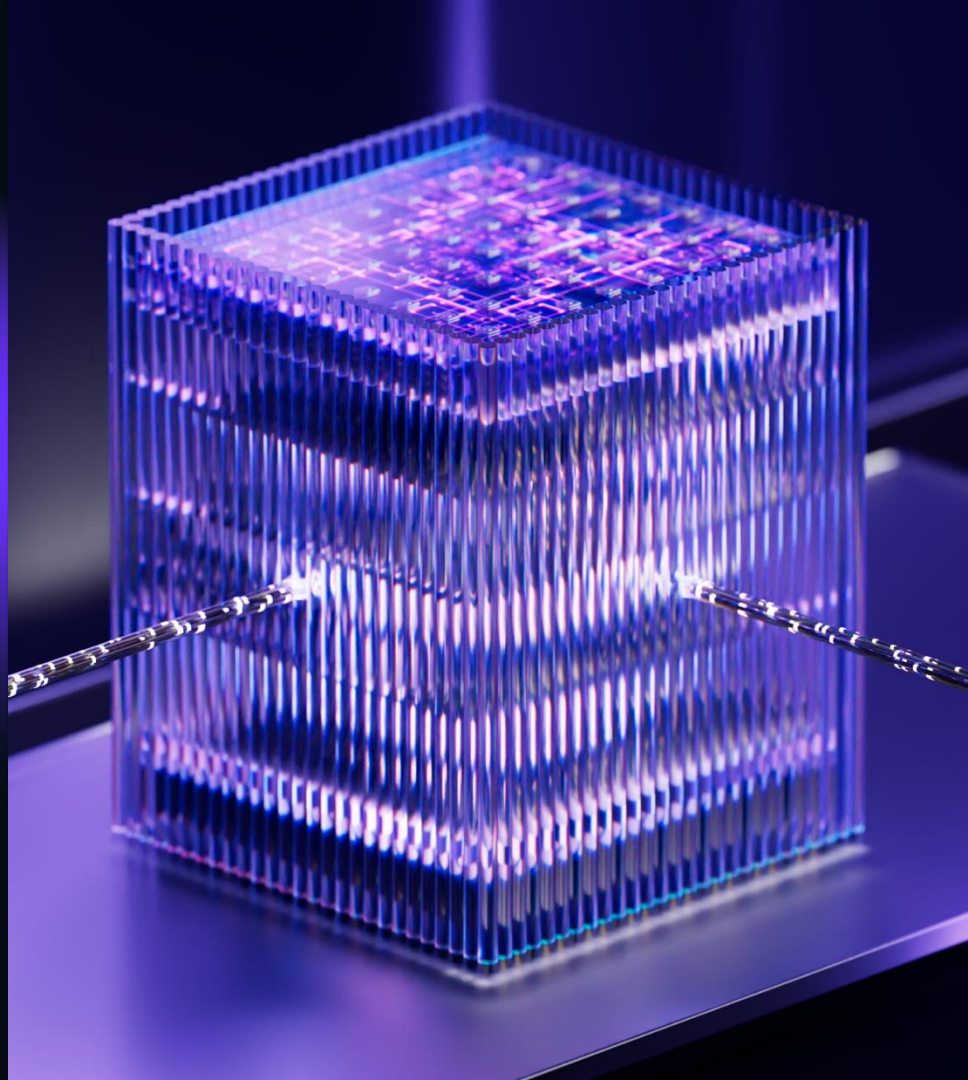
F.A.C.C.T.

FIGHT AGAINST CYBERCRIME TECHNOLOGIES

Взаимодействие с правоохраной - ключ к успеху в расследованиях киберпреступлений

Александр Симонян

Руководитель Департамента технологического сопровождения проектов по кибербезопасности F.A.C.C.T.



НАША МИССИЯ — борьба с киберпреступностью

F.A.C.C.T.

Для общего блага

Мы боремся с киберпреступниками с помощью собственных технологий и исследований, чтобы сделать этот мир безопаснее для всех.

Для наших клиентов

Мы изучаем угрозы, предотвращаем потенциальные атаки, реагируем на инциденты информационной безопасности и исследуем киберпреступления, чтобы создать благоприятные условия для наших клиентов и помочь их бизнесу развиваться.

Для наших сотрудников

Каждый наш сотрудник – герой. Мы поощряем бдительность и находчивость коллег, их способность изобретать новое. Вне зависимости от отдела и должности, каждый член нашей команды вносит вклад в борьбу с киберпреступностью.

КТО МЫ?

F.A.C.C.T.

Мы сочетаем глобальную экспертизу и технологии
со знанием российской специфики

Российский разработчик технологий

Технологии F.A.C.C.T. созданы в России, сопровождаются российскими экспертами и полностью соответствуют требованиям локальных регуляторов

Технологии международного уровня

Запатентованные решения успешно конкурируют с ведущими игроками глобального рынка кибербезопасности

Хранение данных в России

Мы храним данные российских компаний исключительно на серверах, находящихся на территории страны, для неукоснительного соблюдения требований федерального законодательства

Сверхточные данные киберразведки

Уникальные данные об атакующих, расширяющие стратегические, тактические и операционные возможности вашей команды ИБ

Компьютерная криминалистика и исследования

Помощь экспертов с 20-летним опытом в предотвращении атак, понимании мошеннических схем и защите инфраструктуры от угроз

Экосистема F.A.C.C.T.

Обогащение алгоритмов обнаружения за счет взаимодействия между решениями F.A.C.C.T. и использование оригинальных методов мониторинга позволяет обнаружить даже самые сложные нарушения и неуловимых киберпреступников

КРАТКО О F.A.C.C.T.

F.A.C.C.T. — первая в истории частная компания, которая успешно исследовала более тысячи дел по всему миру, следуя ключевой миссии — борьбе с киберпреступностью

Мы исследуем угрозы и создаем продукты с новаторским подходом, чтобы побеждать киберпреступность и делать мир безопаснее.

1 300+
успешных исследований киберпреступлений по всему миру

600
enterprise-клиентов

₽ 20 млрд+
сохраняют наши технологии в бюджете клиентов ежегодно

№1
первый поставщик услуги Incident Response в России

120+
патентов и заявок

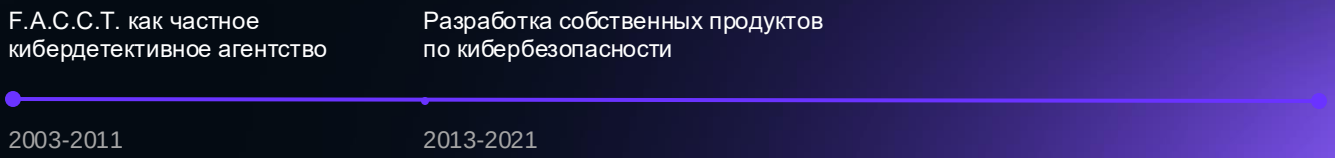
20 лет
практики и уникальной экспертизы на рынке РФ

Признание ведущих международных экспертов

Соответствие требованиям регуляторов РФ

В реестре отечественного программного обеспечения

ИСТОРИЯ F.A.C.C.T.



Технологии F.A.C.C.T

F.A.C.C.T.

Полный перечень продуктов и услуг в рамках единого решения на основе Unified Risk Platform

Платформа

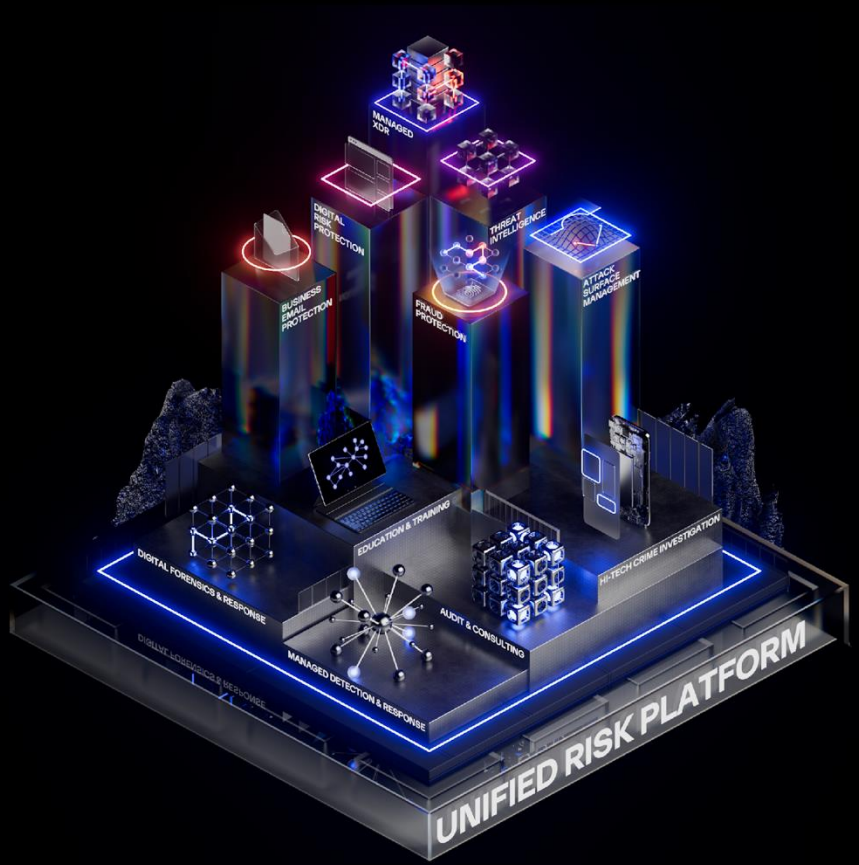
Unified Risk Platform

Продукты

- Threat Intelligence
- Fraud Protection
- Managed XDR
- Attack Surface Management
- Digital Risk Protection
- Business Email Protection

Сервисы

- Реагирование на инциденты и цифровая криминалистика
- Исследование высоко-технологичных преступлений
- Аудит и консалтинг
- Образовательные программы



ЛАБОРАТОРИЯ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

F.A.C.C.T.

Современная методология и собственная лаборатория исследования вредоносного кода

Возможность анализировать даже самые сложные образцы вредоносного ПО в совокупности с передовыми данными кибербразведки позволяют идентифицировать угрозы и реагировать на них быстро и эффективно.

Мобильная команда реагирования на инциденты

В случае необходимости, команда Лаборатории готова помочь клиентам реагировать на инциденты и расследовать любую кибератаку 24/7.

Реагирование на самые сложные кибератаки

Знание самых последних тактик, техник и процедур (TTPs) самых развитых группировок, таких как RedCurl, Cobalt, Lazarus и MoneyTaker, а также операторов программ-вымогателей Maze, Egregor, Revil и других, позволяет специалистам F.A.C.C.T. действовать быстро и безошибочно при реагированиях на инциденты.

Уникальный подход к каждому инциденту

Специалисты F.A.C.C.T. провели более 70 000 часов реагирования на различные инциденты. Команда Лаборатории использует проактивный, основанный на киберразведданных подход, чтобы реконструировать атаку и возобновить работу бизнеса как можно скорее.

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

F.A.C.C.T.

Оперативно устраняем инциденты любого масштаба и уровня сложности

ПОЧЕМУ НЕОБХОДИМО РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ:

Локализация текущих инцидентов

Профессиональное и своевременное реагирование на инцидент позволяет получить четкое представление о его масштабе, а также разработать необходимые меры для локализации угрозы и предотвращения дополнительного ущерба.

Восстановление после инцидента

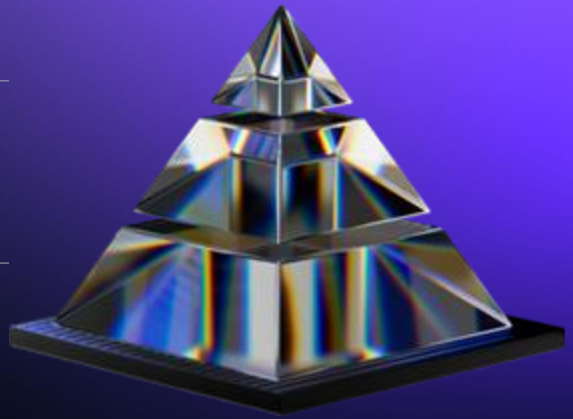
Глубокое понимание природы инцидента на основе корректного криминалистического расследования и анализа вредоносного ПО помогает выработать эффективную стратегию по устранению последствий и восстановлению инфраструктуры

Предотвращение повторных инцидентов

Реконструкция действий атакующих позволяет выявить уязвимости затронутых систем и повысить общий уровень защищенности организации благодаря улучшению механизмов обнаружения и предотвращения угроз

ЭТАПЫ РЕАГИРОВАНИЯ

#	Этап	Описание
1	Оперативный анализ и локализация инцидента	**Сбор и исследование данных с рабочих станций и серверов, задействованных в инциденте:** • Обнаружение каналов управления злоумышленников и их блокирование • Выявление скомпрометированных устройств • Выявление вектора первоначальной компрометации • Предоставление рекомендаций по локализации инцидента • Атрибуция злоумышленников
2	Мониторинг в режиме 24/7	**Внедрение F.A.C.C.T. Managed XDR:** • Обнаружение нелегитимной активности на конечных точках и вредоносного трафика • Круглосуточное реагирование и локализация возникающих угроз специалистами F.A.C.C.T. • Проактивный поиск угроз
3	Углубленный криминалистический анализ данных и вредоносного программного обеспечения	**Анализ данных с систем, задействованных в инциденте:** • Детальный анализ действий атакующих на различных этапах атаки • Исследование обнаруженных образцов вредоносных программ • Выявление информации, скомпрометированной злоумышленниками • Реконструкция событий инцидента и подготовка отчета
4	Разработка стратегии восстановления и рекомендаций	**Разработка рекомендаций, направленных на:** • Устранение последствий инцидента и эффективное восстановление работоспособности инфраструктуры • Повышение общего уровня защищенности ИТ-инфраструктуры компании • Конфигурирование имеющихся средств безопасности в соответствии с лучшими практиками • Совершенствование информационной безопасности



Высокотехнологичные расследования

F.A.C.C.T.

Цель расследования – привлечь виновных к ответственности. При необходимости мы будем продолжать участвовать в деле до тех пор, пока приговор не будет приведен в исполнение, консультируясь с адвокатами и давая показания в суде.

80% высокотехнологичных преступлений в России расследуется с участием наших специалистов

Кража данных

Экономические преступления

Атаки инсайдеров

Информационные войны

Вредоносные атаки

Уголовные дела

НАШИ ПРЕИМУЩЕСТВА:

- Глубокое знание криминальных схем
- Запатентованные технологии для обнаружения преступников
- Индивидуальный подход специальной проектной группы
- Сотрудничество с правоохранительными органами

ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ РОССИИ

F.A.C.C.T.

Уголовный розыск:
- ГУУР МВД России
- ГУ МВД России по г. Москве

С нами взаимодействуют по расследованию различных видов преступлений

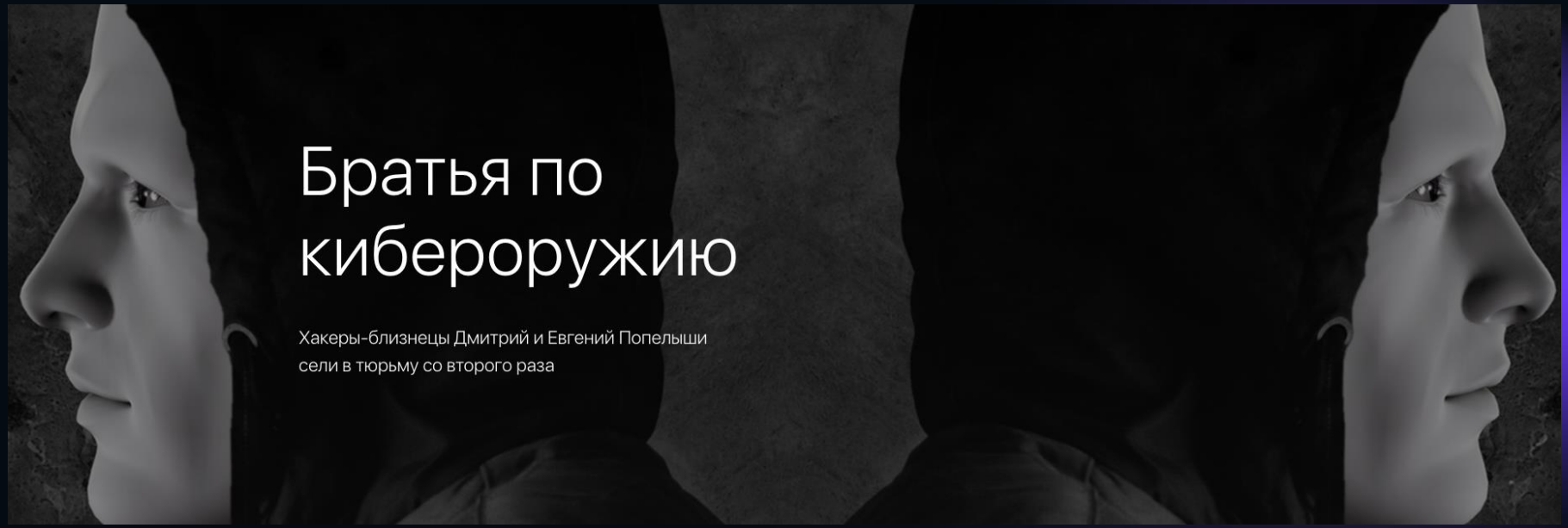
Специальные подразделения по борьбе с киберпреступностью:
- Управление «К» БСТМ МВД России
- Территориальные отделы «К» в субъектах РФ

С нами взаимодействуют по расследованию взломов, DDoS-атак, шифровальщиков, поиску хакеров и других сложных случаев

«Киберотделы» при различных подразделениях МВД:
- ГУТ МВД России (транспортная полиция)
- ГУЭБиПК МВД России (экономическая полиция)

Расследуют киберпреступления, касающиеся их сферы деятельности

Май 2015 - День сантехника



Попелыши руководили группой, в которую входили «программисты», «трафферы» — люди, которые распространяли вредоносные программы, «крипторы» – специалисты, которые проводили своевременное обновление (изменение) кода вредоносных программ, «дропы» — люди, которые занимаются обналичкой украденных денег, «прозвонщики».

Май 2015 - День сантехника

F.A.C.C.T.

Попелышам и их подельникам были предъявлены обвинения создании и использовании вредоносных программ (ст. 273 УК РФ), в неправомерном доступе к компьютерной информации и (ст. 272 УК РФ) и мошенничестве (ст. 159 УК РФ).

В понедельник, 18 июня, Савеловский суд Москвы признал вину подсудимых – Евгений и Дмитрий Попелыши получили по 8 лет лишения свободы, Сарбин — 6 лет, Шарычев — 5 лет, Вьюков — 4 года, Бельский получил условный срок.