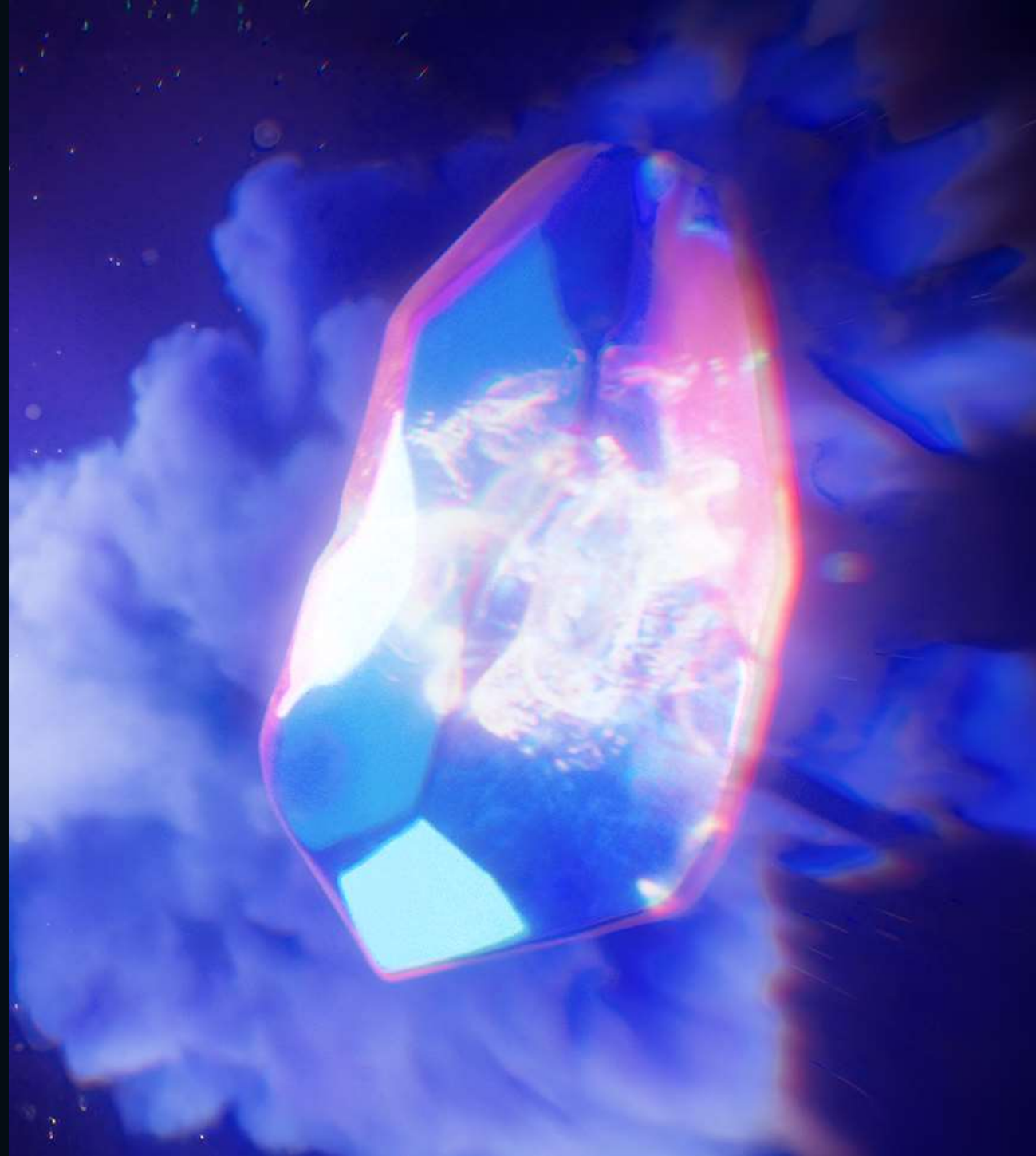
F6

Ведущий разработчик технологий для борьбы с киберпреступностью, предотвращения и расследования киберпреступлений



F6 в цифрах

Лидер в информационной безопасности
и расследовании киберпреступлений

1 300+

успешных исследований киберпреступлений по всему миру

600+

enterprise-клиентов

20+ млрд

рублей сохраняют наши технологии в бюджете клиентов ежегодно

№1

первый поставщик услуги Incident Response в России

47

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

Факты о F6

Мы сочетаем глобальную экспертизу и технологии
со знанием российского ландшафта угроз

Российский разработчик технологий

Технологии F6 созданы в России, сопровождаются российскими экспертами и полностью соответствуют требованиям регуляторов

Технологии международного уровня

Запатентованные решения мирового уровня, которые успешно внедрены в системы защиты ведущих и компаний

Сверхактуальные данные кибербразведки

Уникальные данные об атакующих дают новые возможности для защиты компаний на стратегических, тактических и операционных уровнях

Компьютерная криминалистика и расследования

Поиск и сбор цифровых улик для восстановления полной картины инцидента и установления причастных лиц

Хранение данных в России

Хранение данных российских компаний исключительно на серверах, находящихся на территории страны

Образовательные программы по информационной безопасности

Документы установленного образца, подтверждающие освоение практических навыков противодействия современной киберпреступности

Миссия компании — борьба с киберпреступностью

«Мы боремся с киберпреступниками с помощью инновационных решений, чтобы сделать этот мир безопаснее.

Мы предотвращаем атаки и реагируем на реальные инциденты, чтобы защитить клиентов и помочь их бизнесу в развитии».

История F6

F6

2003 — Основание

2011 — Открытие первого в России CERT

2013 — Threat Intelligence

2014 — Threat Hunting Framework

2015 — Fraud Protection

2017 — Digital Risk Protection

2021
- Attack Surface Management
- Business Email Protection

2022 — Managed XDR

2024 — Фонд «Сайберус» приобрел компанию F.A.C.C.T.

2025 — Ребрендинг. F6 — новое имя в мире кибербезопасности

«Каждое решение, которое мы создаем, основано на передовых знаниях о киберпреступности и многолетнем опыте реагирования на инциденты. Продукты F6 помогают компаниям быть уверенными в своей безопасности, предугадывая и останавливая киберугрозы»

Никита Кислицин
Технический директор

Пионеры исследования киберпреступлений

F6

F6 — первая в истории частная компания, которая успешно исследовала более тысячи дел по всему миру, следуя миссии — борьбе с киберпреступностью

Первая компания, запустившая в России CERT - круглосуточная группу реагирования на инциденты компьютерной безопасности

Первая компания, оказывающая услуги исследования в комплексе: от поиска причин атаки до помощи в юридическом сопровождении дела

Первыми осуществили частное партнерство с правоохранительными органами России: ГУУР МВД, ГУ МВД по г. Москве, УБК МВД, ГУТ МВД, ГУЭБиПК МВД России

1300+ исследований

Объекты исследований

- DDoS –атаки;
- банковские трояны на ПК и Android;
- разработчики эксплоит-китов;
- операторы бот-сетей;
- авторы фишинговых и скам-атак

Первыми вывели на российский рынок уникальные услуги

- компьютерная криминалистика и реагирование на инциденты;
- киберразведка;
- антифрод-аналитика;
- антифишинг;
- антипиратство

Влияние на индустрию

Выводим из тени злодеев. Создаем продукты и снабжаем индустрию самой актуальной информацией

Наши инициативы	Как это повлияло на рынок
Исследовали ТОП-3 разработчиков эксплоит-китов	После ареста преступников атаки с использованием эксплоит-китов практически прекратились
Остановили использование злоумышленниками банковских троянов для ПК и Android в регионе RUCIS	Количество атак с использованием банковских троянов сократилось на 99%
Изучили и остановили всех известных киберпреступников, ответственных за ограбление банков	Количество подобных атак сократилось практически до нуля по всему миру
Открыли первый в России частный центр реагирования CERT	Оперативное удаление опасных сайтов в доменах .ru, .рф позволяет сохранять безопасность рунета
Запустили такие продукты, как Threat Intelligence, Attack Surface Management, Fraud Protection, Digital Risk Protection, MXDR, Business Email Protection	Наши решения способствовали развитию рынка кибербезопасности в России, стали первооткрывателями во многих направлениях

Первый отчет F6

Скачать отчет

Основные статистические выводы

Сумма выкупа:
Малый бизнес

1000$ – 50 000$

Рекорд по сумме запрошенного выкупа

$3 млн

Сумма выкупа:
Крупные и средние организации

от 50 000$

Диверсии

10% атак

Рост числа кибератак шифровальщиками

На 44%

В 2024 году количество кибератак с помощью программ-вымогателей возросло

Топ отраслей, которые атаковали шифровальщиками:

Производство, инжиниринг

ИТ

Строительство, девелопмент

Розничная торговля

Добывающая промышленность

ВПК

Число прогосударственных хакерских групп, атаковавших Россию и страны СНГ

2023	14
2024	27

Количество фишинговых и мошеннических сайтов на один бренд

2023	7 878
2024	10 112

Утечки баз данных организаций в России и СНГ

2023	246
2024	455

Технологии F6

F6

Threat Intelligence

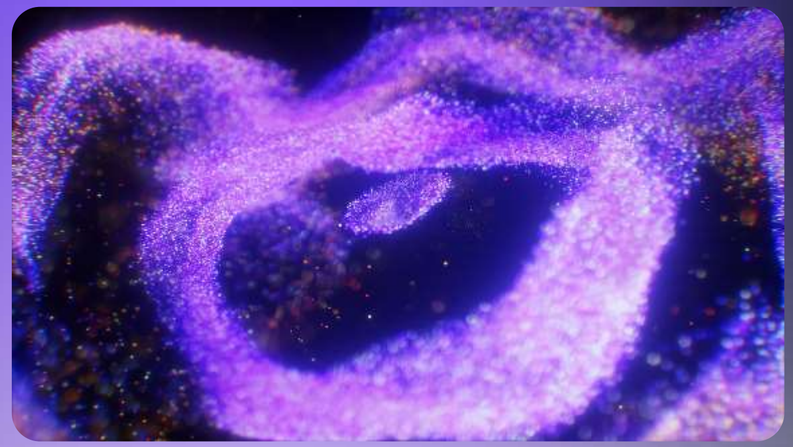
Managed XDR

Business Email Protection

Attack Surface Management

Digital Risk Protection

Fraud Protection

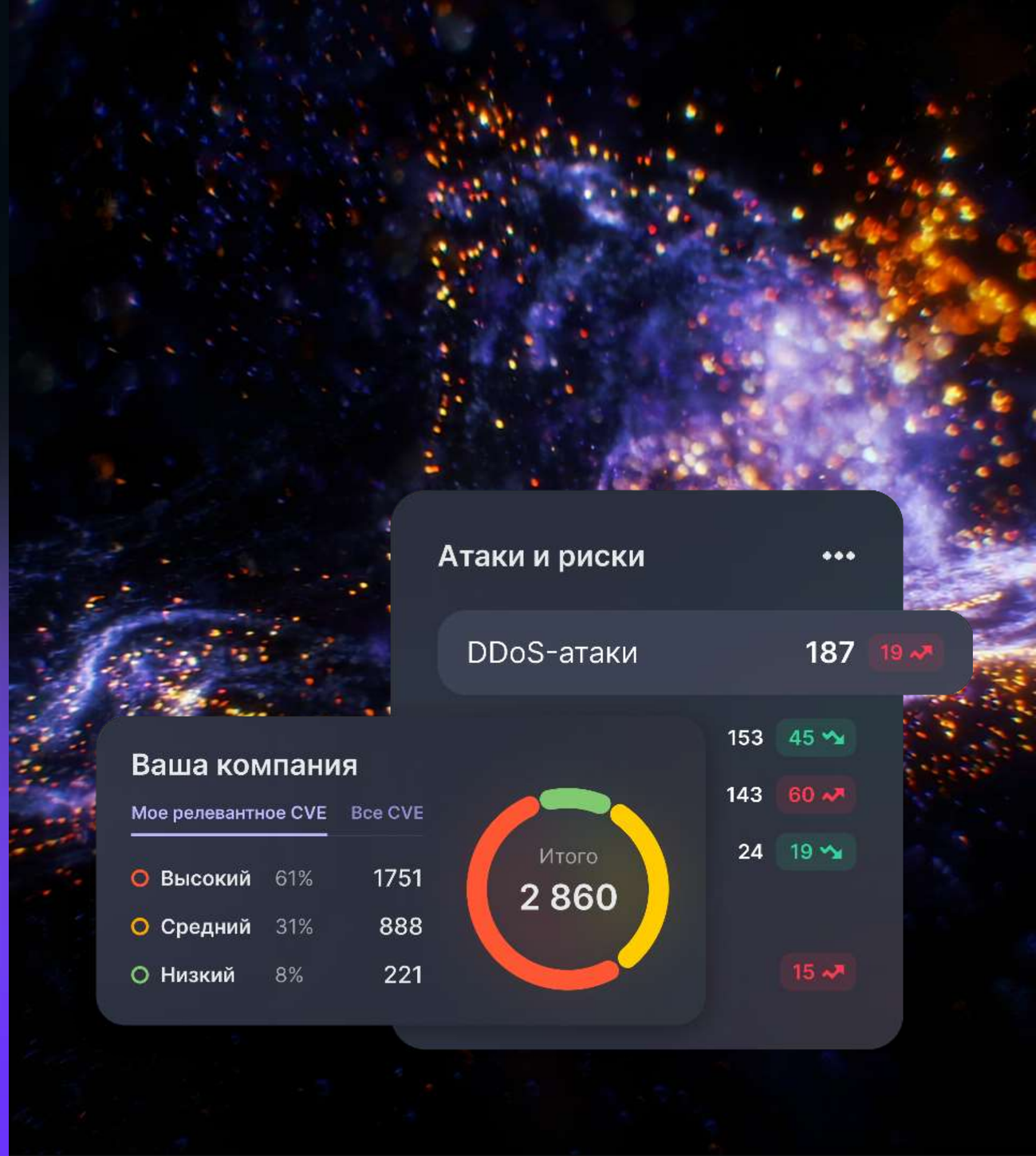


F6

Узнать подробнее

Threat Intelligence

С Threat Intelligence от F6 Вы получаете персонализированную, проверенную и значимую информацию из сотен источников, необходимую для построения эффективной защиты вашей компании от финансовых потерь и репутационных рисков.



Ключевые возможности Threat Intelligence

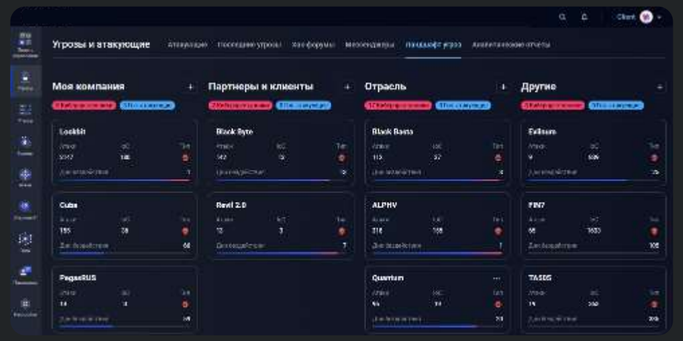
- Полный ландшафт угроз
- Сбор данных из Darkweb
- Атрибуция
- Утечки данных
- Графовый анализ
- Индикаторы компрометации
- Уязвимости
- Детонация ВПО

Ключевые возможности Threat Intelligence

F6

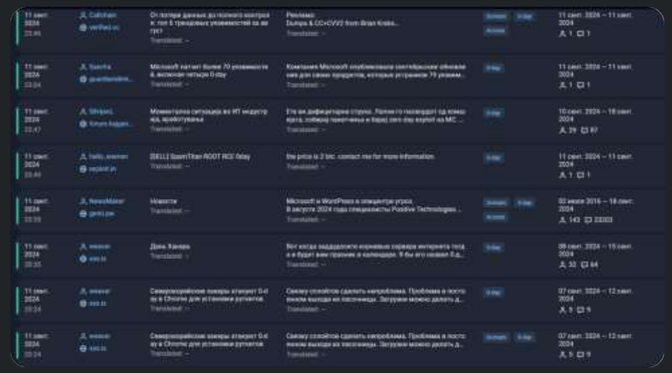
Полный ландшафт угроз

Получайте актуальные для вашей компании стратегические данные для оптимизации ИБ-стратегии в виде персонализированного дашборда, ежемесячных рассылок, годовых отчетов о трендах и прогнозах.



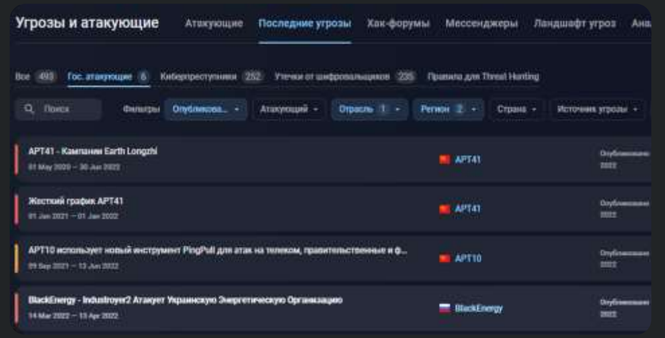
Сбор данных из DarkWeb

F6 собирает самую полную в отрасли базу данных Darkweb. Она включает информацию из закрытых хакерских сообществ, недоступную при использовании стандартных методов, таких как краулеры, скрипты или Big Data.



Атрибуция угроз

Threat Intelligence от F6 отслеживает активность киберпреступников, хактивистов и прогосударственных атакующих и предоставляет информацию об используемых ими тактиках, техниках и процедурах.

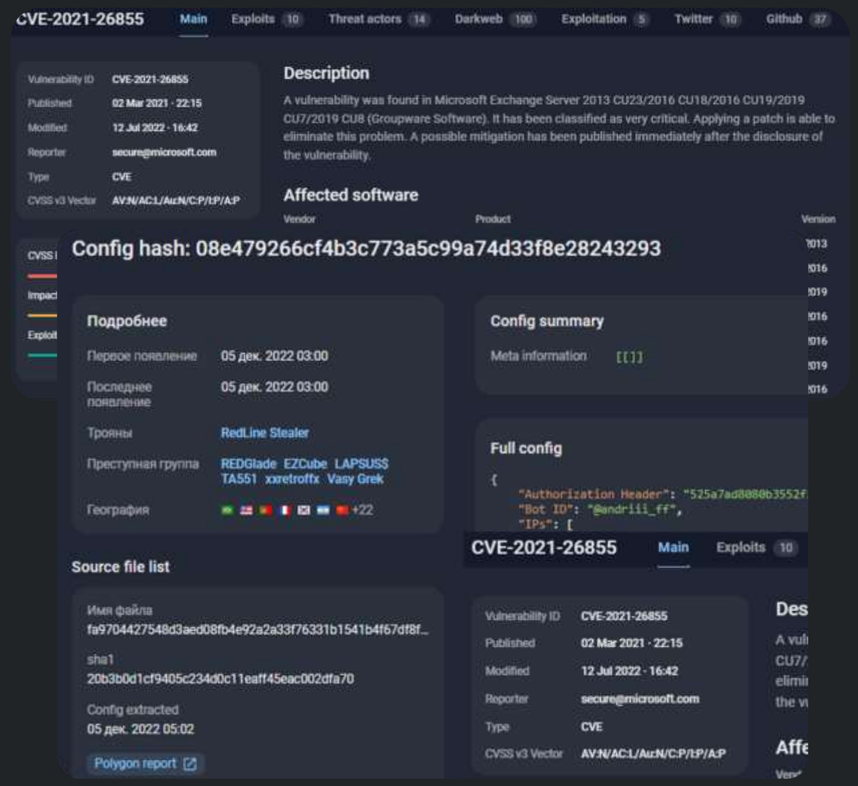


Ключевые возможности Threat Intelligence

F6

Данные о ВПО и уязвимостях

Эксперты F6 ежедневно исследуют тысячи вредоносных файлов, собранных в ловушках honeypot, а также полученных в ходе реагирований на инциденты и отслеживания ботнетов.



Графовый анализ

Система графового анализа от F6 визуализирует данные киберразведки и выявляет ранее неизвестные связи с помощью запатентованных алгоритмов

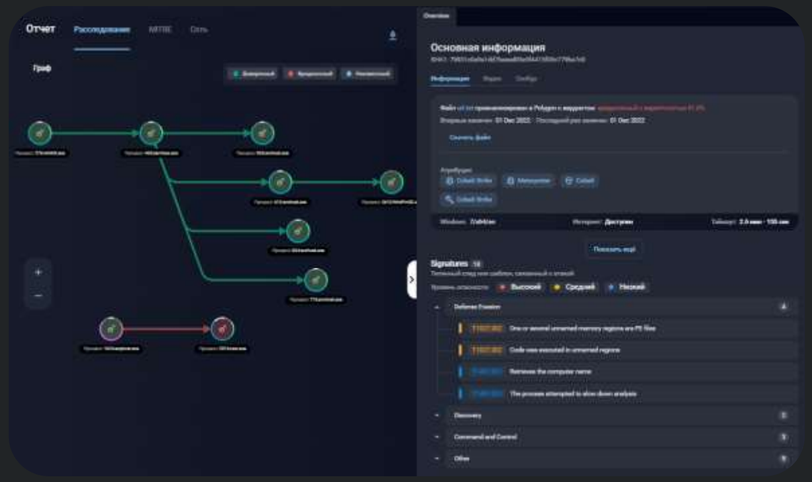
Объекты исследования

- Регистрационные данные доменов из базы данных WHOIS;
- DNS-записи доменов;
- Данные SSL сертификатов;
- Баннеры и отпечатки сервисов на IP-адресах;
- Активность в Darkweb.
- Скрытые регистрационные данные;
- Бэкенды, спрятанные с помощью прокси-сервисов;
- История регистрационных данных, перемещений по хостингам и изменений сервисов;

Ключевые возможности Threat Intelligence

Детонация ВПО

Подозрительные файлы и ссылки можно отправлять на детальный анализ с помощью платформы детонации F6 или ручной реверс-инжиниринг напрямую из интерфейса Threat Intelligence.

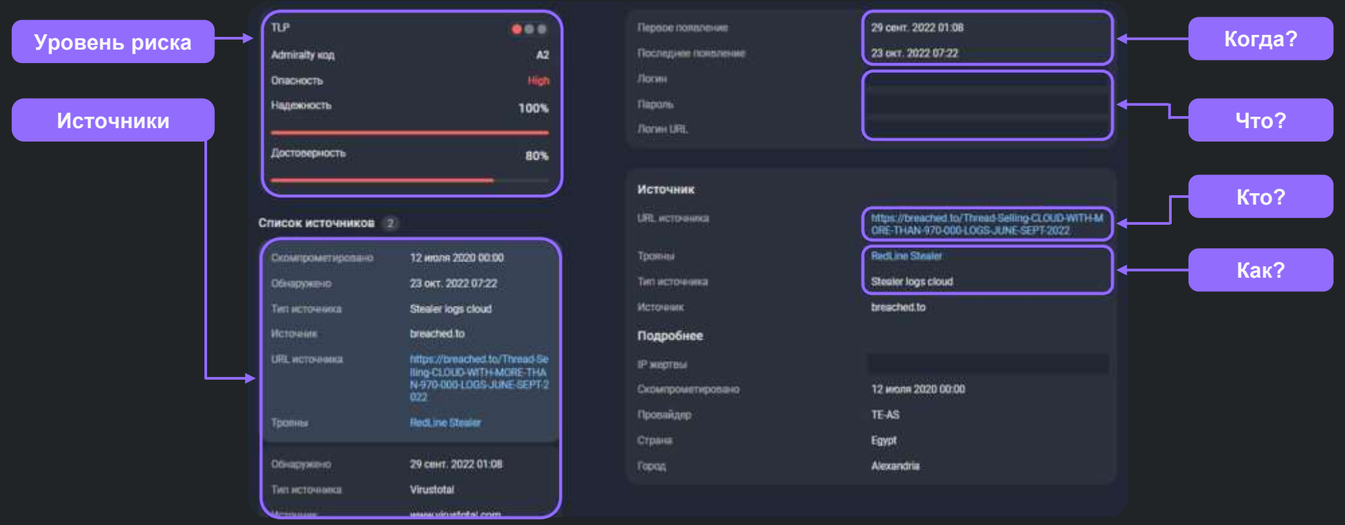


Данные о ВПО и уязвимостях

- Оценка вредоносной активности;
- Поведенческие анализ;
- Сетевая активность;
- Дерево процессов;
- Файловая структура;
- Матрица MITRE ATT&CK;
- Скринкаст действий ВПО.

Утечки данных

Платформа отслеживает утечки данных, обеспечивая защиту клиентских аккаунтов, VIP-персон и сотрудников организации. Наши источники и методы получения данных киберразведки включают данные с бот-сетей, отслеживание автоматического перевода средств ВПО, мониторинг кардшопов и сервисов проверки скомпрометированных данных, а также информацию из Darkweb.



Ключевые преимущества Threat Intelligence

Threat Intelligence от F6 предоставляет данные о всех угрозах, направленных на вашу компанию. Интеграция этих данных в вашу систему безопасности позволяет:

Обнаруживать, идентифицировать и приоритизировать угрозы до того как они нанесут ущерб

Получайте информацию о последних угрозах, включая индикаторы компрометации, тактики, техники и процедуры, которые используются злоумышленниками и сокращайте время на обнаружение угроз.

Оценивать ландшафт угроз вашей компании

Threat Intelligence открывает компаниям доступ к аналитическим отчетам об угрозах за пределами их собственных сетей и цифрового присутствия, а также за пределами экспертизы поставщиков решений SIEM.

Оптимизировать защиту организации

Данные Threat Intelligence позволяют принимать обоснованные решения по улучшению политики безопасности и внедрению необходимых защитных мер. Это позволяет компаниям быстрее реагировать на угрозы.

Минимизировать финансовые потери от кибератак

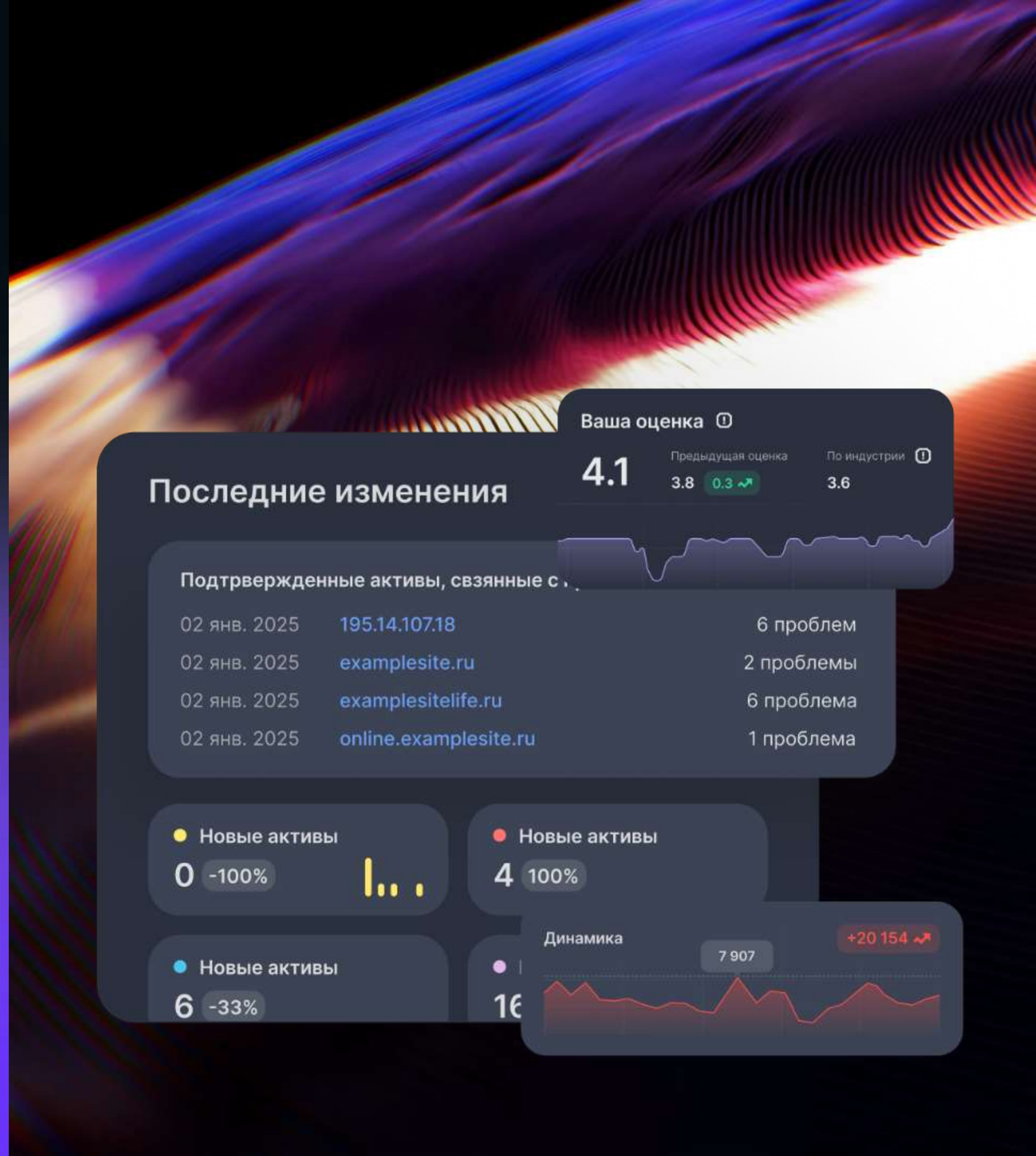
Убытки организаций, использующие атрибутированные данные киберразведки, снижаются на 20-30% в сравнении с компаниями, которые не используют продвинутые решения по управлению угрозами.

F6

Узнать подробнее

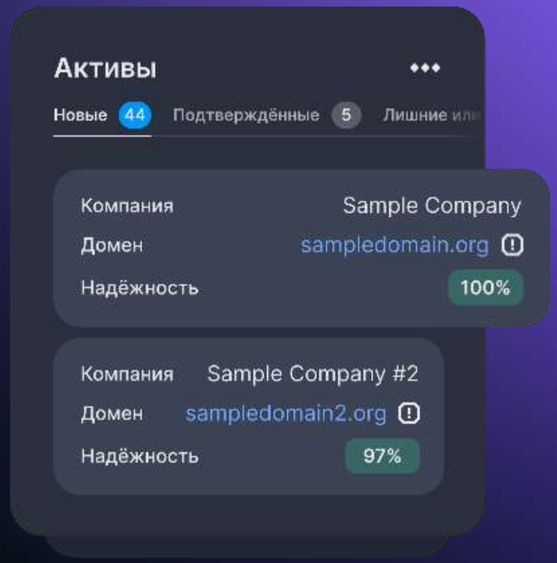
Attack Surface Management

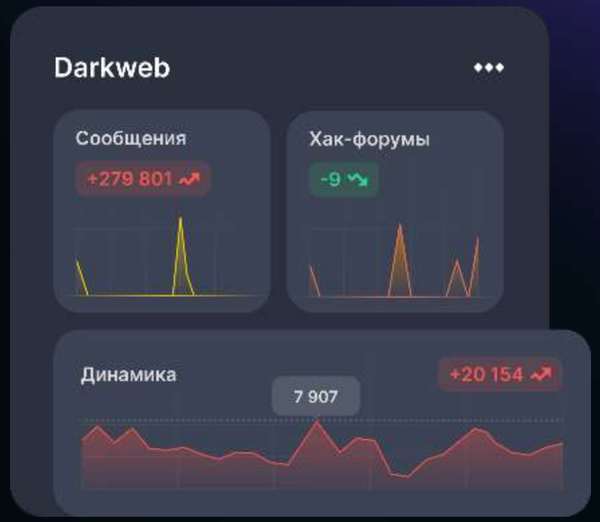
Решение для управления поверхностью атаки и отслеживания цифровых активов компании

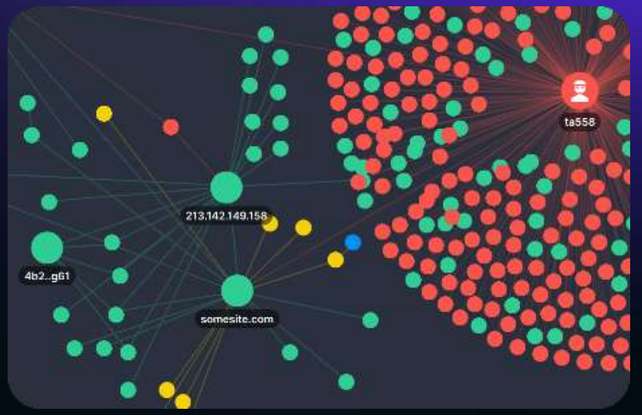


Функциональные возможности Attack Surface

Получайте актуальные для вашей компании стратегические данные для оптимизации ИБ-стратегии в виде персонализированного дашборда







- Обнаружение активов
- Непрерывный мониторинг
- Выявление уязвимостей
- Оценка уровня защищенности компании
- Графовый анализ
- Данные киберразведки
- Поддержка центра Кибербезопасности F6

Функциональные возможности Attack Surface Management

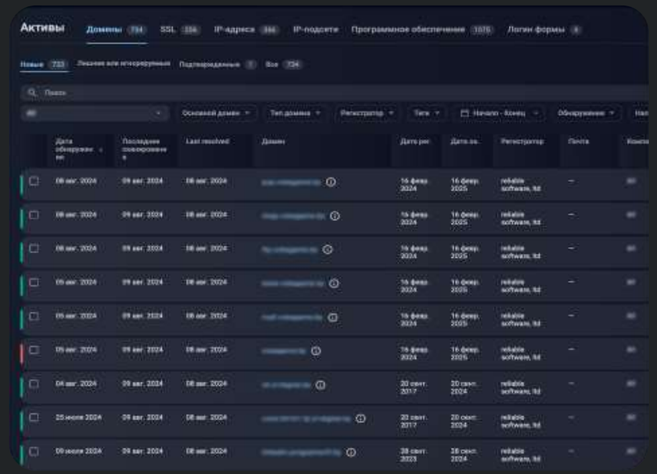
F6

Непрерывный мониторинг

Система осуществляет ежедневный мониторинг всех изменений во внешней поверхности атаки, что позволяет компании сформировать точное представление о текущем уровне защищенности

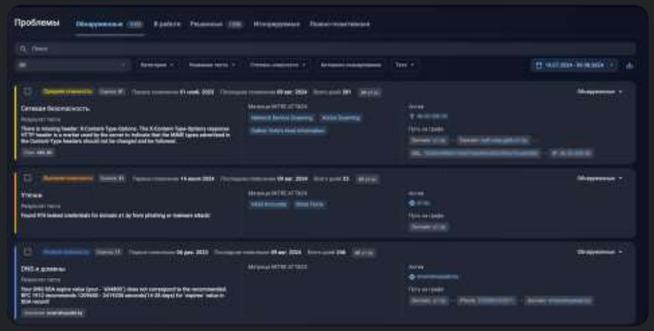
Обнаруженные активы

Attack Surface Management использует информацию об основном домене вашей компании для идентификации используемых и забытых активов. Это помогает выявить теневую инфраструктуру и другие системы, подверженные риску



Выявленные уязвимости

Attack Surface Management выявляет уязвимости и некорректные настройки в компании на уровне операционных систем, приложений, программного обеспечения и аппаратных средств, основываясь на результатах сканирования и анализа обнаруженных служб и их версий



Функциональные возможности Attack Surface Management

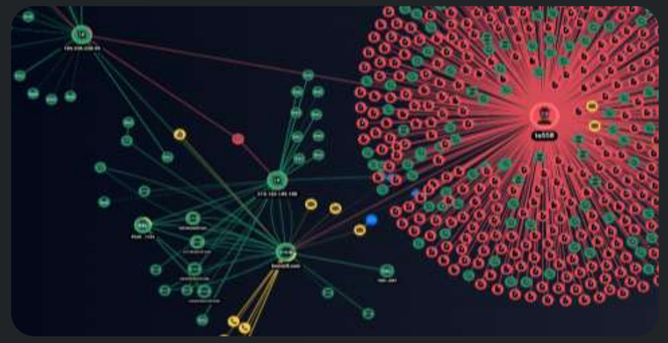
F6

Оценка уровня защищенности

Решение обеспечивает полную инвентаризацию всех интернет-ресурсов организации, выявляет уязвимости и приоритизирует критические риски для принятия должных мер, присваивая общий рейтинг защищенности организации

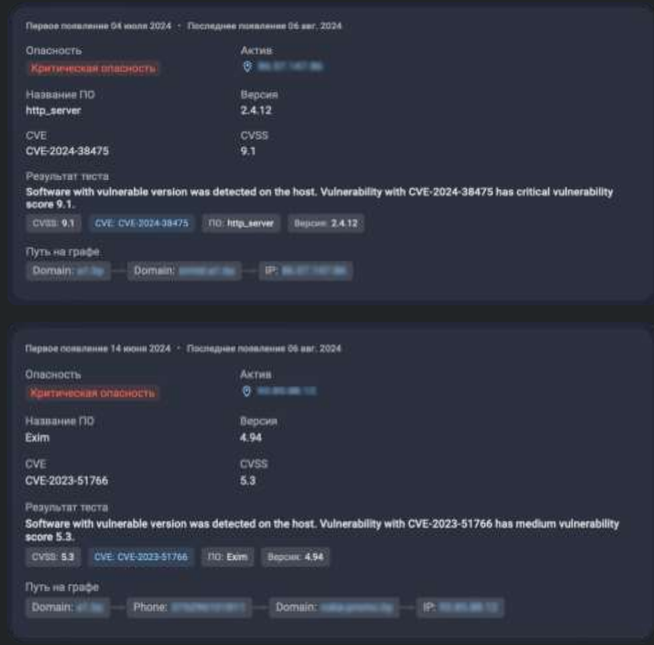
Графовый анализ

Система графового анализа от F6 визуализирует данные вашей цифровой инфраструктуры и выявляет ранее неизвестные связи с помощью уникальных алгоритмов.



Данные киберразведки

Система оценки рисков Attack Surface Management обогащается уникальными данными Threat Intelligence от F6



Поддержка Центра кибербезопасности (CDC)

Доверьте обнаружение потенциальных угроз команде Центра кибербезопасности с опытом более 20 лет. Сосредоточьтесь на важных событиях и реагируйте на них по готовым рекомендациям от команды F6

Ключевые преимущества Attack Surface Management

F6

Решение использует данные киберразведки F6 Threat Intelligence

Не требует внедрения — достаточно добавить домен заказчика в интерфейс в браузере

Не требует остановки бизнес-процессов при сканировании активов

Осуществляет непрерывный автоматический мониторинг периметра организации

Возможность мониторинга и поддержки Центра Кибер-безопасности F6

Возможность интеграции с SIEM, TIP и др. системами

Отлично дополняет сканеры внутренних уязвимостей

Помогает защитить периметр между регулярными пентестами и аудитами ИБ

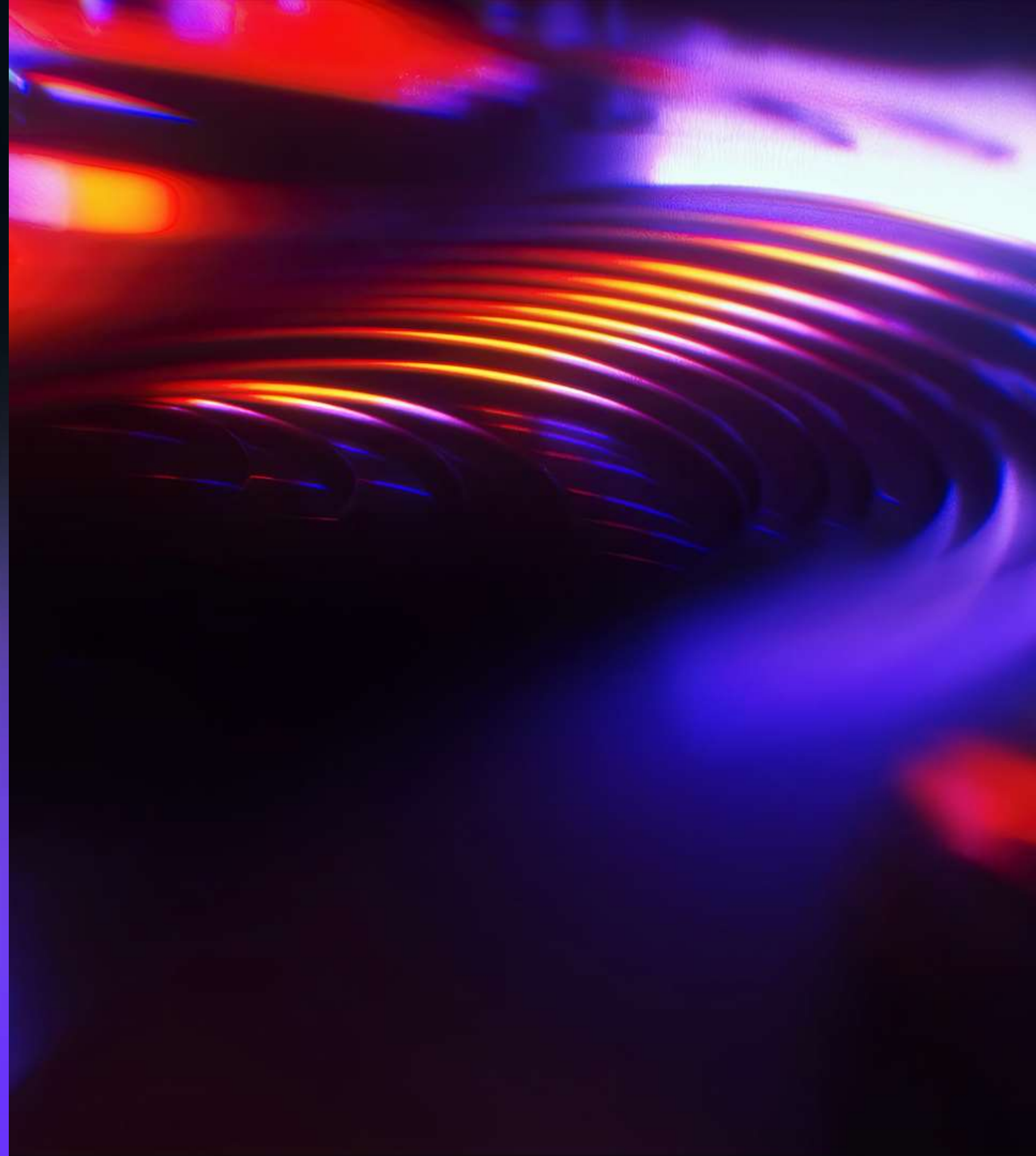
Помогает компаниям оценить периметр при поглощении других компаний или открытии новых филиалов

F6

Узнать подробнее

Managed XDR

Защитите компанию от кибератак с системой, которая отслеживает и блокирует угрозы 24/7



Функциональные возможности F6 Managed XDR

Модульное решение приоритизирует инциденты, изолирует зараженные хосты, блокирует спам, фишинг, вредоносные письма, противостоит целевым атакам.
И главное: F6 Managed XDR повышает эффективность ИБ-команды и освобождает ее от рутины.

Защита конечных станций и реагирование

Персональные компьютеры и серверы

Защита корпоративной почты

Вложения, ссылки, фишинг и спам

Детонация вредоносного ПО

Изолированная среда, анализ файлов и ссылок

Анализ сетевого трафика

Мониторинг сети, обнаружение аномалий

Threat Intelligence

Атрибуция угроз, отчеты и индикаторы

Управление поверхностью атаки

Контроль защищенности периметра

Функциональные возможности F6 Managed XDR

Сбор и анализ данных

Агрегирует телеметрию со всех компонентов продукта: EDR, NTA, MDP, BEP

Обнаружение угроз в реальном времени

Сверяется с индикаторами компрометации (IoC) и тактиками злоумышленников (TTP) по данным Threat Intelligence

Корреляция событий и атрибуция угроз

Связывает разрозненные события в цепочку атаки, чтобы определить источник угрозы и метод ее распространения

Реагирование на инциденты

Изолирует скомпрометированные хосты и блокирует вредоносную активность

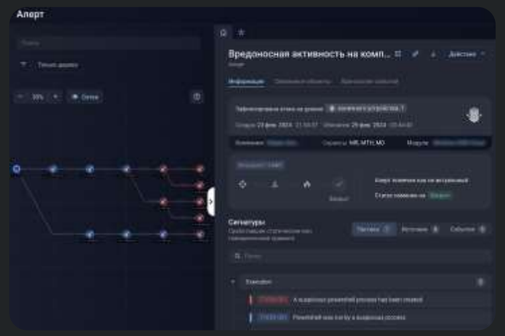
Функциональные возможности F6 Managed XDR

F6

Защита корпоративной почты

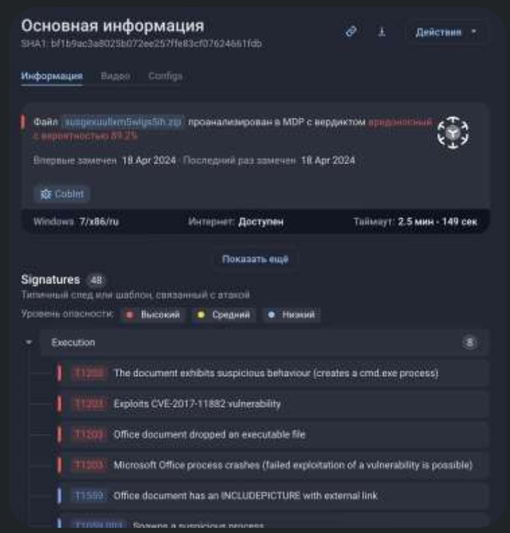
Локальная и облачная защита от сложных киберугроз и блокировка изощренных кибератак.

Защита конечных станций и реагирование



Анализ сетевого трафика

Детонация вредоностного ПО



Ключевые преимущества F6 Managed XDR

Защищает корпоративную почту, серверы, рабочие станции и сетевой трафик компании от современных угроз

Предотвращает атаки вирусов и шифровальщиков, минимизирует риски утечек данных

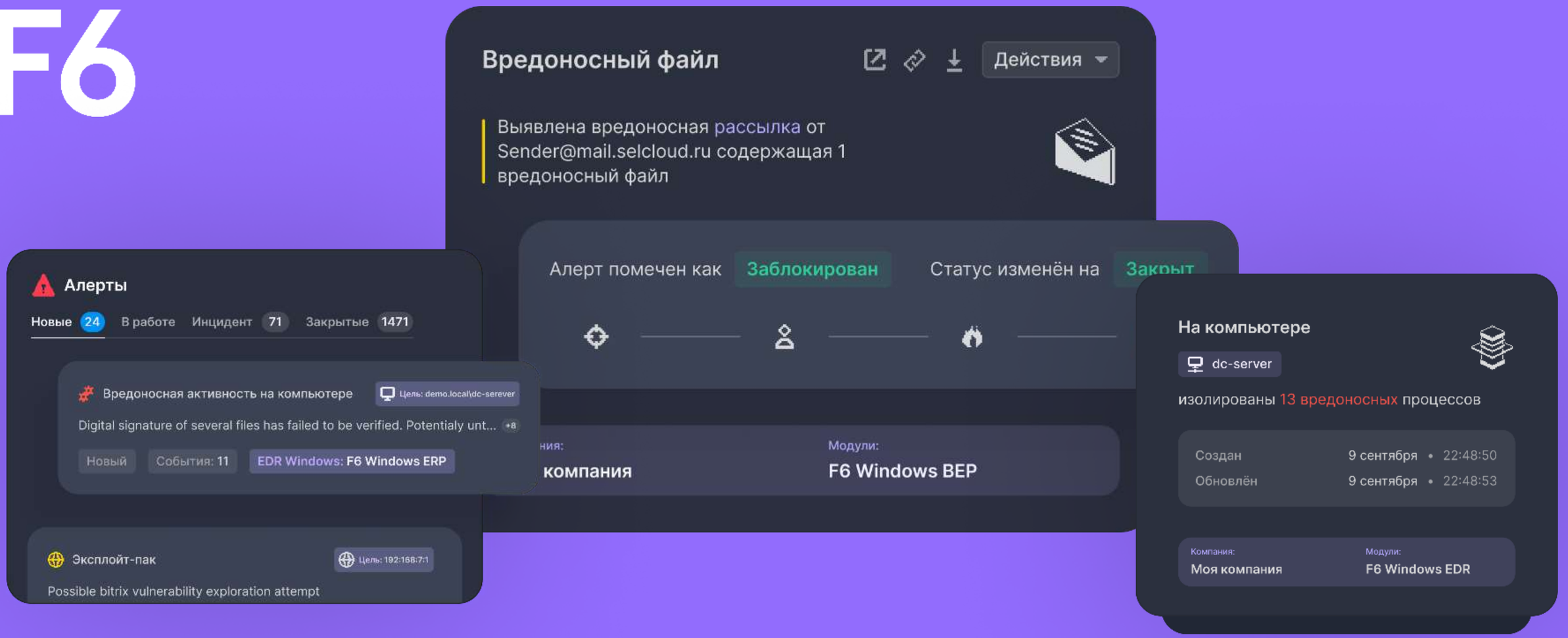
Заменяет зарубежные ИБ-инструменты, предлагая комплексную и надежную защиту

Обеспечивает защиту распределенных активов в сложных инфраструктурах

Автоматизирует рутинные задачи, повышая эффективность команды ИБ

Использует данные Threat Intelligence, чтобы обнаруживать действия злоумышленников быстрее и точнее аналогов

F6



Сервисы F6 Managed XDR

Круглосуточный мониторинг, проактивный
поиск угроз и своевременное реагирование

Функциональные возможности сервисов F6 Managed XDR

20 лет опыта DFIR и расследований для реагирования на инциденты и проактивного поиска угроз

Интеграции

XDR F6 | ASM F6 | THREAT INTELLIGENCE | SIEM

Расширяйте имеющиеся ресурсы

Решает задачу поиска и подготовки ресурсов для круглосуточного мониторинга и реагирования

Оставайтесь на связи с экспертами 24/7/365

Круглосуточная поддержка в случае инцидента, триаж алертов, специалисты по проактивному поиску угроз

Получайте персонализированный ландшафт угроз

Передовые данные кибербразведки раскроют, кто конкретно может быть нацелен на вашу компанию и как защититься от потенциальной угрозы

Ускоряйте обнаружение и реагирование

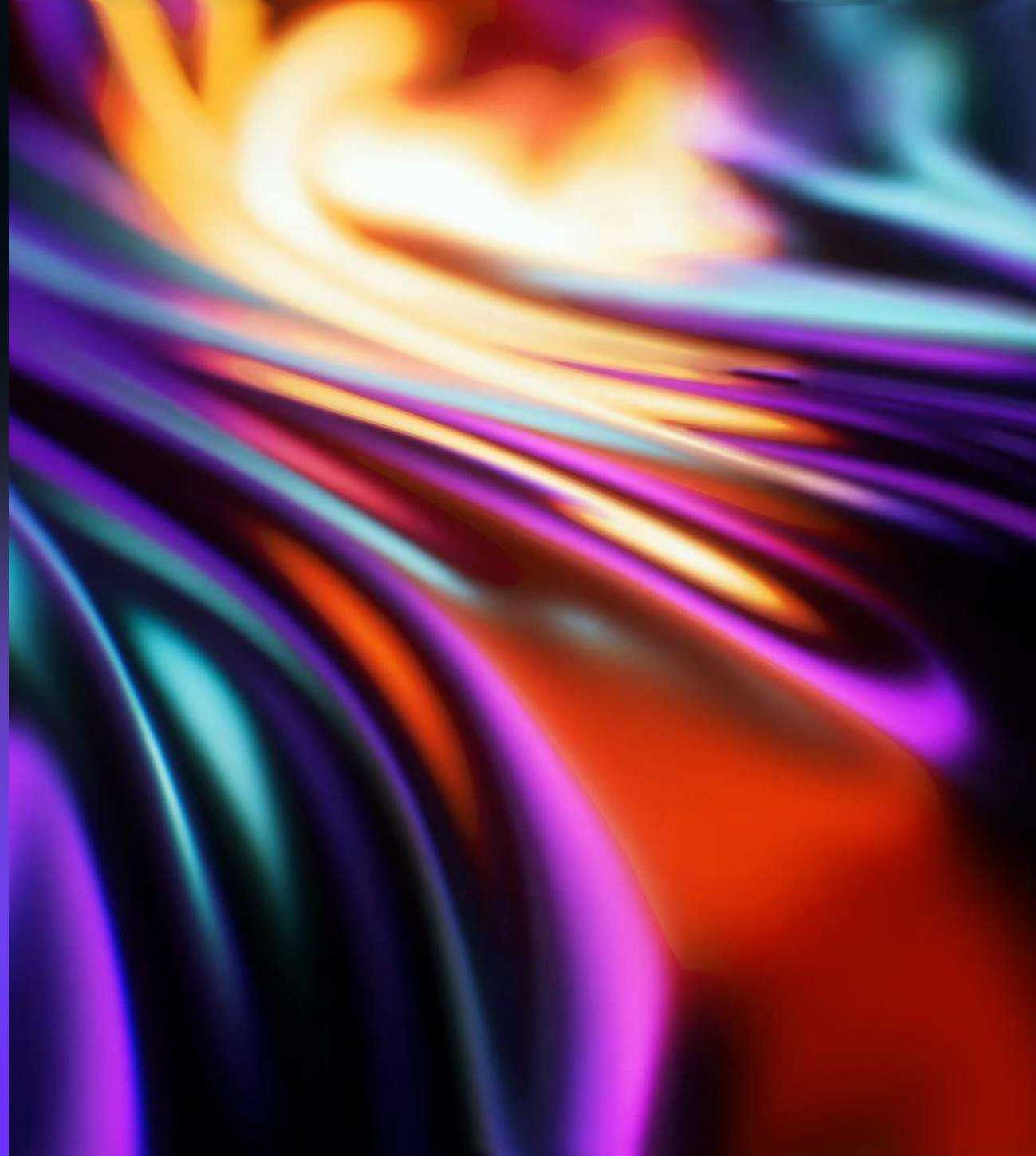
Увеличение эффективности существующей ИБ-команды. Аналитики и эксперты Центра кибербезопасности F6 всегда под рукой.

F6

Узнать подробнее

Business Email Protection

Защитите корпоративную почту от спама, фишинга, вредоносного ПО и BEC-атак



Функциональные возможности F6 Business Email Protection

Решение для защиты корпоративной почты от фишинга, спама, вредоносных вложений и BEC-атак.

- **Антиспам и антифишинг**
- **Песочница в комплекте**
- **Быстрое внедрение**
- **Блокировка вредоносных вложений и ссылок**
- **Защита от подмены личности, BEC-атак**
- **AI и ML для обнаружения сложных угроз**

Варианты развертывания:

On-premise

от 1000 пользователей

Cloud

от 300 пользователей

Функциональные возможности F6 Business Email Protection

Технология Time-of-click

проверяет ссылки в момент перехода по ним

Искусственный интеллект (AI)

изучает письма на наличие спама и фишинга

Данные киберразведки

позволяют атрибутировать угрозы к группировкам

Компьютерное зрение (CV)

обнаруживает формы ввода логина и пароля

Песочница с морфингом

детонирует ВПО в имитации инфраструктуры компании

Технология туннелирования

позволяет перенаправлять трафик через защищенный канал

Ключевые преимущества F6 Business Email Protection

Противодействие обходу обнаружения

Передовые технологии детонации, кастомизация песочницы, а также гибкая настройка маршрутов и проксирования не позволяют киберпреступникам обойти средства обнаружения

Анализ вложений и ссылок

- Поддержка более 300 форматов файлов помогает проанализировать все почтовые вложения
- Проверка ссылок, в том числе использующих техники обфускации, а также исполняемых файлов без расширения и зашифрованных архивов

Многофакторный продвинутый анализ

- Учитываются заголовки письма, параметры сессии
- Производится проверка SPF/DKIM/DMARC, QR-кодов
- Применяются технологии компьютерного зрения, статические и эвристические правила

Пользовательская фильтрация и кастомизация детекта

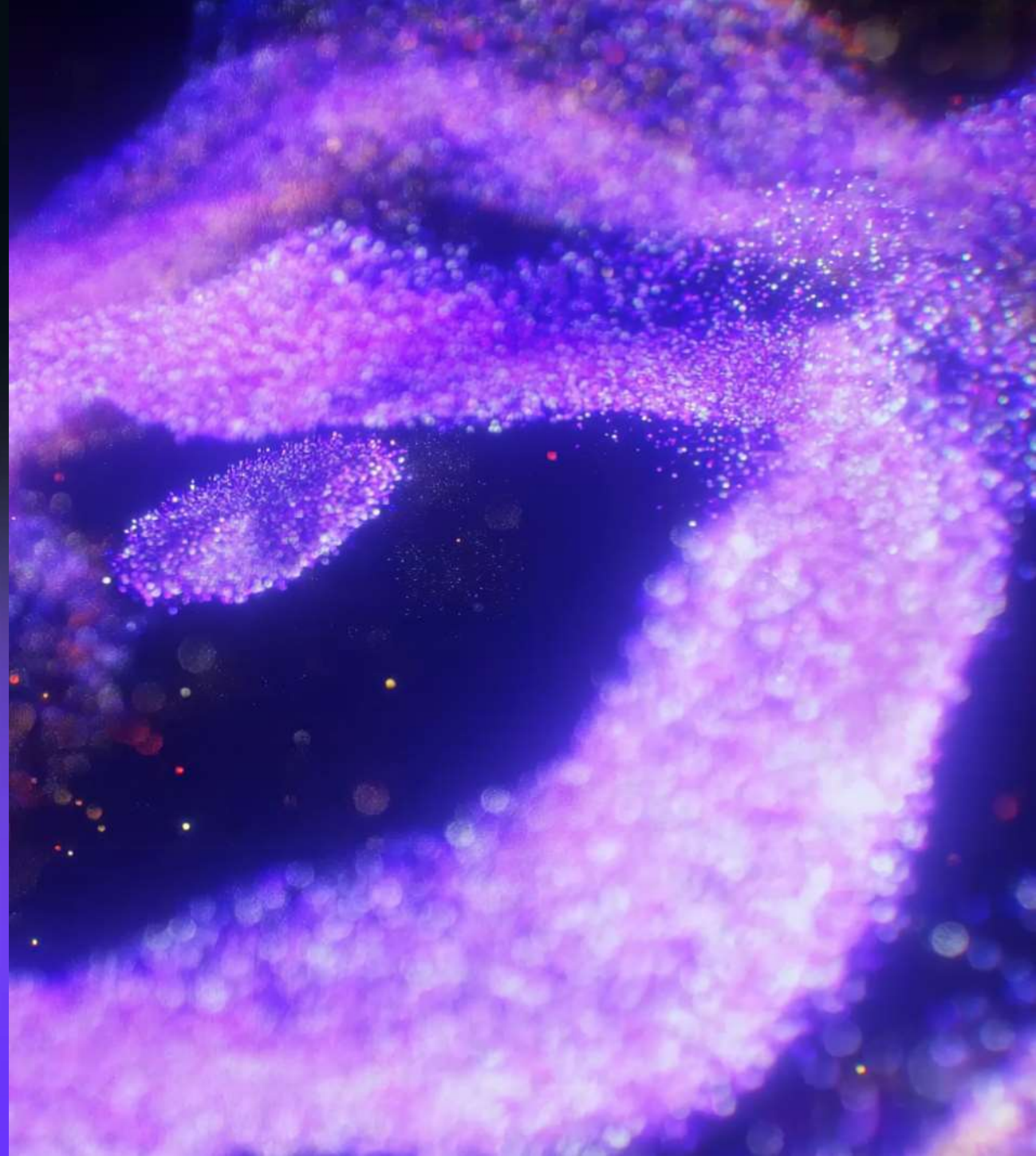
- Возможность определять правила фильтрации и обрабатывать письма по заданным параметрам и контенту.
- Настройки пользовательских лимитов, YARA-правил и grey листов

F6

Узнать подробнее

Fraud Protection

Fraud Protection от F6 — это комплексное решение, в котором используются технологии снятия цифровых отпечатков устройств, выявления мошенничества и поведенческий анализ для защиты мобильных и веб-приложений.



Функциональные возможности F6 Fraud Protection

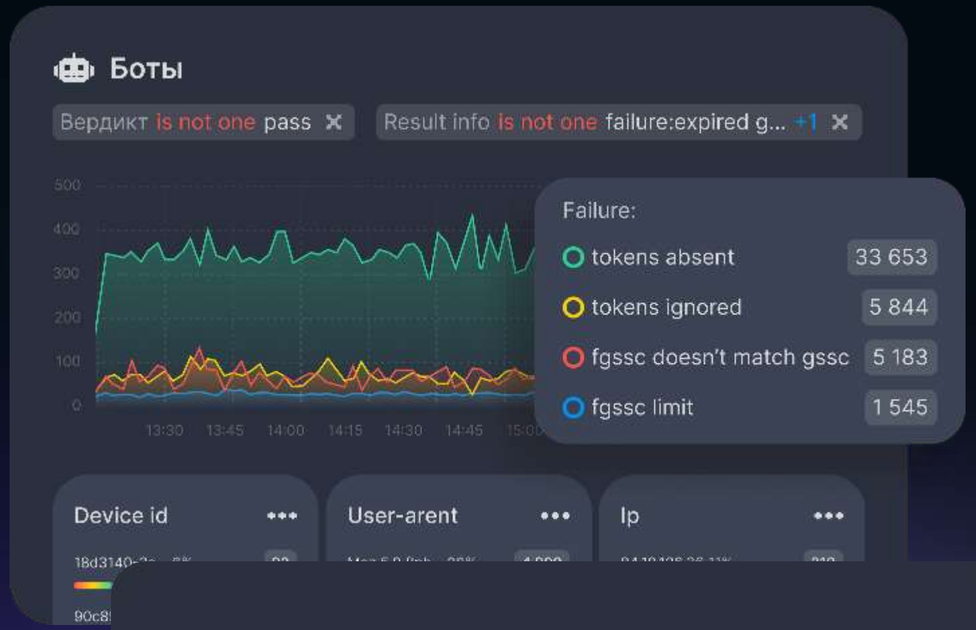
F6

Проактивно выявляйте и блокируйте ботов до нанесения вреда бизнесу и инфраструктуре

Запатентованная технология Preventive Proxy выявляет и блокирует все типы бот-атак, включая скрапинг данных, брутфорс-атаки, нелегитимное использование API, и т.д.

Обеспечьте верификацию пользователя на всех уровнях

Fraud Protection анализирует активность пользователя с помощью алгоритмов машинного обучения и выявляет аномальную активность, позволяя снизить расходы на верификацию транзакций и потери от мошенничества

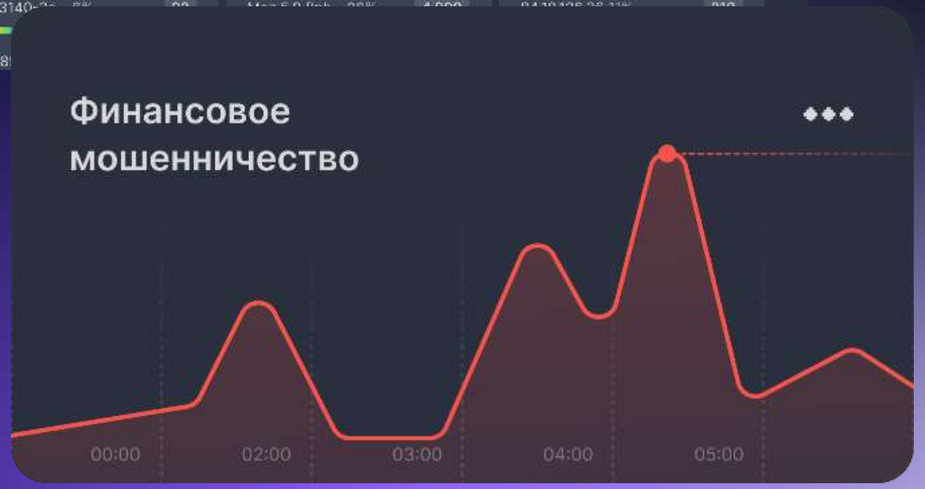


Оптимизируйте защиту вашей организации

Принимайте обоснованные решения по улучшению политики безопасности и внедрению необходимых защитных мер, что помогает компаниям быстрее реагировать на угрозы

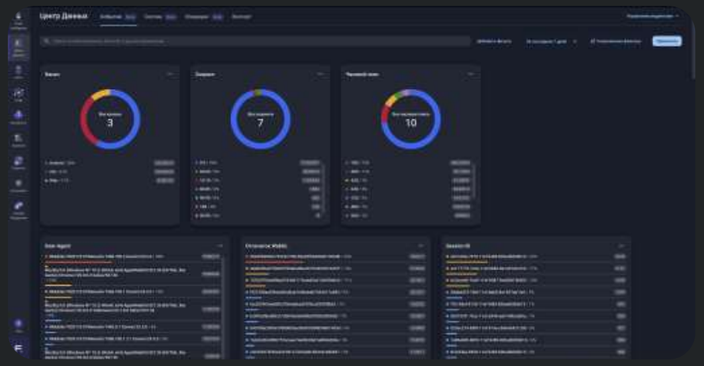
Минимизируйте финансовые потери от кибератак

Снижайте убытки до 30% в сравнении с компаниями, которые не используют продвинутые решения по управлению угрозами

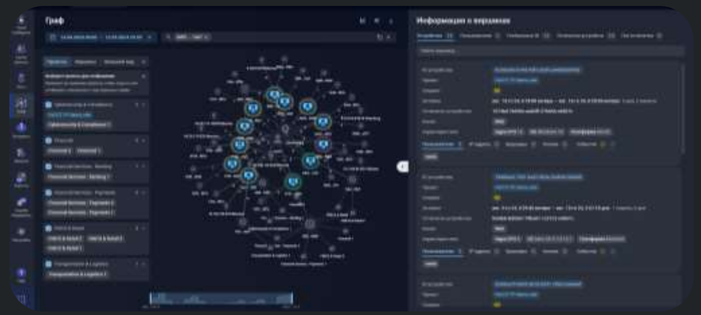


Функциональные возможности F6 Fraud Protection

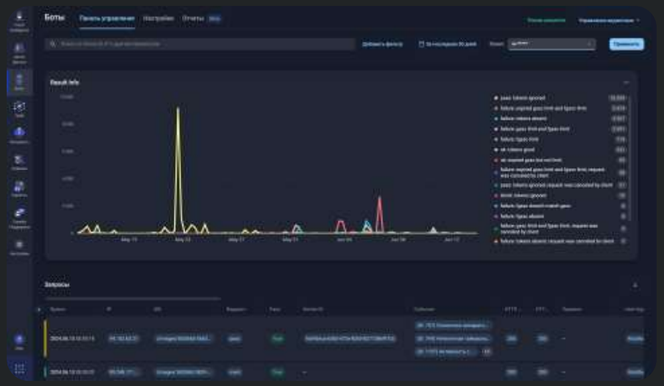
Интерактивная панель управления



Кросс отраслевой графовый анализ

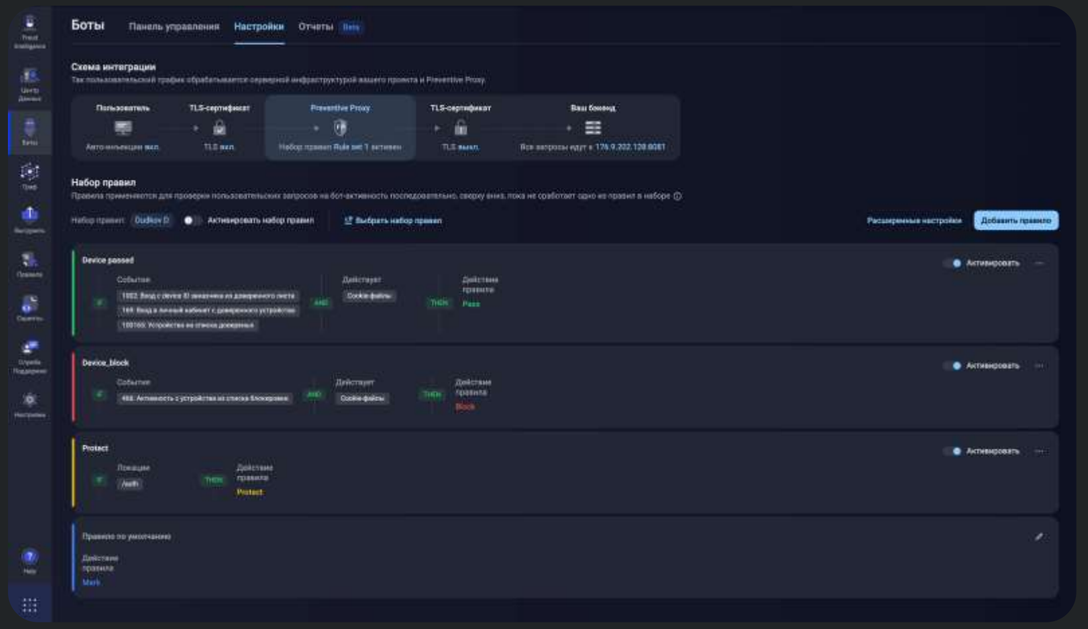


Контроль и оценка всех запросов



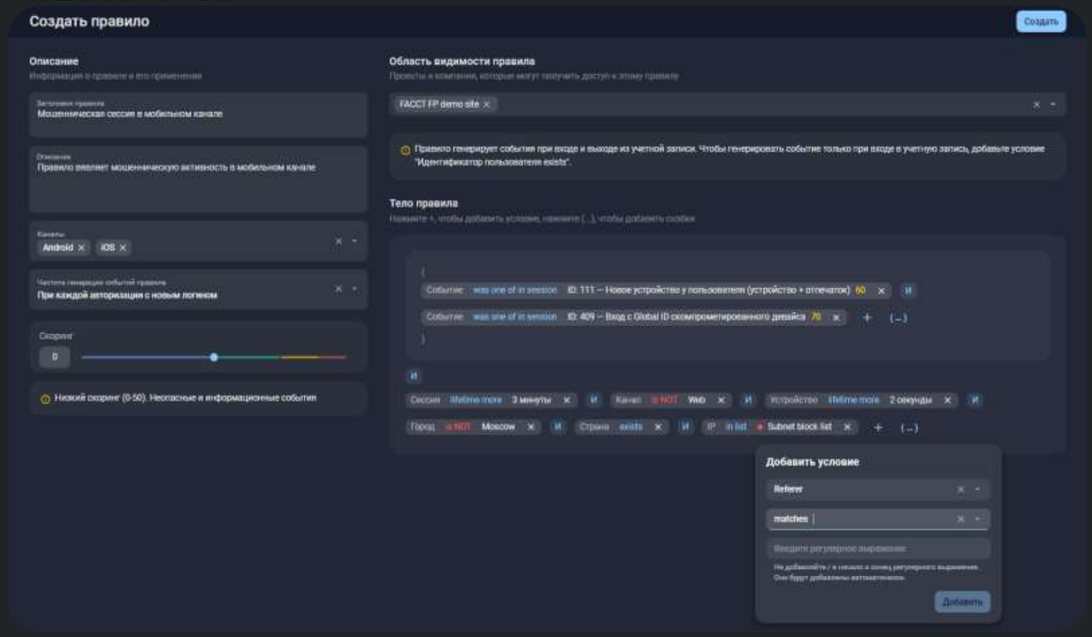
Функциональные возможности F6 Fraud Protection

Универсальная панель управления Правилами реагирования



Конструктор правил

Визуальный конструктор правил позволяющий самостоятельно создавать условия реагирования на новые выявленные случаи мошенничества.



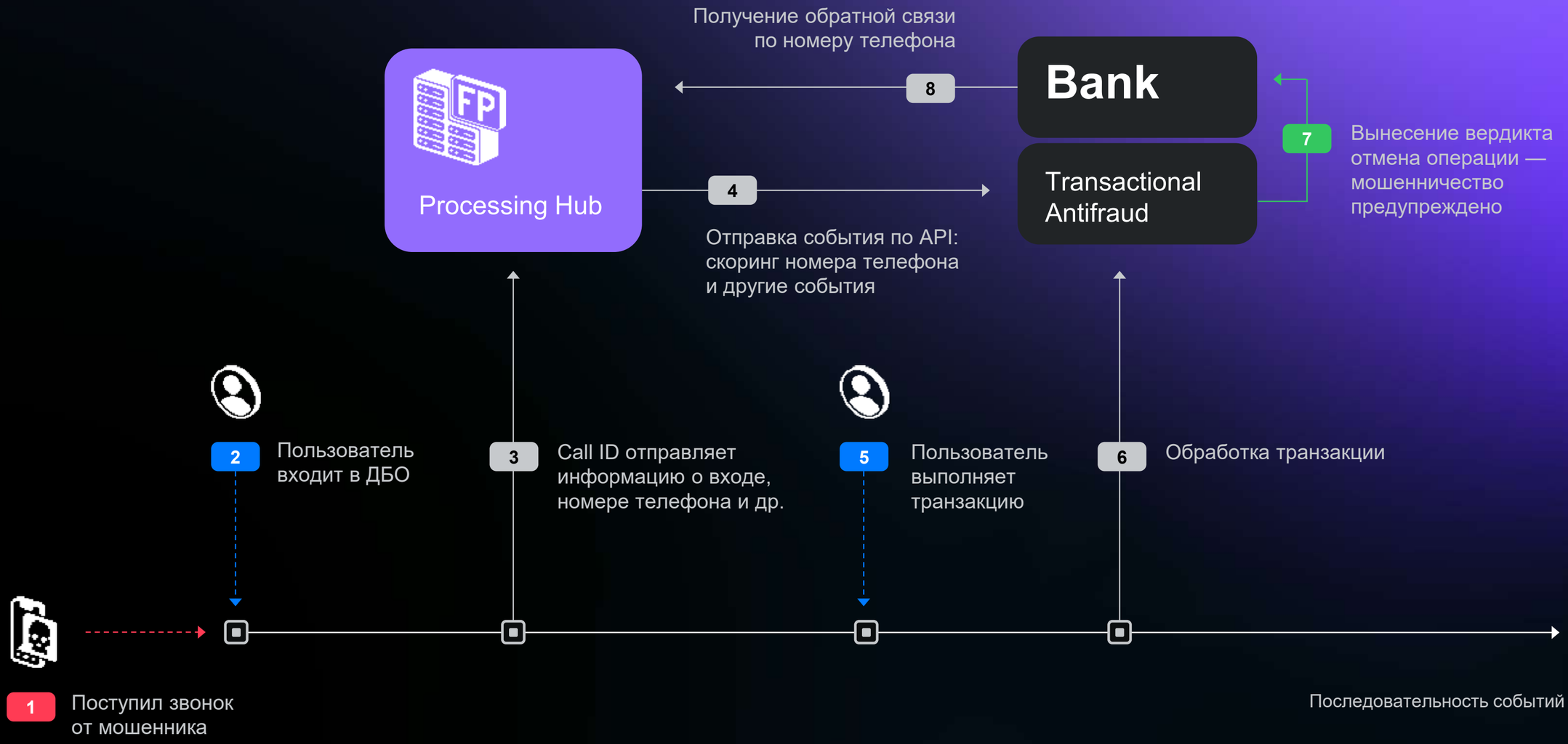
Ключевые преимущества F6 Fraud Protection

F6

- F6 Global ID
- Анализ поведения
- Защита от ботов
- Цифровой отпечаток устройства
- Выявление отмывания денег
- Кросс-канальный анализ
- Предотвращение социотехнических атак
- Предотвращение мошенничества card-not-present
- Графический исследовательский инструмент
- Построение правил и управление ими
- Компьютерная криминалистика и исследования
- Прозрачный искусственный интеллект

Ключевые преимущества F6 Fraud Protection

Выявление мошеннических звонков



Ключевые преимущества F6 Fraud Protection

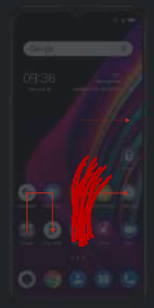
Анализ цифровых «отпечатков» устройств и цифровая биометрия для мобильных приложений

Определение легитимности пользователя: индивидуальные паттерны пользовательского поведения

- Прикосновения к экрану (сила и точки нажатий)
- Углы траектории свайпов
- Анализ свайпов
- Средняя скорость свайпов
- Средний угол отклонения
- свайпов от горизонтальной оси

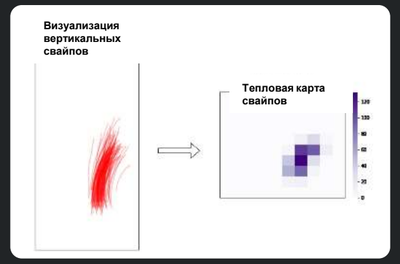
Индикаторы мошенничества в пользовательской сессии

- Отклонения в характеристиках прикосновений к экрану (сила и точки нажатий)
- Отклонения в углах траекторий свайпов
- Отклонения в скорости свайпов
- Нетипичные значения углов отклонения свайпов от горизонтальной оси

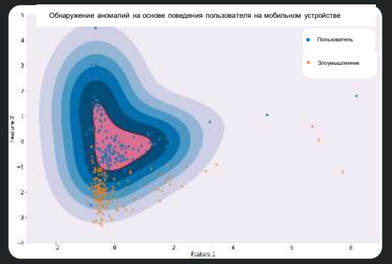


Мобильная биометрия

Использование датчиков мобильных устройств для сбора цифровой биометрии



Показатели акселерометра и гироскопа



Тепловая карта прикосновений и свайпов

Интенсивность и частота прикосновений

Длительность и направление свайпов

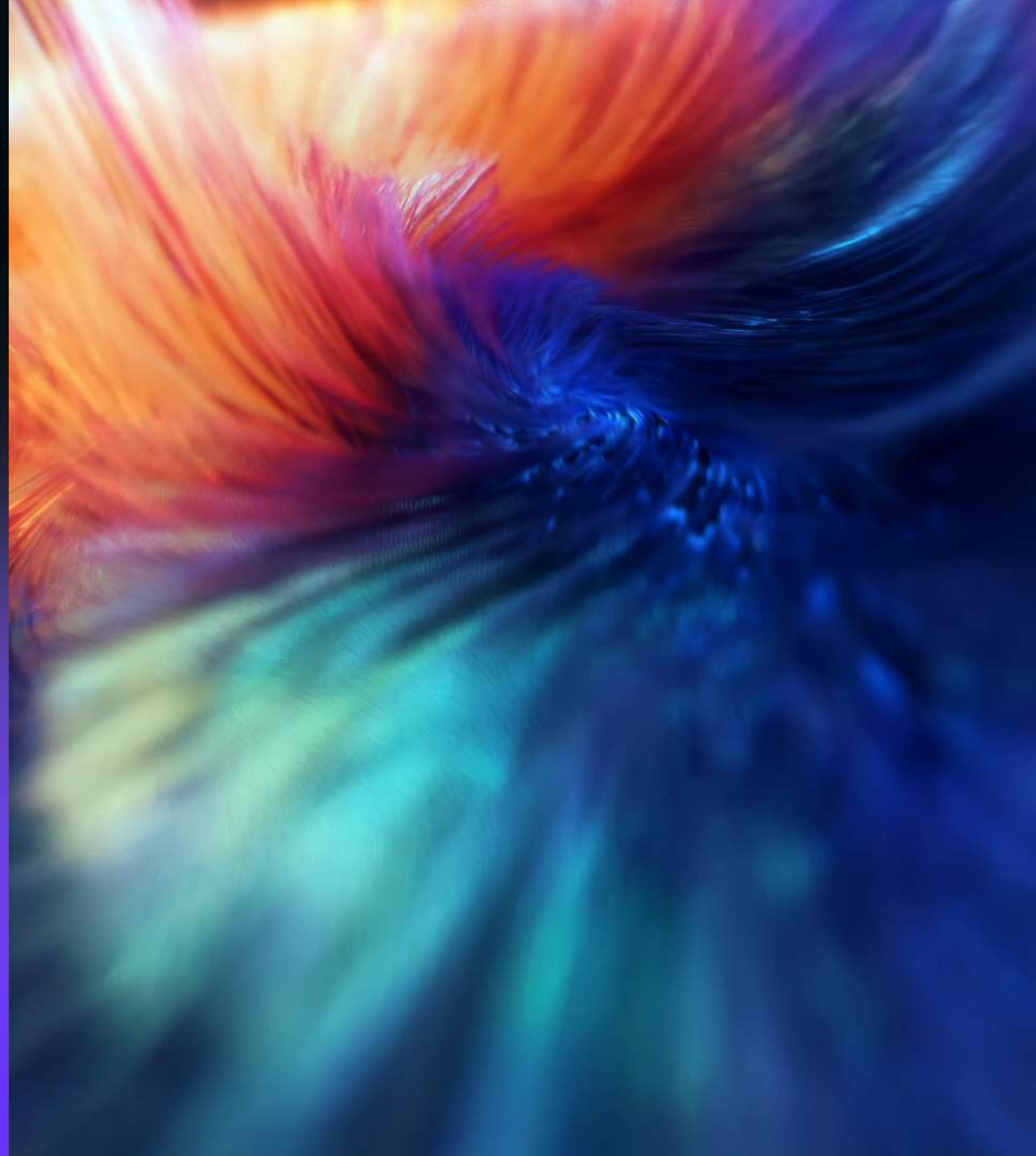
Анализ цифровых «отпечатков» В веб-каналах и цифровая биометрия

F6

Узнать подробнее

Digital Risk Protection

Управление цифровыми рисками



Digital Risk Protection от F6

Это продукт для защиты от цифровых угроз,
таких как онлайн-мошенничество, фишинг
и неправомерное использование бренда

F6

70+

технических специалистов
и юристов в команде

500+

брендов защищено

13+

лет опыта защиты брендов

Функциональные возможности F6 Digital Risk Protection

Искуственный интеллект

Семейство нейронных сетей способное выявлять до 90% нарушений, подобно высококвалифицированному специалисту

Графовый анализ

Сетевой анализ, который помогает выявить инфраструктуру киберпреступников и найти дополнительные методы для успешного устранения нарушений

Скоринговая модель

Запатентованная технология для оценки уровня опасности, что позволяет быстро и точно расставлять приоритеты для реагирования

Аналитика мошеннической деятельности

Инновационный метод анализа, расследования и прогнозирования действий мошенников, для повышения эффективности выявления и предотвращения мошеннических схем

Доверие регуляторов

Налаженные каналы взаимодействия и сотрудничество с крупнейшими интернет-регуляторами, способствующие оперативному устранению выявленных нарушений в досудебном порядке

Автоматизированный инструмент составления обращений

Автоматизированное составление индивидуальных обращений позволяет быстро и безошибочно формировать жалобы, в зависимости от владельцев ресурсов, регуляторов, сложности кейса, типа ресурса, источника и других составляющих

Ключевые преимущества F6 Digital Risk Protection

Выстроенные отношения с крупными площадками

Оперативное устранение нарушений через ускоренное рассмотрение запросов администраторами крупных площадок, поисковых систем и соцсетей

Официальные соглашения

- Координационный центр доменов .RU/.РФ
- Фонд содействия развитию технологий
- АНО «ЦВКС МСК-IX»
- АНО «Росниирос»

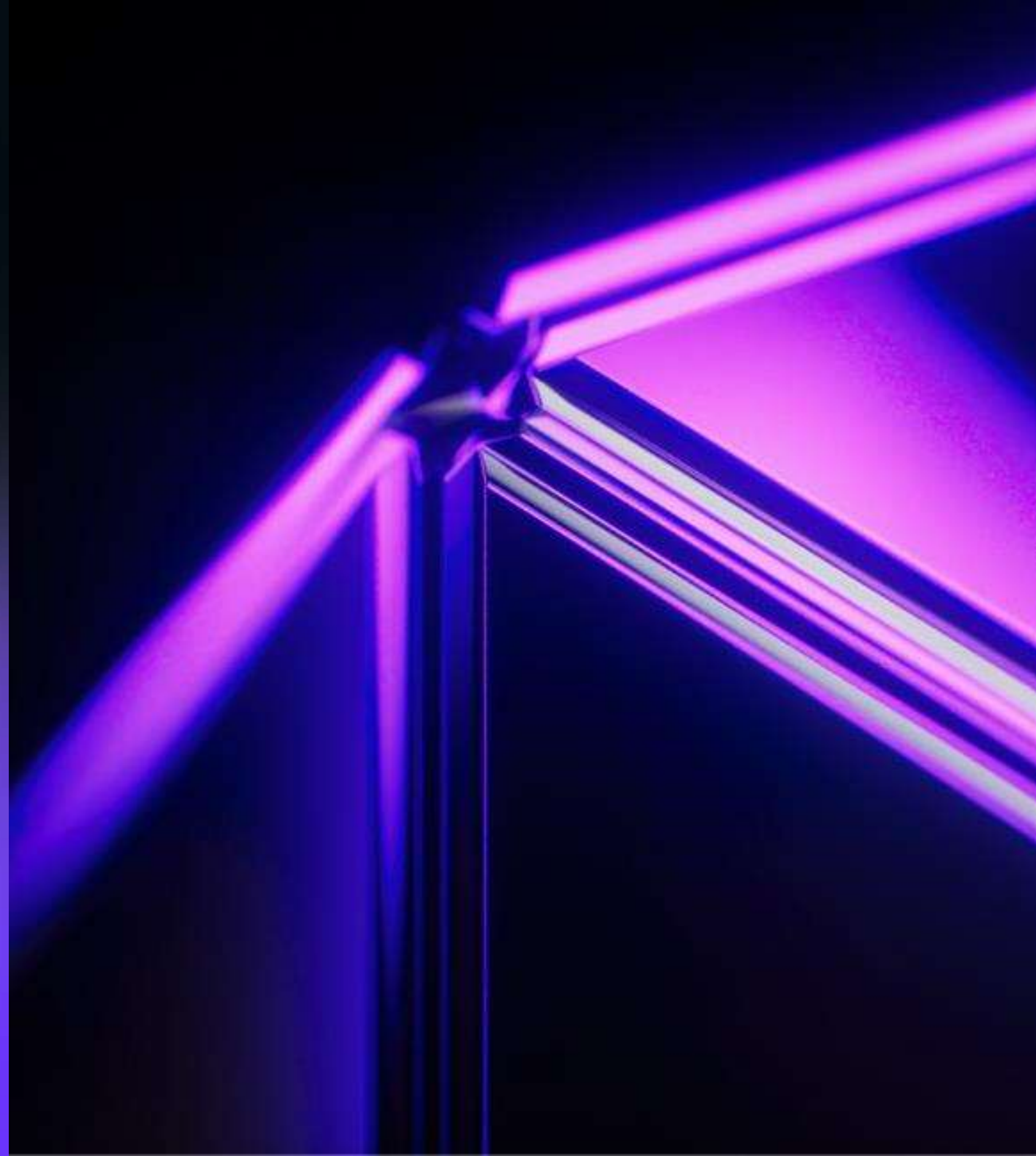
Поддержка команды CERT F6

Круглосуточная группа экстренного реагирования, которая осуществляет мониторинг угроз, выявляет их источники, и способствует устранению нарушения

F6

Узнать подробнее

Сервисы



Функциональные возможности сервисов F6

Работа с инцидентами

Цифровая криминалистика

восстановим хронологию кибератак и предоставим экспертные заключения для вашей победы в суде

Расследование киберпреступлений

мы обеспечим полное сопровождение инцидента: от правовой поддержки и помощи в привлечении к ответственности до расследования причин и последствий атаки

Локализация последствий инцидента

оперативные меры по остановке атаки и ограничению её воздействия на бизнес. Мы быстро выявим и нейтрализуем точки проникновения, устраним последствия компрометации и предотвратим повторные инциденты

Тестирование безопасности

Тестирование инфраструктуры

обнаружим уязвимости вашей ИТ-инфраструктуры и дадим рекомендации по их устранению: проверяем сеть, тестируем системы и сохраняем вашу безопасность под контролем

Тестирование приложений

обнаружим уязвимости ваших приложений и дадим рекомендации по их устранению: комплексное исследование приложений на предмет наличия уязвимостей

Тренировка ИБ-команд

практическая отработка навыков противодействия киберугрозам. Имитация действий злоумышленника и совместная работа атакующих и защитников для повышения эффективности защиты вашей инфраструктуры

Оценка соответствия и консалтинг

Требования регуляторов

проведем оценку выполнений требований законодательства и сформируем рекомендации по их выполнению. Экспертный анализ соответствия требованиям закона и четкие шаги для исправления нарушений

Менеджмент ИБ

проведем комплексный аудит вашей системы и приведем ее в соответствие лучшим практикам в сфере ИБ

Мониторинг и реагирование

SOC

центр мониторинга информационной безопасности, обеспечивающий круглосуточное наблюдение за ИТ-инфраструктурой, оперативное выявление угроз и реагирование на инциденты

Подготовка

поможем выстроить эффективные процессы реагирования: проведем аудит текущей готовности, разработаем план действий и обучим персонал, чтобы вы были готовы к любым сценариям

Образовательный центр F6

Курсы для специалистов ИБ

углубленное обучение для профессионалов в сфере информационной безопасности. Курсы направлены на развитие практических навыков. Подходят для специалистов разного уровня подготовки — от начинающих до экспертов.

Корпоративные программы

комплексные образовательные решения для команд. Программы повышения квалификации адаптированы под цели и задачи компаний: цифровая гигиена, обучение сотрудников основам ИБ, подготовка к сертификациям.

Интерактивные форматы

обучение через практику и симуляции. Они включают тренажёры и сценарные отработки. Участники погружаются в реальные кейсы, принимают решения и анализируют последствия — всё это усиливает усвоение материала и формирует практические компетенции.

Ключевые преимущества сервисов F6

Уникальная экспертиза и лидерство в расследованиях

Первая в России лаборатория, специализирующаяся на расследовании инцидентов ИБ. Мы обладаем уникальными методиками и инструментами для поиска злоумышленников и выявления следов компрометации, что делает нас незаменимым партнером при инцидентах

Практический подход и акцент на результат

Мы не оказываем формальные услуги ради галочки. Каждая наша работа приносит реальную пользу клиентам, повышая уровень их защиты. Именно поэтому компании продолжают работать с нами годами, доверяя нам самые сложные и ответственные задачи в области ИБ

Полный спектр услуг в сфере кибербезопасности

От мониторинга и реагирования до моделирования угроз и тестирования защищенности – мы предлагаем комплексные решения, включая пентесты, Red и Purple Teaming, обучение сотрудников, аудит на соответствие требованиям регуляторов и многое другое

Высокие стандарты качества и надежность

Мы придерживаемся строгих стандартов работы, что позволяет нашим клиентам быть уверенными в надежности своих систем. Наши специалисты обладают глубокой технической экспертизой и помогают компаниям выстраивать устойчивую систему кибербезопасности

F6

Благодарим за внимание!

Решения для предотвращения кибератак, борьбы с мошенничеством и защиты брендов

На связи 24/7

f6.ru team@f6.ru