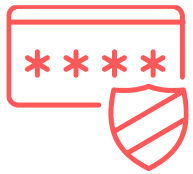
#CloudMTS

Комплексная безопасность цифровых активов предприятия от #CloudMTS

Андрей Пастухов
Менеджер presale #CloudMTS

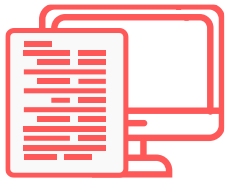
#CloudMTS

Портфель услуг ИБ #CloudMTS



Защищенный
сегмент IaaS 152-ФЗ

Антивирусная
защита VM



Security Operation Center

Защита
от DDoS-атак

Защита веб-приложений
и сайтов (WAF Premium)

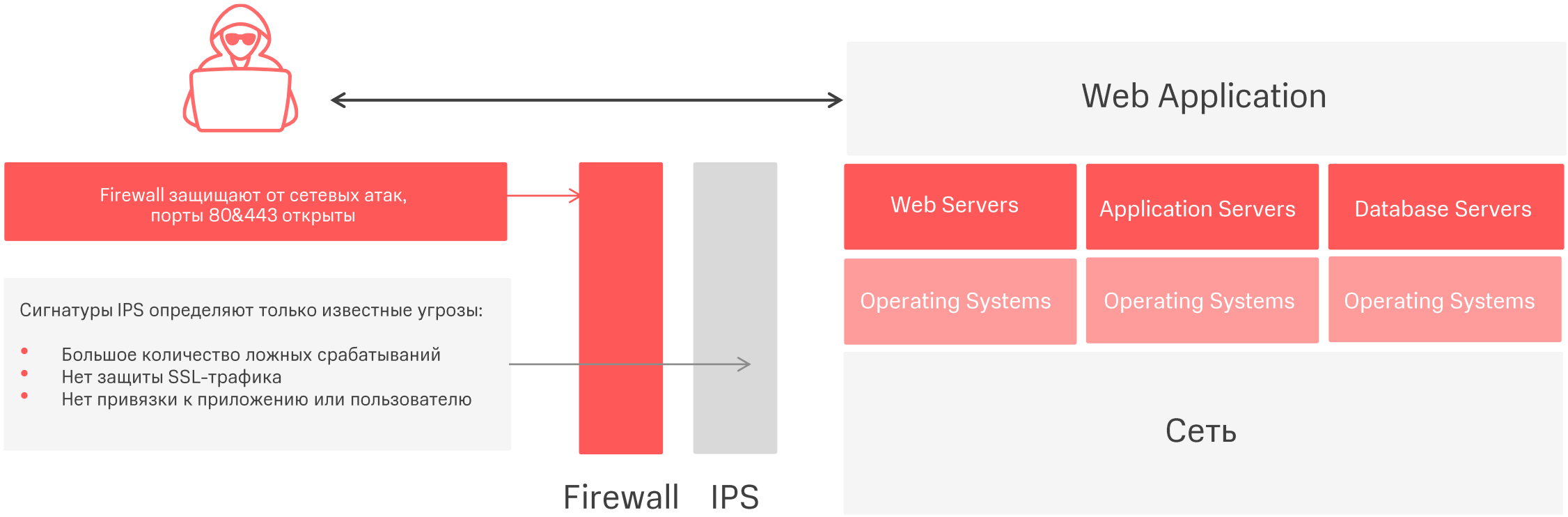
#CloudMTS

WAF Premium

01

#CloudMTS

Фокус более 75% атак направлен на веб-приложения



#CloudMTS

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

#CloudMTS

Кому нужна защита с помощью WAF

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.)

#CloudMTS

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.

#CloudMTS

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)

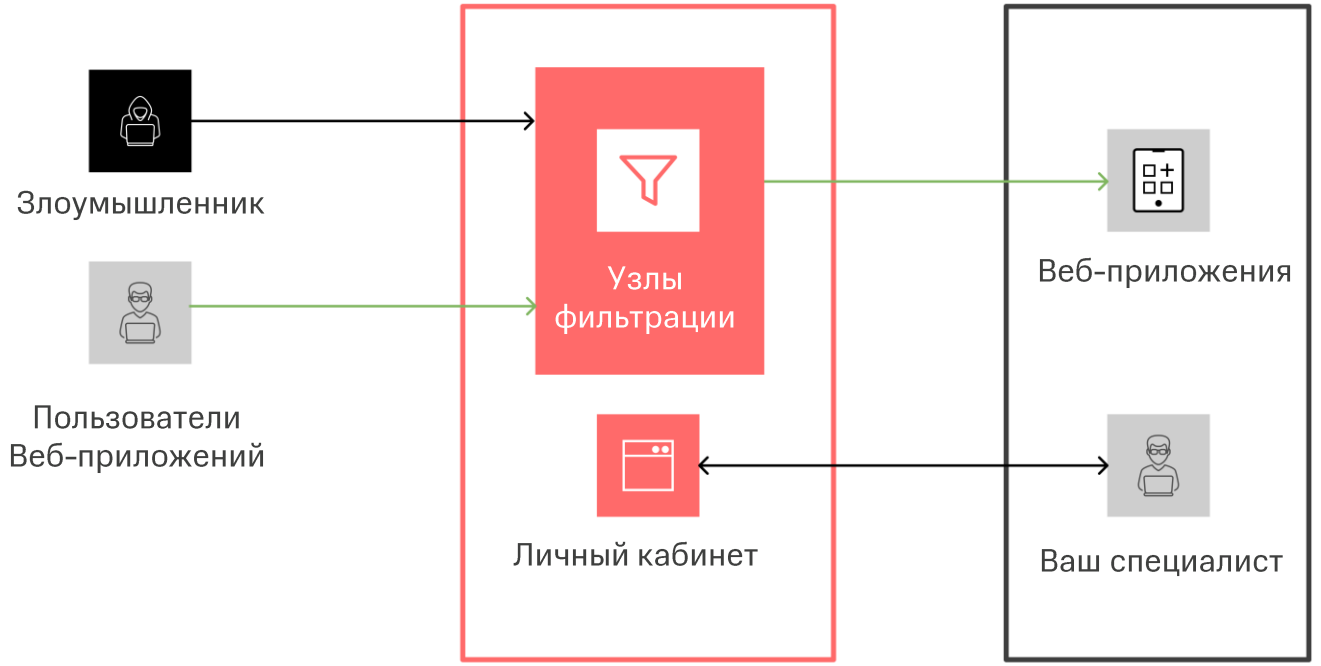
Выявление попыток использования скомпрометированных учетных записей

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

#CloudMTS

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

IaaS ФЗ-152

02

#CloudMTS

Основной вопрос клиента — владельца ИСПДн

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

«ДА!»

#CloudMTS

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

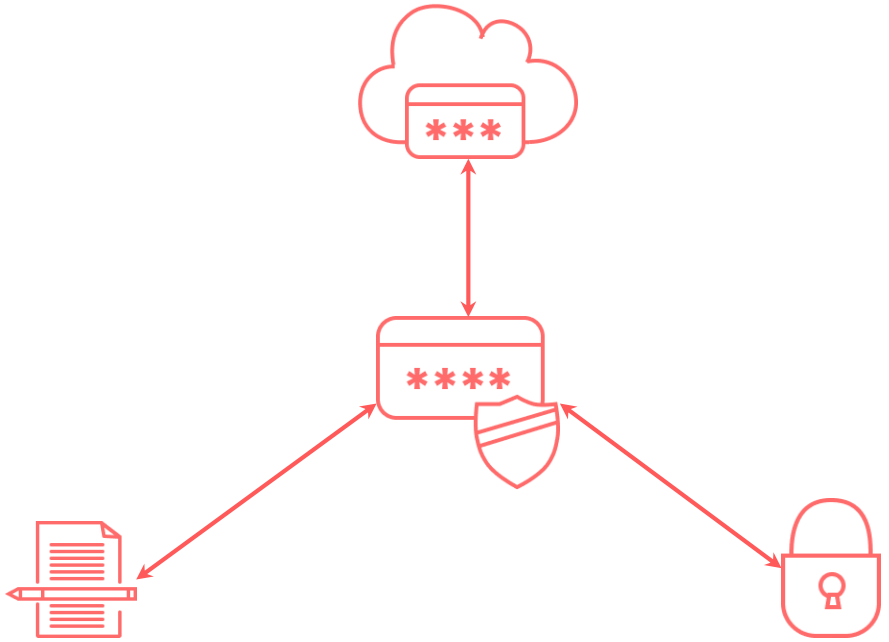
Сертифицированные специалисты исполнителя

#CloudMTS

IaaS 152-ФЗ

Безопасная обработка персональных данных в защищенном облаке, полностью соответствующем требованиям ФЗ-152

Предоставление в пользование виртуальной ИТ-инфраструктуры, удовлетворяющей требованиям законодательства РФ по защите информации, для размещения информационных систем персональных данных клиента

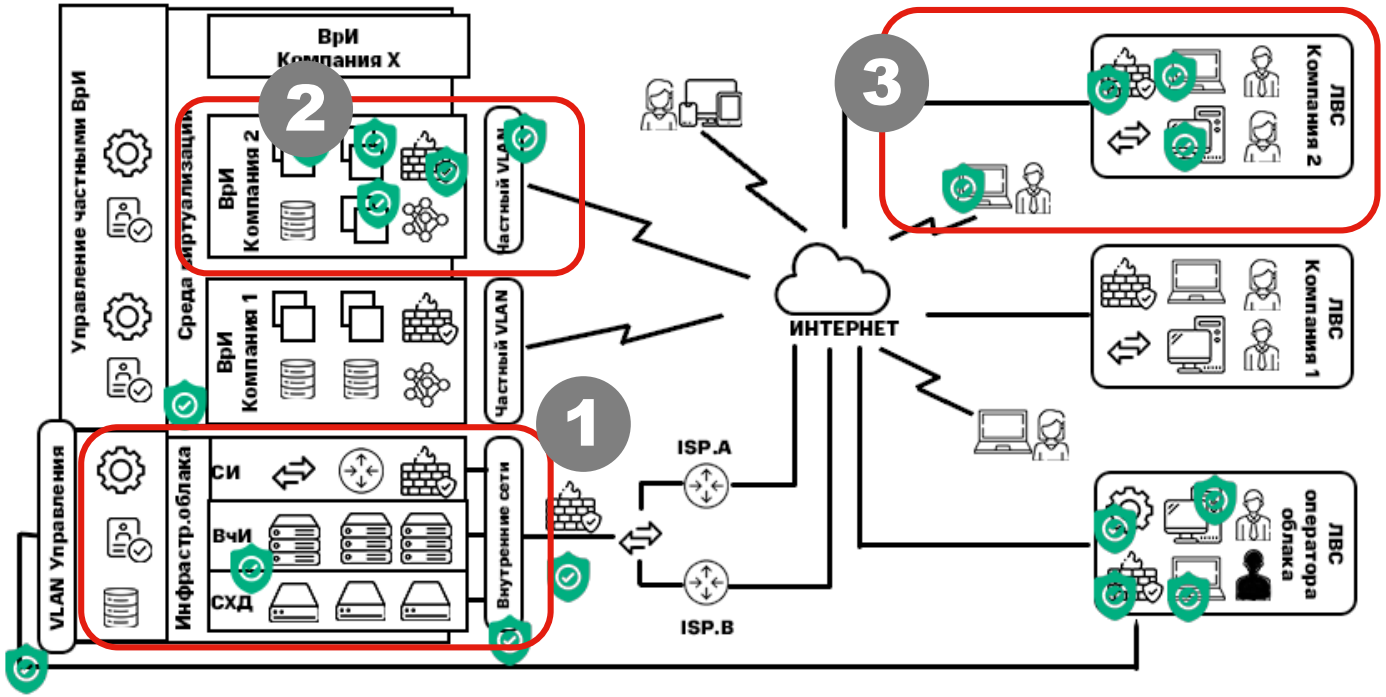


Возможность заключения **официального договора-поручения на обработку ПДн** и помощь в подготовке необходимой документации

Отдельный защищенный аттестованный сегмент облака для размещения мощностей заказчика и обработки ПДн

#CloudMTS

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

Для клиента:
+ Аттестат УЗ-1
+ SOC
+ BaaS

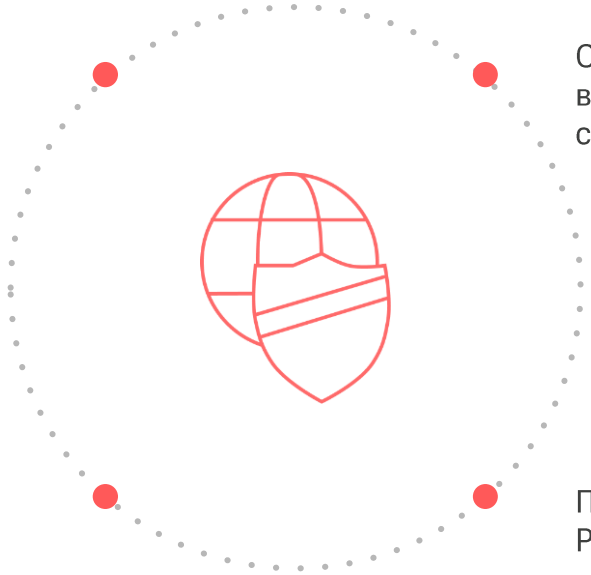
В нашей инфраструктуре:
+ Подключение к SOC
+ СОВ
+ Backup инфраструктуры

#CloudMTS

Что получает клиент в защищенном сегменте #CloudMTS

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

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



Набор типовой документации, частную модель угроз для ИСПДн в облаке

Поддержку в случае проведения проверок РКН, ФСТЭК

#CloudMTS

SOC

03

#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).**

#CloudMTS

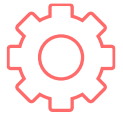
Цель и составляющие SOC

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

#CloudMTS

Иерархия защиты с помощью SOC

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

Контроль событий ИТ и ИБ-инфраструктуры в режиме 24 на 7 (*комплексная защита*)

Набор систем защиты - антивирус, firewall, защита от DDoS-атак, WAF и др. (*инструменты защиты*)

Уровень клиентской ИТ инфраструктуры и производства (*предмет защиты*)

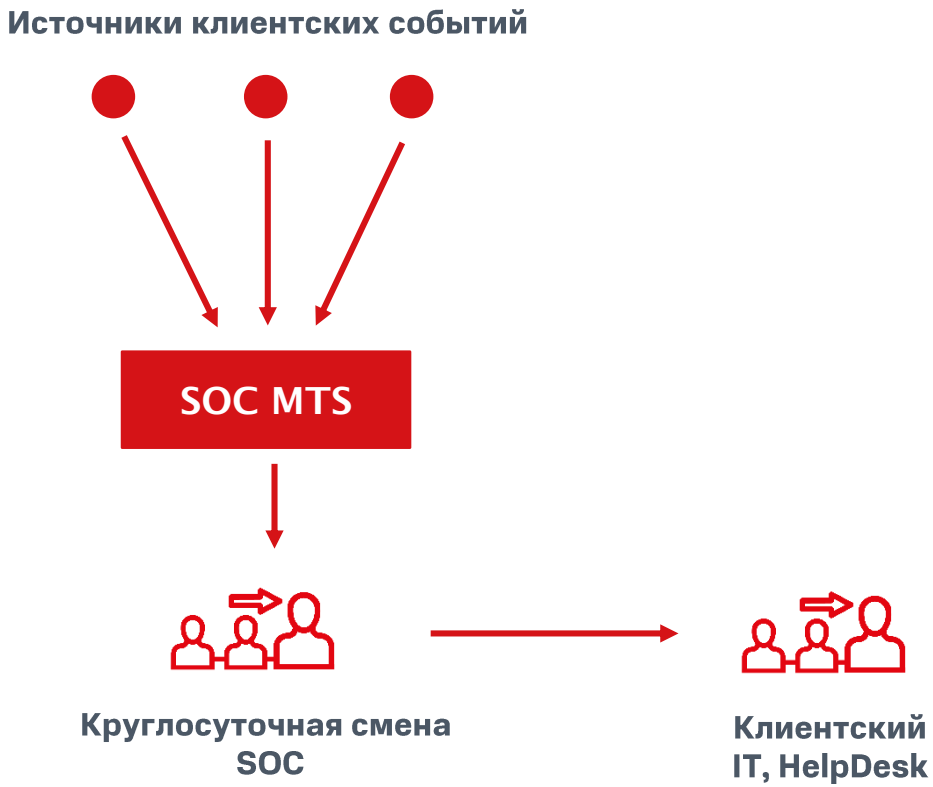
#CloudMTS

Как работает SOC?

1. Мы собираем события

2. Анализируем события на предмет ИБ

3. Реагируем и уведомляем заказчика



#CloudMTS

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»

#CloudMTS ГОССОПКА
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»)

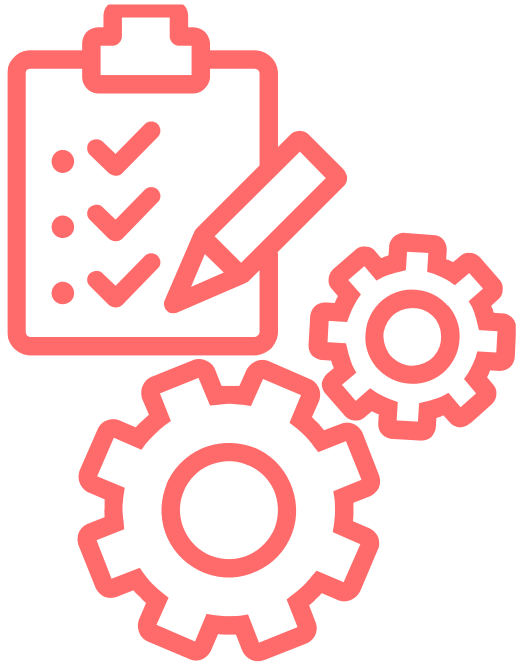
Является **дополнительной опцией** при подключении SOC

#CloudMTS

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

Менеджер presale #CloudMTS

+7 921 858 96 61

andrey.pastukhov@it-grad.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!