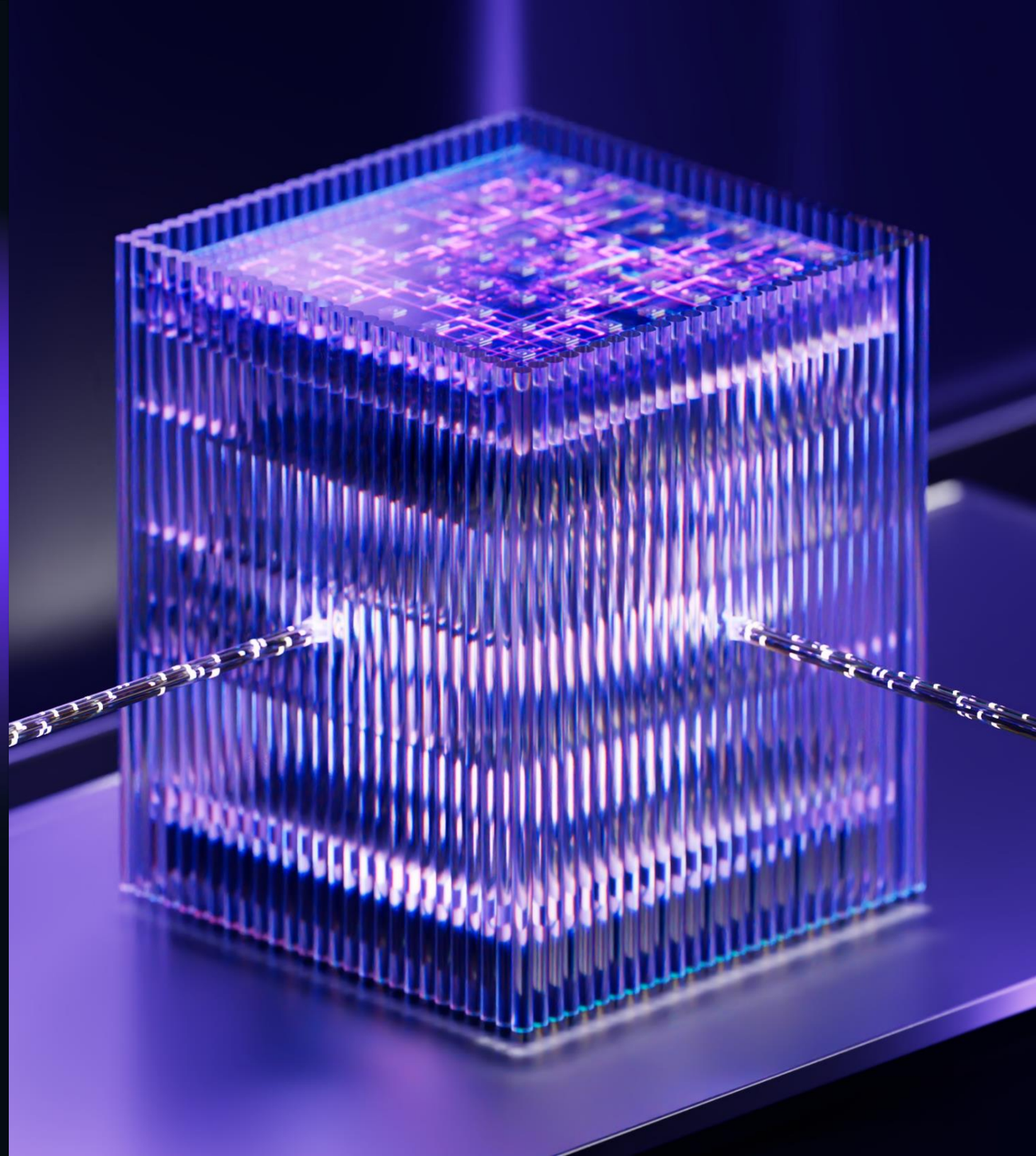
F.A.C.C.T.
Fight Against Cybercrime Technologies

Истории из практики: как продукты F.A.C.C.T. защищают наших клиентов

Денис
Мерцалов

Директор по работе с партнёрами

+7 903 592 28 02
d.mertsalov@facct.ru



Софтлайн – партнёр №1.
Дружба, доверие и экспертиза.

Ежегодное партнёрская конференция F.A.C.C.T. 2024 год

История F.A.C.C.T.

F.A.C.C.T.

Основание F.A.C.C.T.

Запуск Threat Intelligence

Запуск платформы Fraud Protection

Managed XDR

Unified Risk Platform

2003 • • • 2011 2013 2014 2015 2017 • • • 2021 2022

Открытие первого в России CERT

Запуск MXDR

Запуск Digital Risk Protection

Запуск Attack Surface Management

Запуск Business Email Protection

F.A.C.C.T. как частное кибердетективное агентство

2003–2024

Разработка собственных продуктов по кибербезопасности

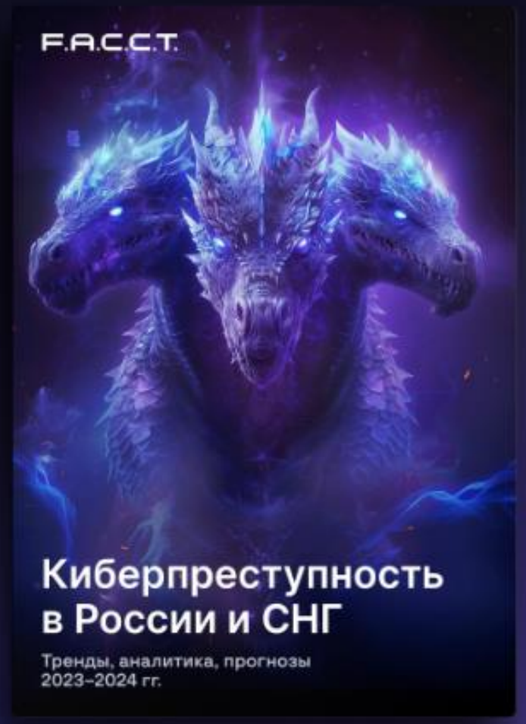
2013–2024

F.A.C.C.T.

Киберпреступность в России и

facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/

F.A.C.C.T. Продукты Сервисы Решения Ресурсы Блог Компания Сообщить об инциденте Связаться с менеджером



← Исследования

Киберпреступность в России и СНГ. Тренды, аналитика, прогнозы 2023–2024

Ежегодный флагманский отчет компании F.A.C.C.T. — единственный и наиболее полный источник стратегических и тактических данных о киберугрозах, актуальных для России и СНГ в период острого геополитического конфликта.

Имя* Фамилия*

Корпоративный Email* Должность*

Компания* Страна*

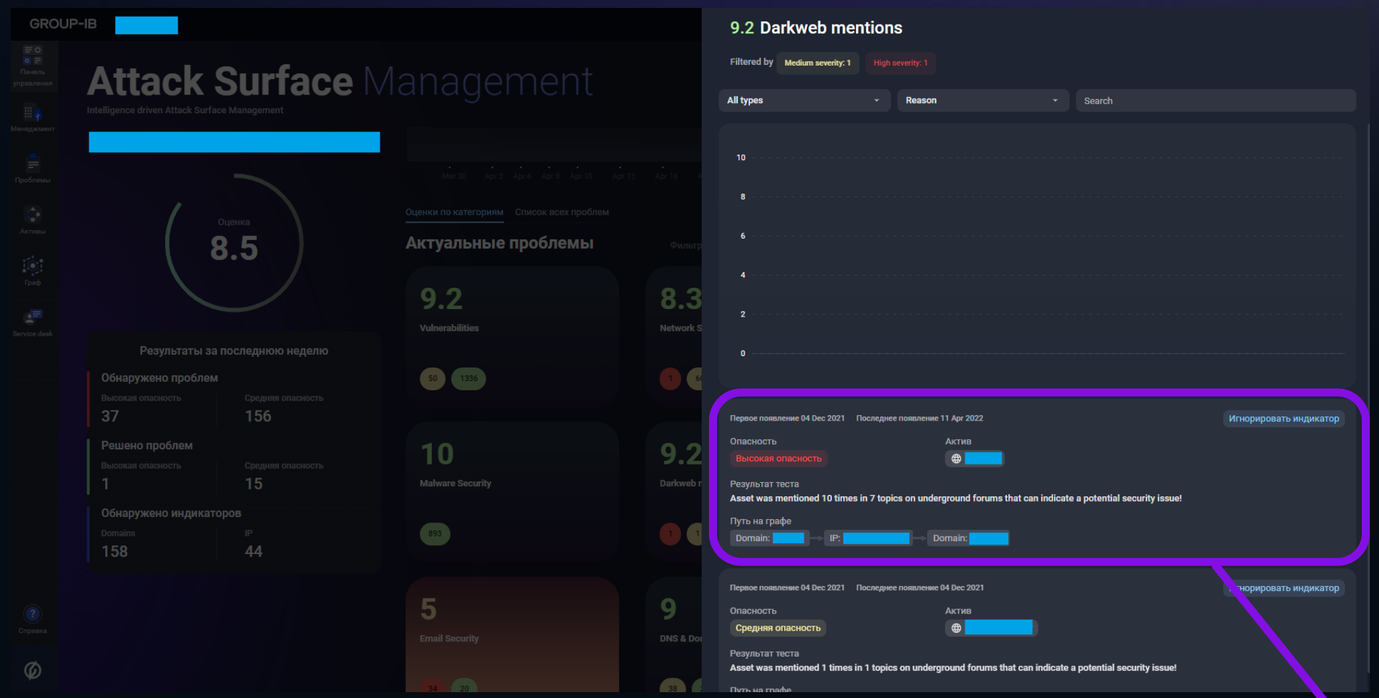
F.A.C.C.T.

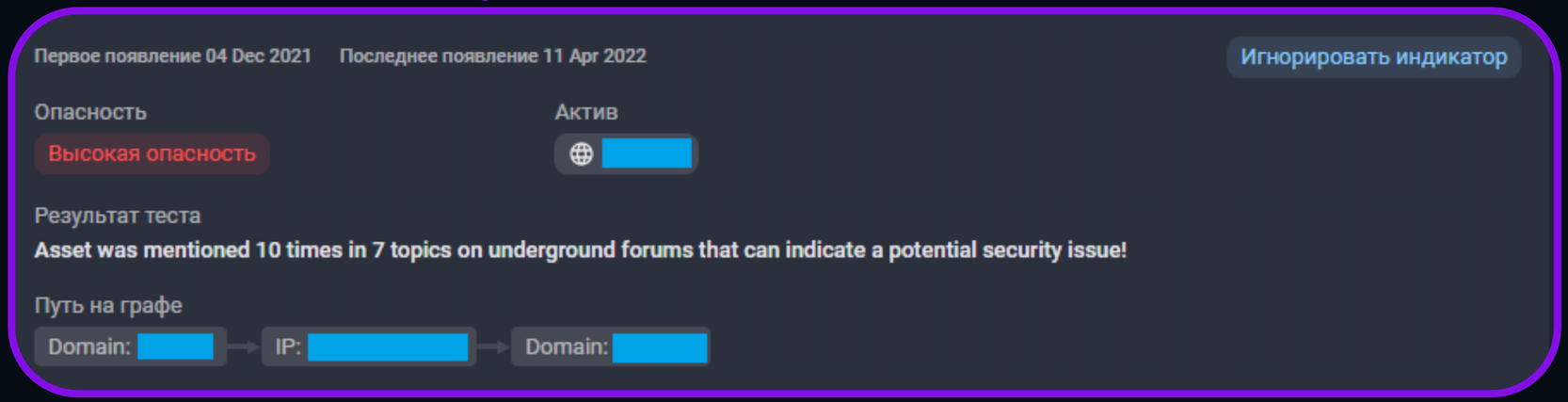
Реальная история №1

Информирует о подготовке атаки

F.A.C.C.T.

Attack Surface Management



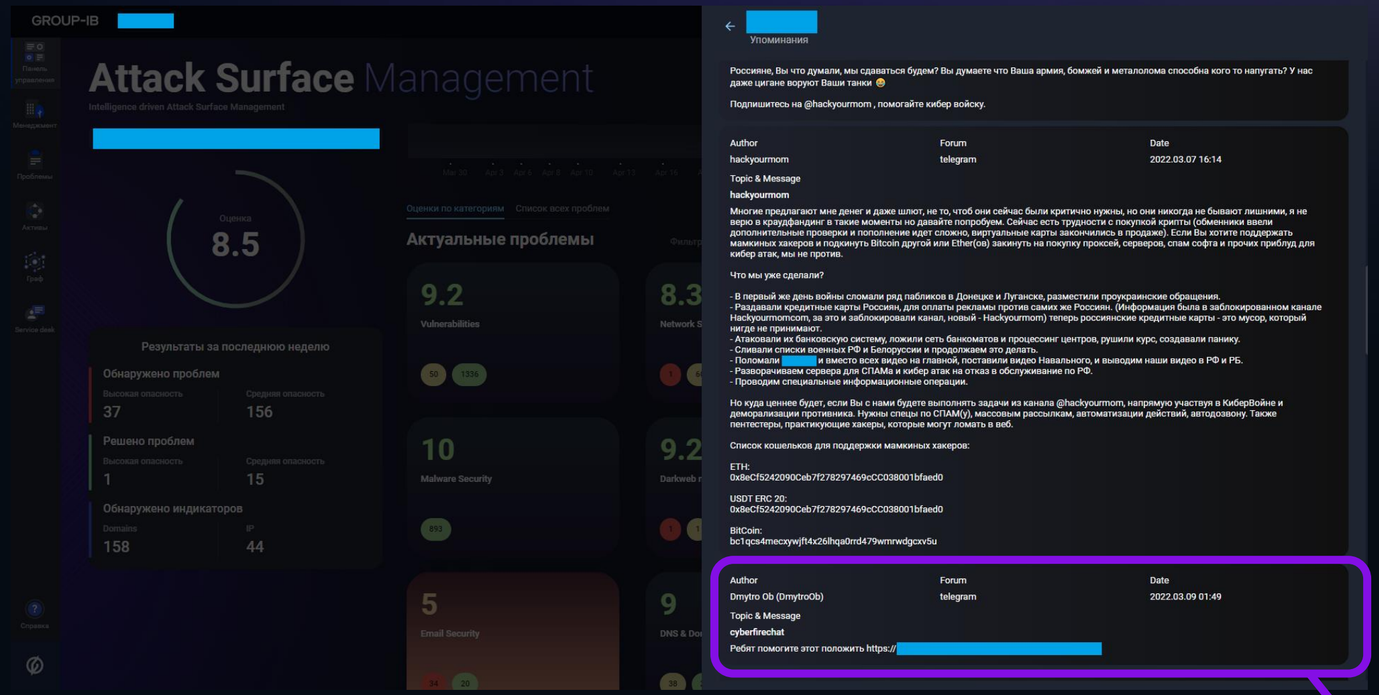


Реальная история №1

Информирует о подготовке атаки

F.A.C.C.T.

Attack Surface Management



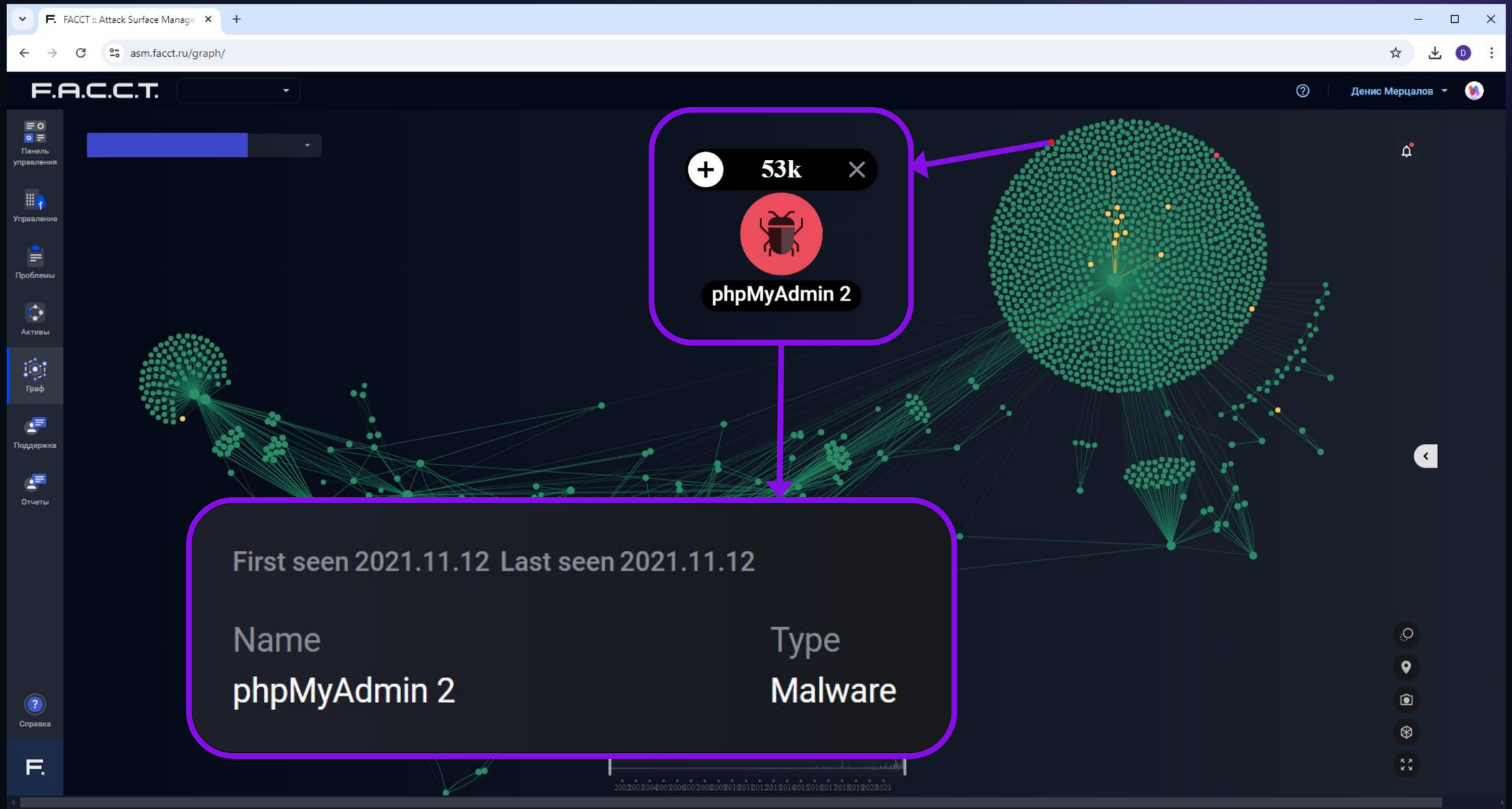
Author
Forum
Date
Dmytro Ob (DmytroOb)
telegram
2022.03.09 01:49
Topic & Message
cyberfirechat
Ребят помогите этот положить https://[redacted]

Реальная история №2

Выявляет заражённые активы и следы компрометации

F.A.C.C.T.

Attack Surface Management

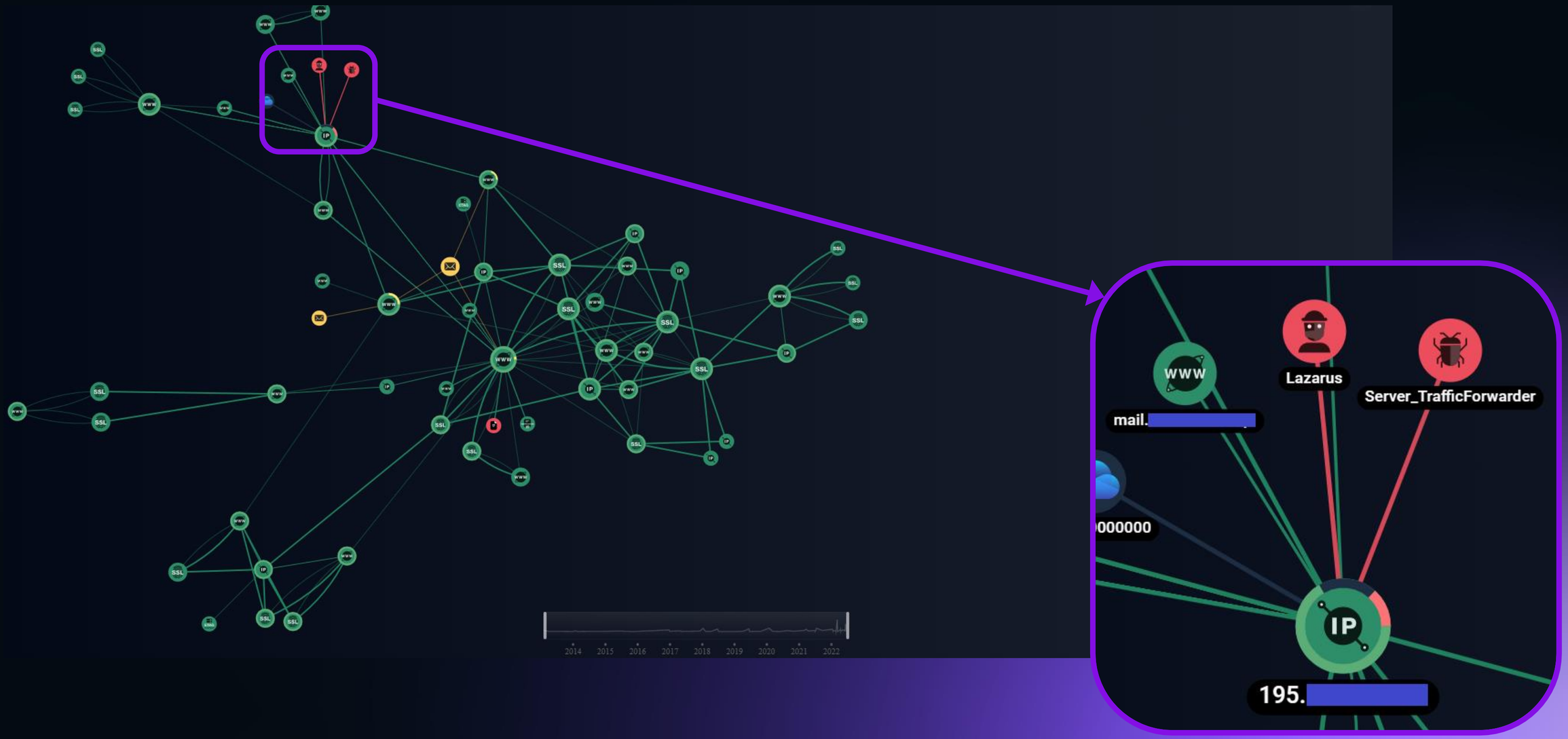


Реальная история №2

Выявляет заражённые активы и следы компрометации

F.A.C.C.T.

Attack Surface Management



«585 Золотой» и ASM

опыт приоретизации киберугроз
по степени критичности

585 золотой

Сергей Самойлов

Инженер информационной безопасности

«Наша федеральная ювелирная сеть работает с высоко ценными товарными запасами, конфиденциальной информацией, финансовыми структурами, что повышает риск стать целью для киберпреступников. Решение F.A.C.C.T. Attack Surface Management — оптимальный продукт под наши задачи, он позволяет эффективно управлять рисками и получить полное представление о поверхности возможной атаки, включая наши внешние ресурсы, веб-приложения, облака, мобильные приложения и другие цифровые активы».

F.A.C.C.T.

Attack Surface Management

Продукт **F.A.C.C.T. Attack Surface Management** был внедрён в декабре 2023 года.

Решение отслеживает теневые ИТ-активы, незащищенные участки инфраструктуры, потенциальные уязвимости и некорректно настроенные элементы сети, которые могут быть использованы злоумышленниками в своих целях.

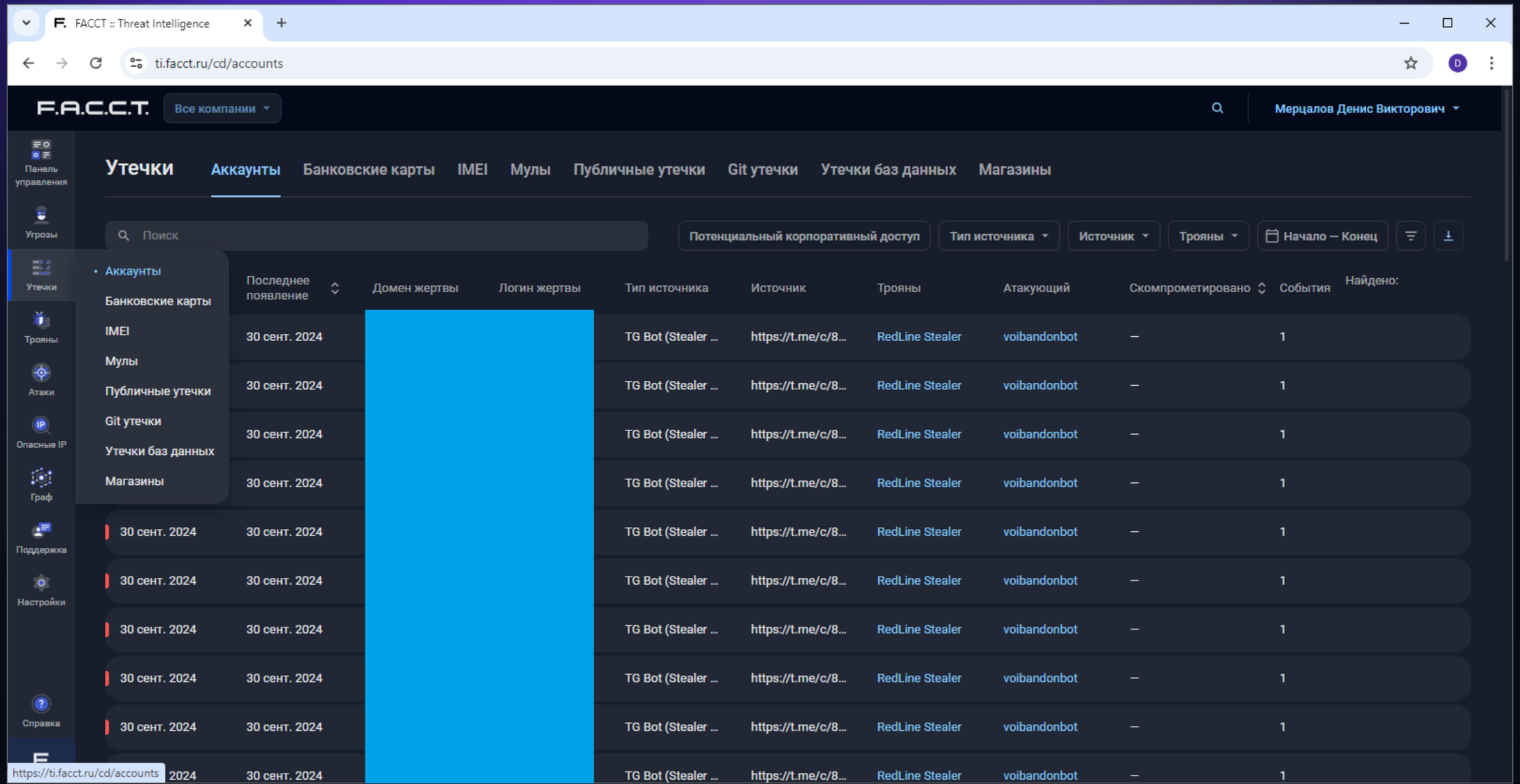
Attack Surface Management использует AI-технологии и аналитические алгоритмы для сбора, анализа и интерпретации данных, связанных с поверхностью атаки. Это помогает организации понять, какие уязвимости и риски являются наиболее критичными, и предоставить релевантные рекомендации по их устранению.

Реальная история №3

Выявляет утёкшие логины и пароли, банковские карты и пр.

F.A.C.C.T.

Threat Intelligence



Технологические партнёрства

F.A.C.C.T.

positive technologies

MaxPatrol SIEM – готовая интеграция

Security Vision

TIP – готовая интеграция
SOAR - запланировано

R-Vision

TIP – готовая интеграция
SOAR - запланировано

Capsule SIEM – готовая интеграция

RUSIEM
Всё под контролем

SIEM - запланировано

Универсальные интеграции по протоколам:

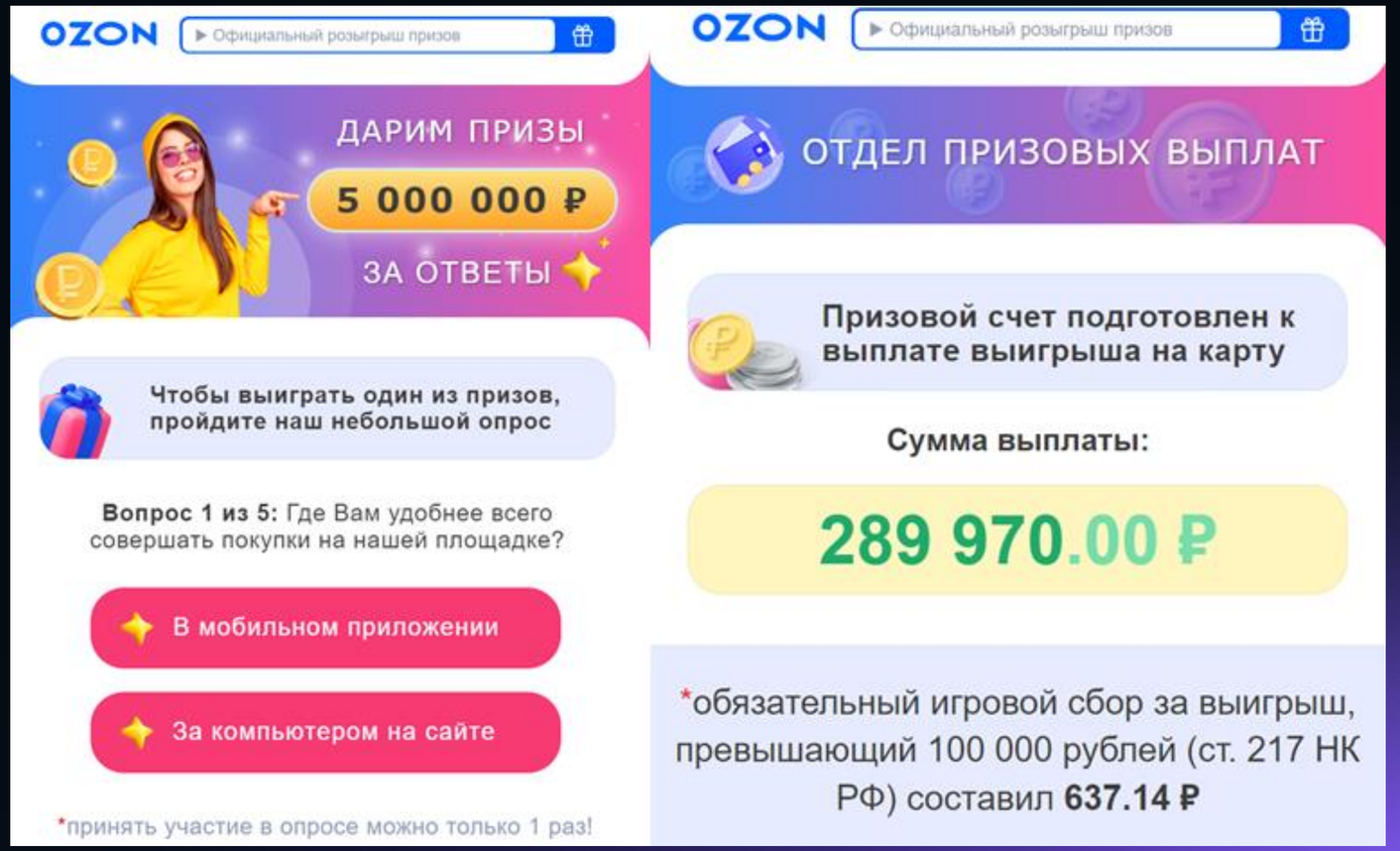
API 2.0, STIX/TAXII 2.1 и т. д.

Реальная история №4

Блокирует скам и фишинговые сайты

F.A.C.C.T.

Digital Risk Protection



Пример мошеннической схемы с раздачей призов — пользователю предлагается прокрутить Колесо Фортуны. На 3-ю попытку гарантировано выпадает денежный приз, но, чтобы его получить, победителю необходимо оплатить «комиссию» по реквизитам злоумышленников. В результате чего жертва безвозвратно теряет свои деньги.

«OZON» и DRP

опыт противодействия скаму и фишингу

Кирилл Мякишев

Директор по информационной безопасности Ozon

«Онлайн-шоппинг на маркетплейсах стал нормой для миллионов пользователей: только на Ozon в 2024 году число активных покупателей достигло более 50 млн человек. Мошенники пытаются использовать популярность известных сервисов и прибегают к различным методам для обмана клиентов. Чтобы обезопасить пользователей мы применяем инструменты для быстрого отслеживания и блокировки подозрительных ресурсов, а также повышаем осведомленность клиентов, рассказывая о новых приемах злоумышленников».

F.A.C.C.T.

Digital Risk Protection

Решение **F.A.C.C.T. Digital Risk Protection**.

Ozon, ведущая e-commerce-платформа в России, и компания F.A.C.C.T., российский разработчик технологий для борьбы с киберпреступлениями, в первом полугодии 2024 г. заблокировали 9 341 скам-ресурсов и 3 621 фишинговых сайтов, которые пытались использовать бренд маркетплейса для обмана пользователей. Основными видами мошенничества, с которыми чаще всего сталкивались специалисты, стали интернет-аферы с фейковыми розыгрышами от имени маркетплейса, фишинговые страницы авторизации, покупки или возврата товара. Главный способ продвижения мошеннических сайтов в этом году — это реклама в мессенджерах и соцсетях.

«Столото» и DRP

опыт противодействия скаму и фишингу

Екатерина Тутон

Заместитель генерального директора многопрофильного холдинга S8 Capital, в который входит «Столото»

«Столото» совместно с правоохранительными органами и специалистами в сфере кибербезопасности продолжает вести усиленную работу против мошеннических групп в цифровом пространстве 365 дней в году в режиме 24/7. Мы видим, что в течение всего года мошенническая активность снижалась, достигнув минимальных значений за последние три года. Это показывает, что наши усилия в борьбе с кибермошенниками дают свои результаты. Кроме того, мы ведем постоянную работу по информированию граждан, поскольку это один из ключевых инструментов для того, чтобы предупредить мошенничество».

F.A.C.C.T.

Digital Risk Protection

Решение **F.A.C.C.T. Digital Risk Protection**.

В целом в 2023 году количество мошеннических ресурсов, которые действовали под видом популярных государственных лотерей и/или нелегально использовали бренд «Столото», кратно снизилось относительно показателей 2022 года. Так, если в 2022 году было обнаружено и заблокировано 38 470 таких мошеннических ресурсов, то в 2023 году было выявлено и нейтрализовано почти в 4 раза меньше таких ресурсов.

«Азбука вкуса» и BEP

опыт импортозамещения решений
для защиты электронной почты

Дмитрий Кузеванов

Технический директор
«Азбуки вкуса»

«Электронная почта — один из основных инструментов внешних коммуникаций в большинстве компаний. Защита этого канала связи очень важна: необходимо на ранних этапах детектировать и блокировать вредоносные письма. Не всегда даже подготовленный специалист может сразу отличить фишинговое письмо от легального или понять, что в письме есть вредоносное вложение — например, в макросах Excel-файла. А вектор атаки через такое вложение и дальнейшее его распространение внутри сети очень популярен и эффективен и может привести к парализации работы. Решение F.A.C.C.T. для защиты корпоративной почты предоставляет высокий уровень защиты и аналитики, является более качественным отечественным аналогом уже проверенных, но ушедших с нашего рынка, решений подобного класса».

F.A.C.C.T.

Business Email Protection

Решение **F.A.C.C.T. Business Email Protection** было внедрено в марте 2022 года. За это время было заблокировано более **60 000 вредоносных почтовых рассылок**, направленных сотрудникам «Азбуки вкуса».

Business Email Protection выявила и заблокировала сотни тысяч нежелательных писем и фишинговых рассылок, включая попытки целевого фишинга с целью хищения учетных записей сотрудников для последующего проникновения в инфраструктуру организации.

«Агропромкомплектация» и XDR

опыт защиты от сложных и неизвестных угроз, шифровальщиков с помощью XDR

F.A.C.C.T.

Managed XDR

Алексей Леонов

Директор Департамента ИТ
ГК «Агропромкомплектация»

«Очевидно, что высокотехнологичные преступления давно перешли из области фантастики в реальный мир, и на первом плане сегодня превентивные меры: выявление и ликвидация вероятных кибератак вместо привычного ранее постинцидентного реагирования. Я уверен, что совместно с компанией F.A.C.C.T мы выведем процессы предупреждения инцидентов на качественно новый уровень и зададим новые стандарты информационной безопасности в отрасли с учетом ее специфики и тренда на импортозамещение.»

Решение **F.A.C.C.T. XDR** было внедрено в мае 2023 года. ГК «Агропромкомплектация» объединяет 15 территориально разнесенных локаций, **более 3500 рабочих станций и 3 000 активных пользователей**, обрабатываемый трафик превышает 5Гб/с.

Внедренное решение F.A.C.C.T для проактивного поиска и защиты от сложных и неизвестных киберугроз уже продемонстрировало эффективную защиту от целевых атак злоумышленников, вредоносных рассылок шифровальщиков, шпионского ПО, троянов удаленного доступа.

«Первый Бит» и Managed XDR

опыт защиты от сложных и неизвестных угроз, шифровальщиков с помощью XDR

Марьяна Досымбекова

Руководитель департамента
ИТ компании «Первый Бит»

«Учитывая растущее количество кибератак «Первый Бит» вместе с F.A.C.C.T. договорились о партнерском взаимодействии в вопросах информационной безопасности и защиты ИТ-инфраструктуры наших заказчиков в России и СНГ»

F.A.C.C.T.

Managed
XDR

Решение **F.A.C.C.T. Managed XDR** было внедрено в сентябре 2024 года.

Интегратор эффективных ИТ-решений «Первый Бит» и F.A.C.C.T., разработчик технологий для борьбы с киберпреступлениями, подписали соглашение о сотрудничестве в сфере кибербезопасности. В рамках партнерства продуктовую линейку «Первого Бита» пополнили флагманские решения от компании F.A.C.C.T. для защиты от сложных и неизвестных киберугроз, предотвращения кибератак на этапе их подготовки, защиты от киберрисков, связанных с утечками данных, финансовым мошенничеством и фишингом.

«Лига ставок» и Fraud Protection

опыт защиты от мошенничества

F.A.C.C.T.

Fraud Protection

Елена Гонзина

Директор департамента управления клиентскими рисками БК «Лига Ставок»

«Защита от диджитального мошенничества во времена скоростного развития технологий имеет первостепенное значение. Мы призываем наших клиентов проявлять бдительность и остерегаться сомнительных предложений получения быстрого заработка. Клиент, рассматривающий беттинг как способ развлечения и проверки своих аналитических способностей, не должен ставить под угрозу собственные данные и накопленную историю сотрудничества с букмекером. Совместная работа “Лиги Ставок” и F.A.C.C.T. по фрод-мониторингу позволяет нам эффективно противодействовать угрозам. Мы нацелены на продолжение эффективной работы, чтобы обеспечить безопасность игры наших клиентов, а также функциональность и надежность нашей платформы»

Решение **F.A.C.C.T. Fraud Protection**.

Компания F.A.C.C.T., российский разработчик технологий для борьбы с киберпреступлениями, и букмекерская компания «Лига Ставок» в первом квартале 2024 года предотвратили мошенническую активность более 3000 мультипользовательских аккаунтов. Один злоумышленник может управлять 5—10 аккаунтами в разных букмекерских компаниях, а суммарный оборот операций может достигать 300 000 рублей в месяц.

F.A.C.C.T.

Технологии для борьбы с кибер-преступностью

facct.ru
info@facct.ru

facct.ru/blog
+7 (495) 984 33 64

Что делать и куда бежать, если злодеи уже проникли инфраструктуру?

F.A.C.C.T.

Сервис:
«Реагирование на инциденты»

1. **Сообщить об инциденте любому сотруднику F.A.C.C.T.**

2. **Обозначить:**
   - Адрес сайта клиента
   - В чем суть инцидента и когда он произошел (со слов клиента)
   - Какие СЗИ имеются в его инфраструктуре

   Если инцидент связан с шифровальщиком*:
   - исполняемый файл программы

   и/или
   - записка с требованием о выкупе

Как убедиться, что в вашей сети нет хакеров и «закладок»?

F.A.C.C.T.

Сервис:
«Выявление следов компрометации»

Предпосылки:

1. Ранее состоявшиеся атаки на инфраструктуру и подозрения на компрометацию
2. Слияния и поглощения компаний
3. Недостатки детектирующей логики средств защиты информации