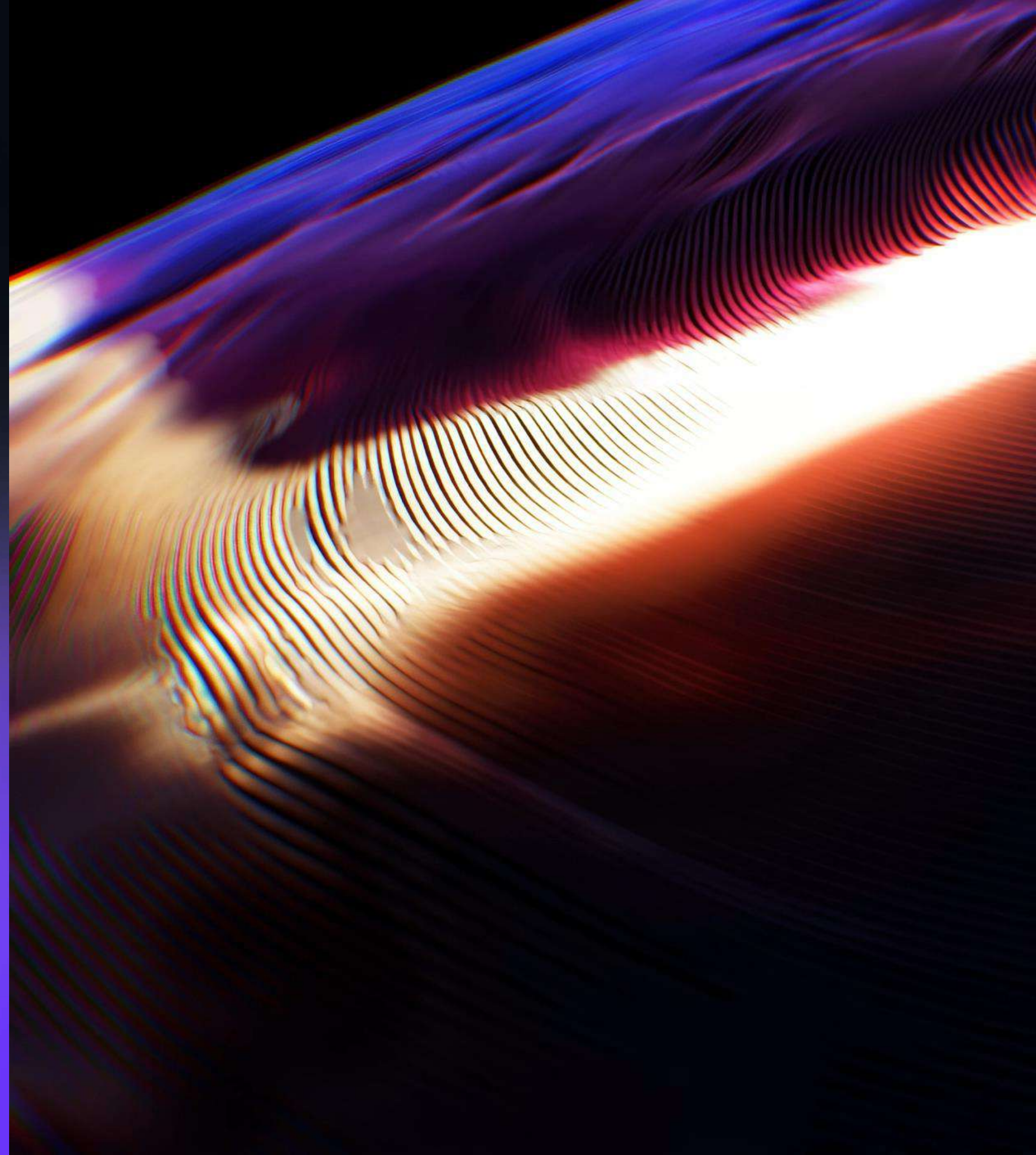


F6

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+

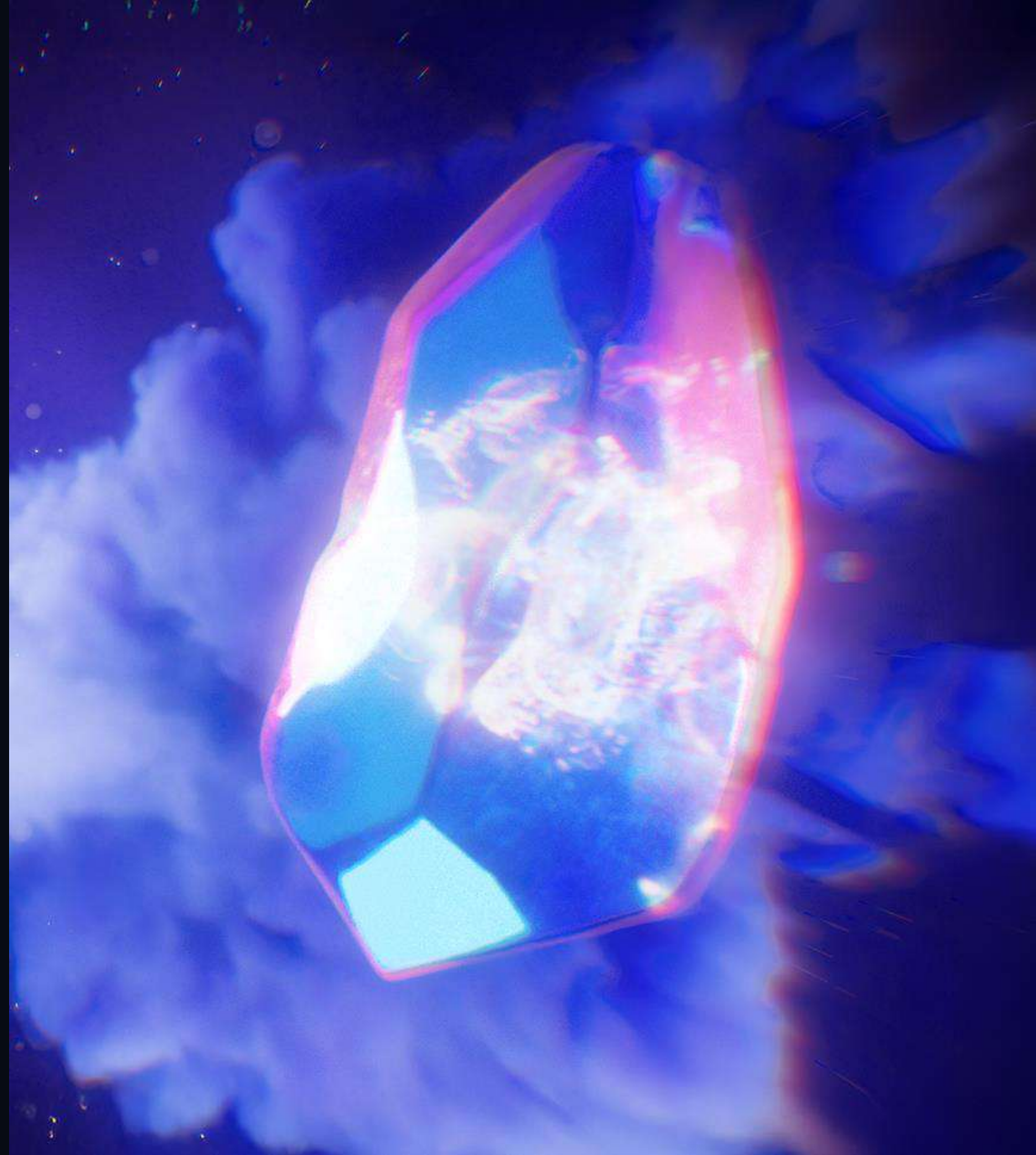
патентов и заявок

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

Разработка собственных продуктов по кибербезопасности

2003-2011

2013-2025

Attack Surface Management от F6

F6

Решение для управления
поверхностью атаки
и отслеживания цифровых
активов компании



АКТИВЫ

Новые **44** Подтверждённые **5** Лишние или

Компания

Sample Company

Домен

sampledomain.org ⓘ

Надёжность

100%

Компания

Sample Company #2

Домен

sampledomain2.org ⓘ

Надёжность

97%

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 теньную 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

Уязвимости



Оценка:

7.5

Найдено:

↑ Высокая опасность 8

↑ Средняя опасность 27



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

F6

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



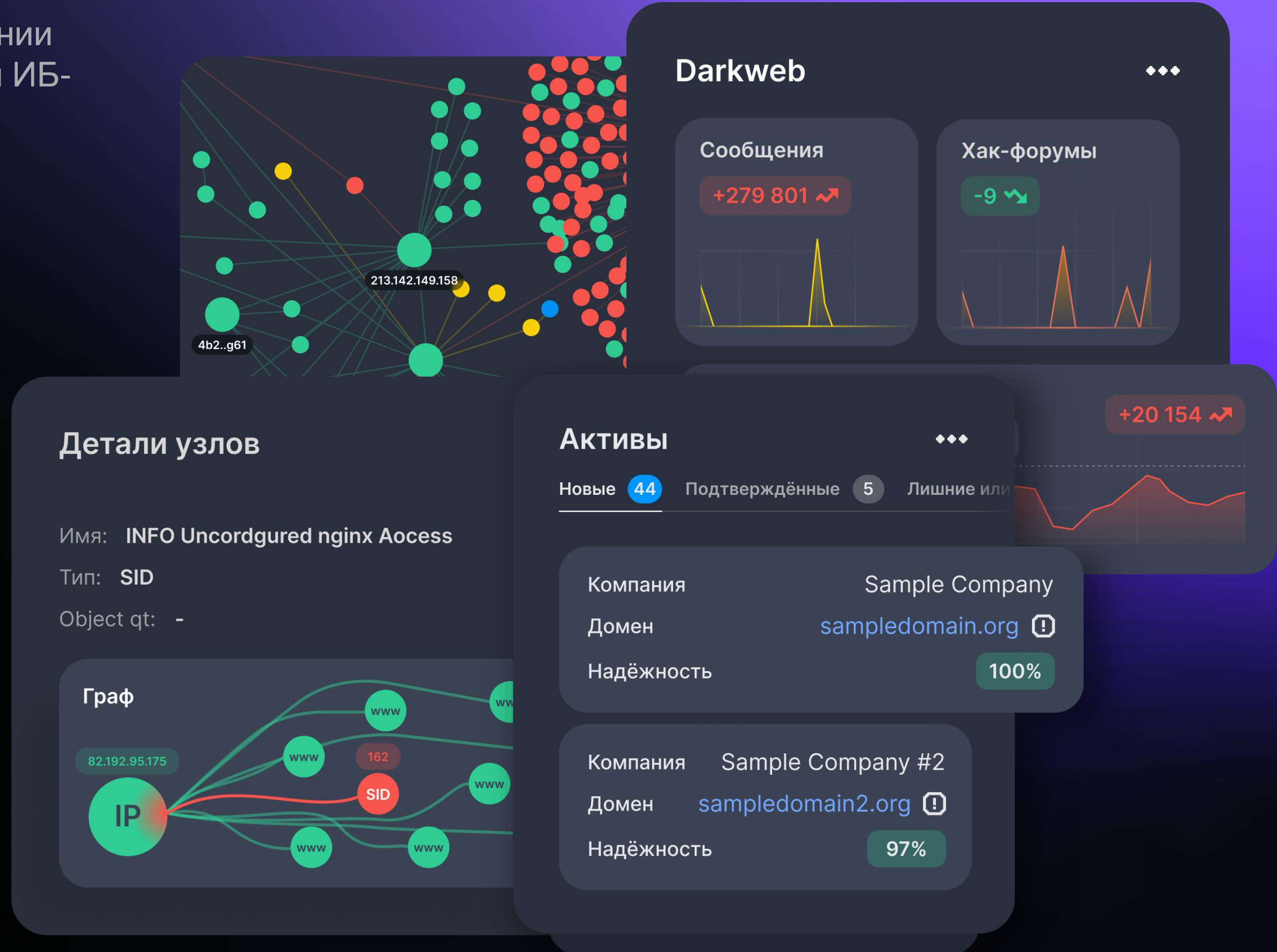
Учетные данные пользователей

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



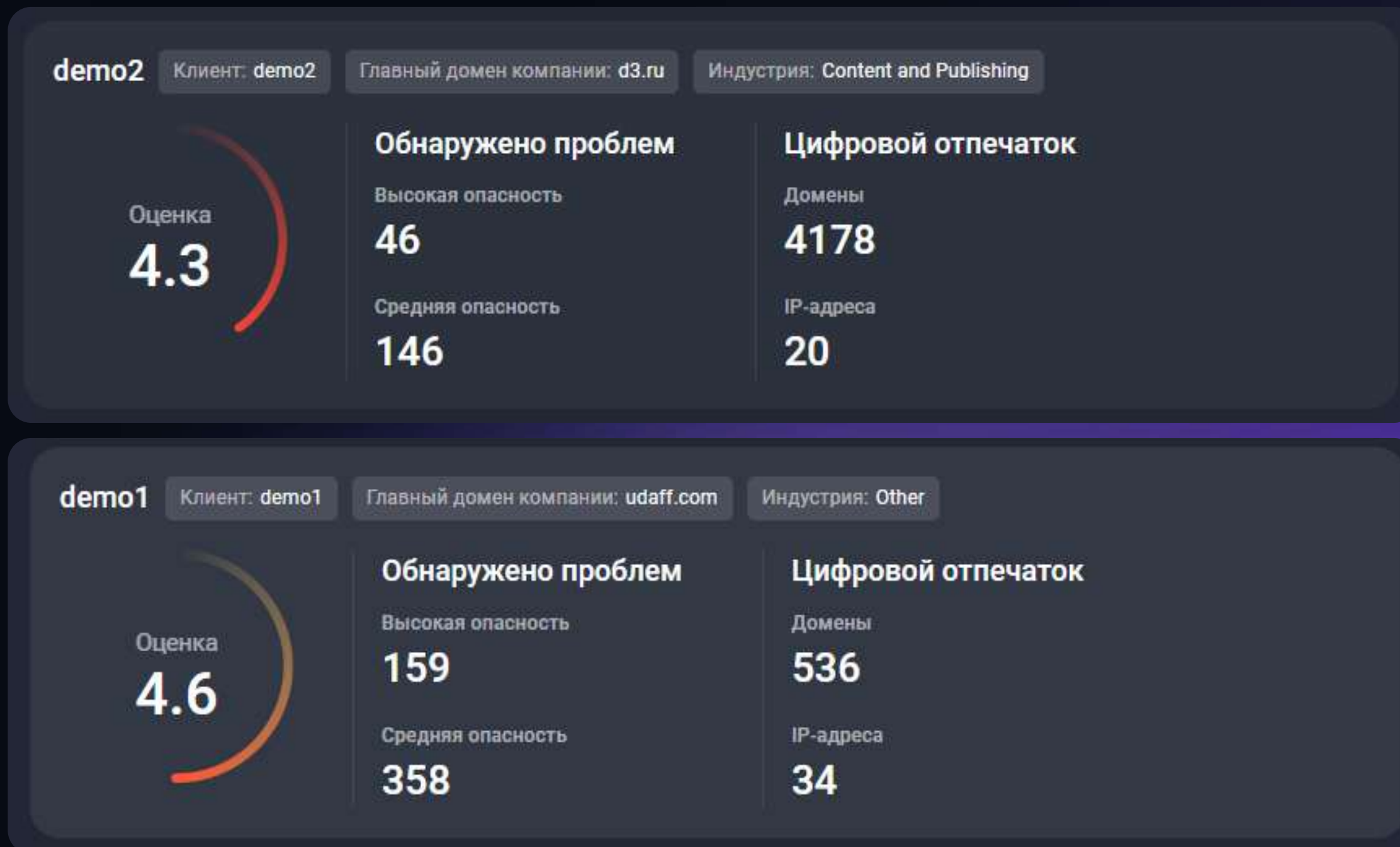
Непрерывный мониторинг

F6

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

Система использует комплексный подход к обнаружению уязвимостей

- Пространство IPv4, IPv6
- DNS-сервера, домены
- Информация из SSL-сертификатов
- Сетевые порты 1 – 65536
- Конфигурация ПО
- >Login-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

Активы										
Домены 734 SSL 256 IP-адреса 366 IP-подсети Программное обеспечение 1075 Логин формы 4										
Новые 733 Лишние или игнорируемые Подтвержденные 1 Все 734										
Поиск										
Основной домен Тип домена Регистратор Теги Начало - Конец Обнаружение Нал										
	Дата обнаружен ия ↓	Последнее сканировани е	Last resolved	Домен	Дата рег.	Дата ок.	Регистратор	Почта	Компа	
☐	08 авг. 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	16 февр. 2024	16 февр. 2025	reliable software, ltd	—	АО	
☐	08 авг. 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	16 февр. 2024	16 февр. 2025	reliable software, ltd	—	АО	
☐	08 авг. 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	16 февр. 2024	16 февр. 2025	reliable software, ltd	—	АО	
☐	05 авг. 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	16 февр. 2024	16 февр. 2025	reliable software, ltd	—	АО	
☐	05 авг. 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	16 февр. 2024	16 февр. 2025	reliable software, ltd	—	АО	
☐	05 авг. 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	16 февр. 2024	16 февр. 2025	reliable software, ltd	—	АО	
☐	04 авг. 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	20 сент. 2017	20 сент. 2024	reliable software, ltd	—	АО	
☐	25 июля 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	20 сент. 2017	20 сент. 2024	reliable software, ltd	—	АО	
☐	09 июля 2024	09 авг. 2024	08 авг. 2024	reliable-secure.ru ⓘ	28 сент. 2023	28 сент. 2024	reliable software, ltd	—	АО	

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

Проблемы

Обнаруженные1003В работеРешенные1098ИгнорируемыеЛожно-положительные

Поиск

Категория

Название теста

Степень опасности

Активное сканирование

Теги

10.07.2024 - 09.08.2024

Средняя опасностьОценка: 41Первое появление 01 нояб. 2023Последнее появление 09 авг. 2024Всего дней 281All a1.by

Обнаруженные

Сетевая безопасность

Результат тестаThere is missing header: X-Content-Type-Options. The X-Content-Type-Options response HTTP header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and be followed.

Порт: 443, 80

Матрица MITRE ATT&CKNetwork Service ScanningActive ScanningGather Victim Host Information

Актив44.53.200.30Путь на графеDomain: a1.by → Domain: web-sms-gate.a1.by → SSL: 1020122F9B0775A2776C0F4D9B535A734E2784 → IP: 44.53.200.30

Высокая опасностьОценка: 51Первое появление 14 июля 2024Последнее появление 09 авг. 2024Всего дней 25All a1.by

Обнаруженные

Утечки

Результат тестаFound 976 leaked credentials for domain a1.by from phishing or malware attack!

Матрица MITRE ATT&CKValid AccountsBrute Force

Активa1.byПуть на графеDomain: a1.by

Низкая опасностьОценка: 17Первое появление 06 дек. 2023Последнее появление 09 авг. 2024Всего дней 246All a1.by

Обнаруженные

DNS и домены

Результат тестаYour DNS SOA expire value (your - `604800`) does not correspond to the recommended. RFC 1912 recommends 1209600 - 2419200 seconds(14-28 days) for `expires` value in SOA record!

Значение: smartshopsale.by

Матрица MITRE ATT&CK

Активsmartshopsale.byПуть на графеDomain: a1.by → Phone: 375294101811 → Domain: smartshopsale.by

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



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 киберразведки

F6

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

Первое появление 04 июля 2024 · Последнее появление 06 авг. 2024

Опасность

Актив

Критическая опасность

📍 95.95.95.12

Название ПО

Версия

http_server

2.4.12

CVE

CVSS

CVE-2024-38475

9.1

Результат теста

Software with vulnerable version was detected on the host. Vulnerability with CVE-2024-38475 has critical vulnerability score 9.1.

CVSS: 9.1

CVE: CVE-2024-38475

ПО: http_server

Версия: 2.4.12

Путь на графе

Domain: 10.10.10.10 → Domain: 10.10.10.10 → IP: 95.95.95.12

Первое появление 14 июня 2024 · Последнее появление 06 авг. 2024

Опасность

Актив

Критическая опасность

📍 95.95.95.12

Название ПО

Версия

Exim

4.94

CVE

CVSS

CVE-2023-51766

5.3

Результат теста

Software with vulnerable version was detected on the host. Vulnerability with CVE-2023-51766 has medium vulnerability score 5.3.

CVSS: 5.3

CVE: CVE-2023-51766

ПО: Exim

Версия: 4.94

Путь на графе

Domain: 10.10.10.10 → Phone: 812345678901 → Domain: 10.10.10.10 → IP: 95.95.95.12

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

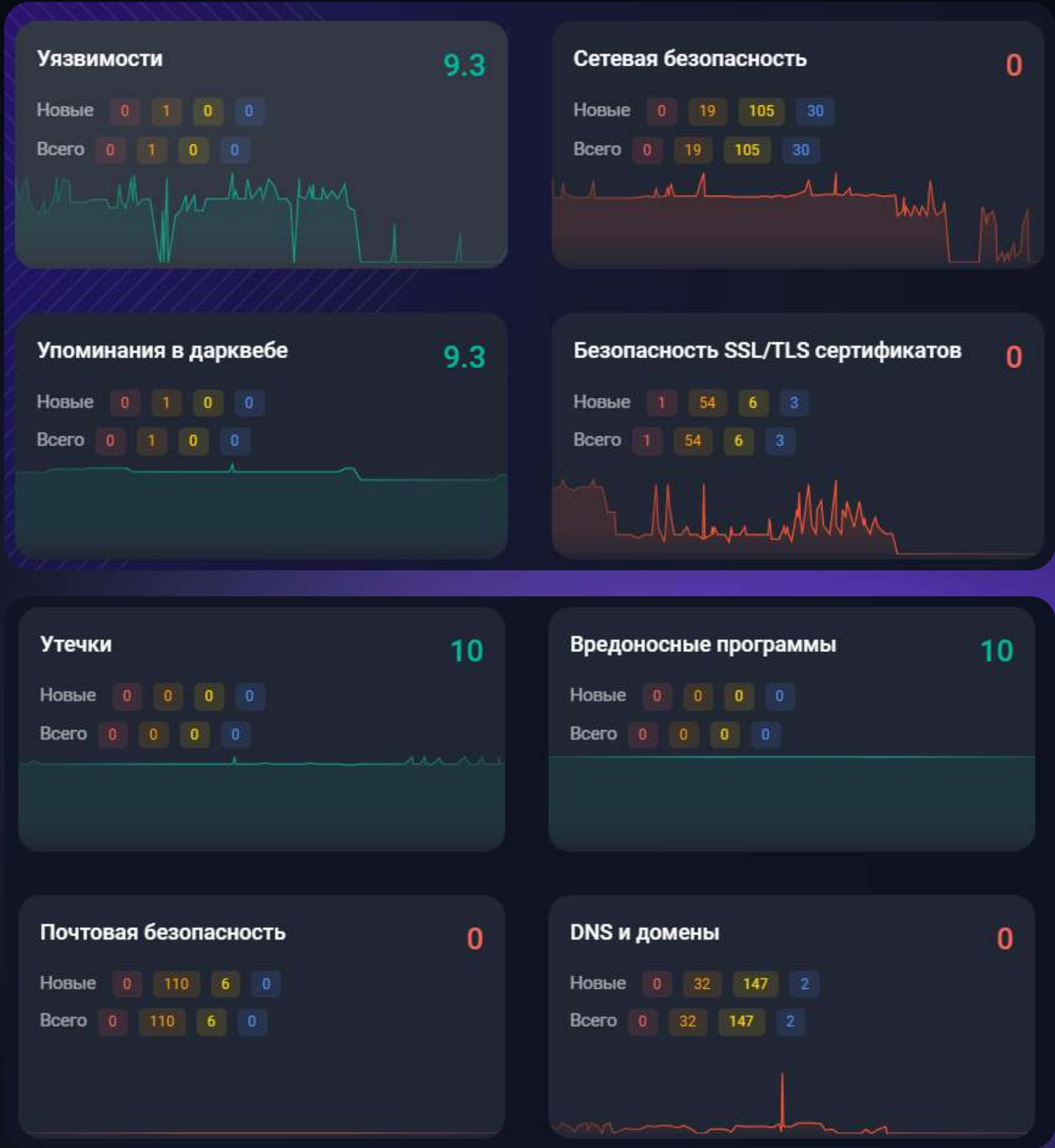
Защищенность от ВПО Взаимодействия между вредоносной активностью и выявленными цифровыми активами

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**



f6.ru
info@f6.ru

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

**Технологии для борьбы
с киберугрозами**