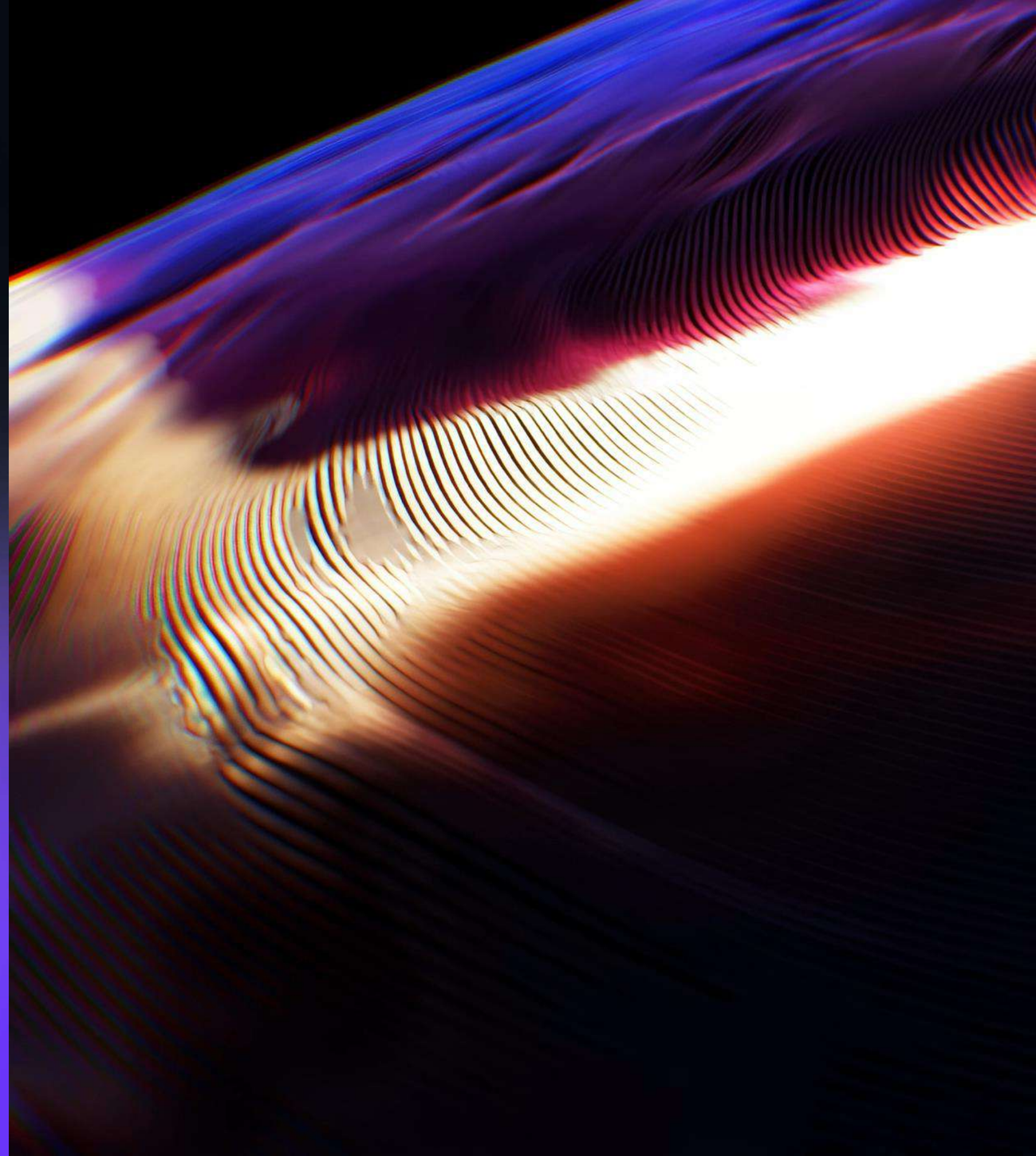
F6

Attack Surface Management

Контроль
внешней поверхности атаки



F6

1 300+
успешных исследований киберпреступлений по всему миру

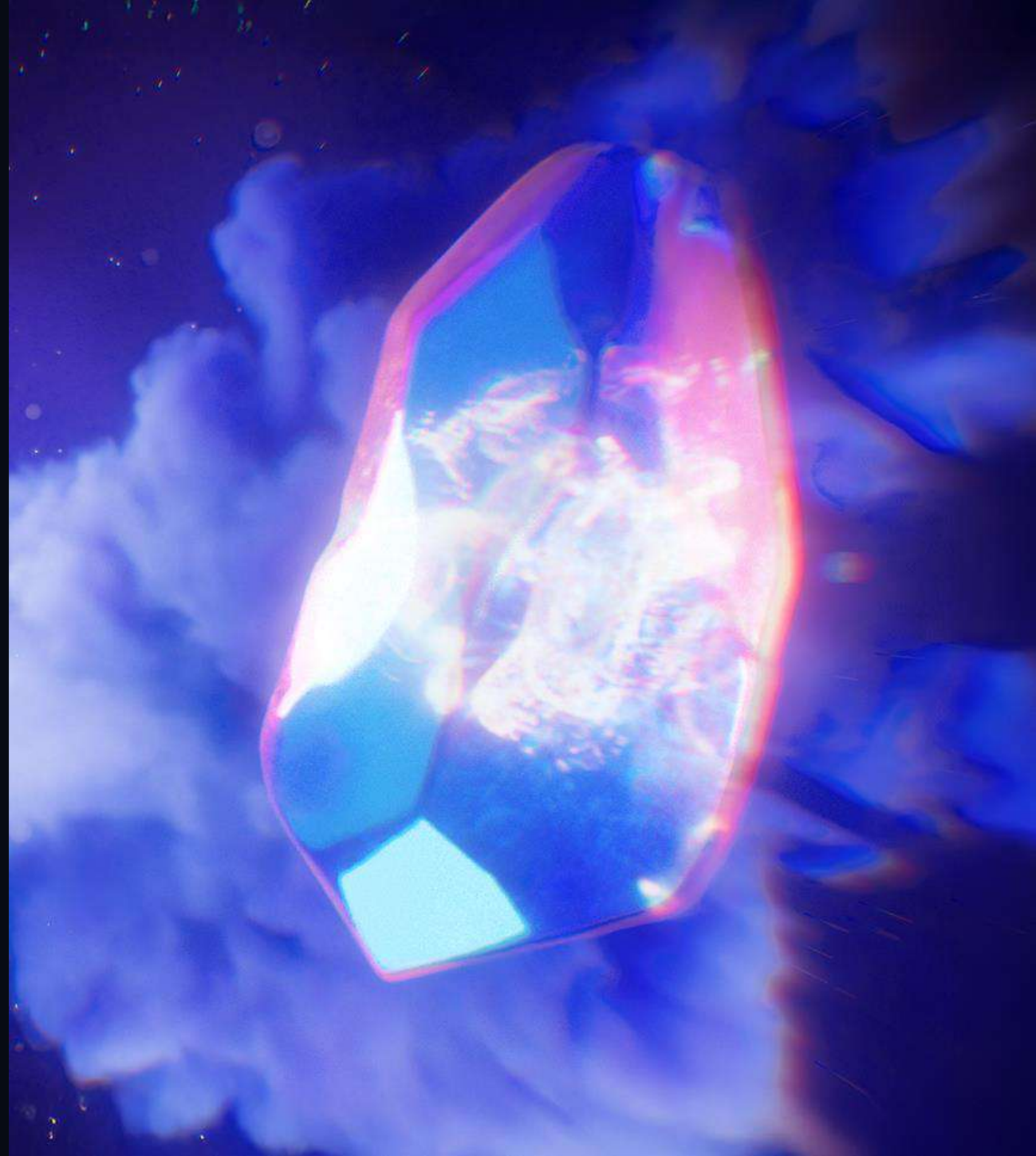
550+
enterprise-клиентов

№1
первый поставщик услуги Incident Response в России

120+
патентов и заявок

20 млрд+
рублей сохраняют наши технологии в бюджете клиентов ежегодно

20 лет
практики и уникальной экспертизы на рынке РФ



История F6

F6

Компания основана как частное кибердетективное агентство

2003-2011

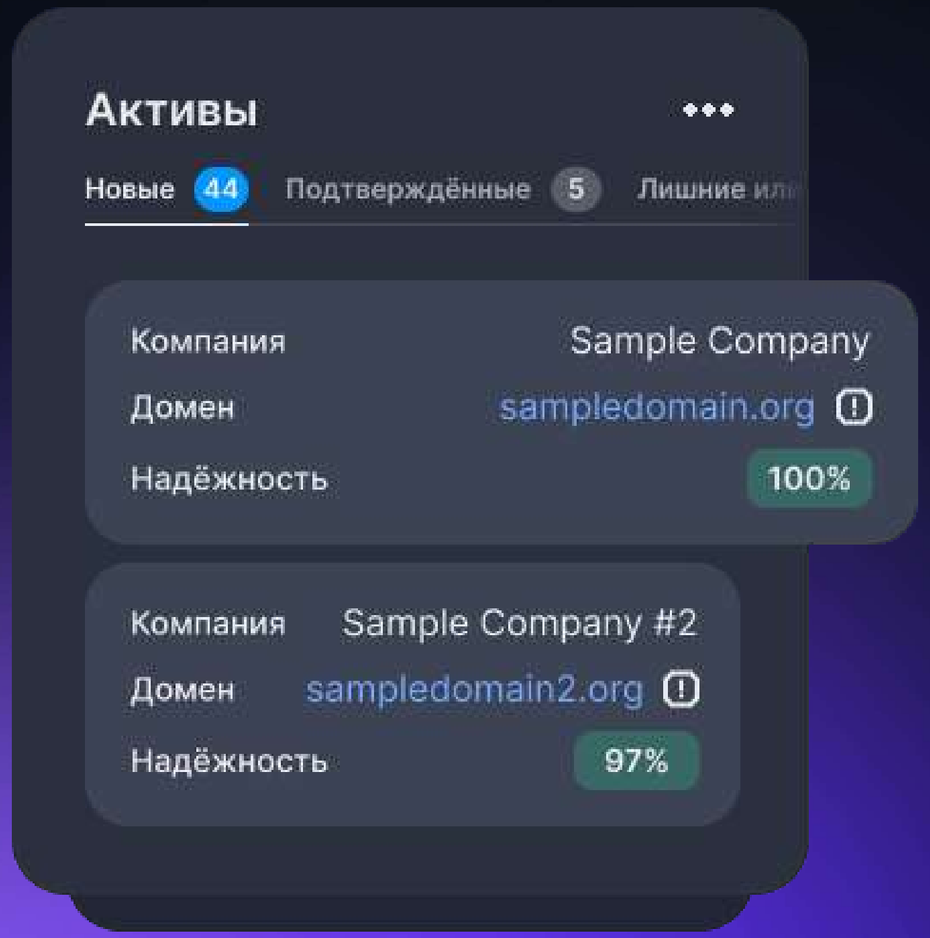
Разработка собственных продуктов по кибербезопасности

2013-2025

Attack Surface Management от F6

F6

Решение для управления
поверхностью атаки
и отслеживания цифровых
активов компании



Как Attack Surface Management помогает предотвращать атаки на вашу компанию?

F6

Обнаруживает и классифицирует активы

Идентифицирует теневые активы внешнего периметра компании

Производит круглосуточный мониторинг активов и проблем внешнего периметра

Выявляет внешние угрозы:

- Утечки
- Упоминания в Darkweb
- Вредоносное ПО
- Уязвимость электронной почты

Оповещает об инфраструктурных рисках

Оптимизирует рабочие процессы ИБ

Отслеживает и определяет уровень защищенности в динамике

Ваша компания является жертвой успешной атаки, если

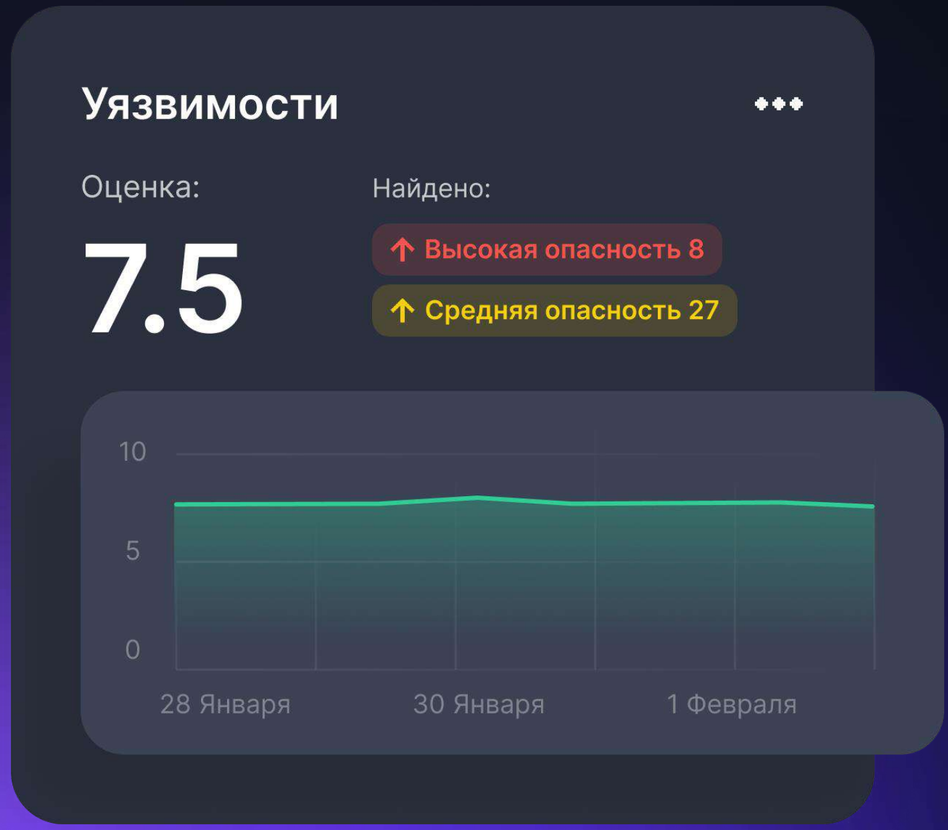
F6

Отсутствует актуальная информация об уязвимых активах, включая теневую инфраструктуру

Нет полного контроля и классификации активов

Цифровые активы хранятся бесконтрольно и обрабатываются несистемно

Автоматизация процессов по выявлению уязвимостей на периметре находится на низком уровне



Статистика инцидентов

F6

Ежегодный отчет

Киберугрозы в России и СНГ 2024/25

55%

Всех инцидентов, которыми занимались специалисты F6, были вызваны уязвимостями на внешнем периметре цифровой инфраструктуры

173%

Прирост количества предложений по продаже удаленного доступа к крупным корпоративным сетям

200,5 млн

Общее количество строк данных пользователей, попавших в утечки в 2024 году

Почему важно контролировать цифровые активы

Плохо защищенные активы — это точки компрометации вашей компании номер один

Злоумышленники регулярно проводят автоматическую разведку и находят незащищенные активы жертвы:

- Облачные сервисы с уязвимым программным обеспечением
- Базы данных, случайно ставшие доступными в сети
- Самостоятельно развернутый веб-сервер
- Учетные данные пользователей

Ключевые функции Attack Surface Management

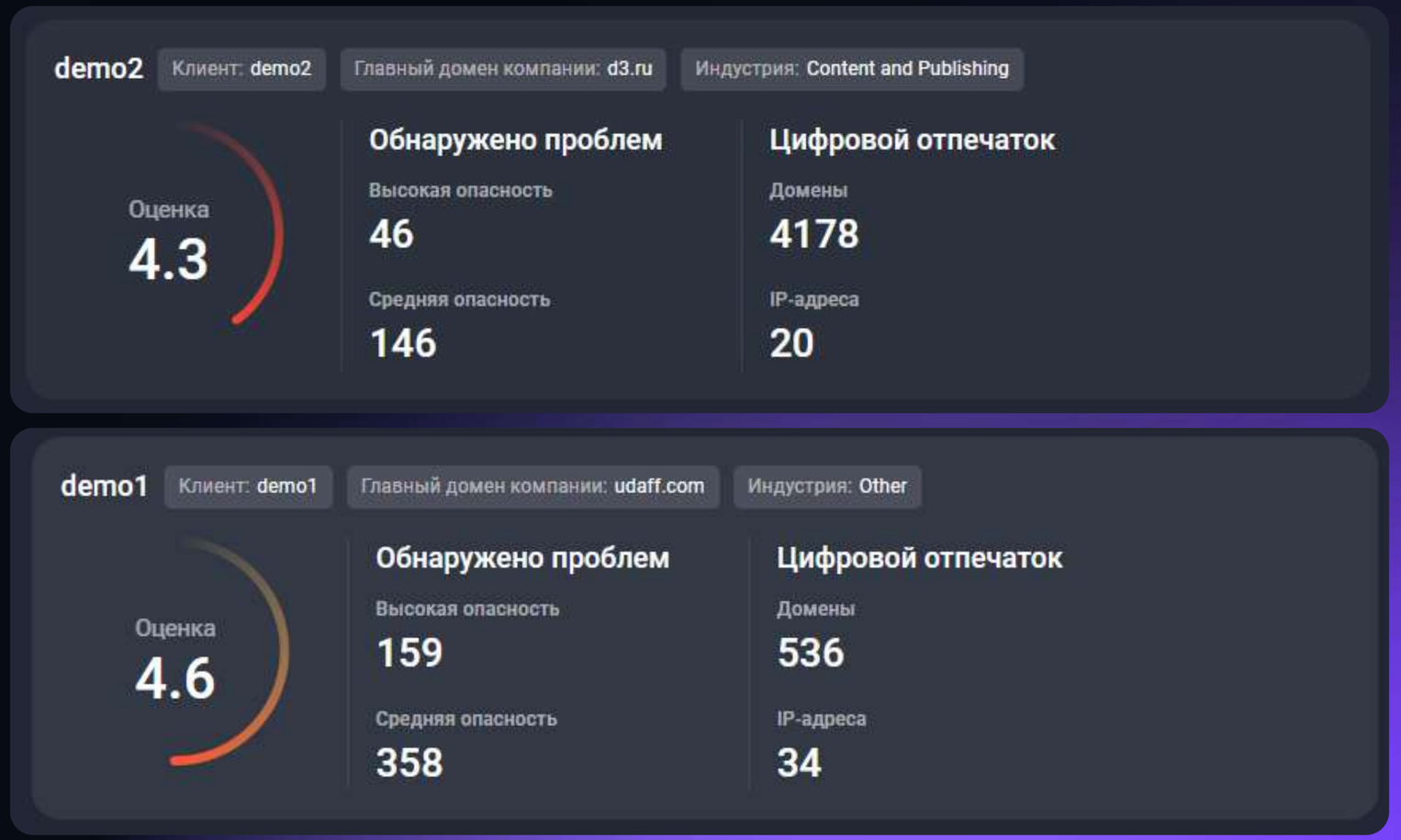
F6

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

Непрерывный мониторинг

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



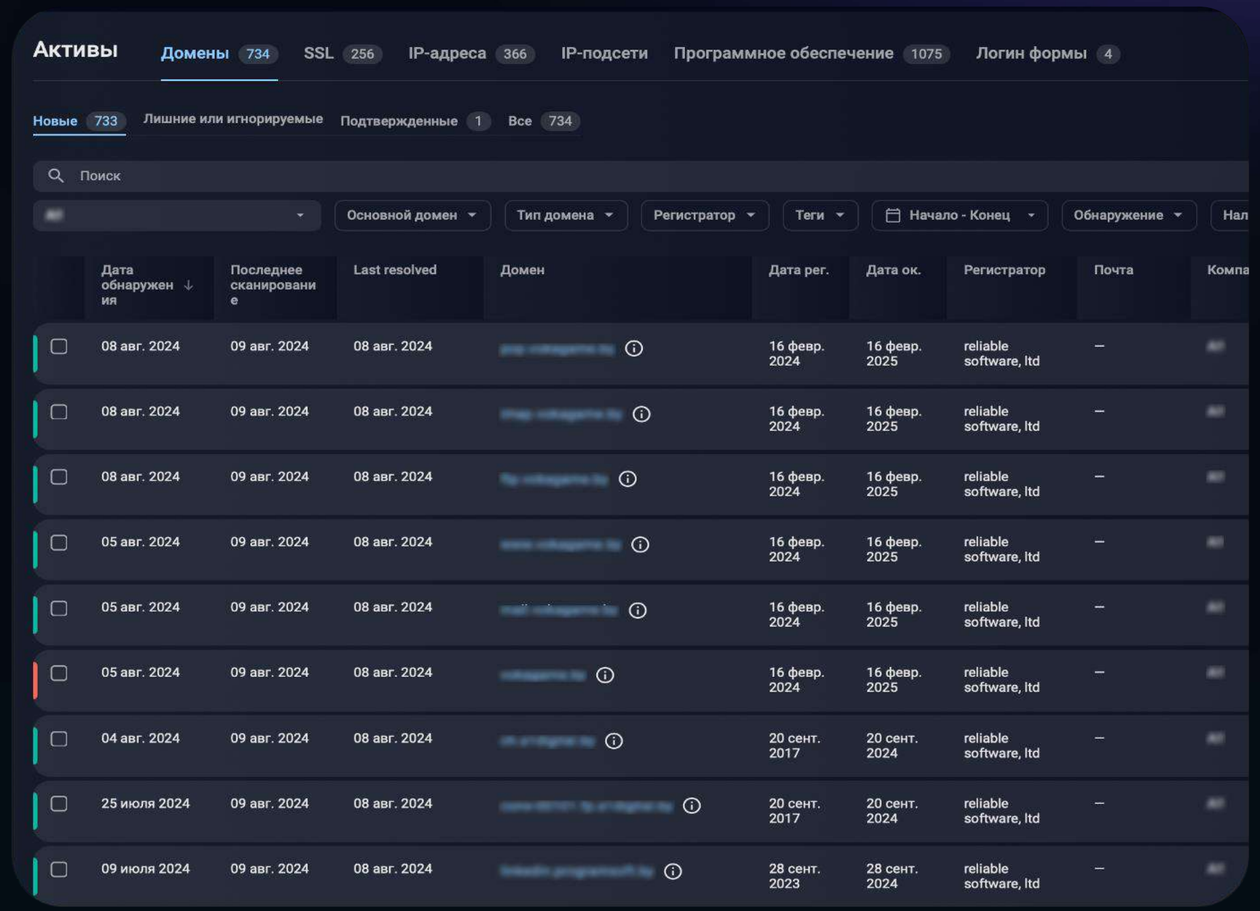
F6

Система использует комплексный подход к обнаружению уязвимостей

- Пространство IPv4, IPv6
- DNS-сервера, домены
- Информация из SSL-сертификатов
- Сетевые порты 1 – 65536
- Конфигурация ПО
- Логин-формы
- Утечки, ВПО и Darkweb
- Почтовые сервера
- Открытые базы данных

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

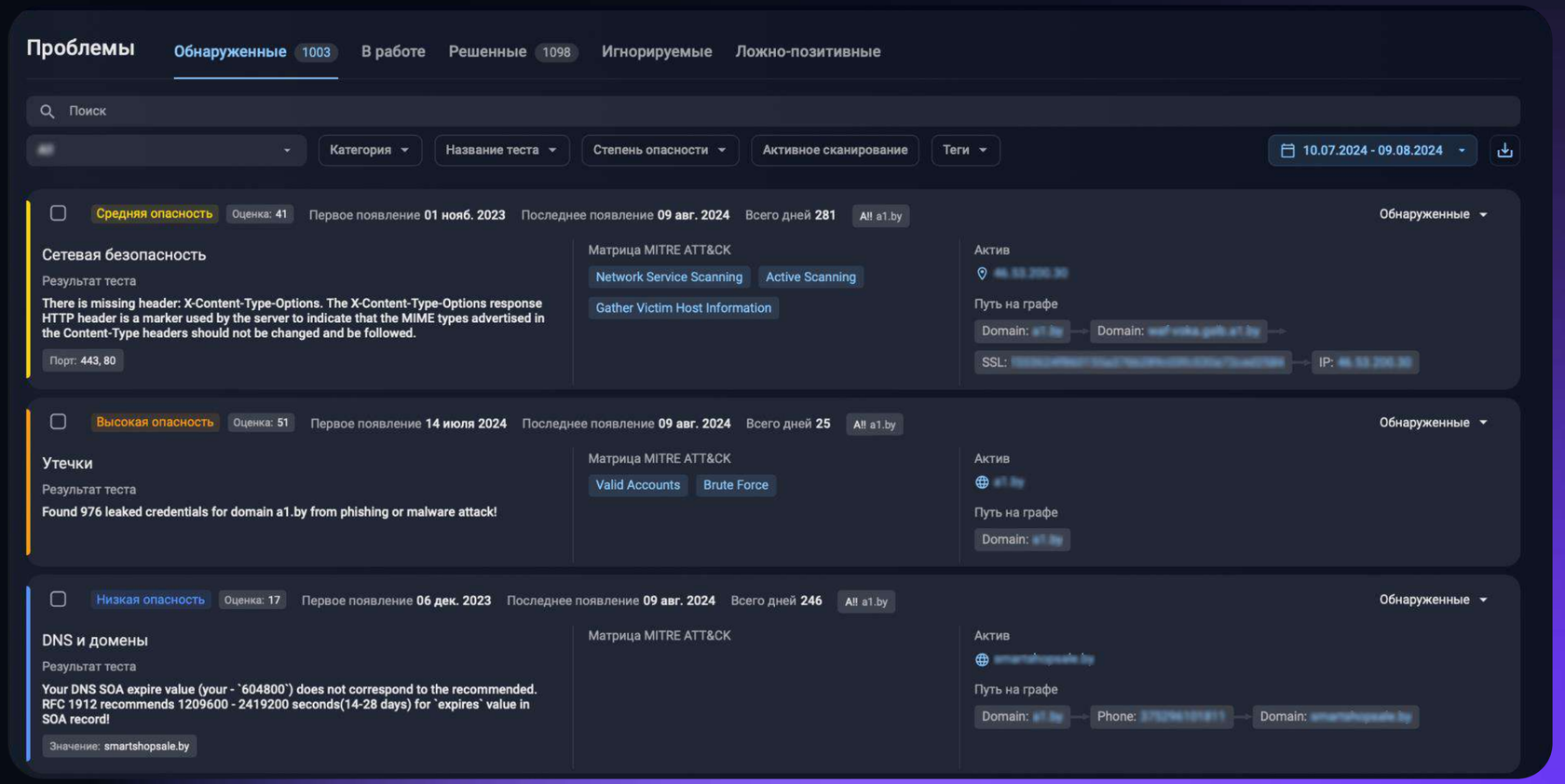


Обнаруженные активы включают

- Доменные имена
- SSL-сертификаты
- IP-адреса
- IP-подсети
- ПО (на серверах)
- Логин-формы

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



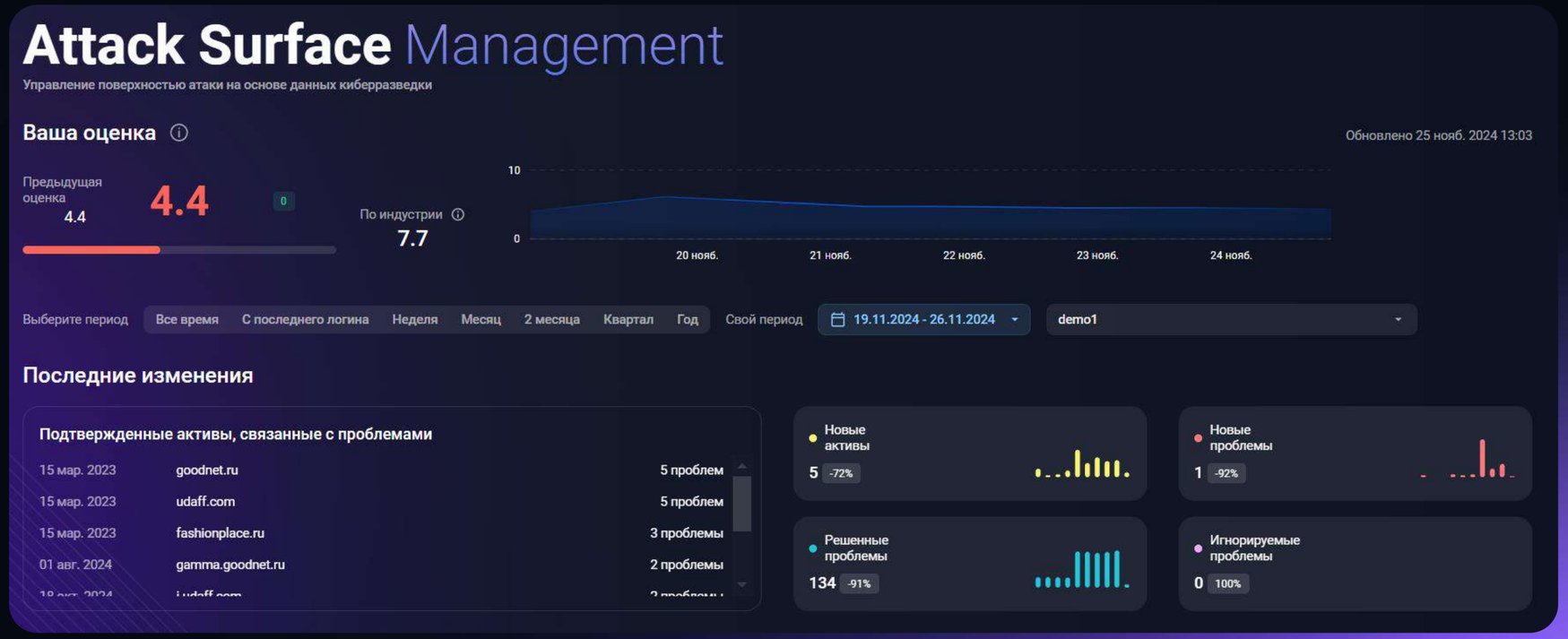
Система использует комплексный подход к обнаружению уязвимостей

- Выявляет баннеры и службы, запущенные на сервере, сопоставляет найденную информацию с известными уязвимостями
- Посещает каждый IP-адрес, домен и путь веб-сайта для обнаружения технологий, которые используются для создания веб-приложений
- Проверяет на сервере базы данных в открытом доступе, бакеты файловых хранилищ, открытые листинги каталогов и другие признаки некорректной конфигурации

Оценка уровня защищенности

F6

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



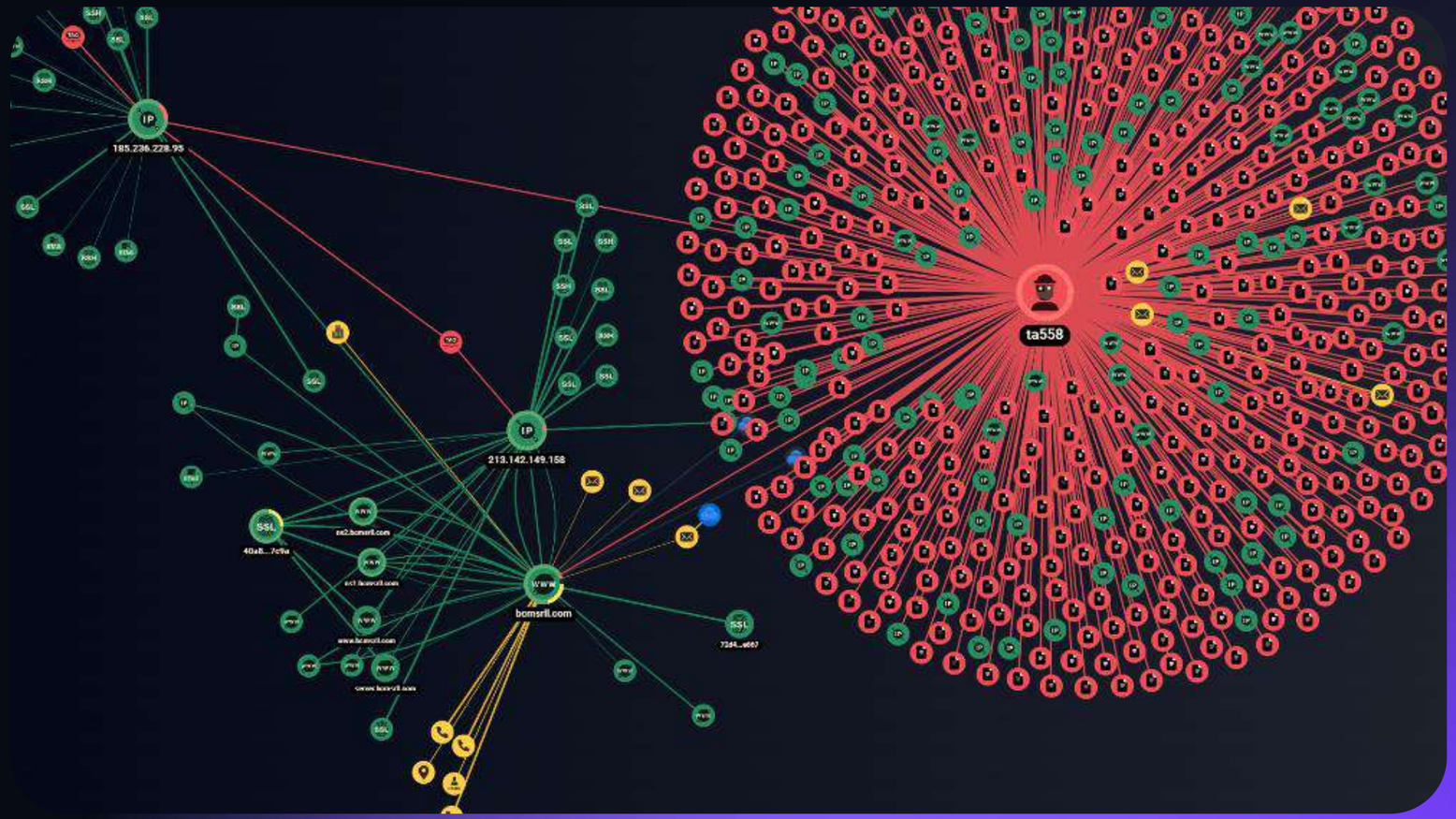
Attack Surface Management оценивает уровень защищенности компании на основании восьми категорий

- Уязвимости
- Сетевая безопасность
- Утечки учетных данных
- Защищенность от вредоносного ПО
- Упоминания в Darkweb
- Безопасность SSL/TLS
- Безопасность электронной почты
- DNS и домены

Графовый анализ

F6

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

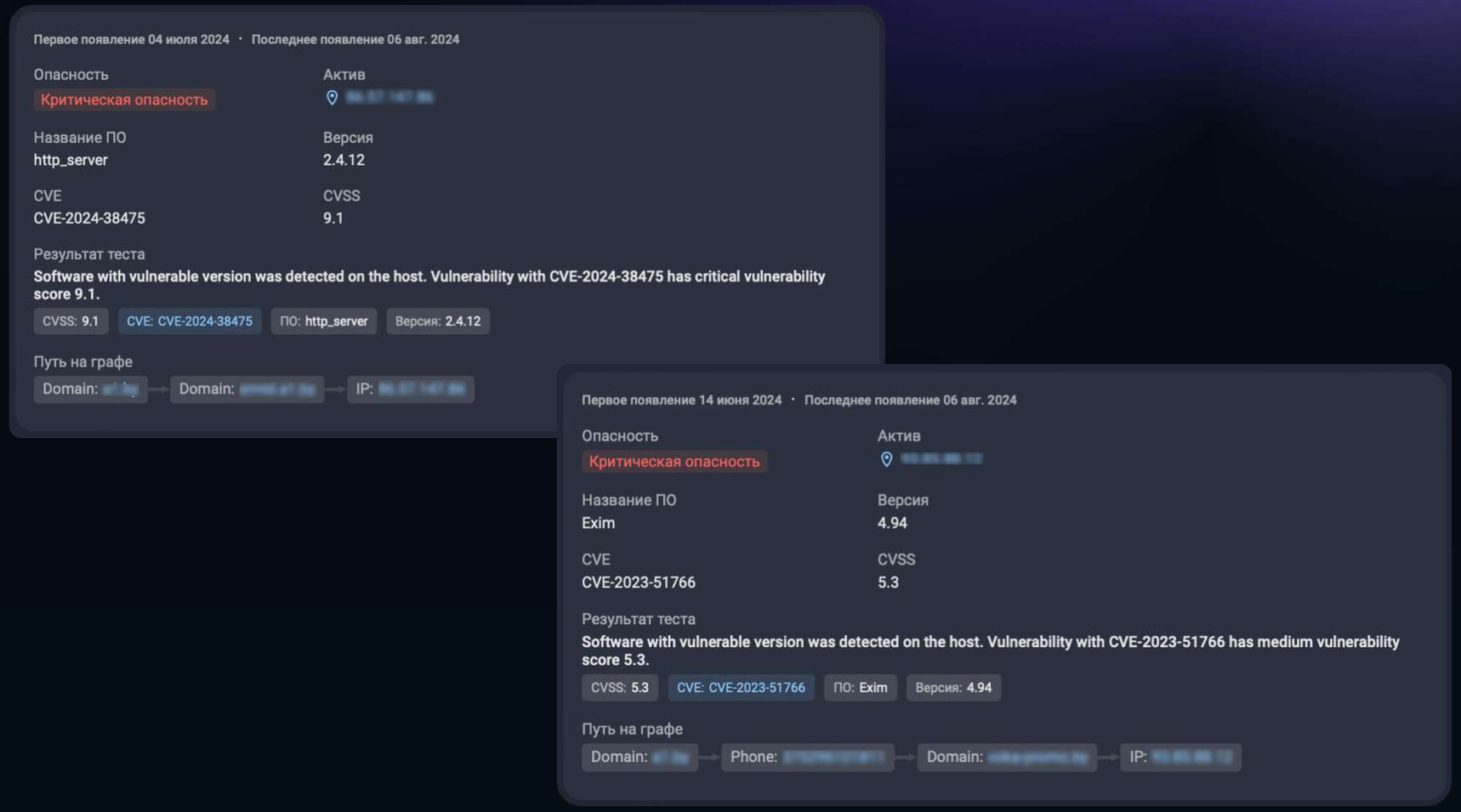


Исследуйте связи между атакующими, их инфраструктурами и инструментами и узнавайте подробную информацию в один клик

Данные кибербразведки

F6

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



Тесты оценки рисков проводятся по 8 категориям проблем и могут иметь один из пяти результатов

- Критическая опасность
- Высокая опасность
- Средняя опасность
- Низкая опасность
- Тест пройден

Поддержка Центра Кибербезопасности (CDC)

F6

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

Оптимизируйте имеющиеся ресурсы

Экономьте ресурсы для круглосуточного мониторинга и реагирования с поддержкой Центра Кибербезопасности

Оставайтесь на связи с экспертами 24/7

Получайте круглосуточную поддержку в случае инцидента, а также ручную обработку и анализ выявленных уязвимостей от специалистов Центра Кибербезопасности

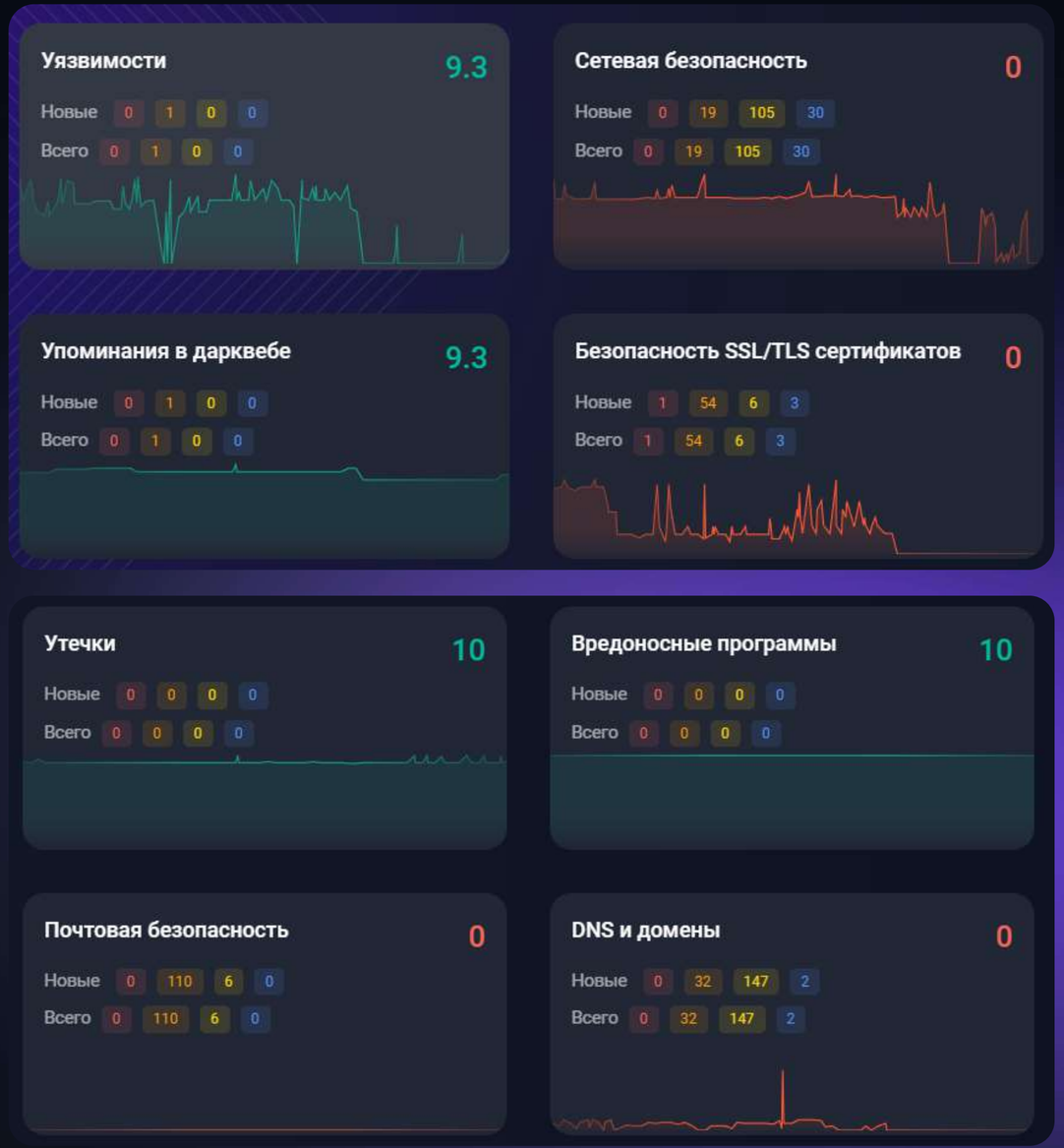
Ускоряйте обнаружение и реагирование

Увеличьте эффективность существующей ИБ-команды, используя опыт и знания экспертов F6

Полная видимость активов

F6

Уязвимости	ПО без патчей, CVE, некорректная конфигурация на уровне служб, приложений, ПО
Сетевая безопасность	Открытые порты, службы и веб-приложения
Утечки учетных данных	Утечки учетных данных, связанные с выявленными цифровыми активами
Защищенность от ВПО	Взаимодействия между вредоносной активностью и выявленными цифровыми активами
Упоминания в дарквебе	Обнаруженные на андеграундных форумах разговоры хакеров о ваших цифровых активах
Безопасность SSL/TLS	Классификация самоподписанных сертификатов, версий SSL/TLS и стойких алгоритмов шифрования
Безопасность электронной почты	Выявление некорректно настроенных SPF и DMARC
DNS и домены	Проверка работоспособности и настроек DNS



F6

Закажите бесплатный пилот прямо сейчас

Технологии для борьбы с киберугрозами

f6.ru
info@f6.ru

f6.ru/blog
+7 (495) 984-33-64