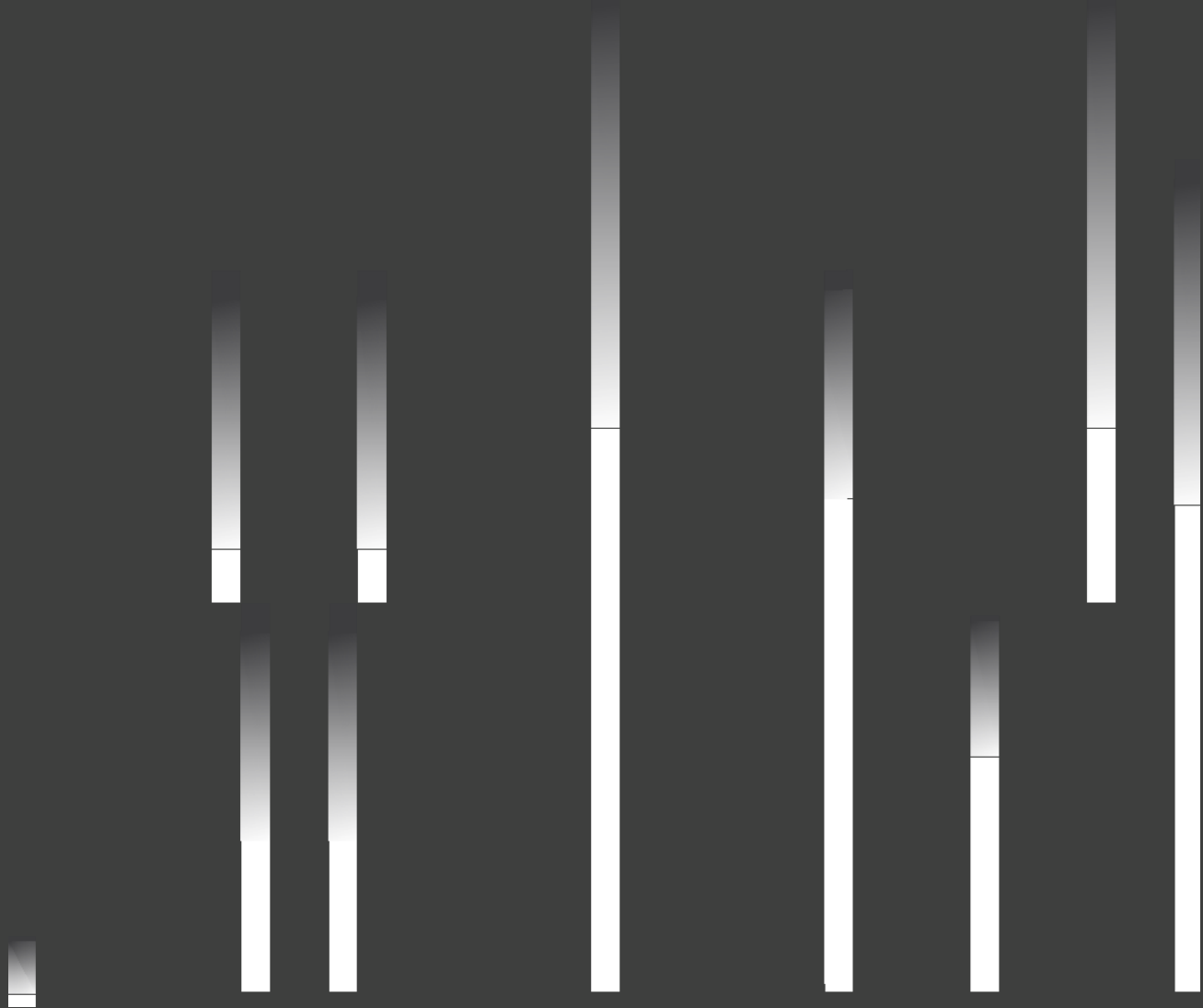


#CloudMTS

Современные сервисы кибербезопасности от #CloudMTS

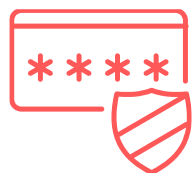


Андрей Пастухов
Менеджер presale #CloudMTS



#CloudMTS

Портфель услуг ИБ #CloudMTS



**Защищенный
сегмент IaaS 152-ФЗ**



**Антивирусная
защита VM**



Security Operation Center



**Защита
от DDoS-атак (Qrator Labs)**



**Защита веб-приложений
и сайтов (WAF Premium)**

#CloudMTS

IaaS Ф3-152

01

#CloudMTS

Основной вопрос клиента — владельца **ИСПДн**

Можно ли в России пользоваться «**облачными технологиями**»
при обработке персональных данных?

«ДА!»

Что делать если строить защиту ПДн “с нуля”: шаги и план действий

Аудит существующей ИС.

При разработке “с нуля” начинаем с разработки модели угроз

Модель угроз и нарушителя

Технический проект системы защиты включает в себя список средств защиты в соответствии с уровнем защищенности используемых ПДн и актуальным для данной системы типом угроз

Размещение или миграция в Защищенный сегмент облака #CloudMTS + реализация технического проекта

Разработка пакета документов

(модель угроз, технический проект, организационная документация, письмо в Роскомнадзор)

Аттестация или оценка соответствия ИС (проверка соответствия системы модели угроз и техническому проекту)

Подача документов в Роскомнадзор

Реализация ИСПДн: плюсы облачного решения



Реализация на собственной Инфраструктуре

Высокие единовременные затраты и стоимость владения

Уникальность каждой системы защиты ПДн

Долгий срок реализации (проект, поставка, внедрение)

Необходимость мониторинга и изучения законодательства

Необходимость разработки документации на ИСПДн

Необходимость иметь в штате высококвалифицированных специалистов



Реализация на облачной Инфраструктуре

Низкие единовременные затраты и стоимость владения

Отработанное типовое решение в облачной инфраструктуре

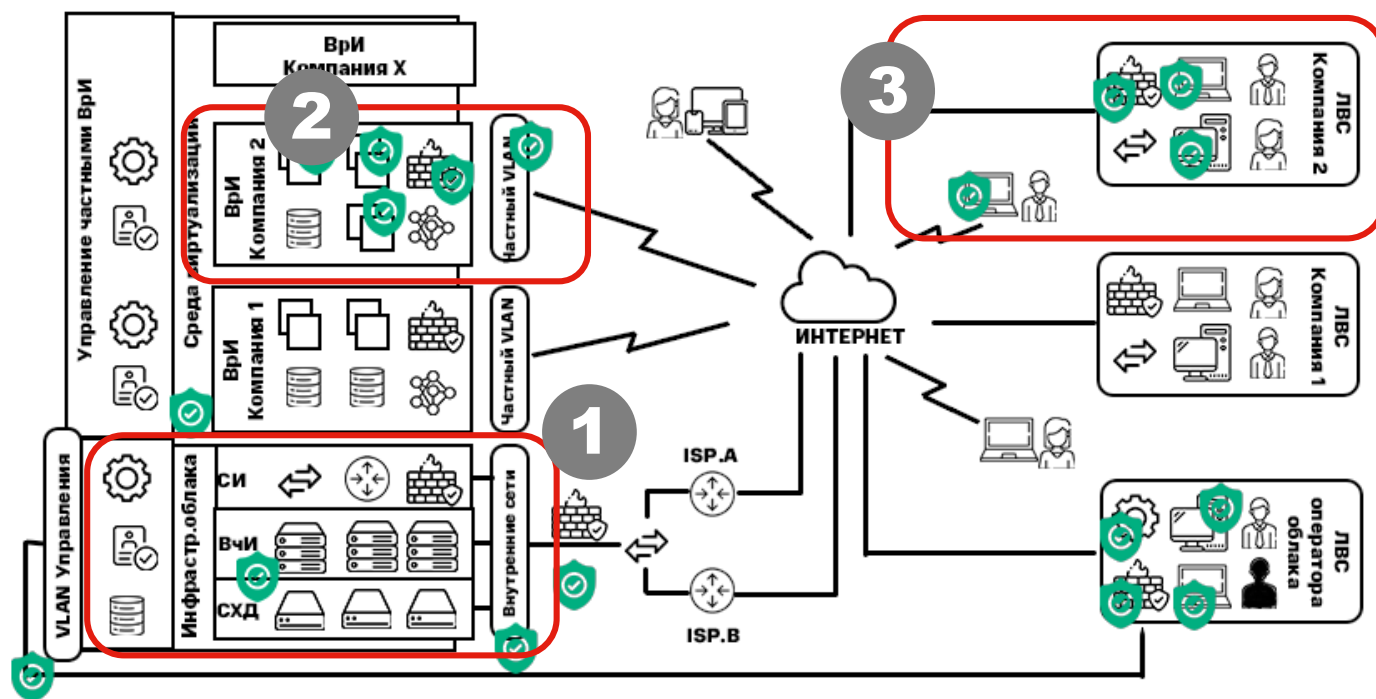
Оперативное развертывание (от 1 дня)

Мониторинг и обеспечение соответствия законодательству — зона ответственности исполнителя

Все необходимые шаблоны документов предоставляет исполнитель

Сертифицированные специалисты исполнителя

Архитектура защищенного сегмента #CloudMTS и сервисов ИБ



1. СЗИ на уровне Инфраструктуры Облака и средств управления Облаком
2. СЗИ на уровне ИС Заказчика в Виртуальной инфраструктуре
3. СЗИ на площадке/на стороне Заказчика



В нашей инфраструктуре:

- + Аттестат УЗ-1, К-1
- + Подключена к SOC
- + СОВ\ЗВИ\АНЗ и т.д.
- + Васкуп инфраструктуры

Платные опции для ИС клиента:

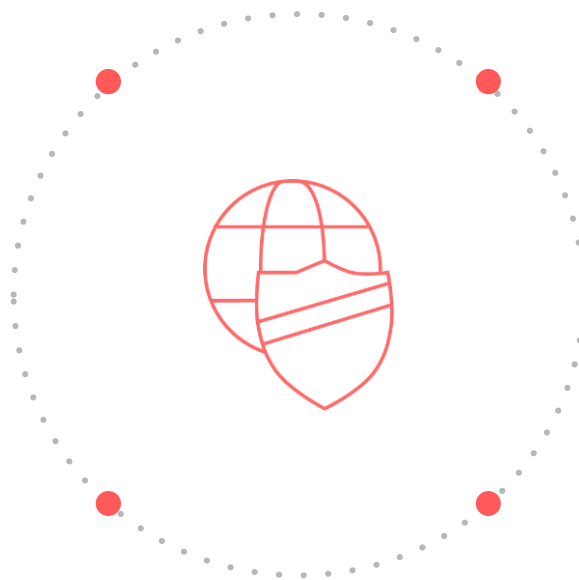
- + SOC
- + WAF
- + AntiDDoS
- + Антивирус
- + BaaS



Что **получает клиент** в защищенном сегменте #CloudMTS

Гарантию выполнения требований 21 и 17 Приказов ФСТЭК России на уровне средств связи и инфраструктуры — аттестат на облако (на продукты IaaS)

Набор типовой документации, частную модель угроз для ИСПДн в облаке



СЗИ и СКЗИ для реализации ИСПДн на уровне виртуальных машин и локальной вычислительной сети по схеме аренды

Поддержку в случае проведения проверок РКН, ФСТЭК

Обновление сегмента IAAS-ФЗ-152

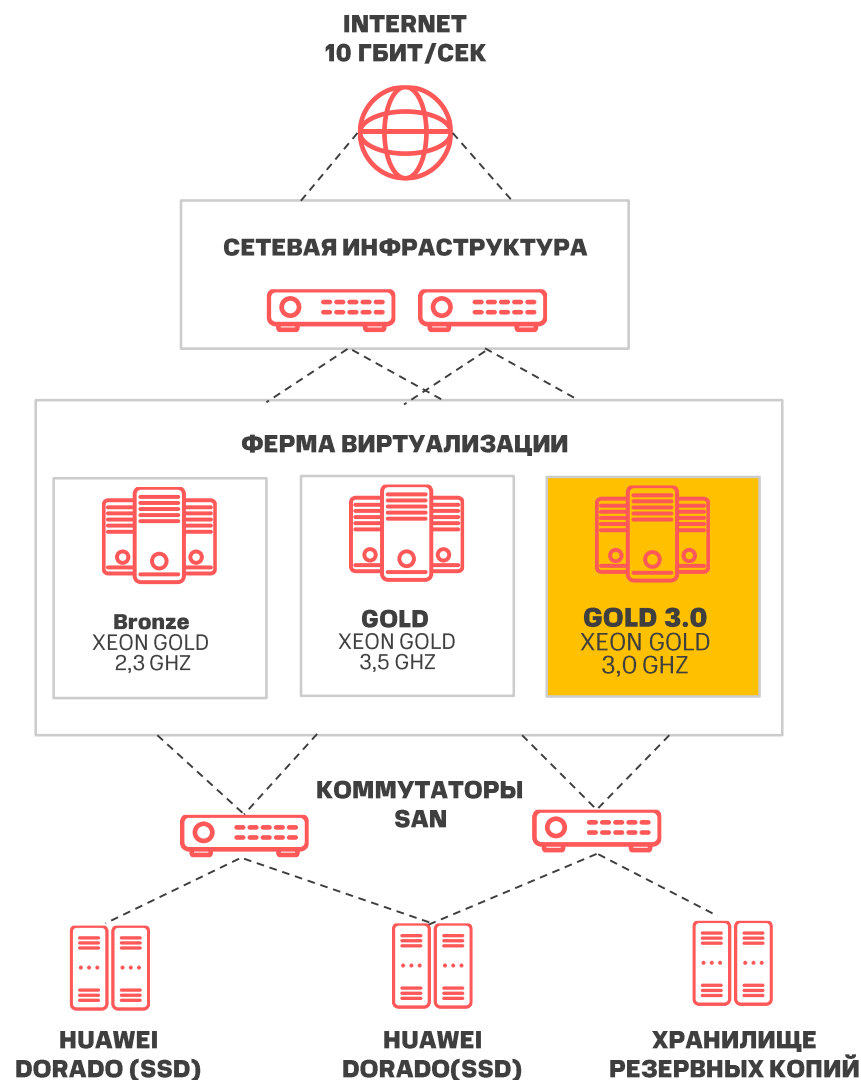
В сегменте могут размещаться ИС, требовательные к вычислительным ресурсам.

Узлы вычислений

- ✓ 2 x Xeon Gold 6248R 3,0 Ghz / 1536 GB RAM

Система хранения данных - Huawei Dorado:

- ✓ SSD Basic - производительность 0,4 IOPS на 1 ГБ
- ✓ SSD Fast - производительность 2 IOPS на 1 ГБ
- ✓ SSD Ultra – производительность 10 IOPS на 1 ГБ
- ✓ SSD Ultra+ - производительность 30 IOPS на 1 ГБ

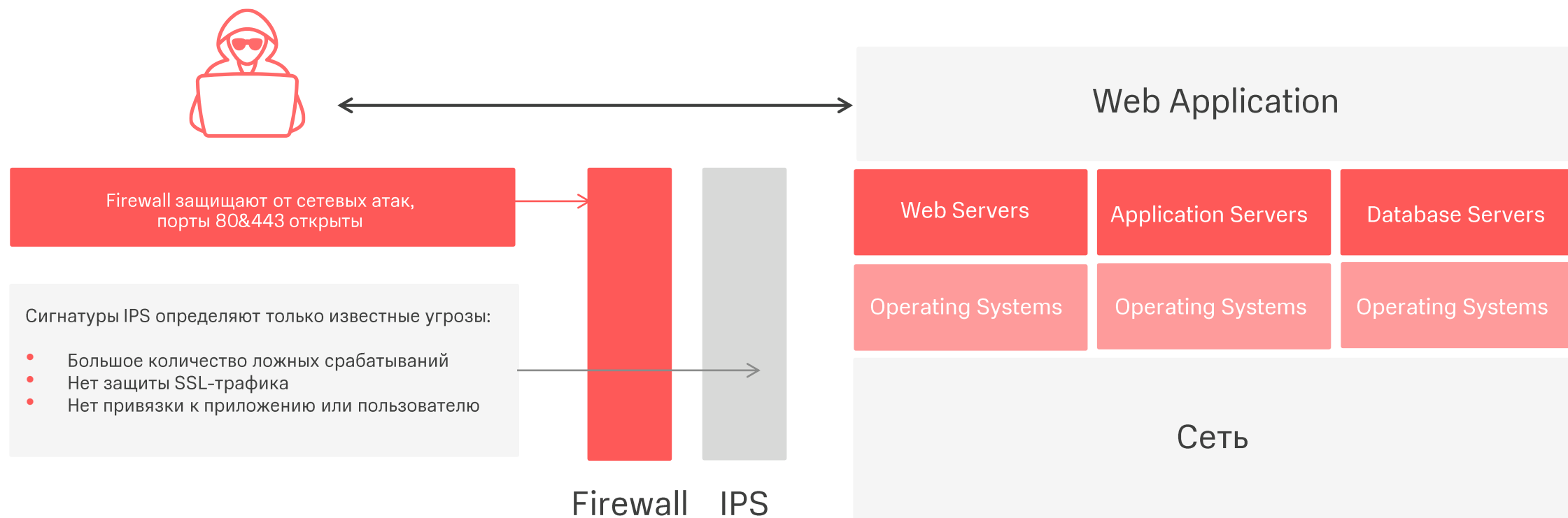


#CloudMTS

WAF Premium

02

Фокус более **75% атак** направлен на веб-приложения



Что **интересно** злоумышленникам?

Кража персональных данных и другой конфиденциальной информации

Хищение денежных средств пользователей

Атаки на пользователей сайта путём заражения страниц сайта вирусами и размещения ссылок, содержащих инструменты взлома

Понижение позиций ресурса в поисковых системах

и нарушение рекламной политики путём манипуляций с кодом сайта

Нарушение работоспособности веб-приложений, включая удаление или искажение файлов, баз данных и т.п.

Подмена содержания страниц (размещение противозаконного или ложного контента, в том числе, поддельных новостей, неправильных цен на товары, ложной контактной информации, адресов электронной почты и т.д.)

Выполнение мошеннических действий от лица пользователей

Ботнет активности (рекламный бюджет уходит на нецелевые клики, сбиваются аналитические метрики по продажам)

Проникновение в инфраструктуру, используя взломанное веб-приложение как плацдарм для развития дальнейшей атаки

Кому нужна защита с помощью **WAF Premium**

Все вертикали бизнеса, использующие интернет в качестве среды взаимодействия с пользователями и заказчиками (сайт, веб-приложения чаты и т.д.)

Бизнес-процессы построены (оптимизированы) благодаря веб-приложениям/сайтам



Банки, страховые и финансовые организации



Госсектор, бюджетные организации (фед. и рег.)



ТЭК, предприятия



Транспорт



Все бизнесы интернет-индустрии, интернет магазины и различные сайты (игровые, развлекательные, новостные и т.д.)



Причина появления **WAF Premium**

Предпосылки:

Обычно сервис-провайдерами предоставляется инструмент фильтрации

В зону ответственности не входит эксплуатация решения, мониторинг и реагирование на атаки, внесение правил блокировки

Что мы предлагаем в комплексной услуге WAF Premium:

1. Конфигурирование

Управление конфигурацией защищаемых веб-приложений.

Тонкая настройка прохождения трафика через узлы фильтрации с учетом специфики защищаемых веб-приложений

2. Эксплуатация

Выявление ложных срабатываний механизмов фильтрации и корректировка профиля защиты.

Актуализация профиля защиты с учетом специфики трафика.

Масштабирование компонентов по мере роста нагрузки на веб-приложение.

3. Мониторинг и реагирование на инциденты

Мониторинг и реагирование на инциденты в режиме 24/7.

Предоставление отчетов по зафиксированным инцидентам и обращениям в техническую службу по запросу заказчика.



Функциональные возможности услуги

Нейтрализация рисков из списка OWASP TOP 10

WAF Premium задействует разнообразные механизмы защиты — от сигнатурного и динамического анализа трафика до настраиваемых правил безопасности

Предотвращение ботнет-активности

WAF Premium определяет и блокирует подозрительную активность по цифровому отпечатку браузера — набору таких признаков как часовой пояс, в котором находится пользователь, а также язык, список расширений и версия браузера

Выявление уязвимостей и предотвращение их эксплуатации

WAF Premium выявляет уязвимости с помощью пассивного сканера, а механизм виртуального патчинга позволяет оперативно предотвращать эксплуатацию найденных ошибок, не дожидаясь следующего релиза веб-приложения

Поведенческий анализ

WAF Premium защищает от атак методом перебора (brute-force) и сканирования каталогов (dirbusting) по именам файлов на серверах веб-приложений. Эту задачу выполняют технологии поведенческого анализа, которые обнаруживают аномальное поведение, и алгоритмы ограничения частоты запросов (rate limiting)

Выявление попыток использования скомпрометированных учетных записей

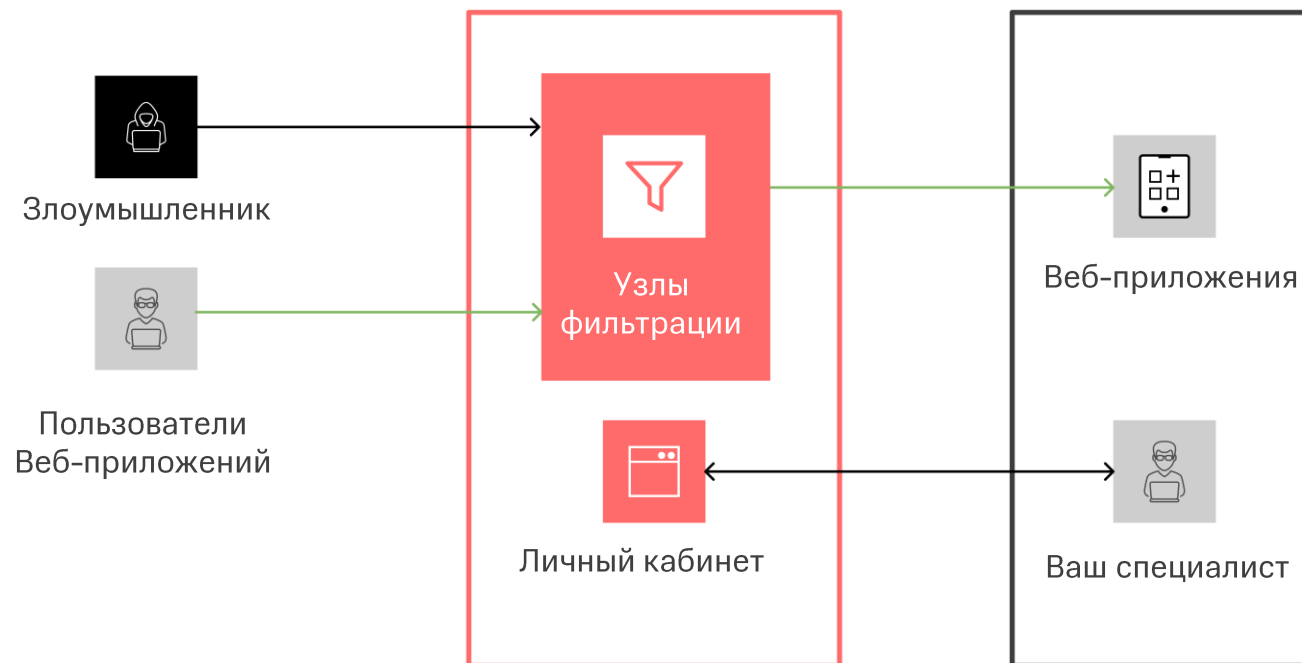
WAF Premium предотвращает атаки типа credential stuffing, используя собственные базы данных и настраиваемые правила корреляции

Формирование индивидуального профиля

На основе собранных WAF метрик формируется индивидуальный профиль защищаемых ресурсов, с последующим применением тонко настроенных правил безопасности

Принципы работы услуги

- Трафик пользователей, поступающий заказчику из интернета и направленный на защищаемое веб-приложение, проходит через узлы фильтрации WAF Premium
- Входящие запросы проверяются в соответствии с настроенной политикой защиты. Если они содержат в себе следы веб-атаки (вредоносной активности), трафик помечается как зловредный и блокируется, прежде чем достичь веб-приложения



#CloudMTS

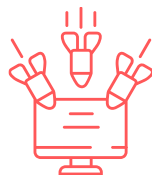
Защита от DDoS

03

Что такое распределенная сетевая атака (DDoS)?

DDoS-атака (от англ. Distributed denial of service) — атака на ресурс клиента (доступный из публичной сети Интернет), выполняемая одновременно с большого числа зараженных и контролируемых хакерами элементов (ботнет-сети) с целью отказа или деградации работы ресурса, при котором легальные пользователи не могут воспользоваться ресурсом.

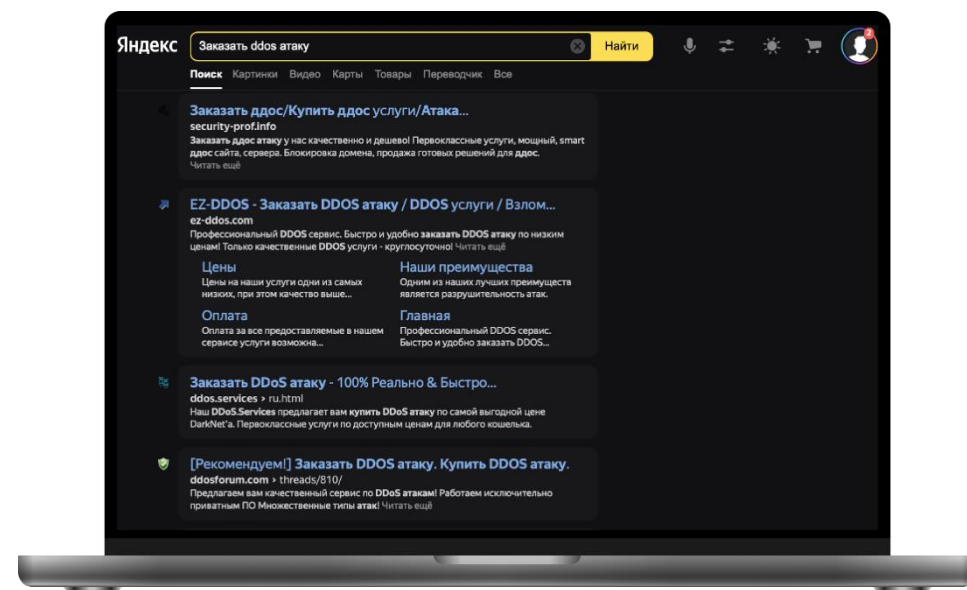
Потери клиента от недоступности ресурсов (онлайн-заказы, процессинг, интернет-магазин, веб-сайт и т. д.) за несколько минут/часов могут быть несоизмеримо выше стоимости защиты от нее.



Кто применяет?

- конкуренты;
- недовольные клиенты;
- мошенники, требующие деньги за прекращение атаки;
- хакерские группировки по политическим и другим мотивам (введение санкций, ограничений).

Тысячи сайтов предлагают организовать DDoS-атаку **от 50\$**



Портрет клиента

Общий портрет потенциальных пользователей услуги — это компании любой сферы деятельности, чей бизнес прямо или косвенно зависит от доступности ресурсов данных компаний (веб-сайт, личный кабинет, CRM, системы приема/обработки заказов).

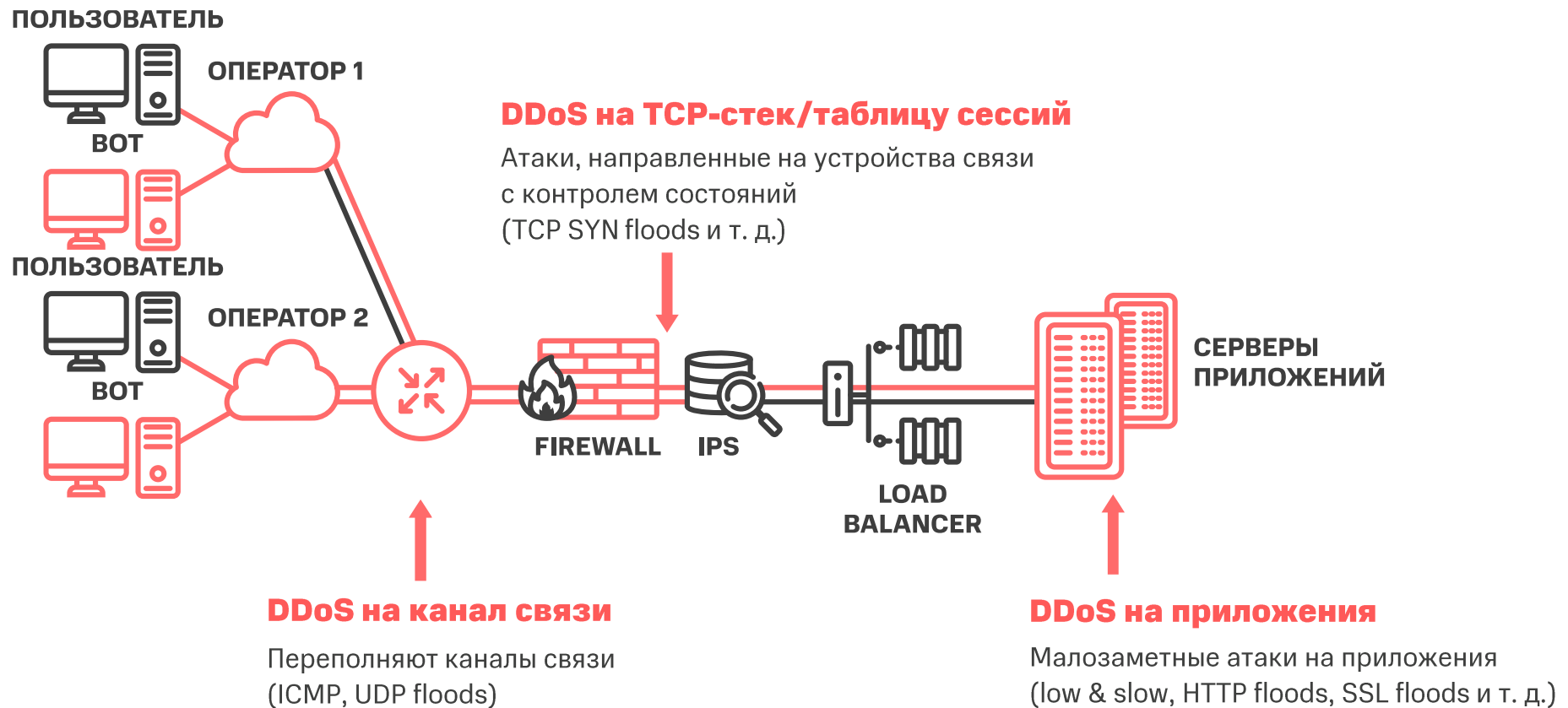
Клиенты, у которых основной источник дохода — это онлайн-канал продаж или обслуживания.

Основные сегменты:

- Банки и финансовые организации;
- Страховые компании;
- Клиенты дата-центра с публичными сервисами и службами;
- Интернет-магазины, системы приема заказов и платежей, хостинговые клиенты и торгово-сервисные компании, развивающие онлайн-каналы продаж (рестораны, кафе, пиццерии, службы доставки и такси);
- Малый, средний бизнес, для которого каждый клиент — большая ценность.



К чему приводит отсутствие защиты от DDoS-атак



К чему приводит отсутствие защиты от DDoS-атак

- **Услуга #CloudMTS «Защита от распределенных сетевых атак на базе Qrator Labs»** — это защита приложений от любых хакерских DDoS-атак вне зависимости от сложности по всему миру на базе партнерской платформы.
- Подходит для мобильных приложений и API и не использует технологии вроде CAPTCHA.
- При подключении услуги трафик, поступающий к защищаемым ресурсам, проходит постоянный поведенческий анализ на предмет возникновения в нем не свойственных для данного ресурса запросов.

Комплексное решение #CloudMTS «Защита от распределенных сетевых атак на базе Qrator Labs» включает в себя:



Всегда включенная защита в автоматическом режиме 24/7 с пропускной способностью сети - свыше 3 ТБ/с



Обучение и адаптивное построение модели распределения трафика для штатных условий работы защищаемых сетей и онлайн-сервисов



Выявление DDoS-атак на основе отклонений и аномалий



Блокирование нелегитимного трафика методом динамической фильтрации сетевых пакетов с автоматической генерацией сигнатур DDoS-атаки



Личный кабинет предлагает широкий спектр отчетов по сетевому трафику, что позволяет легко контролировать производительность сети клиента

Преимущества услуги от #CloudMTS

01

Отсутствие капитальных затрат на приобретение и установку дополнительного оборудования на стороне клиента

02

Успешный и регулярный опыт отражения атак большого объема и интенсивности

03

Отказоустойчивая инфраструктура и более 15 Центров очистки

04

Несколько этапов обучения, что позволяет снизить уровень ложных срабатываний системы

05

Устранение DDoS-атак на всех уровнях ISO OSI, включая L7

06

Возможностью фильтрации HTTPS трафика без раскрытия ключей шифрования

07

Круглосуточная техническая поддержка. Создание заявки и получение квалифицированной помощи 24/7

08

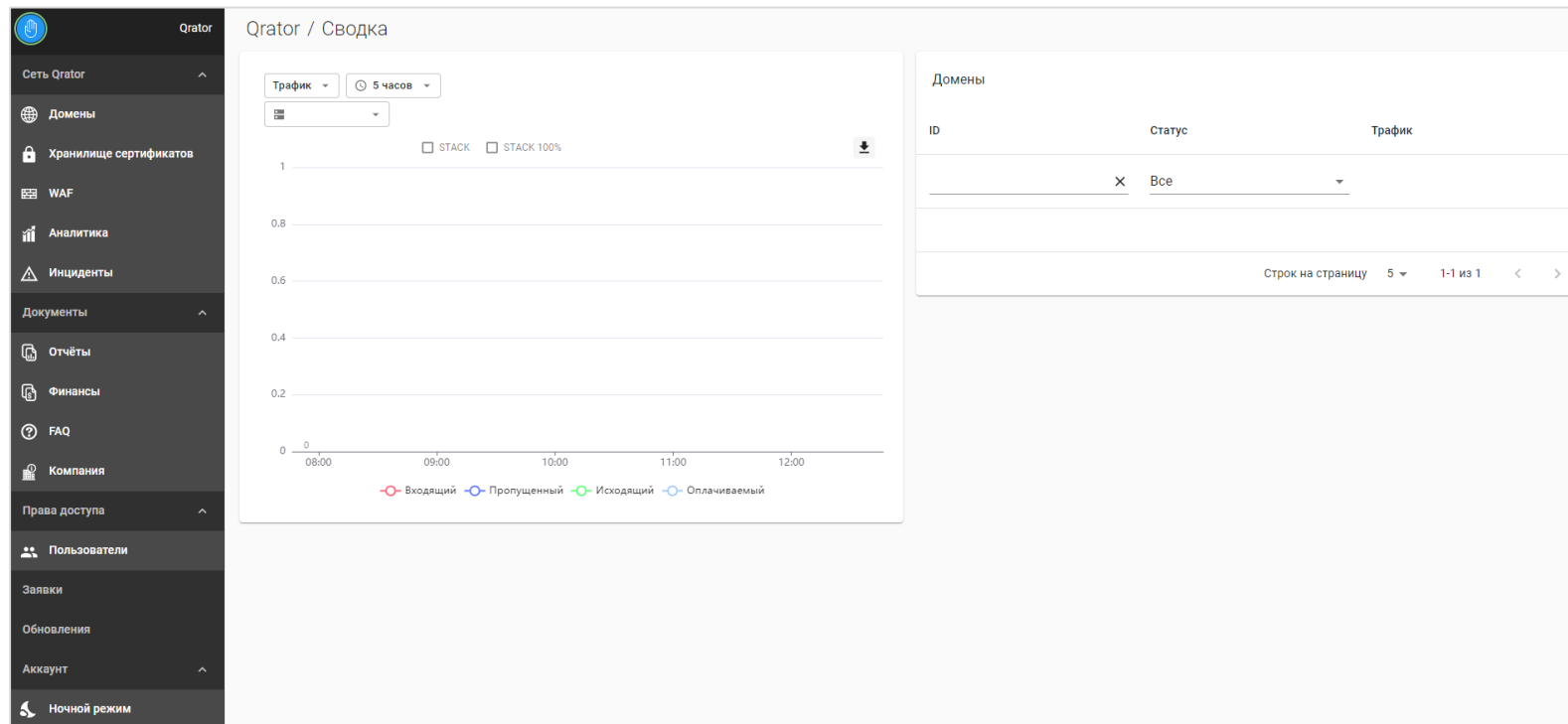
Простая интеграция с API, мобильными приложениями

09

Доступ в личный кабинет для управления и просмотра статистики трафика и DDoS-атак

Личный кабинет и отчетность

- В рамках услуги предусмотрен доступ
- В личный кабинет
- В Личном кабинете доступны отчеты о работе услуги, атаках и возможность конфигурации параметров



#CloudMTS

SOC

04

#CloudMTS

Security Operations Center (SOC)



Центр обеспечения безопасности (SOC) объединяет технологии (программные и аппаратные) и людей для обеспечения комплексной защиты от киберугроз **при помощи мониторинга и реагирования (в режиме 24/7)** на события (инциденты) информационной безопасности **(ИБ)**.

Цель и составляющие SOC

SOC занимается контролем защиты ИТ-инфраструктуры и снижением рисков, за счет использования экспертов кибер-безопасности и современных технологий обнаружения, анализа и предотвращения инцидентов (систем **SIEM** - Security information and event management и технологий кибер-разведки **Threat Intelligence**)

SOC строится на базе **технологий** мониторинга и реагирования на угрозы, поддерживается **людьми** (специалистами ИБ) и позволяет контролировать **процессы ИБ**, которые начинаются с обнаружения угроз и заканчиваются их предотвращением.

SOC



Люди



Технологии



Процессы

Иерархия **защиты** с помощью SOC

Отдельные инструменты ИБ обеспечивают защиту от профильных частных угроз, однако **не защищают заказчика комплексно от инцидентов ИБ**



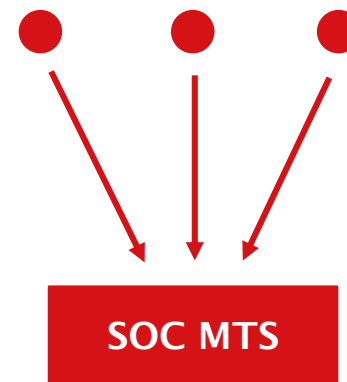
Как работает SOC?

1. Мы собираем события

2. Анализируем события на предмет ИБ

3. Реагируем и уведомляем заказчика

Источники клиентских событий



Круглосуточная смена SOC



Клиентский IT, HelpDesk



Про SOC МТС

С 2005 года

существует
Корпоративный SOC

С 2016 года

предоставляем услуги
Коммерческим
заказчикам

Клиенты

несколько десятков
клиентов в различных
сферах деятельности

Сотрудники

высококвалифицированный
штат сотрудников SOC

SOC

один из крупнейших
SOC не только в России,
но и в Европе

SIEM

реализация крупного
промышленного SIEM
как сервис

Лицензия

лицензия ФСТЭК ТЗКИ №2012
на услуги по мониторингу
информационной
безопасности средств
и систем информатизации
(пункт «в»)

700 млн.

обрабатывается
около 700 млн. событий
в сутки

24/7

мониторинг
и реагирование на
инциденты 24/7

Сертификат

Сертификат ISO 27001
«Предоставление услуг
мониторинга и реагирования
на инциденты информационной
безопасности»



Обнаружение • Предупреждение • Ликвидация •

Подключение к ГОССОПКА

Постоянное усовершенствование SOC. МТС является Корпоративным центром **ГосСОПКА** (**Государственная Система Обнаружения, Предупреждения и ликвидации последствий Компьютерных Атак**)

Во главе **ГосСОПКА** стоит Национальный координационный центр по компьютерным инцидентам (**НКЦКИ**)

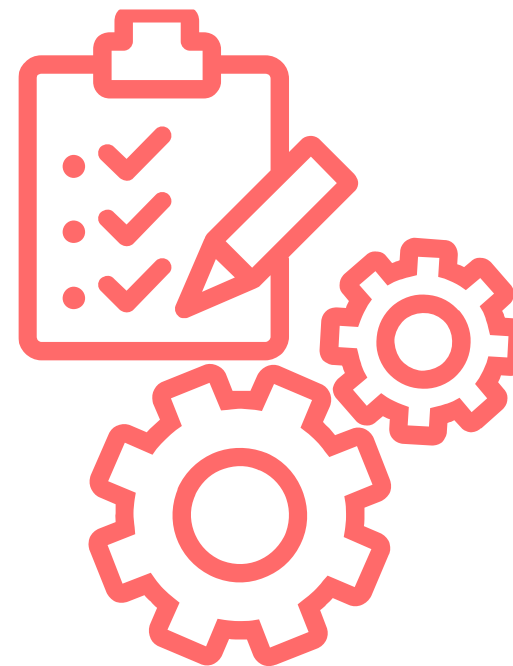
Субъекты критической информационной инфраструктуры (**КИИ**) **обязаны сообщать НКЦКИ** о произошедших компьютерных инцидентах (Федеральный закон от 26.07.2017 №187 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»)

Является **дополнительной опцией** при подключении SOC

Тарификация и набор **опций SOC**

В основе стоимости услуги лежит *количество обрабатываемых событий*
(Events per second - EPS)

- В качестве **дополнительных опций** (в составе клиентского договора SOC):
- Контроль уязвимостей внешнего периметра / сканирование на уязвимости
- Проведение анализа и расследования инцидентов ИБ
- Подключение к **ГосСОПКА**



#CloudMTS



Андрей Пастухов

Product presale #CloudMTS

+7 921 858 96 61

aspastu6@mts.ru

www.cloud.mts.ru



#CloudMTS

Узнавайте первыми:

- о новинках и обновлениях продуктов #CloudMTS
- об актуальных мероприятиях
- о последних важных событиях месяца

Подпишитесь на рассылку:



#CloudMTS

Спасибо!

