Attack Surface Management

F6

Контроль внешней поверхности атаки

Attack Surface Management от F6 — решение для управления поверхностью атаки и отслеживания цифровых активов компании

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 и оборудование на периметре с уязвимым программным обеспечением
- Базы данных, случайно ставшие доступными в сети
- Забытые открытые сетевые порты

Ключевые функции Attack Surface Management

Данные киберразведки

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

Обнаружение активов

Использует информацию об основном домене вашей компании для идентификации используемых и забытых активов

Непрерывный мониторинг

Осуществляет постоянный мониторинг всех изменений внешней поверхности атаки, что позволяет сформировать представление о текущем уровне защищенности

Выявление уязвимостей

Проверяет наличие уязвимостей и некорректных настроек в компании на уровне доступных из интернета операционных систем, служб, приложений, программного обеспечения и аппаратных средств

Оценка уровня защищенности компании

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 визуализирует данные вашей цифровой инфраструктуры и выявляет ранее неизвестные связи с помощью уникальных алгоритмов

Отслеживание андеграундных площадок

Обнаруживает упоминания вашей компании злоумышленники в Dark Web, Telegram, Discord и других источниках

Поддержка центра кибербезопасности F6

При подключении мониторинга Центром Кибербезопасности, опытные аналитики подскажут, какие алерты необходимо обработать в первую очередь исходя из современного ландшафта угроз

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 по сравнению с 2022

90 млн ₽

Средняя сумма выкупа за возможность дешифровки взломанной инфраструктуры злоумышленниками

Attack Surface Management дает ответы на ключевые вопросы

- Как выглядит ваша инфраструктура глазами хакера или пентестера в интернете?
- Что именно необходимо защищать и какие элементы уязвимы?
- Сколько всего цифровых активов у вашей компании?
- Какие данные вашей компании доступны в сети?
- Как выглядит периметр организации по сравнению с другими игроками отрасли?

Info@f6.ru +7 495 984-33-64 f6.ru

Выявляйте и устраняйте слабые места на внешнем периметре

Уязвимости

ПО без патчей, CVE, некорректная конфигурация, службы, приложения

Защищенность от ВПО

Взаимодействия между вредоносной активностью и выявленными цифровыми активами

Безопасность электронной почты

Выявление некорректно настроенных SPF и DMARC

Сетевая безопасность

Открытые порты, службы и веб-приложения

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

DNS и домены

Проверка работоспособности и настроек DNS

Ключевые преимущества

- Усиливает любую стратегию безопасности
- Доступна облачная и on-prem поставка
- Работает как самодостаточное решение, не требует внедрения
- Не требует остановки процессов при сканировании активов
- Возможна интеграция с внутренними системами компании
- Доступен мониторинг и поддержка Центром Кибербезовасности F6
- Осуществляет непрерывный мониторинг периметра по 8 категориям
- Предоставляются практические рекомендации по устранению угроз

Узнать более подробную информацию

Перейти на сайт →

Главные новости и тренды кибербез-опасности в нашем Telegram-канале

Info@f6.ru +7 495 984-33-64 f6.ru