Сервисы кибербезопасности

Ростелеком Solar

Константин Черезов

Киберландшафт 2018 - злоумышленники

- Массовые атаки (WannaCry, BadRabbit и сотоварищи)
- И это только вершина инструментария: «Спасибо» The Shadow Brokers
- Экосистема оргпреступности:
  - Хактивисты
  - Кибервойска
  - «Обычные» воры

CISCOпад и критическая инфраструктура

- 6 апреля 2018 массовая атака
- Уязвимы от 180 до 250 тысяч устройств
- Объекты КИИ атакуются в 20-30 раз интенсивнее
- Don`t mess with our elections…

Эксперты: атака с помощью уязвимости Cisco нацелена на информационную инфраструктуру РФ

Экономика и бизнес 8 апреля, 15:17 UTC+3

Интенсивность атак возрастала в 20-30 раз в случае, если была направлена на объекты критической инфраструктуры России

Поделиться

Предпосылки перехода на сервисную модель

Динамика угроз и рисков

- 18+ инцидентов каждые 12 часов
- 13 новых атакующих tool-ов в месяц
- 2-3 новых вида атак в месяц

Темп внешней среды

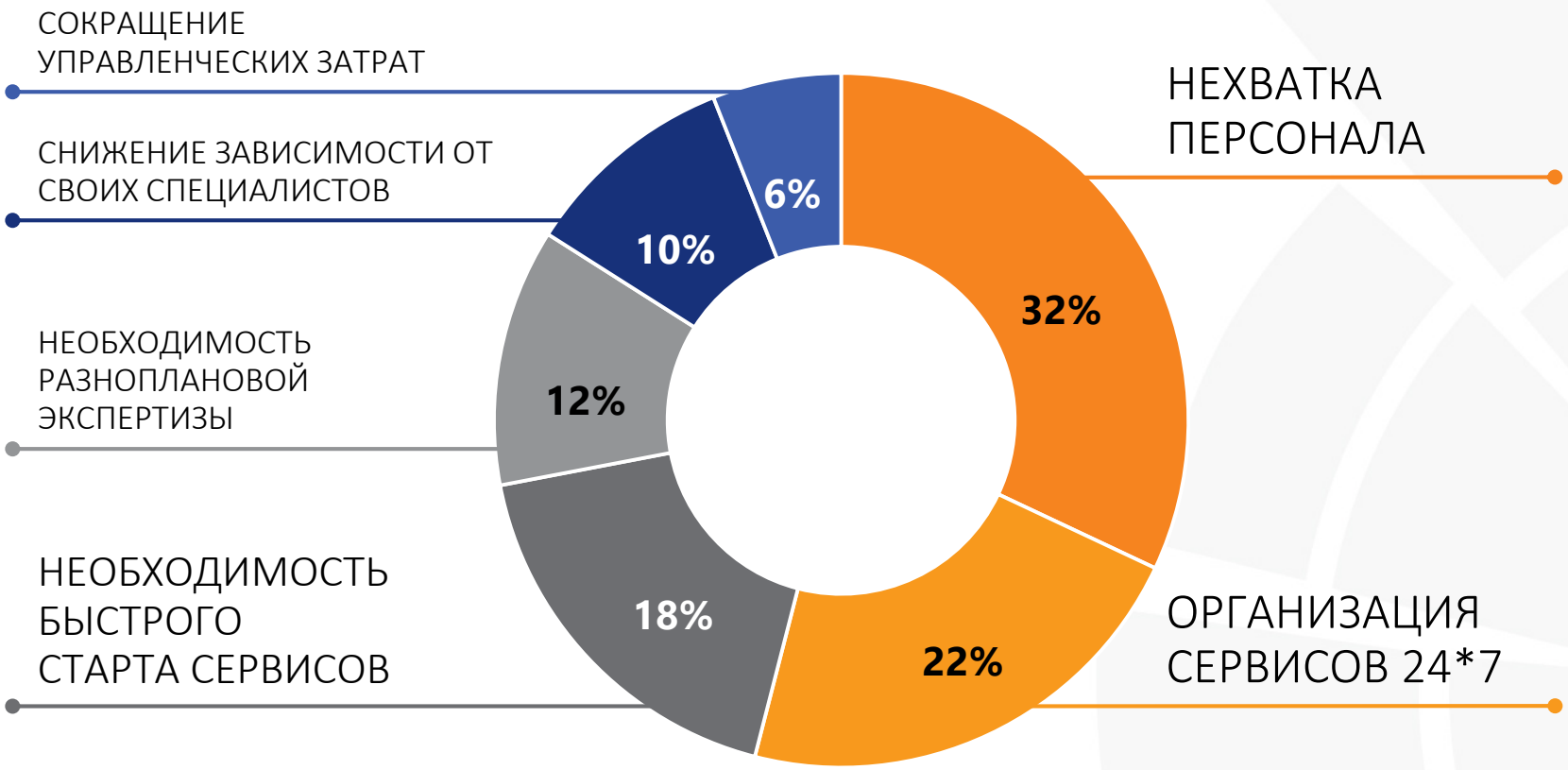
- 3-4 новых больших релиза бизнес-систем в месяц
- До 10ти новых сервисов на периметре в неделю
- Движение бизнеса в digital и индустриализация 4.0
- Ключевое преимущество – постоянная трансформация

Вызовы для ИБ

- Необходимость гарантированного уровня ИБ на предприятиях
- Тяжелый compliance и давление регуляторов, КИИ, ГосСОПКА
- Традиционный подход: проектирование, внедрение, аттестация .... 3 года....
- Отсутствие квалифицированных кадров на рынке труда
- Оптимизация и повышение прозрачности расходов на ИБ

4

Предпосылки перехода на сервисную модель



Линейка сервисов по кибербезопасности

Сервисы РТК-Solar

Мониторинг и управление ИБ

Сервисы сетевой безопасности из облака

Актуальные средства ИБ

Каталог сервисов

Сервисы мониторинга и управления ИБ

На базе центра мониторинга и реагирования на киберугрозы Ростелеком-Solar JSOC

- Мониторинг, реагирование и анализ инцидентов
- Контроль защищенности и управление уязвимостями
- Техническое расследование инцидентов
- Специальные сервисы ГосСОПКА

Актуальные средства ИБ

- Выявление уязвимостей (Vulnerability assessment)
- Повышение осведомлённости персонала в ИБ (Security Awareness Training Platform)

Сервисы сетевой безопасности из облака

На базе сетей передачи данных и ЦОД-ов ПАО «Ростелеком»

SaaS или **SaaS + эксплуатация**

Защита каналов связи

- Защита от DDoS-атак
- Шифрование каналов связи ГОСТ VPN
- Контентная фильтрация трафика

Аренда и эксплуатация ИБ-инфраструктуры из облака

- Unified Threat Management, FW, NGFW, IPS
- Web Application Firewall
- Secure Email Gateway

Основные сервисы по ИБ

Сервис JSOC – ситуационный центр по ИБ

Главные цифры

60+ крупных коммерческих клиентов	**100+** специалистов по ИБ в штате	**6+** лет оказания услуг
99,4% общая доступность сервиса	**10 мин** Время реакции на инцидент	**30 мин** Время анализа/противодействия

- Первый коммерческий центр сервисов ИБ-аутсорсинга в России
- Географически распределен по двум городам: Москва и Нижний Новгород
- Основные сервисы – мониторинг и анализ инцидентов, защита от киберугроз

Публичные клиенты

БАНК САНКТ-ПЕТЕРБУРГ

Росфинмониторинг

Тинькофф

БАШКОМСНАББАНК

Министерство информационных технологий и связи Хабаровского края

НСПК
НАЦИОНАЛЬНАЯ СИСТЕМА ПЛАТЕЖНЫХ КАРТ

ПОЧТА БАНК

ЮНИ ПРО

МТС Банк

media

Уральский Банк реконструкции и развития

Статистика Solar JSOC

Средний суточный поток обрабатываемых событий ИБ

1 квартал	2 квартал
9,2 млрд	18,8 млрд

* Динамика – рост на 104%

Доля критичных инцидентов

1 квартал	2 квартал
17,2%	19,4%

Распределение общего количества инцидентов - в дневное время

1 квартал	2 квартал
89,2%	88,1%

Количество событий с подозрением на инцидент, обработанных JSOC

1 квартал	2 квартал
138 256	219 450

* Динамика – рост на 59%

Распределение инцидентов по внешнему/внутреннему вектору атаки

1 квартал	2 квартал
50,3%/49,7%	52,2%/47,8%

Распределение критичных инцидентов в дневное время

1 квартал	2 квартал
72,1%	69,5%

История из жизни JSOC

Шёл спокойный 2017й год

Petya и WannaCry использует уязвимость EternalBlue

ETERNALBLUE

Кто заранее установил соответствующие обновления от Microsoft

Повысили свою безопасность

История из жизни JSOC

Первые сообщения об атаке на крупные организации

Работает вредоносный продукт **Petya**
Канал распространения – предположительно EternalBlue

15:00
МСК

Активное отслеживание СМИ и форумов вендоров и CERT
Поиск дополнительной информации и индикаторов

Оповещение клиентов
Разбор вируса с технологическими и техническими партнёрами

Первая линия переведена в состояние повышенной бдительности,
Ручной мониторинг IPS, WAF, Anti-DDoS и периметровых сетевых устройств на предмет выявления аномалий

История из жизни JSOC

Первичное заражение через почтовый фишинг,
Имеются сетевые индикаторы и MD5 тела вируса

Ретроспективная проверка по заказчикам
Нет положительных срабатываний

15:30 МСК

Клиенты получили оповещение о необходимости блокировки указанных адресов на сетевом оборудовании

Все сетевые индикаторы компрометации поставлены на контроль обращения через межсетевые экраны и прокси, мониторятся DNS-запросы

Оперативное информирование заказчиков и их проверка.

Рассылка инструкции клиентам

Создается инструкция по минимизации рисков

Обновление ОС Windows и баз АВС.
Закрытие TCP-порта 445 там, где это возможно и не нарушает штатного функционирования сервисов.
В некоторых случаях может оказаться эффективной защита MBR от перезаписи.

15:30 МСК

15:50 МСК

Заказчик

В 15:40 мы получили первый звонок от аналитика с оповещением о том, что наблюдается массовое заражение инфраструктур крупных компаний сферы энергетики, нефтегазового, финансового сектора и ретейла.
Эпидемия очень похожа на WannaCry, но **возможны новые каналы распространения**. Каналом попадания, по первым предположениям, является почта. Сервис-менеджер предупредил, что дальнейшее распространение в инфраструктуре, возможно, происходит не только с помощью эксплуатации EternalBlue, обновления к которой у нас стояли.

Также **в течение 10 минут** была получена рассылка от Solar JSOC с результатами ретроспективного анализа и сетевыми индикаторами, которые необходимо было внести в черные списки на периметровых средствах защиты.
Мы заранее предупредили ответственных специалистов, поэтому, как только оповещение пришло, внешние адреса были заблокированы **в течение 5 минут**.

История из жизни JSOC

Первые выводы о работе вредоносного ПО

На хост изначально попадает дроппер, состоящий из нескольких компонент:
Модифицированная версия криптолокера Misha и Petya.
Модуль-сканер, выявляющий потенциально уязвимые к EternalBlue хосты.
Модуль, использующий для распространения связку PsExec+Mimikatz (дамп паролей и распространение по windows-машинам в сети через штатную утилиту удаленного администрирования Microsoft, для работы которой нужен открытый 445 порт).

15:50 МСК

16:30 МСК

Попадая на хост, вирус пытается повысить привилегии до Системы.
В случае успеха – рестарт и шифрование MFT. В случае неуспеха – шифрование файлов (как стандартный криптер).

Спустя некоторое время выявляется второй канал распространения в инфраструктуре – PsExec+Mimikatz. Чуть позже еще один – удаленный доступ к консоли WMI (Windows Management Instrumentation).

Дополнение инструкции

Блокировка запуска ПО «PSEXEC.EXE» на потенциально уязвимых машинах.
В качестве временной меры – отключить удаленный доступ к WMI

История из жизни JSOC

Заказчик

После получения информации о дополнительных способах распространения критичные сегменты и хосты были временно изолированы по 135, 445, 1024-1035 портам либо поставлены на особый контроль.

Solar JSOC сообщил о том, что антивирусный вендор, чье решение используется в банке, выпустил сигнатуры для детектирования известных сэмплов Petya.

Оперативно было выполнено принудительное обновление на всем парке защищаемых машин и запущена полная проверка на критичных хостах.

В течение последующих часов мы получали информацию о функционале других сборок вредоносного ПО.

Новые индикаторы компрометации проверялись в ретроспективе и ставились на активный контроль.

Дежурный аналитик оперативно взаимодействовал с техническими специалистами заказчиков, в том числе в ночное время.

Все подозрительные почтовые вложения проверялись с особой тщательностью.

История из жизни JSOC

Заказчик

На ночное время мы согласовали с коллегами из JSOC нештатный режим работы, в рамках которого по инцидентам, связанным с аномальной сетевой либо хостовой активностью и вирусными заражениями, помимо штатного оповещения ответственных специалистов банка звонок поступал бы сразу мне для организации оперативного реагирования и проведения проверки по факту инцидента.

Еще после эпидемии WannaCry стало понятно, что использование уязвимостей, обнародованных (и планируемых к публикации) известной хакерской группировкой, будет трендом ближайшего времени, и любые меры, касающиеся мониторинга, кастомных сигнатур и работы антивируса, стоит рассматривать лишь как компенсирующие.

Поэтому служба эксплуатации Solar JSOC в еще более интенсивном режиме продолжила работать с обновлением систем, в том числе и legacy, для которых появились актуальные патчи в инфраструктурах заказчика.

История из жизни JSOC

Активных заражений удалось избежать, потому что:

1. Постоянный контроль состояния защищенности ИС
2. Экосистема из базовых и «продвинутых» средств ИБ
3. Своевременное получение информации об атаках
4. Мониторинг и анализ инцидентов
5. Реагирование и оперативная защита
6. Анализ причин возникновения и корректировка состояния ИБ

Сервис JSOC – ситуационный центр по ИБ

SOC – ситуационный центр по ИБ

Обеспечивает оперативное управление инцидентами и уровнем защищенности с учетом как изменений в инфраструктуре и бизнес-процессах внутри, так и появлением новых угроз и векторов атаки снаружи

Основные функции SOC

- Мониторинг, выявление и анализ инцидентов информационной безопасности
- Техническое противодействие атакам
- Контроль состояния защищенности, выявление уязвимостей, ошибок настройки
- Техническое расследование возникающих критичных инцидентов
- Аналитика по выявляемым инцидентам, их причинам для принятия решений

«Пирамида» JSOC

Кратко о JSOC – всё включено

- **Команда JSOC** - дежурные смены мониторинга и команда реагирования в режиме 24x7, аналитики и инженеры, расположенные в офисах в Москве и Нижнем Новгороде
- **Выстроены процессы**, позволяющие выдерживать наивысшие SLA по обнаружению (менее 20 минут) и реагированию на инциденты (менее 30 минут)
- **Агрегация и использование** открытых, вендорских и собственных **репутационных баз Threat Intelligence**
- Предоставление подробной **отчетности** периодично и по запросу
- За каждым Заказчиком закреплён **аналитик и сервис-менеджер**
- Работа с Заказчиком построена через систему **Incident Response**, интегрированную с SIEM
- Все необходимые **лицензии** ФСБ и ФСТЭК, в т.ч. на мониторинг
- Работа с **ГосСОПКА** под ключ

Линейка сервисов по кибербезопасности

Сервисы сетевой безопасности

На базе сетей передачи данных и ЦОД-ов Ростелеком

SaaS или **SaaS + эксплуатация**

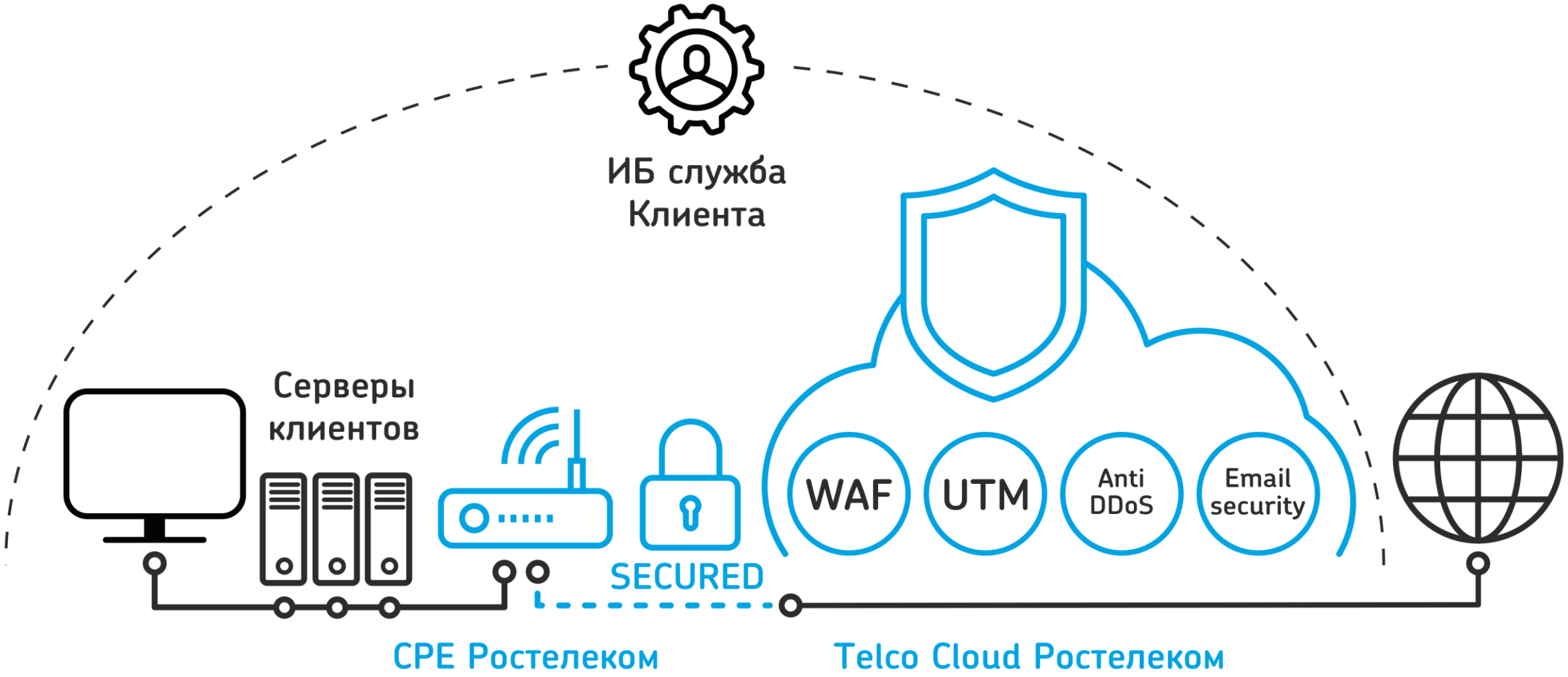
Защита каналов связи

- Защита от DDoS-атак
- Шифрование каналов связи ГОСТ VPN
- Контентная фильтрация трафика

Аренда и эксплуатация ИБ-инфраструктуры из облака

- Unified Threat Management, FW, NGFW, IPS
- Web Application Firewall
- Secure Email Gateway

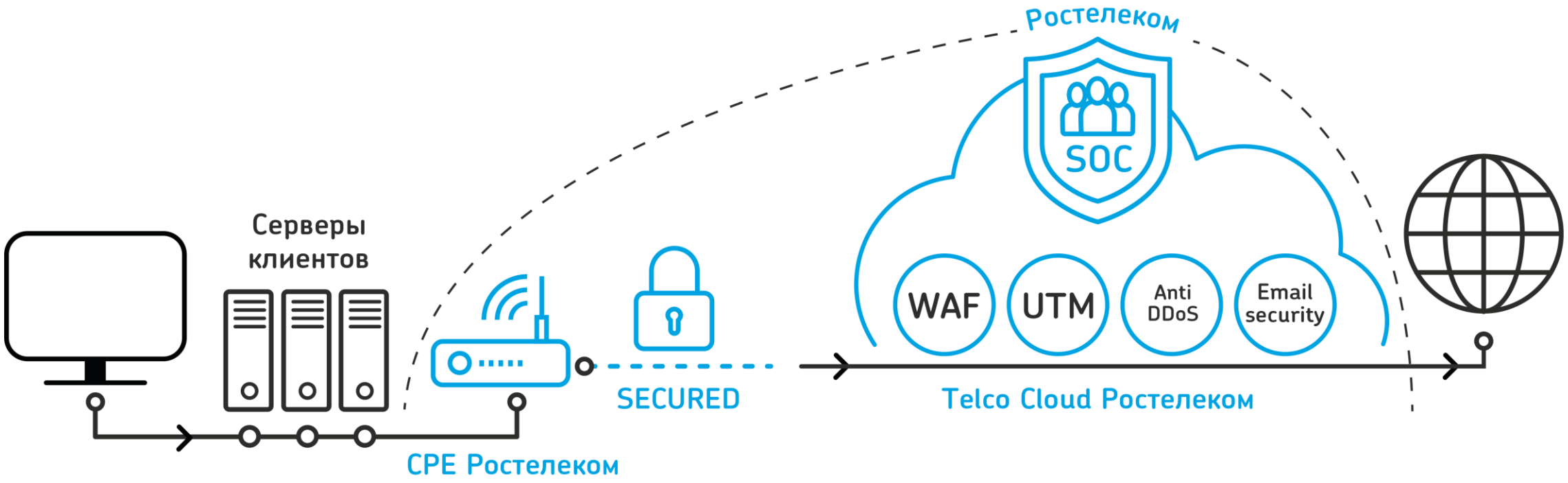
Сервис – облачный вариант



Сервисы – в ЦОД Ростелеком

Виртуальный ЦОД Ростелеком

Сервисы – облако + эксплуатация РТК



Заключение

Почему Ростелеком-Solar

Самый широкий выбор апробированных ИБ-сервисов в России

Первый и крупнейший российский SOC

Отлаженные процессы и структура провайдера ИБ-сервисов

Сервисы оказываются в режиме end-to-end со сквозными SLA

Опора на сервисную модель услуг и ЦОД ПАО Ростелеком

Собственные программные средства защиты

10+ лет опыт реализации проектов информационной безопасности национального масштаба

Кадровый потенциал для реализации самых масштабных проектов

Спасибо за внимание!