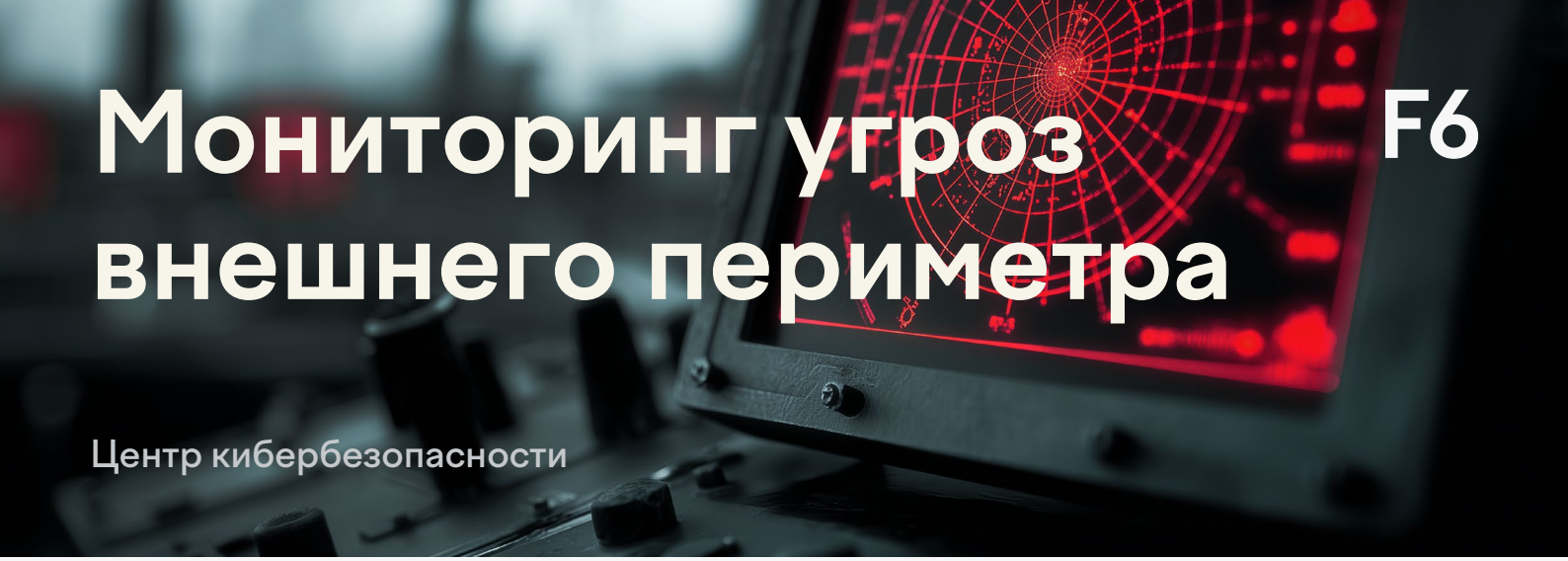


Мониторинг угроз внешнего периметра

F6

Центр кибербезопасности

Круглосуточный сервис обнаружения и предупреждения внешних угроз на базе собственного решения F6 Attack Surface Management. Входит в комплекс услуг SOC MDR от Центра кибербезопасности F6.

Как мы локализовали инцидент с компрометацией учетной записи

Что включено в сервис

1.

Выявление проблем и оценка критичности

Attack Surface Management непрерывно отслеживает и собирает доступные извне ресурсы организации, после чего автоматически формирует информацию о выявленных проблемах с присвоением уровня критичности

2.

Валидация актива с проблемой

Проверяем принадлежность актива к инфраструктуре заказчика и фильтруем нерелевантные активы

3.

Анализ выявленной проблемы на периметре

Верифицируем проблемы с использованием киберразведданных, открытых информационных источников и стороннего ПО

4.

Оценка компрометации

Проводим криминалистическое исследование уязвимого актива с целью выявления следов его компрометации

5.

Приоритизация и рекомендации

Оповещаем ответственных лиц о подтвержденных проблемах на внешнем контуре с рекомендациями, приоритизацией и консультацией по устранению проблем

В результате организация получает проактивную оборону периметра, предотвращая инциденты и сокращая риски финансовых и репутационных потерь

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

Почему важно контролировать внешний периметр

55%

всех инцидентов были реализованы через уязвимости на внешнем периметре инфраструктуры

177%

прирост количества предложений по продаже удаленного доступа к крупным корпоративным сетям

>200 млн

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

Что мы отслеживаем

Уязвимости

Устаревшие версии ПО, некорректная конфигурация, службы, приложения

Утечки учетных данных

Утечки учетных данных, связанные с выявленными цифровыми активами

Упоминания в дарквебе

Обнаруженные на андеграундных форумах обсуждения ваших цифровых активов

Сетевая безопасность

Открытые порты, службы и веб-приложения

Преимущества сервиса

Данные кибербразведки

Применяем собственное TI-решение, чтобы проактивно выявлять актуальные угрозы на внешнем периметре клиента

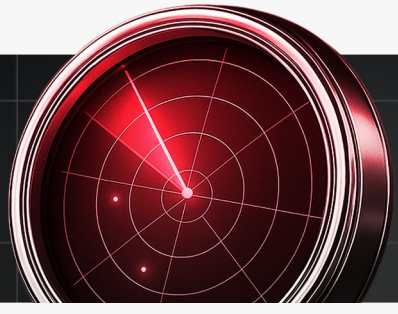
Проведение расследований

Не просто сообщаем о проблеме, а оцениваем компрометацию актива, определяя степень поражения и потенциальное влияние на бизнес

Автономная работа

Мониторинг осуществляется без вашего включения, что снижает операционную нагрузку на вашу ИБ-команду

Оставьте заявку на пилот



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