Киберзащита: как бизнесу ответить на вызовы нового времени

МегаФон

Кибербезопасность и облачные решения

Сетевая безопасность

- Защита от DDoS
- WAF
- Криптозащита
- Межсетевые экраны
- Программно-аппаратный комплекс «Информационный периметр» (ПАК ИП)

Консалтинговые услуги и антифрод

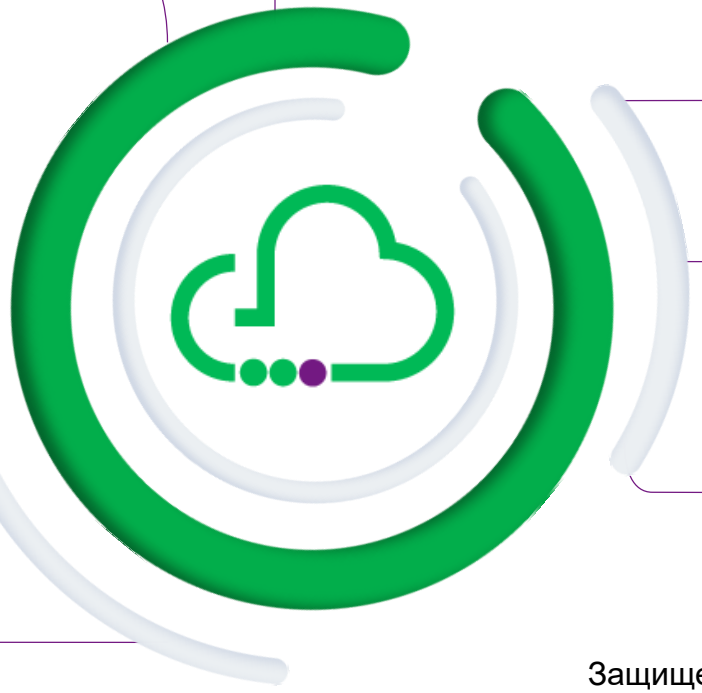
- Поиск уязвимостей Lite
- Аудит на соответствие требованиям регуляторов
- Анализ защищенности \Pentest
- Security Awareness

Защита данных

- Защита баз данных
- МегаФон DLP
- МегаФон NTA
- МегаФон MDM
- МегаФон Облако

МегаФон

МегаФон Облако



Сервисы SaaS

- Почта для бизнеса
- Хранилище документов
- Мессенджер

Платформы PaaS

- Machine Learning
- Дистанционный офис и VDI
- Kubernetes
- S3-хранилище
- DBaaS (My\MS-SQL)

Высоконагруженные системы

- High Performance IaaS (1C, SQL, SAP)
- Графические вычисления vGPU
- Доставка мультимедиа-контента CDN

Безопасность

- Anti-DDoS
- WAF
- ГОСТ-VPN
- Kaspersky Security
- 2FA

Непрерывность организации

- Резервное копирование (BaaS)
- Аварийное восстановление (DRaaS)
- Мониторинг

Professional Services

- Professional Services для ИТ-систем
- ИТ-Аудит
- Администрирование баз данных

Облако IaaS

- Защищенное Облако ФЗ-152
- Частное и гибридное облако
- Colocation ЦОД Tier III
- Собственные L2\L3-каналы

МегаФон

Ваши преимущества с МегаФон Облаком

Полная защита систем и данных

В соответствии с требованиями регуляторов РФ и международными стандартами

Современное оборудование

Наше облако работает на оборудовании последнего поколения

SLA 99,95%

Строгий SLA, который включает любые технологические и регламентные работы

Контроль инфраструктуры

Как на уровне платформы, так и на уровне ЦОДов и каналов связи

Производительность, отказоустойчивость

Выделенная поддержка 24/7

Круглосуточная экспертная поддержка, закрепленный сервис-менеджер, единое окно ответственности

Надежные площадки

Платформа в Москве, Tier III Certification of Operational Sustainability

Супербыстрые SSD-хранилища

Мы не используем устаревшие HDD

Защищенное облако ФЗ-152

Лицензии

ФСТЭК России
ФСБ России

Аттестаты

К1 и 1Г (согласно 17 приказу ФСТЭК)
УЗ-1 (в соответствии с ФЗ -152)

Сертификаты

ISO 9001, 20000, 27001
Соответствия PCI DSS

МегаФон

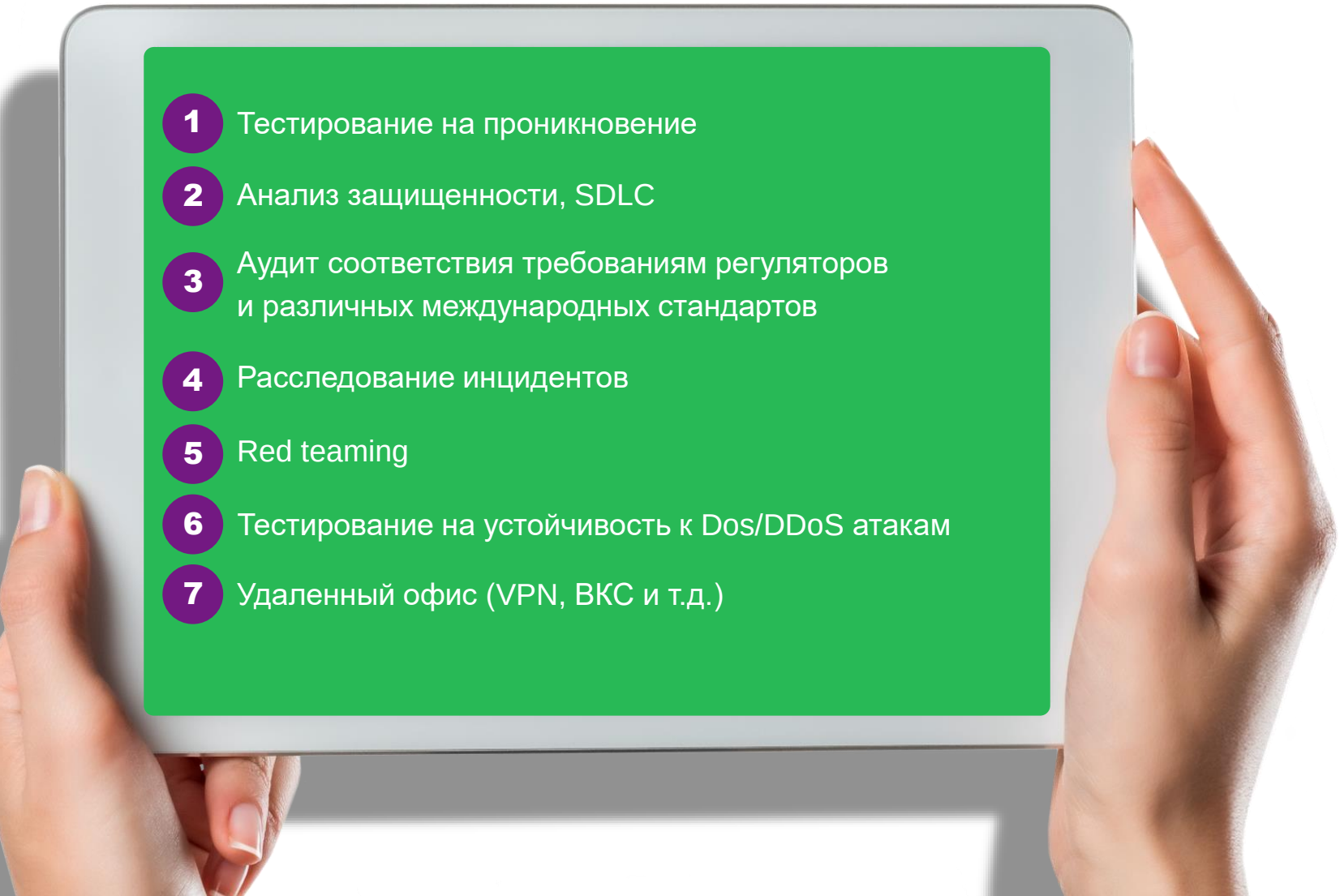
Комплекс решений по кибербезопасности

МегаФон

Security Assessment

Наши предложения

Услуги



1. Тестирование на проникновение
2. Анализ защищенности, SDLC
3. Аудит соответствия требованиям регуляторов и различных международных стандартов
4. Расследование инцидентов
5. Red teaming
6. Тестирование на устойчивость к Dos/DDoS атакам
7. Удаленный офис (VPN, ВКС и т.д.)

Объекты тестирования

- Сети Wi-Fi
- Веб-приложения
- Мобильные приложения
- ДБО
- Бизнес приложения (ERP, CRM и т.д.)
- АБС
- Алгоритмы машинного обучения
- Блокчейн проекты
- Внешний периметр
- Внутренний периметр
- Социальная инженерия

По итогам работ

1. Описание поверхности атаки исследуемого объекта глазами потенциального злоумышленника

2. Актуальная модель угроз и нарушителя

3. Влияние обнаруженных уязвимостей и недостатков в безопасности на бизнес-процессы компании, также будут перечислены наихудшие последствия атаки и предоставлены результаты их подтверждающие

4. Описание каждой обнаруженной уязвимости:

— PoC (Proof of concept) – эксплуатация обнаруженной уязвимости,
— анализ ее критичности и уровня риска,
— конкретные рекомендации по устранению уязвимости

5. Общий вывод о состоянии безопасности приложения Заказчика:

— техническая оценка рисков обнаруженных уязвимостей,
— общие рекомендации по улучшению безопасности,
— рекомендации по устранению текущих недостатков

МегаФон

Наша команда

- Участники программ Bug Bounty

Закрытые уязвимости в GitHub, Mail.ru, Ozon, Qiwi, PayPal и т.д.

- Наличие сертификатов: CEH, CHFI, CND, MCSE, EXIN, OSCP, CISSP
- Опыт реализации различных кейсов в социальной инженерии
- Опыт расследования инцидентов ИБ
- Внедрение процессов SDLC
- Отбор на должность по реальному опыту
- Оперативная команда для выезда на инциденты
- Обучение правильному внедрению SDLC

МегаФон

Security Awareness

МегаФон SA –

это платформа по повышению осведомленности сотрудников в сфере информационной безопасности с понятным запоминающимся контентом и возможностью проверить знания при помощи имитированных фишинговых атак.

МегаФон

Что мы предлагаем

Набор курсов

Платформа содержит в себе материалы и набор теоретических блоков — всё необходимое для обучения базовым понятиям и правилам работы с информационными ресурсами.

Имитация фишинга

Встроенный в систему фишинговый модуль с множеством настроек. Фишинговый модуль проверяет, как поведут себя сотрудники компании при реальной атаке, и вычисляет, кто из них наиболее уязвим к этому виду социальной инженерии.

Гибкость и контроль

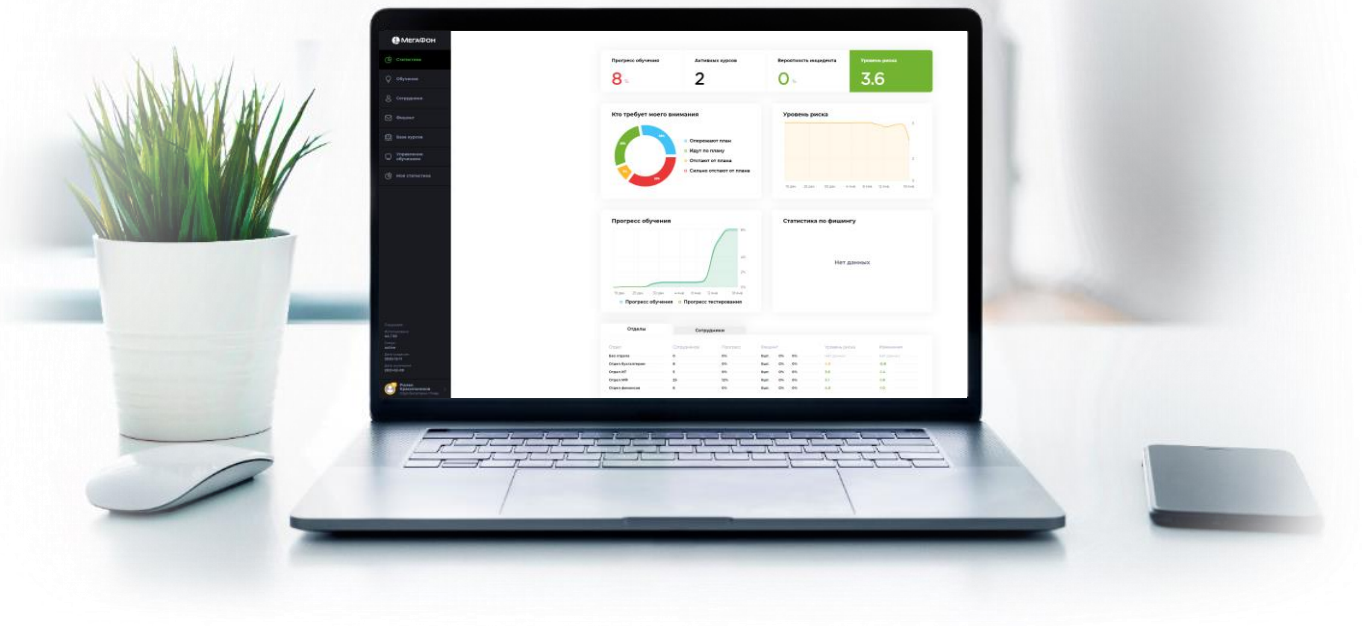
- Добавление собственных курсов
- Контроль процесса прохождения курсов
- Автоматизация процесса обучения при помощи гибкой системы

МегаФон

Обучайте сотрудников и повышайте информационную безопасность компании

Платформа в лёгкой и понятной форме повышает осведомлённость сотрудников в сфере информационной безопасности и цифровой гигиены.

При помощи имитации фишинговых рассылок у компании есть возможность проверить степень уязвимости сотрудников к действиям злоумышленника.



Теория	Практика
Обучающие курсы	Тестовые задания
Имитация фишинга	Вирусные вложения
Подробная аналитика	Выявление уязвимых сотрудников

МегаФон

WAF от МегаФона

Технические возможности

- WAF от МегаФона – лидер Magic Quadrant for Web Application Firewalls 2018*
- Защита от атак на уровне приложений (7 уровень OSI), атак из OWASP TOP-10 и атак нулевого дня
- Отсутствие задержек при обработке трафика и обнаружение ранее неизвестных атак благодаря асигнатурным методам анализа
- Возможность работы в автоматическом режиме
  Фильтрация трафика по заданным параметрам
- Устойчивость к распространенным методикам обхода механизмов защиты WAF

МегаФон

*Отчет Magic Quadrant for Web Application Firewalls 2018 доступен по адресу: https://www.gartner.com/en/documents/3888676

Преимущества обслуживания

- Полный спектр услуг у одного поставщика
- Не требуется дополнительное оборудование со стороны клиента
- Круглосуточная техническая поддержка
- Гарантированная доступность услуги (SLA 9X,X%)
- Подключение в течение нескольких часов
- Два варианта оплаты – единовременная или абонентская плата

МегаФон

Защита от DDoS-атак

Что такое DDoS-атака?

DDoS от англ. Distributed Denial of Services – распределенный отказ в обслуживании

Это сетевая атака, заключающаяся в большом количестве одновременных запросов на сервера компании с целью доведения системы до отказа.

Успешная атака **парализует работу сайта.**

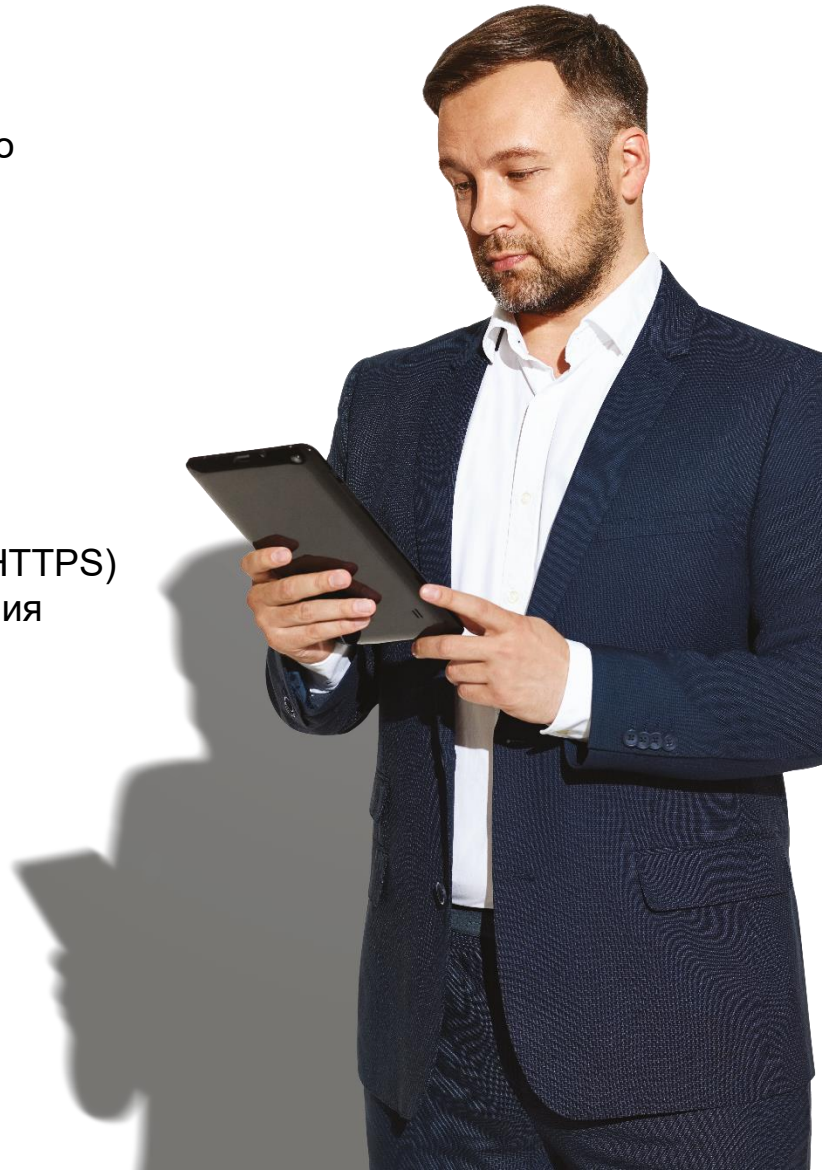
Пользователи не могут получить к нему доступ,
либо он сильно затруднен. Это может привести
к серьёзным финансовым и репутационным потерям, вымогательству
и краже информации.

FireWall в случае DDOS-атаки не средство защиты, а мишень для атакующего

МегаФон

Технические преимущества

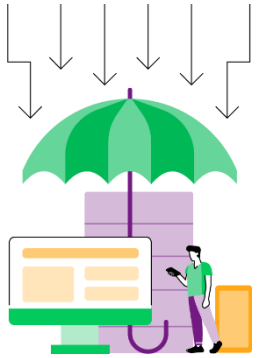
- Не замедляет работу ресурса
- Отражение DDoS-атак мощностью до 300 Гбит/с на 3-7 уровнях модели OSI, включая атаки slow HTTP*
- Автоматическое отслеживание и очистка трафика. Время включения фильтрации 5-15 секунд благодаря технологии Fast Flood Detection
- Три варианта технического обслуживания
- Ежедневное обновление базы угроз
- Возможность фильтрации шифрованного трафика (HTTPS) при установке оборудования в разрыв канала



МегаФон

*Возможно при наличии клиентского устройства

От чего защитит наше решение



Flood Attacks

Атаки, переполняющие каналы связи за счет отправки большого числа запросов, не приводящих к установке соединения и создающих очередь «полуоткрытых соединений». Сервер перестает отвечать, а создание новых подключений невозможно

Amplification Attacks

Атаки с использованием эффекта усиления (амплификатора) для увеличения мощности. Сравнительно небольшие ресурсы злоумышленника становятся причиной значительно большего ущерба или полного отказа работы системы-жертвы

Volumetric Attacks

Атаки, перегружающие каналы или оборудование для препятствования работе сервиса. Уровни OSI 3-4

«Медленные» атаки

Отправка большого числа запросов, передающихся с очень медленной скоростью, из-за чего ресурсы сервера используются гораздо дольше, препятствуя обработке запросов других пользователей

Application Layer Attacks

Атаки на приложения (веб-серверы, серверы баз данных, VoIP-телефонию и т. д.). Уровень OSI 7

МегаФон

Контакты

Валеев Марат
Эксперт по внедрению цифровых решений

+7 911 110 17 03
Marat.valeev@megafon.ru

8 800 550 05 55
b2b.megafon.ru

МегаФон