Комплексный подход к обеспечению ИБ

Спикер

Николай Климцев

Заместитель директора
Центра региональных продаж

RED

С чем мы сталкиваемся

>67%

Кибератак имеют целенаправленный характер

6+ мес.

До атаки злоумышленник может находиться в инфраструктуре компании

Тенденции

На рынке

- Нехватка профильных специалистов и отток профессионалов в области ИБ
- Тернистый путь закупки зарубежных решений
- Увеличение количества таргетированных атак на цепочки поставок (ФАКТ!)
- Усиление требований регуляторов к ИБ

В компаниях

- Нет кадров для внедрения и поддержки средств защиты информации
- Нет вычислительных ресурсов/ возможности продлить/закупить лицензии и оборудование
- Необходимо обеспечить ИБ и в головной организации, и в филиалах
- Необходимо оперативно выполнять требования законодательства

*Данные на основе открытых источников и внутренних исследований МТС RED

MTC RED – разработчик решений для кибербезопасности

- Опыт работы с компаниями из разных сфер российской экономики, понимание отраслевой специфики
- Филиалы во всех крупных городах и часовых поясах Российской Федерации
- В ядре сервисов - разработки отечественных вендоров, не подлежащие санкционным рискам

300+
Команда экспертов

10+
Лет опыта защиты лидирующего оператора связи

10+
Готовых продуктов и сервисов

20+
Продуктов и сервисов до конца 2025 года

2005 — Запуск корпоративного MTC SOC

2017 — Выход MTC SOC на коммерческий рынок

2022 — Создание MTC RED – со специализацией в ИБ

2023 — Запуск новых сервисов и продуктов MTC RED

2024 — Расширение портфеля за счет собственных новых разработок

MTC RED

Что мы видим по итогам общения с клиентами

Нет единых стандартов
и подходов к ИБ

Отсутствие компетенций
по ИБ в штате

Отсутствие зрелых ИБ-процессов

Недостаток человеческих ресурсов →
невозможность реализовать СОИБ
и требования регуляторов

Решения западных и российских
вендоров не интегрируются друг с
другом

Отсутствие поддержки используемых
иностранных решений/привлечение
«no-name-компаний» для обеспечения
их работоспособности

MTC RED

MTC RED

ПРОГНОЗИРОВАНИЕ
- Подготовка к угрозам, которые не стали инцидентами
- Предиктивное выявление угроз

ЗАЩИТА
- Борьба с известными угрозами

Цель: полная автоматизация жизненного цикла ИБ

РЕАГИРОВАНИЕ
- Ответные меры и политики реагирования на выявленные инциденты
- Исключение повторного инцидента

ВЫЯВЛЕНИЕ
- Обнаружение ранее неизвестных угроз
- Приоритизация и обработка инцидентов

MTC RED

Сервис защиты от DDoS-атак (Anti-DDoS)

Блокировка DDoS-атак для обеспечения стабильного доступа пользователей к веб-ресурсам и инфраструктуре компании

в 1,5 раза

выросло количество DDoS-атак в 1-м квартале 2024 года относительно H2 2023 года

Защищаем круглосуточно

выделенная дежурная смена обеспечивает работу сервиса в режиме 24/7/365

800 руб.

требуется заплатить для запуска DDoS-атаки

Экономим деньги

сервис от интернет-провайдера выгоднее облачного, гибкая тарификация в зависимости от бизнес-требований

Обманный маневр

DDoS-атака часто является прикрытием для других хакерских атак

Защищаем комплексно

блокировка атак уровня сетевых и транспортных протоколов (L3-L4) и прикладном уровне (L7) без раскрытия ключей HTTPS-трафика

МТС RED успешно отразил самую мощную за год DDoS-атаку на ШПД МТС

«

Мощнейшая за год DDoS-атака на сеть МТС была одновременно из Турции, Испании, Польши, Эквадора и Китая, нападение велось с 20 тысяч устройств, а хакеры пытались взломать сеть оператора на протяжении 2 часов, но им не удалось

РИА Новости

20+ тыс.

устройств, нацеленных более чем на 500 IP-адресов телеком-оператора, было задействовано в нападении.

Атака продолжалась около 2 часов, время срабатывания системы мониторинга сервиса защиты от DDoS-атак "МТС RED" составило считанные минуты

207 Гб/с

мощность зафиксированной DDoS-атаки; на границе сети мощность могла достигать нескольких терабит.

В случае успеха атаки она привела бы к отключению доступа в интернет для пользователей оператора целого региона

МТС RED

Сервис защиты веб-приложений (WAF)

Блокировка целевых и массовых атак для предотвращения взлома веб-приложений, краж и подмены данных

ТОП-3

атакуемых отраслей занимают госсектор, финансовые организации, телеком

Защищаем круглосуточно

выделенная дежурная смена обеспечивает работу сервиса в режиме 24/7/365

53%

инцидентов привели к прерыванию бизнес-процессов

Экономим деньги

фиксированные ежемесячные платежи, цена зависит от нагрузки на веб-приложения

на 56%

увеличилось число успешных атак на веб-приложения

Защищаем от всех типов атак на веб-приложения

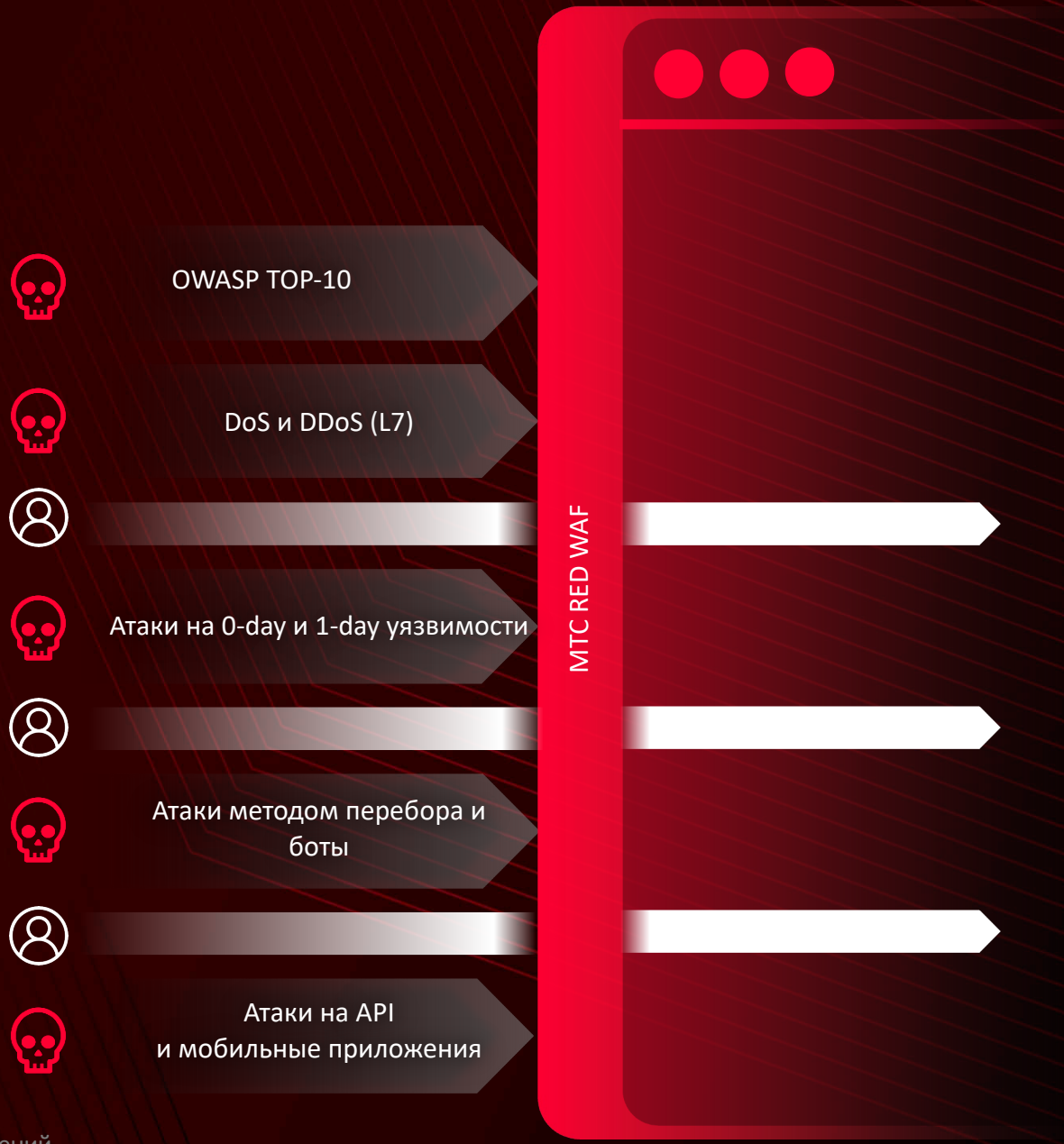
включая атаки на мобильные приложения и API, 0-day уязвимости, на которые еще не выпущены патчи

MTC RED WAF + Bot Security

Сервис защищает веб-приложения компании от действий злоумышленников. Блокирует атаки OWASP TOP-10, DoS- и DDoS-атаки уровня приложений, новые и ранее неизвестные атаки.

В рамках сервиса специалисты MTC RED настраивают правила работы с запросами. Легитимные запросы направляются к веб-приложению заказчика, подозрительные – блокируются (в автоматическом или ручном режиме).

Команда MTC RED обеспечивает сервис «под ключ»: подключение и настройку защиты, круглосуточный мониторинг и реагирование на атаки. Отслеживать работу сервиса можно в личном кабинете.



MTC RED

Web Application Firewall – межсетевой экран для защиты приложений.

Сервис шифрования каналов связи (ГОСТ VPN)

Криптографическая защита передаваемой по каналам связи конфиденциальной информации в соответствии с требованиями регуляторов

на 100%

выполняет требования регуляторов
по криптографической защите данных:
149-ФЗ, 152-ФЗ, 187-ФЗ, отраслевые требования,
приказы ФСТЭК и ФСБ России

в 3 раза

быстрее, чем закупить, настроить
и подключить оборудование своими силами

Оптимизируем время

быстрое подключение и гибкое масштабирование криптозащиты

Экономим деньги

сервис по подписке выгоднее покупки оборудования

Избавляем от рутины

специалисты МТС RED берут на себя закупку, настройку и обслуживание оборудования

МТС RED

МТС RED ГОСТ VPN

Сервис реализуется с применением сертифицированных средств криптографической защиты информации (СКЗИ)*.

Позволяет передавать конфиденциальную информацию в зашифрованном виде между филиалами компании, а также обеспечивает ее защиту при передаче во внешние информационные системы по сетям общего пользования.

Обеспечивает защиту информации с требуемой стойкостью на базе российских криптографических алгоритмов.

В рамках сервиса МТС RED разрабатывает спецификацию под требования заказчика, берет на себя закупку, установку, обслуживание и техническую поддержку СКЗИ согласно уровню оказания сервиса (SLA).

МТС RED

* Лицензия ФСБ России на предоставление защищенных с использованием шифровальных (криптографических) средств каналов связи для передачи информации. №0018041 от 24.11.2020г.

Сервис многофакторной аутентификации (MFA)

Комплексное решение для защиты удаленного доступа и учетных данных корпоративных пользователей

99,9%

Защита от автоматизированных кибератак на пароль

6+

Поддерживаемых способов аутентификации: аппаратные и программные OTP, SMS, звонок на телефон, код в Telegram или на почту

5+

Сценариев использования: VPN и VDI-подключения, RDP, облачные приложения и Web

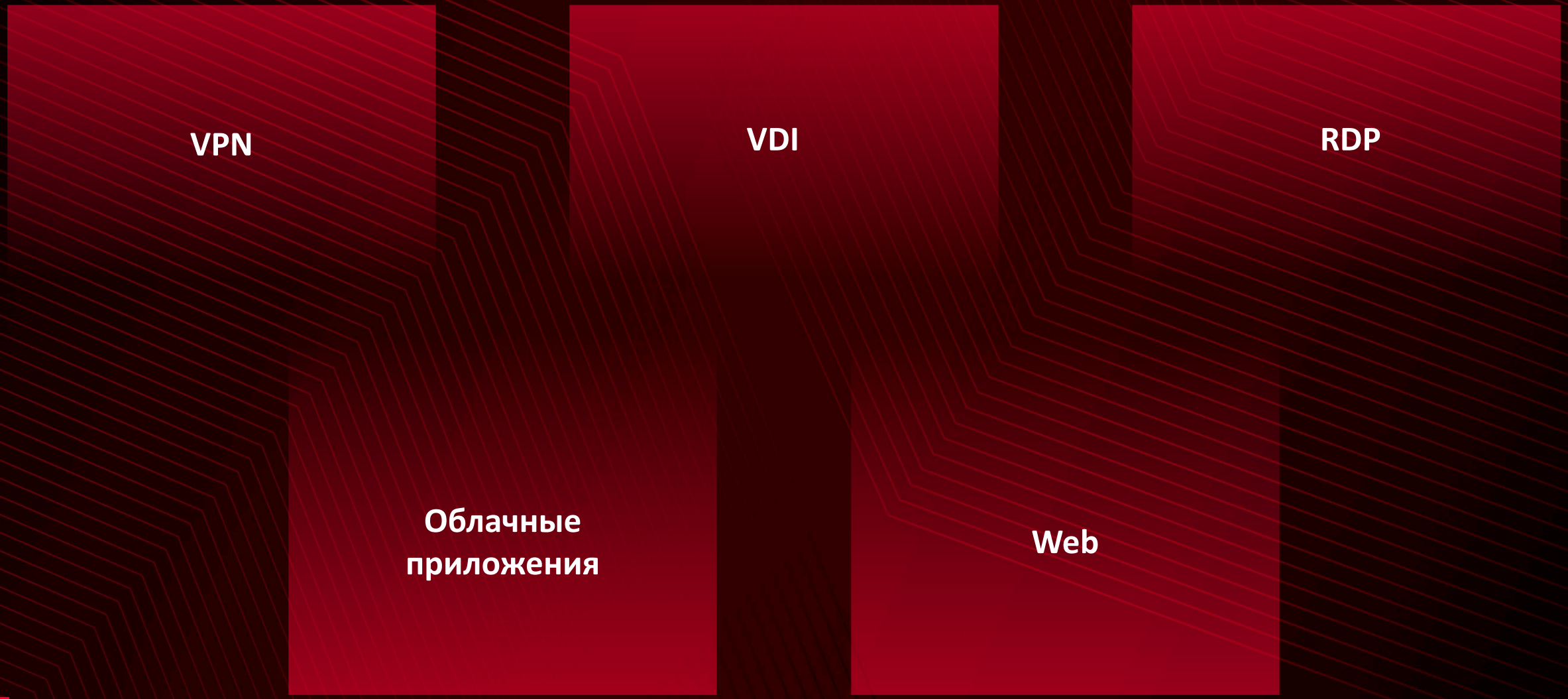
Защищаем
учетные данные с помощью одноразовых паролей

Предотвращаем
компрометацию учетных записей и утечки данных

Помогаем
обеспечить непрерывность рабочих процессов

M T C RED

Защищаемые типы подключений



Поддерживаемые способы аутентификации

Центр круглосуточного мониторинга и реагирования на киберугрозы (SOC)

>8,6 млрд

анализируемых событий в сутки

>55

опытных аналитиков

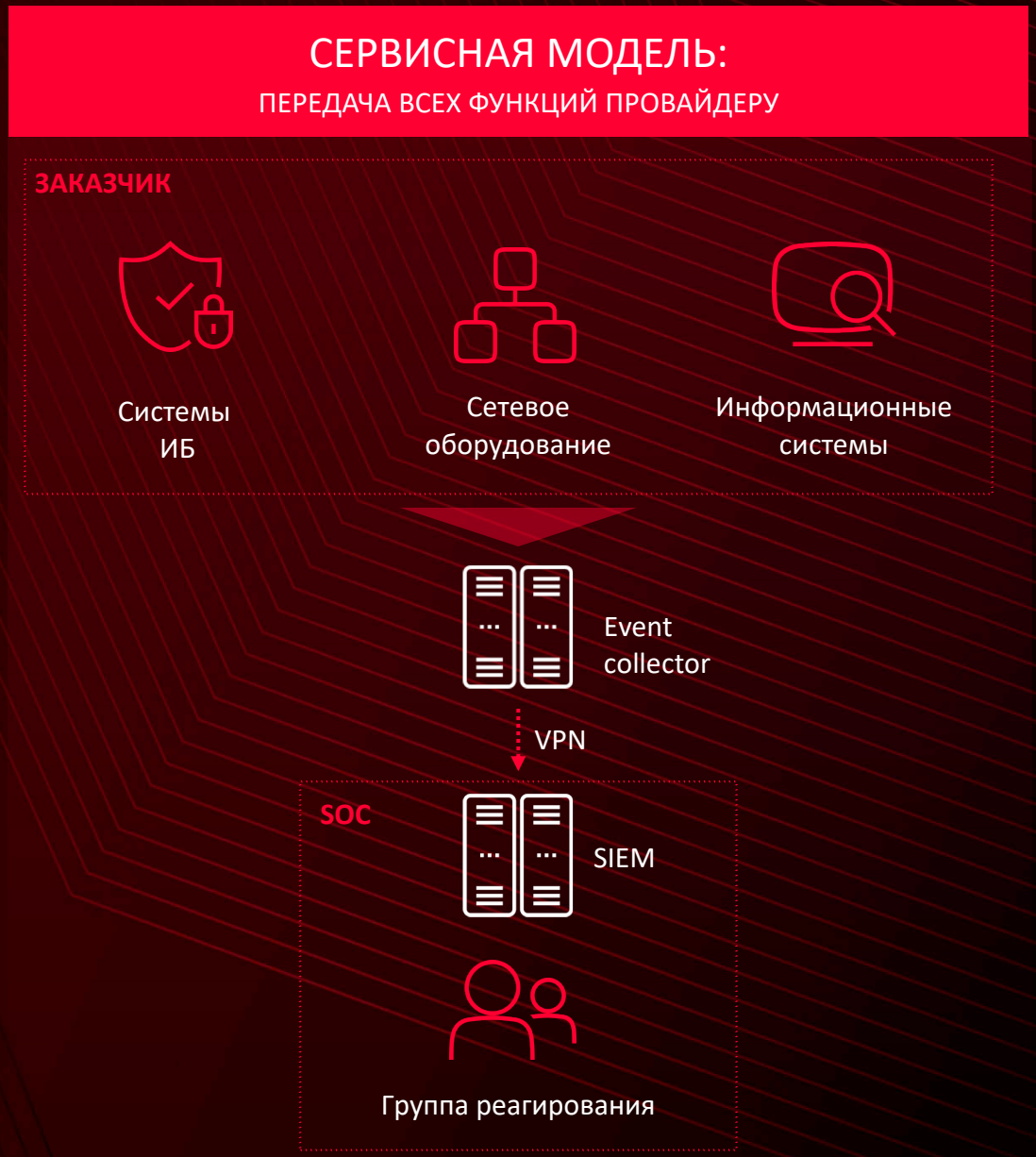
- Знаем отраслевую специфику заказчики - крупные компании из различных секторов экономики
- Реализуем эффективные процессы повышение скорости реагирования и блокировки целевых атак и вредоносного ПО (вкл. шифровальщики)
- Оптимизируем затраты на штат специалистов по ИБ Мониторинг событий ИБ 24/7: 3 линии аналитиков, отдельная команда для проактивного анализа новых типов угроз
- Берем на себя задачи по взаимодействию с ГосСОПКА
- Обеспечиваем прозрачность процессов удобный личный кабинет с наглядными дашбордами и расширенной статистикой по событиям для принятия эффективных решений
- Предоставляем гибкую тарификацию и SLA по анализируемым событиям – для наилучшего соотношения цены и качества. Переводим CAPEX в OPEX

Модели подключения

MSSP SOC по сервисной модели

Кому актуально?

- Нет бюджета для собственного SOC или найма дорогостоящих специалистов
- Не хватает квалифицированных кадров ИБ/недостаточно экспертизы
- Нужно быстро обеспечить мониторинг (для выполнения 250 УП и пр.)
- Нет вычислительных ресурсов/ проблемы с закупками СЗИ



Модели подключения

Гибридная модель — делим функции SOC между клиентом и нами

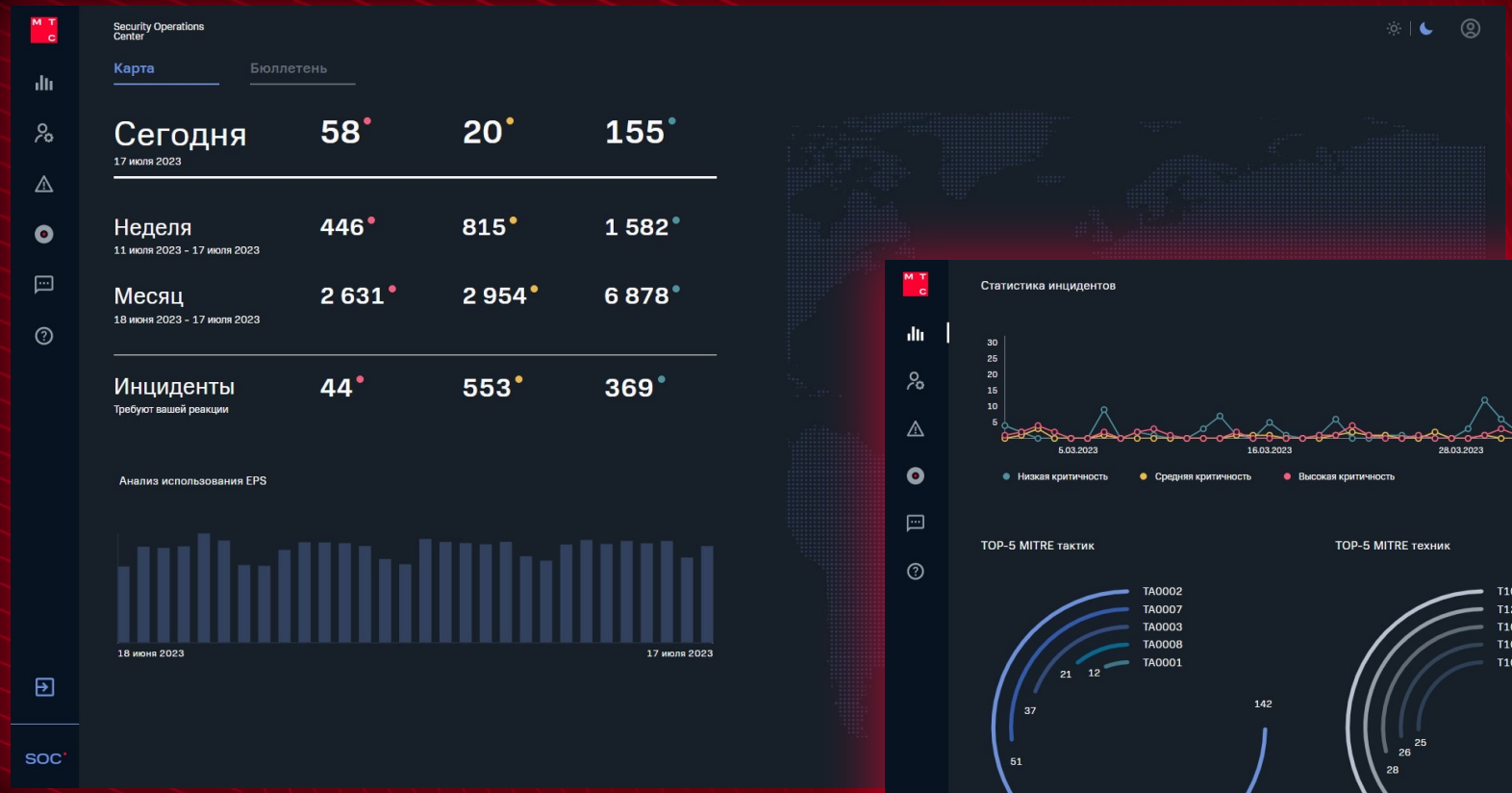
Кому актуально?

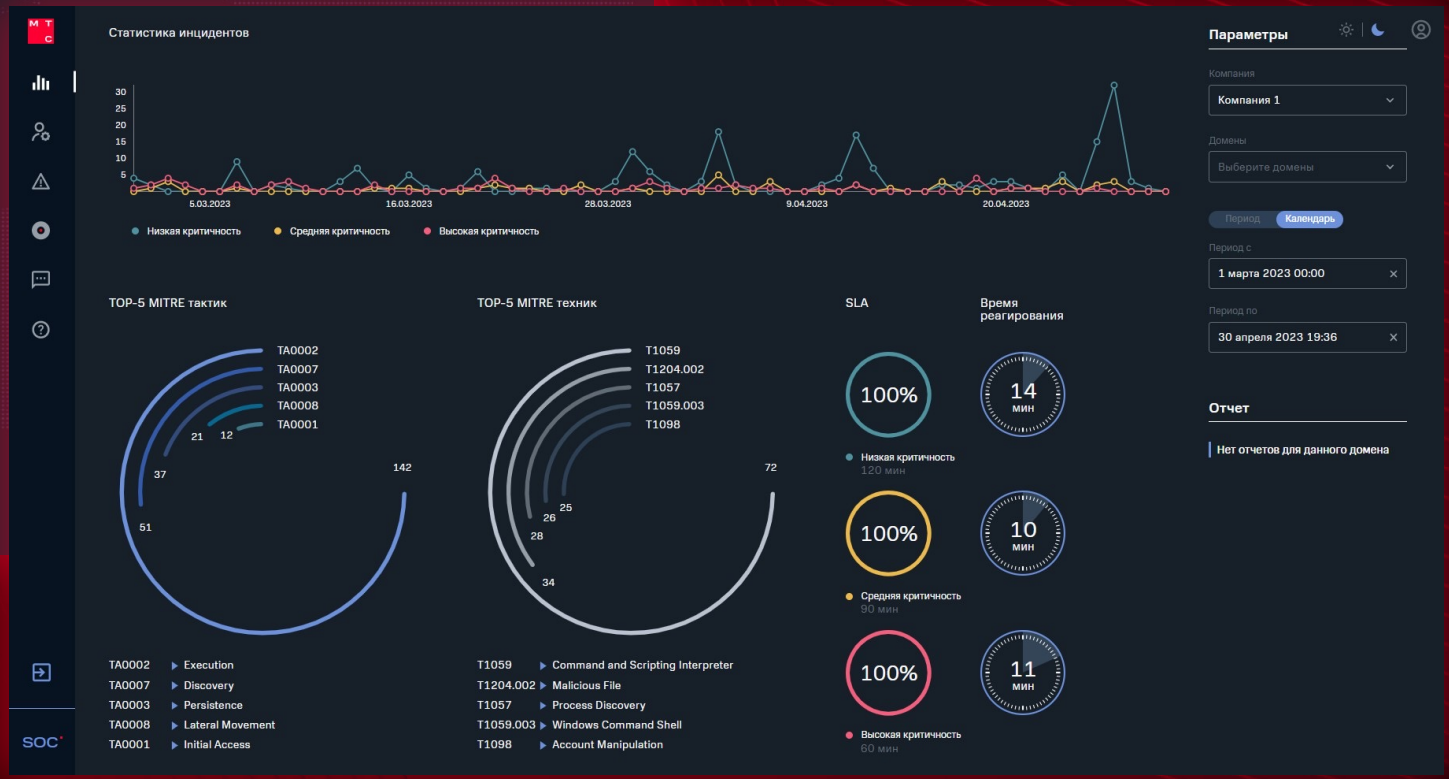
- У клиента уже есть технические средства SOC (SIEM, SOAR),
  но не хватает специалистов
- Отсутствуют аналитики SOC
- Нужны отдельные компоненты SOC

ГИБРИДНАЯ МОДЕЛЬ:
РАЗДЕЛЕНИЕ ФУНКЦИЙ

Что подключается к мониторингу?

Личный кабинет





Сервис повышения киберграмотности сотрудников (Security Awareness)

Комплексное решение для формирования устойчивости к фишинговым атакам

на 70%

меньше событий ИБ, связанных с фишингом, в 1-й месяц использования

Оптимизируем время

быстрое подключение, все работы – на стороне МТС RED

в 3 раза

выше уровень осведомленности сотрудников

Экономим деньги

сервис из облака на мощностях МТС RED, операционные затраты

до 80%

меньше повторных инцидентов информационной безопасности

Защищаем превентивно

учим сотрудников не вестись на уловки хакеров

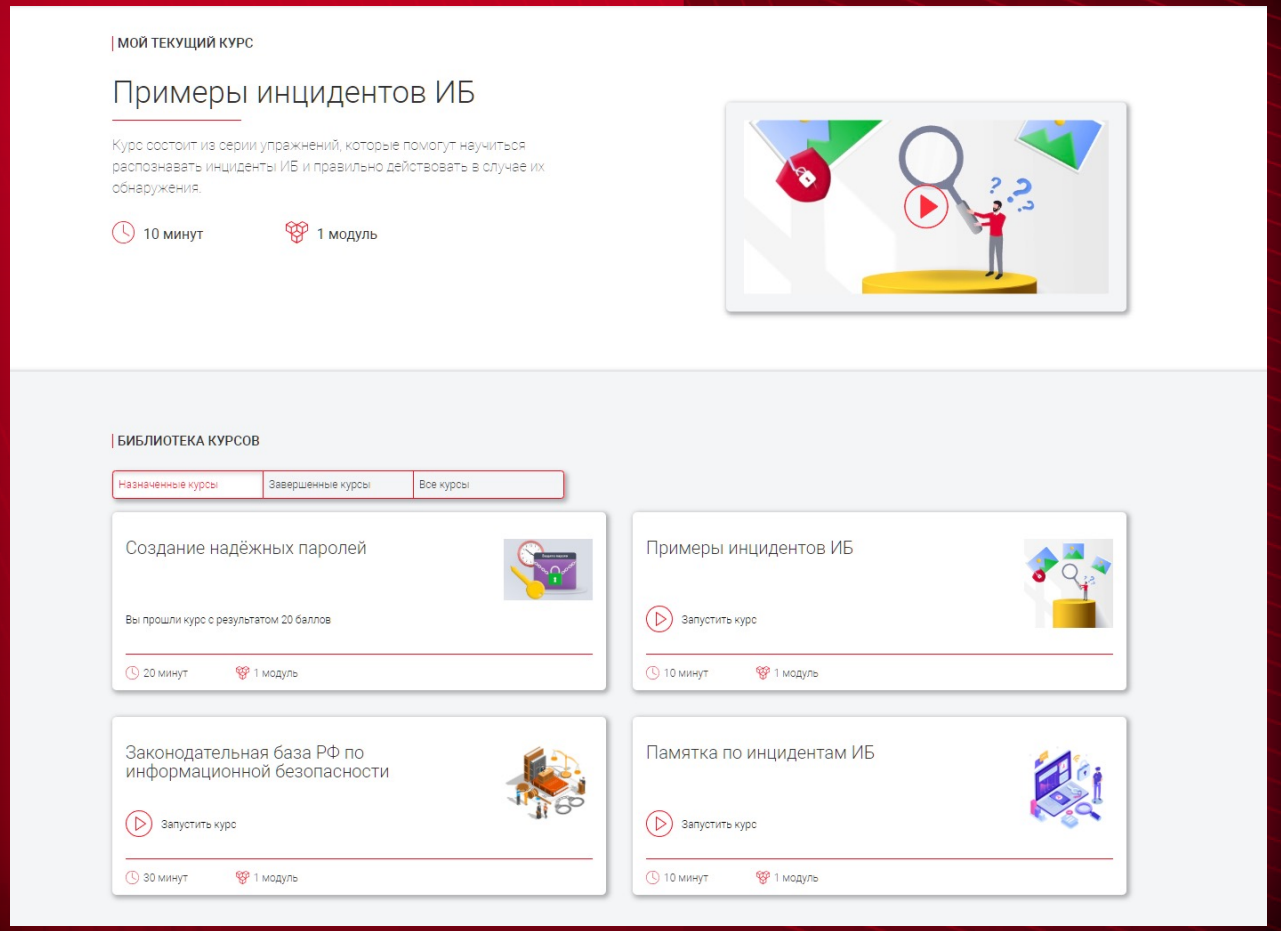
МТС RED

Сервис оказывается на базе вендора Phishman

Интерфейс личного кабинета сотрудника

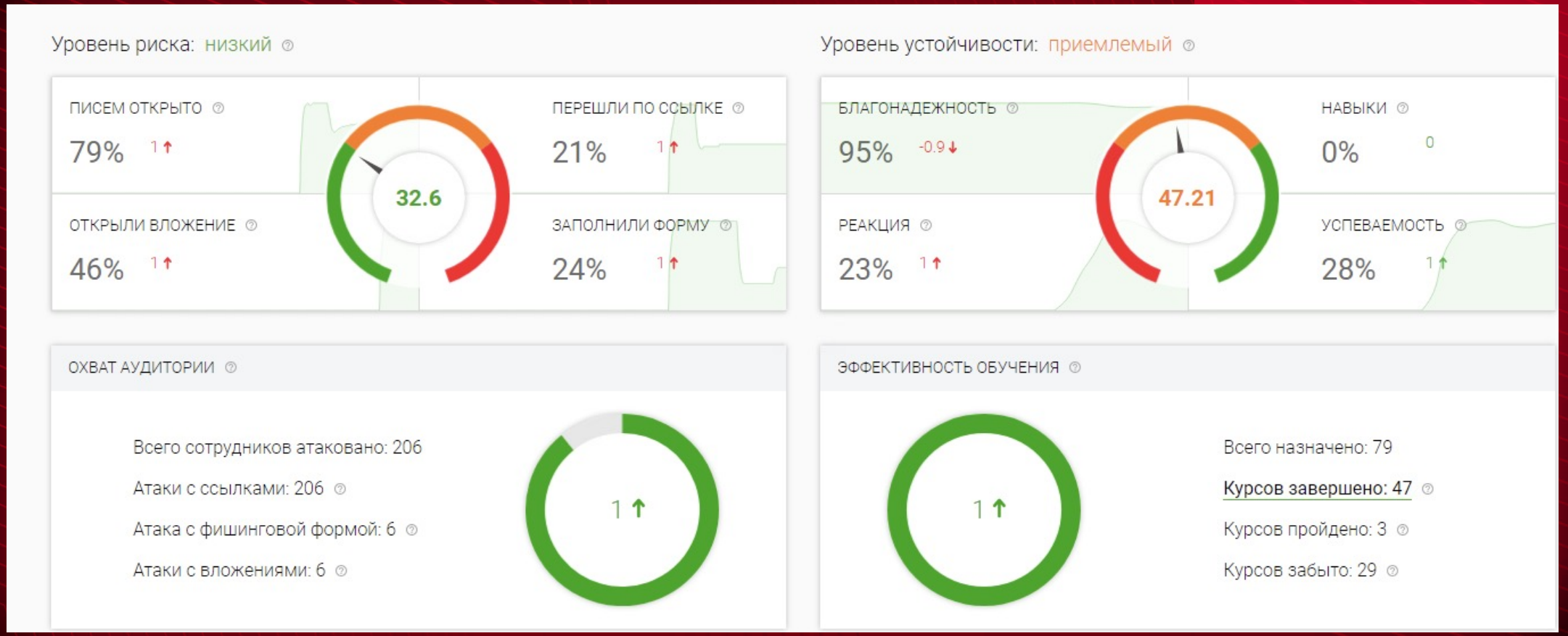
Онлайн-курсы содержат короткие (до 30 минут) сценарии с интерактивными элементами и простым интуитивно понятным интерфейсом

В конце каждого курса пользователь проходит тестирование, в котором необходимо набрать проходной балл (устанавливается индивидуально сотрудником ИБ)



Интерфейс личного кабинета ИБ-специалиста

Наглядные дашборды и расширенная статистика по результатам обучения сотрудников



Этапы подключения сервиса

5 дней

Стандартный срок подключения облачного решения

1	Интервью с заказчиком: сбор информации о компании, выбор способа предоставления сервиса	~ 1 день
2	Выделение ресурсов и доступов со стороны заказчика	~ 3 дня
3	Подключение и настройка решения	~ 1 день
4	Сервис готов к работе!	

Хотите узнать больше о продуктах и сервисах МТС RED? Свяжитесь с нами!

Климцев Николай,
Заместитель директора
центра региональных продаж
+7-982-731-67-74
n.klimtsev@mts.ru