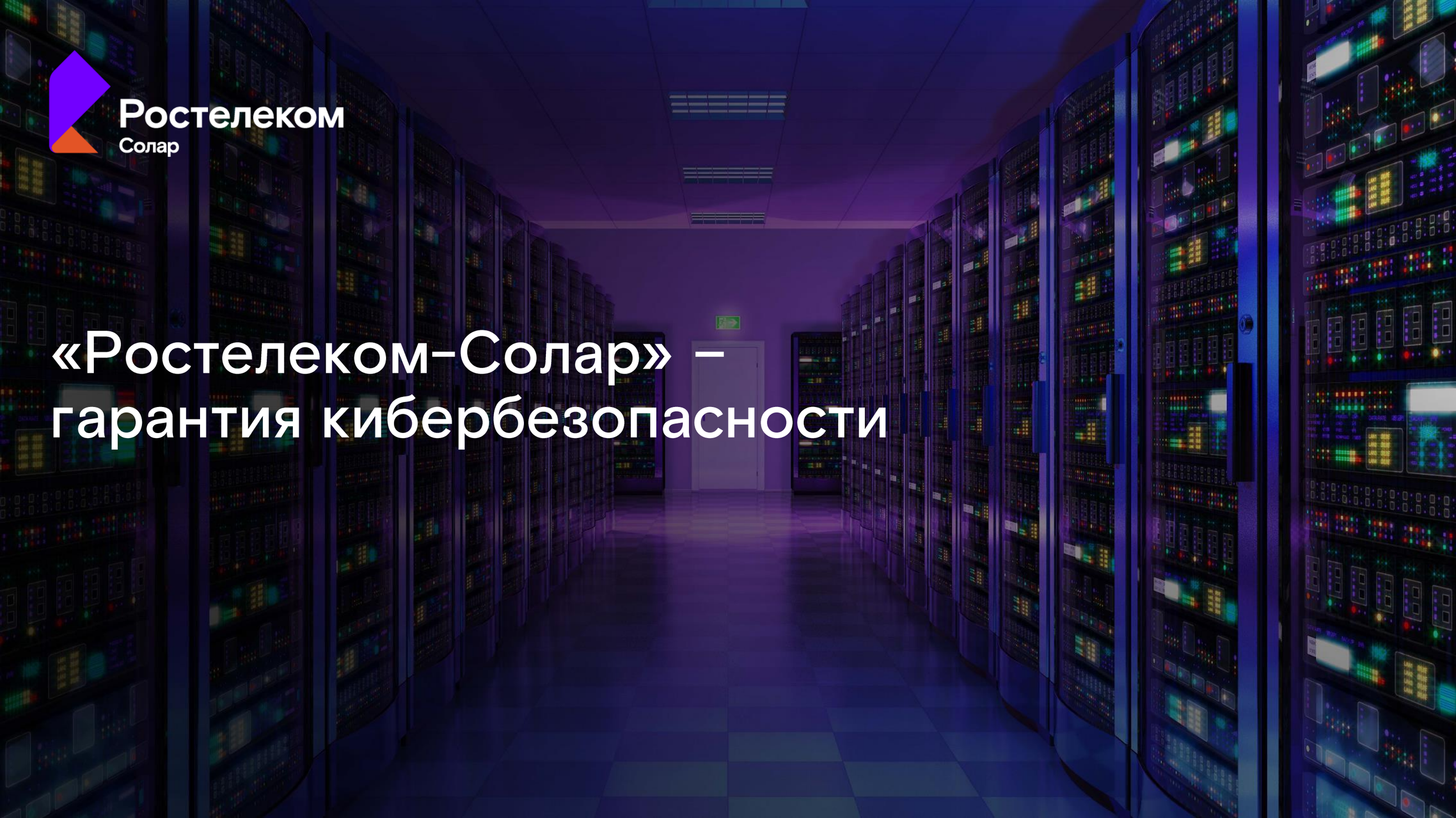


«Ростелеком-Солар» – гарантия кибербезопасности

О компании «Ростелеком-Солар»

Ростелеком
Солар

«Ростелеком-Солар» на рынке кибербезопасности

Защищаем цифровое будущее России

№1
на рынке сервисов кибербезопасности

1100+
экспертов по кибербезопасности

750+
организаций под защитой

24/7
обеспечение кибербезопасности

600+
реализованных проектов в год

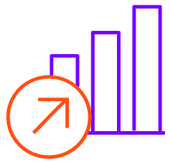
110+ млрд
анализируемых событий в сутки

Ростелеком Солар

Стратегия развития «Ростелеком-Солар»

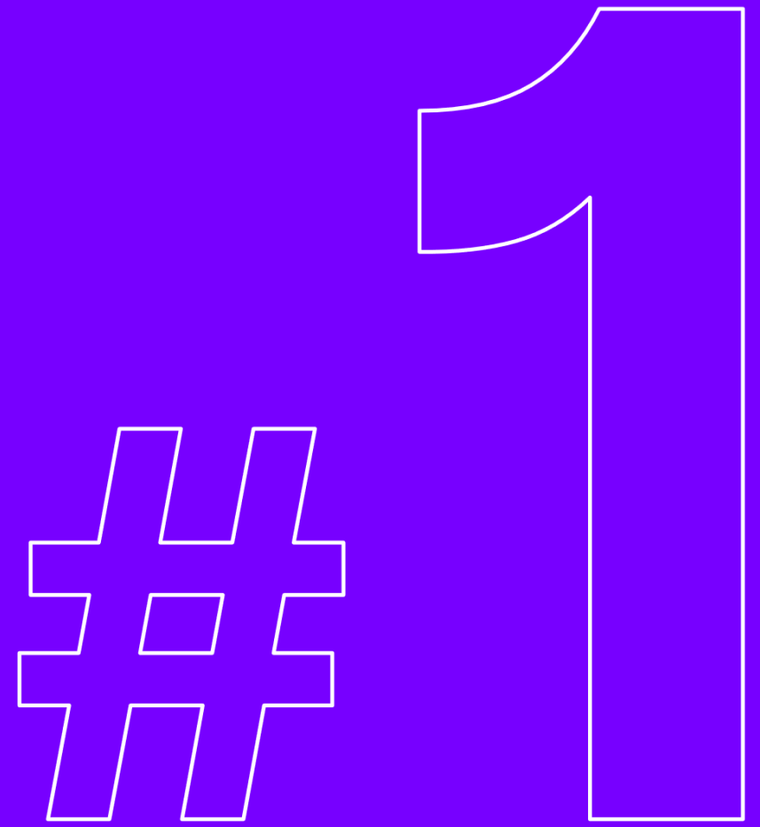
Всеобщий доступ к кибербезопасности за счет сервисной модели

Развитие собственных конкурентоспособных продуктов и технологий в востребованных и перспективных сегментах. Собственные продукты смогут обеспечить стратегическое преимущество



Сервисы кибербезопасности как ключевой элемент высокой ценности и долгосрочных отношений с клиентом. Сервисы обеспечивают опережающее развитие дистрибуции технологий по сервисной и аутсорсинговой модели

Инвестиции в развитие рынка кибербезопасности, формирование и стимулирование спроса, воспитание квалифицированных кадров для себя и для рынка



- Лидерство на рынке кибербезопасности в России
- Быть первыми в технологиях
- Быть первыми в клиентских взаимоотношениях

Ростелеком Солар

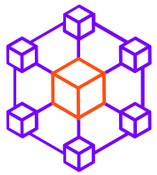
Преимущества сервисной модели

Просчитываемые ежемесячные платежи

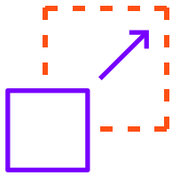
Устранение дефицита кадров

Быстрое подключение

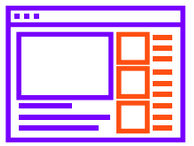
Контроль работы сервисов 24/7



Взаимодополняемые сервисы экосистемы



Простая масштабируемость



Личный кабинет с детальными отчетами

Соответствие законодательству РФ

Ростелеком Солар

Ценности «Ростелеком-Солар»

Лидерство и экспертность

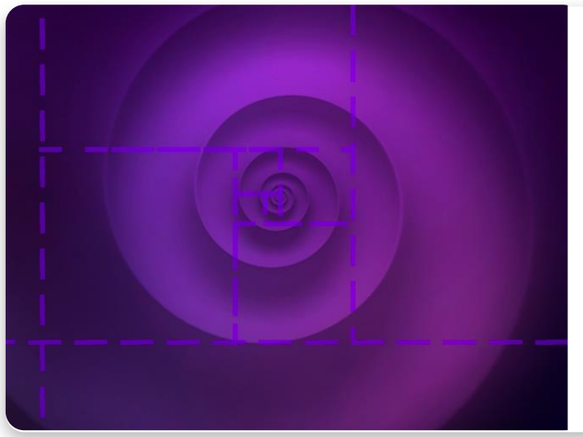
Мы верим, что кибербезопасность – наша ДНК, и гордимся тем, что в нашей команде работают лучшие эксперты

Предприимчивость и энергия

Мы ценим свободу от стереотипов и интерес ко всему новому, поэтому с энтузиазмом смотрим в будущее

Партнерство и ответственность

Мы ценим партнерские отношения с клиентами и друг другом, поэтому ответственно подходим к работе и всегда доводим дело до конца



Эстетика и простота

Мы ценим красоту во всем, что делаем, и считаем, что форма важна так же, как содержание

Ростелеком Солар

Ценности «Ростелеком-Солар» – наш культурный код

«Мы верим, что кибербезопасность – наша ДНК, и в нашей команде работают лучшие эксперты. Я горжусь теми проектами, которые мы делаем, и теми технологиями, которые мы развиваем. Наши ценности – это наш паттерн поведения внутри компании и за ее пределами, с клиентами и партнерами.

Заказчики нас выбирают потому, что мы можем им гарантировать результат. Наша цель – это лидерство на рынке: мы – компания номер один, обеспечивающая кибербезопасность России».

Игорь Валентинович Ляпунов

Генеральный директор «Ростелеком-Солар»,
вице-президент ПАО «Ростелеком» по информационной безопасности

Ростелеком Солар

История «Ростелеком-Солар»

2015

04.2015
Начало работы Solar Security

07.2015
Создание закрытого клуба «SOC в России»

09-10.2015
Выход Solar Dozor 6
Выход Solar inCode
Выход Solar inRights 2

11.2015
Первый SOC-Форум

2016

08.2016
Соглашение с ФинЦЕРТ Банка России об информационном обмене

10.2016
Выход на международный рынок

2017

09.2017
Solar JSOC защитил инфраструктуры заказчиков от атак шифровальщиков WannaCry и Petya

11.2017
Запуск направления по созданию центров ГосСОПКА

2018

05.2018
Приобретение «Ростелекомом» компании Solar Security

06.2018
Обеспечение кибербезопасности чемпионата мира по футболу FIFA 2018

11.2018
Запуск Единой платформы сервисов кибербезопасности

12.2018
Открытие офисов Solar JSOC в Самаре и Хабаровске

Ростелеком Солар

История «Ростелеком-Солар»

2019

01.2019
Выход Solar appScreener 3 (ранее – Solar inCode)

07.2019
Запуск Solar MSS – экосистемы сервисов кибербезопасности

08.2019
Выход Solar webProxy

09.2019
Запуск опорного центра киберполигона на Дальнем Востоке

09.2019
Открытие лаборатории кибербезопасности АСУ ТП

10.2019
Выход Solar Dozor 7 с модулем UBA

2020

02.2020
Запуск направления системной интеграции в сфере кибербезопасности

03.2020
Перевод большого количества федеральных клиентов на удаленную работу

05.2020
Выход MultiDozor

05.2020
Запуск услуги Red Teaming

08.2020
Бизнес-партнерство с компанией «Элвис-Плюс»

10.2020
Взрывное расширение сервисов Solar JSOC (NTA, EDR, IRP)

11.2020
Запуск киберполигона в образовательном центре «Сириус»

2021

05.2021
Официальное открытие Национального киберполигона

05.2021
Выход на рынок нового продукта Solar addVisor

05.2021
Выпуск совместного с НКЦКИ отчета об исследовании серии кибератак на органы государственной власти

06.2021
«Ростелеком-Солар» стал участником крупнейшего международного сообщества FIRST

09.2021
Открытие центра экспертизы по сервисам кибербезопасности Solar MSS в Самаре

Ростелеком Солар

Лицензии «Ростелеком-Солар»

- ФСБ России – на проведение работ, связанных с использованием сведений, составляющих государственную тайну
- ФСБ России – на разработку, производство и распространение шифровальных (криптографических) систем
- ФСТЭК России – на деятельность по технической защите конфиденциальности информации
- ФСТЭК России – на деятельность по разработке и производству средств защиты конфиденциальной информации
- ФСТЭК России – на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации)
- ФСТЭК России – на проведение работ, связанных с созданием средств защиты информации
- Минобороны России – на проведение работ, связанных с созданием средств защиты информации
- Соглашение с ФСБ России в рамках ГосСОПКА о взаимодействии по предупреждению кибератак
- Лицензия на осуществление образовательной деятельности

Ростелеком Солар

Наши заказчики

Банки и финансовые организации

Федеральные органы власти

Региональные органы власти

Электроэнергетика, добыча нефти и газа

Транспорт

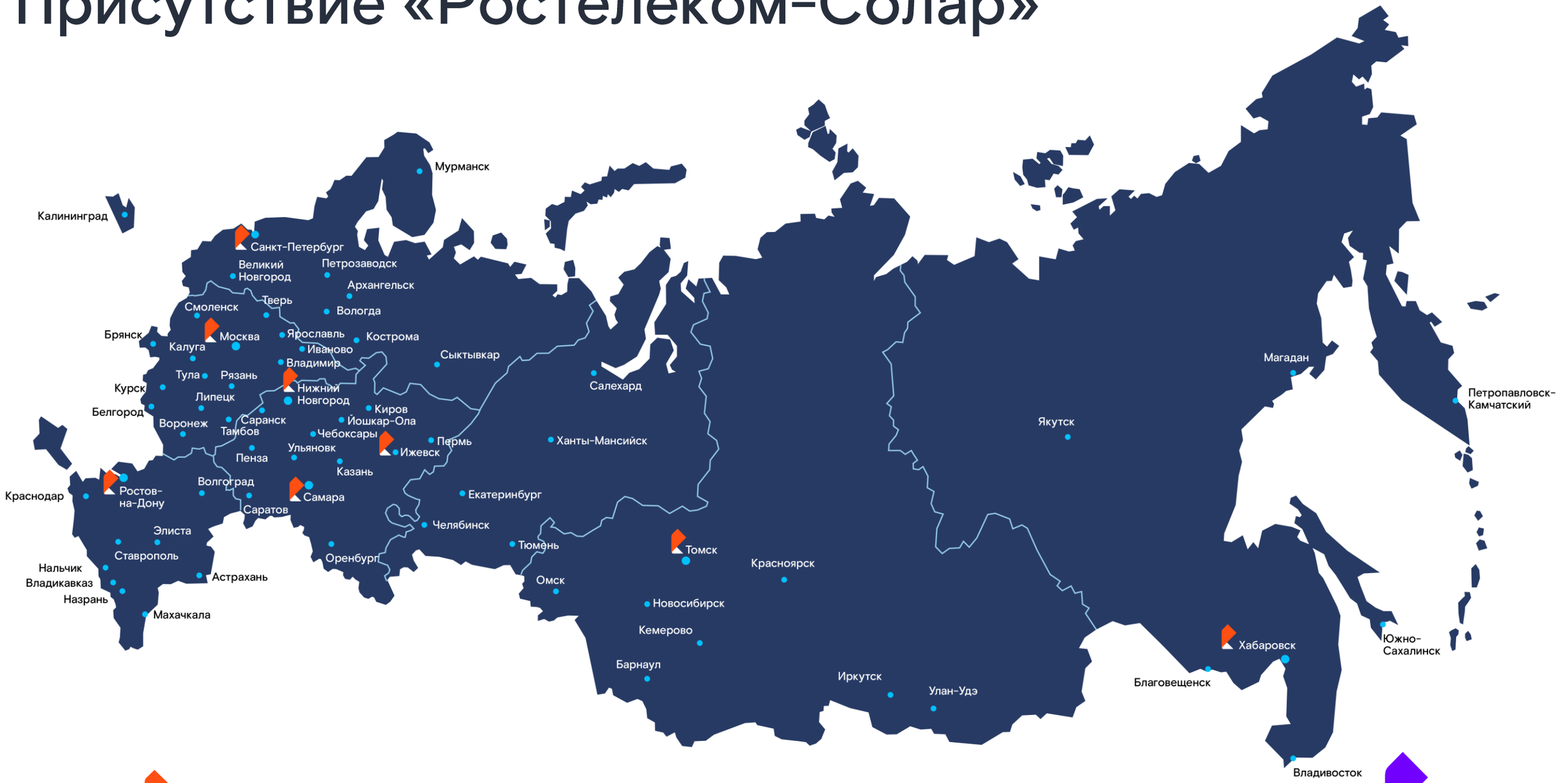
Промышленность

FMCG

Услуги для населения

Ростелеком Солар

Присутствие «Ростелеком-Солар»



Филиалы «Ростелеком-Солар»

Филиалы «Ростелеком»

Ростелеком Солар

Решение задач национального масштаба

Организация безопасного интернета в 45 000 школ по всей России

Создание системы защиты для предоставления безопасного интернета в образовательных учреждениях в 85 субъектах Российской Федерации

Безопасность Государственной единой облачной платформы (ГЕОП)

Обеспечение кибербезопасности при переводе информационных систем федеральных органов исполнительной власти в ГЕОП

Обеспечение безопасности чемпионата мира по футболу FIFA 2018

Оказание операционных сервисов кибербезопасности и обеспечение взаимодействия с ГосСОПКА на различных объектах

Защищенная сеть для Судебного департамента

Построение защищенной сети передачи данных между геораспределенными площадками по всей России всего за полгода

Комплексная безопасность для Генпрокуратуры РФ

Развитие и техническая поддержка защищенной сети по всей стране и обеспечение безопасности 20 000 рабочих мест сотрудников ведомства

Защита ИТ-инфраструктуры Единого правительственного комплекса

Обеспечение безопасности ИТ-инфраструктуры офисного здания и ЦОД в новом едином комплексе для федеральных органов исполнительной власти

Ростелеком Солар

Решение задач крупнейших российских компаний

Самое масштабное внедрение системы предотвращения утечек в Сбере

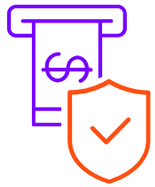
Обеспечение безопасности информационных активов всех подразделений Сбера на территории РФ и мониторинг 250 000+ рабочих станций

Защита от внутренних утечек ряда региональных предприятий «Газпрома»

Внедрение DLP-системы Solar Dozor, обеспечивающей контроль коммуникаций сотрудников для минимизации экономического ущерба

Центр оперативного управления и реагирования на инциденты «ФСК ЕЭС»

Команда Solar JSOC помогла запустить ЦОУР ИБ в сжатые сроки по сервисной модели



Защита единой телекоммуникационной сети для отделений ВТБ

Централизованное размещение всех информационных систем банка в едином защищенном ИТ-пространстве по всей стране

Создание центра мониторинга кибератак для «Трубной металлургической компании»

Созданный центр отслеживает угрозы безопасности и предотвращает атаки на инфраструктуру всех ключевых предприятий ТМК

Комплекс сервисов для защиты ГК «Содружество» от кибератак

«Ростелеком-Солар» обеспечивает кибербезопасность на всех этапах: от настройки и мониторинга систем до активного противодействия атакам

Ростелеком Солар

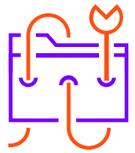
Инициативы «Ростелеком-Солар» в развитии отрасли кибербезопасности

- **Solar JSOC** – первый и крупнейший в России коммерческий центр противодействия кибератакам
- **Аналитический и исследовательский центр TI-CERT** – создание системы раннего оповещения о киберугрозах
- **Национальный киберполигон** – повышение квалификации сотрудников отрасли кибербезопасности
- **Образовательные проекты** по повышению киберграмотности населения
- **Программы стажировок** и переподготовки специалистов по кибербезопасности

Вызовы кибербезопасности

Ростелеком
Солар

Тренды кибератак в 2021 году

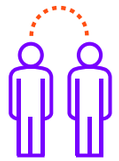


Основные типы атак через ВПО
и атаки на веб-приложения

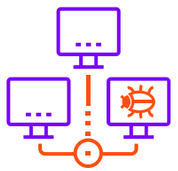
Повышение темпа использования
новых уязвимостей

Фишинг, смишинг и вишинг продолжают
набирать обороты

Рост популярности атак
через подрядчиков



Удаленная работа – основной катализатор
изменений



Расслоение подходов злоумышленников
к атакам на инфраструктуру

Ростелеком
Солар

Ландшафт киберугроз

17%

компаний способны эффективно сопротивляться кибератакам

По данным Accenture, 2020 г .

50,8%

событий удается выявить лишь с помощью сложных интеллектуальных средств защиты или анализа событий

По данным Solar JSOC, 2021 г.

68%

анализируемых компаний, где выявлена активность ВПО

По данным Positive Technologies, 2021 г.

x2

рост атак через подрядчиков на объекты КИИ

По данным Solar JSOC, 2021 г.

+30%

рост атак на получение контроля над инфраструктурой организации

По данным Solar JSOC, 2021 г.

207 дней

среднее время обнаружения компанией взлома ее инфраструктуры

По данным Ponemon Institute, 2020 г.

Ростелеком Солар

«Ростелеком» и НКЦКИ выявили серию масштабных кибератак на органы государственной власти

Цели атак

Кража конфиденциальной информации, в том числе внутренних «закрытых» документов

Закрепление в инфраструктуре, защита от «зачистки» – до 12 резервных каналов доступа

Получение полного доступа ко всем элементам ИТ-инфраструктуры

Чтение почтовой переписки

Уровни злоумышленников

УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
Киберхулиган/ энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
Киберкриминал/ организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, социнжиниринг
Кибернаемники/ продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
Кибервойска/ прогосударственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО и АО, разработанные и внедренные «закладки»

Ростелеком Солар

Решение задач крупнейших российских компаний

Для повышения защищенности при цифровизации компаний недостаточно линейного масштабирования традиционных подходов к кибербезопасности.

Предпосылки

Размывание границ защищаемых сетей

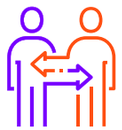
Удаленные доступы и работа с домашних компьютеров, использование частных и публичных облаков

Усложнение и ускорение изменений в ИТ-ландшафте

До 10 новых релизов ИТ-систем в месяц, регулярный перенос новых функций ведомства в онлайн

Неэффективность стандартных СЗИ при современных атаках

Вредоносное ПО не детектируемое антивирусами, уникальные для каждой системы инструменты взлома



Использование сотрудников в качестве точки доступа в организацию

Сотрудники, администраторы и подрядчики – основные векторы взлома (через фишинг) и источники утечек информации

Недостаток квалификации и дефицит специалистов по кибербезопасности

Потребность в значительном расширении службы кибербезопасности, в том числе в регионах, организации выполнения большинства функций 24/7

Повышение эффективности

1. Безопасность через мониторинг и управление
2. Безопасность через контроль действий пользователей и админов
3. Безопасность через системное обучение и воспитание персонала

Ростелеком Солар

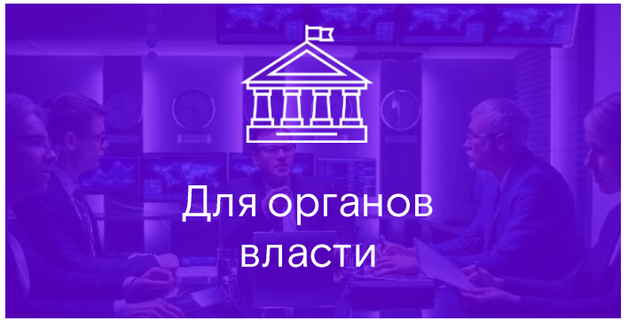
Подход «Ростелеком-Солар» к обеспечению кибербезопасности

Ростелеком
Солар

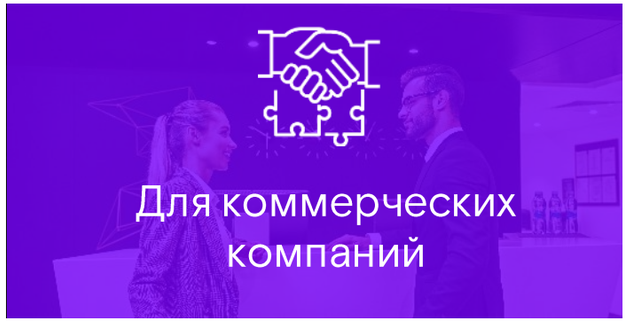
«Ростелеком-Солар» – гарантия кибербезопасности

Мы обеспечиваем и гарантируем кибербезопасность в организациях от малого бизнеса до федеральных органов власти. Наши технологии и распределенные по всей стране центры компетенций позволяют нам работать в режиме 24/7.

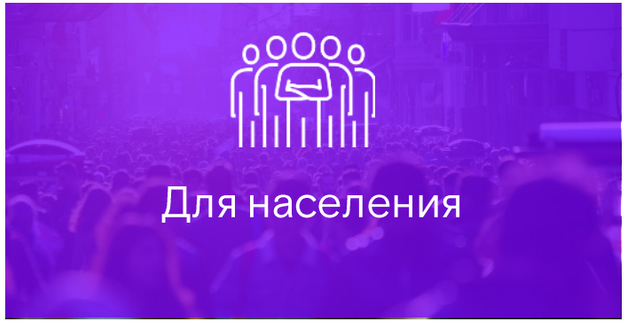
Наш комплексный подход включает в себя анализ угроз, предотвращение вторжений, построение и эксплуатацию систем кибербезопасности, что дает нам возможность нести ответственность за защиту от современных киберугроз.



Единая точка ответственности за кибербезопасность цифровой трансформации органов власти



Партнер, готовый взять ответственность за кибербезопасность компании



Центр экспертизы и помощник по повышению киберграмотности и защите от интернет-угроз

Ростелеком Солар

Комплексный подход «Ростелеком-Солар»

Подтвержденная готовность к отражению кибератак

Сбор данных и консалтинг

- Анализ защищенности и проведение тестирований на проникновение
- Консалтинг и комплексный аудит систем безопасности
- Разработка стратегии развития кибербезопасности и дорожной карты
- Выстраивание процессов кибербезопасности
- Обеспечение соответствия требованиям регуляторов
- Диагностический мониторинг

Оценка текущего состояния кибербезопасности в организации

Выстраивание архитектуры кибербезопасности с учетом бизнес-процессов организации

Технологии и инструменты защиты

- Защита периметра, рабочих станций, баз данных, почты, приложений и веб-сервисов
- Защита каналов связи
- Защита публичных и гибридных облаков
- Управление доступом к информационным системам и аутентификация пользователей
- Защита от внутренних утечек
- Выстраивание процессов безопасной разработки

Построение комплексной защиты на базе собственных продуктов, сервисов Solar MSS и решений сторонних партнеров

Обеспечение кибербезопасности

- Управление кибербезопасностью
- Защита от всех видов кибератак, мониторинг инцидентов
- Анализ угроз из внешней обстановки
- Комплексный контроль защищенности
- Проведение киберучений для специалистов по кибербезопасности
- Повышение квалификации и осведомленности сотрудников
- Техническая поддержка и сопровождение средств защиты

Обеспечение кибербезопасности с помощью Solar JSOC – центра противодействия кибератакам

Ростелеком Солар

Углубленная экспертиза по кибербезопасности

Лучшие компетенции по противодействию кибератакам

Защита от атак любого уровня сложности

- 300+ отраженных атак профессиональных киберпреступников в 2021 году силами экспертов Solar JSOC

Регулярный обмен информацией об атаках

- С российскими и международными организациями (FinCert, ГосСОПКА, НКЦКИ, First)
- Подключение к актуальным базам угроз

Экспертиза и постоянное изучение новых угроз

- Собственная исследовательская лаборатория Solar JSOC CERT
- Ежедневно актуализируемая база Threat Intelligence
- Лаборатория кибербезопасности АСУ ТП

Лучшие компетенции по построению и эксплуатации систем кибербезопасности

Истории успеха во всех отраслях

- Реализация проектов в организациях любого масштаба
- Построение систем кибербезопасности любого уровня сложности

Лучшая техническая экспертиза на рынке

- Собственные продукты – лидеры в своих сегментах
- Экспертиза по 60 российским и зарубежным технологиям

Многообразие сервисов кибербезопасности

- Удобное и мгновенное подключение
- Возможность выбора набора услуг и сервисов в зависимости от решаемых задач

Ростелеком Солар

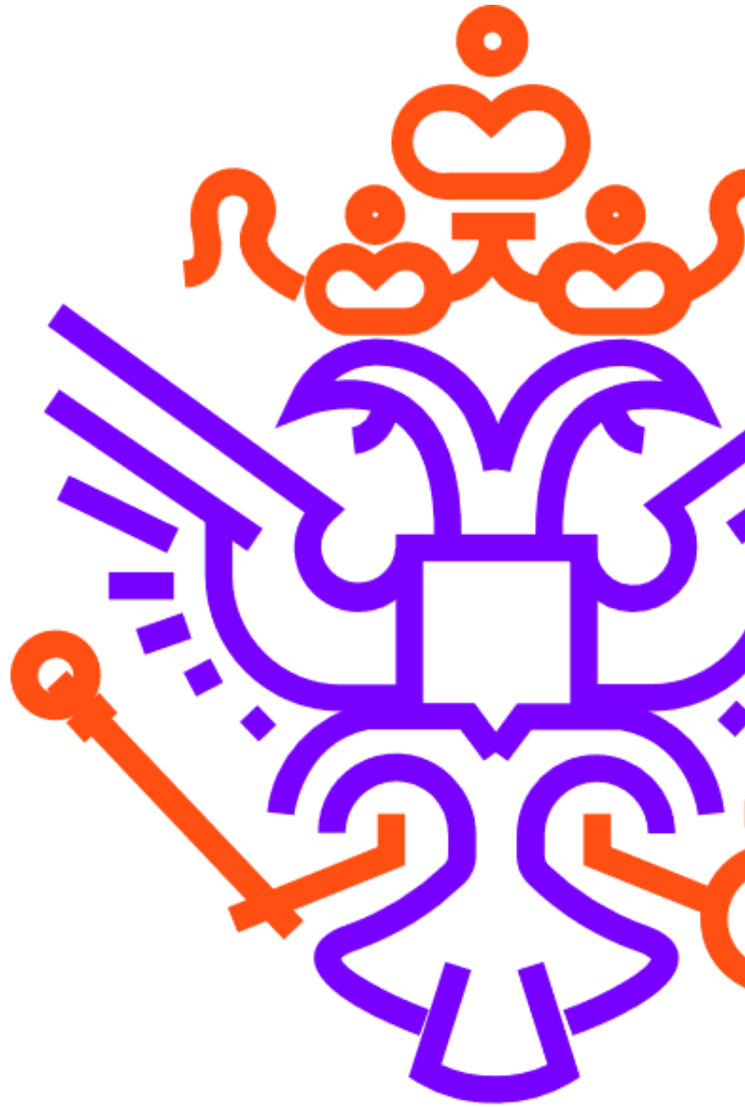
«Ростелеком» – ключевой партнер государства в цифровизации

«Ростелеком-Солар» – единая точка ответственности за реализацию и сопровождение комплексных проектов по безопасной цифровой трансформации органов власти

«Ростелеком» – ключевой партнер государства в цифровизации

№1

поставщик решений для цифровой трансформации органов власти



Реализация масштабных госпрограмм по построению цифровой инфраструктуры

Активная поддержка работы комитетов Минцифры и ФСТЭК России

Обеспечение требований ГосСОПКА «под ключ» и построение безопасных ГИС

Ростелеком Солар

Ключевые преимущества «Ростелеком-Солар» как поставщика услуг для органов власти

КРИТЕРИИ ВЫБОРА ПОСТАВЩИКА	«РОСТЕЛЕКОМ-СОЛАР»
Принятие обязательств: поставщик разделяет ответственность за реализацию киберзащиты и отвечает за кибербезопасность организации, в том числе перед регуляторами	✓
Наличие всех необходимых лицензий регуляторов: поставщик является лицензиатом ФСТЭК России, ФСБ России, Минобороны России, выполняет функции центра ГосСОПКА, сотрудничает с НКЦКИ и ФинЦЕРТ	✓
Прозрачное расходование средств: поставщик предоставляет четкую и понятную структуру расходов и необходимые подтверждающие документы и компетентен в процедурах госзакупок	✓
Решение задач импортозамещения: решения поставщика входят в реестр отечественного ПО	✓
Надежность: поставщик располагает большим штатом экспертов и имеет на рынке многолетнюю надежную репутацию лидера технологий кибербезопасности	✓

Ростелеком Солар

Решение задач государственных организаций

За счет собственных разработок

- Защита от утечек информации
- Контроль соблюдения Кодекса этики и служебного поведения служащих
- Реализация политики использования сети «интернет»
- Управление доступом к информации
- Контроль безопасности кода

За счет собственных сервисов

- Раннее предупреждение, выявление и реагирование на кибератаки
- Оценка рисков и управление уязвимостями
- Шифрование каналов связи
- Повышение квалификации и осведомленности сотрудников
- Защита веб-порталов и приложений

За счет интеграционных услуг

- Комплексный подход к решению задач кибербезопасности
- Защита ГИС и их аттестация в соответствии с требованиями регуляторов
- Защита периметра, ИТ-инфраструктуры, рабочих станций, ЦОД
- Обеспечение выполнения требований законодательства

Ростелеком Солар

«Ростелеком-Солар» – ответственный партнер в обеспечении реальной защиты бизнеса

«Ростелеком-Солар» – команда, которая понимает, как угрозы кибербезопасности отражаются на деятельности компании, и умеет их предотвращать

«Ростелеком-Солар» – партнер в обеспечении защиты бизнеса

Риск-центрированный подход

к обеспечению и управлению кибербезопасностью

Сбалансированное повышение уровня защищенности, соответствующее уровню цифровизации компании

Удобный и простой доступ к экспертизе «Ростелеком-Солар» в режиме 24/7 во всех регионах России

Эффективность расходования средств и высвобождение ресурсов для развития бизнеса и ИТ

Ростелеком Солар

Ключевые преимущества «Ростелеком-Солар» как поставщика услуг для коммерческих организаций

КРИТЕРИИ ВЫБОРА ПОСТАВЩИКА	«РОСТЕЛЕКОМ-СОЛАР»
Принятие ответственности: поставщик отвечает за результат проекта по кибербезопасности и разделяет ответственность за полное обеспечение киберзащиты компании	
Экспертность: сотрудники поставщика – лучшие эксперты, которые создают передовые продукты и технологии и делают компанию лидером отрасли	
Прозрачность и простота взаимодействия: поставщик сопоставляет стоимость возникновения рисков с мерами защиты и предлагает заказчику решение, оптимальное не только по качеству, но и по цене	
Комплексность: поставщик обеспечивает защиту инфраструктуры в комплексе, осознавая, что любая инфраструктура может стать объектом атаки, и защищает не только критичные объекты, но и некритичные	
Надежность: заказчики готовы рекомендовать поставщика и регулярно обращаются к нему за новыми решениями и услугами	

Ростелеком Солар

Решение задач коммерческих компаний

За счет собственных разработок

- Защита от утечек информации, включая коммерческую тайну
- Контроль действий сотрудников и повышение эффективности их работы
- Контроль доступа к веб-ресурсам
- Защита от вредоносного ПО и навязчивой рекламы
- Полноценный контроль доступа к информационным ресурсам
- Обеспечение безопасного процесса разработки

За счет собственных сервисов

- Раннее предупреждение, выявление и реагирование на кибератаки
- Оценка рисков и управление уязвимостями
- Повышение квалификации и осведомленности сотрудников
- Защита онлайн-сервисов и веб-приложений
- Управление кибербезопасностью

За счет интеграционных услуг

- Комплексный подход к решению задач кибербезопасности
- Разработка стратегии развития кибербезопасности
- Защита периметра, ИТ-инфраструктуры, рабочих станций, ЦОД
- Защита бизнес-приложений и данных
- Обеспечение выполнения требований законодательства

Ростелеком Солар

Полный цикл обеспечения кибербезопасности

Аудит
и приведение
в соответствие требованиям

Экспертиза «Ростелеком-Солар»
и полный контроль со стороны
заказчика

Единая точка ответственности
со стороны «Ростелеком-Солар»

Разработка
стратегии

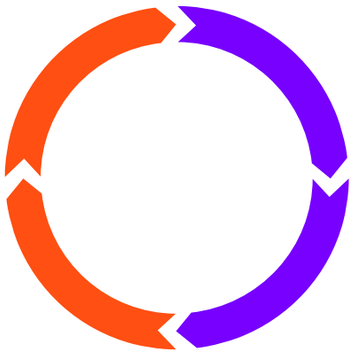
Интеграционная модель

Техническая
поддержка

Тестирование

Внедрение
и настройка

Построение



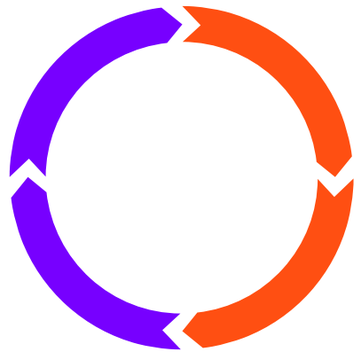
Сервисная модель

Отслеживание
изменений

Быстрое
подключение

Устранение
дефицита
ресурсов

Непрерывная
защита



Развитие

Ростелеком
Солар

Продуктовый портфель «Ростелеком-Солар»

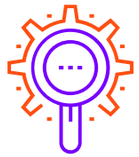
Ростелеком
Солар

Структура бизнеса компании «Ростелеком-Солар» включает четыре ключевых направления

Непрерывное развитие продуктового портфеля и технологий кибербезопасности позволяет предлагать заказчикам решения, максимально отвечающие их потребностям.

Ростелеком Солар

Продуктовый портфель «Ростелеком-Солар»



Сервисы

- Solar JSOC – первый и крупнейший в России коммерческий центр противодействия кибератакам
- Solar MSS – экосистема управляемых сервисов кибербезопасности по подписке

Технологии

- Solar Dozor – предотвращение утечек информации
- Solar webProxy – контроль доступа к веб-ресурсам
- Solar appScreener – анализ кода приложений
- Solar inRights – управление правами доступа
- Solar addVisor – организационное развитие и оценка продуктивности труда

Интеграция

Solar Интеграция

- Реализация комплексных проектов по кибербезопасности
- Кибербезопасность объектов КИИ и АСУ ТП

Киберполигон

- Национальный киберполигон – повышение квалификации сотрудников отрасли кибербезопасности

Ростелеком Солар

Сервисы

Ростелеком
Солар

Solar JSOC – первый и крупнейший в России коммерческий центр противодействия кибератакам

Solar JSOC

Solar JSOC

Первый и крупнейший в России коммерческий центр противодействия кибератакам, действующий по модели MDR (Managed Detection and Response). Обеспечивает защиту крупных государственных и коммерческих организаций от киберугроз и оказывает помощь другим корпоративным SOC.

Предотвращение

Разведка и раннее предупреждение об угрозах, оценка рисков и управление уязвимостями

Выявление

Расширенные возможности мониторинга и анализа событий кибербезопасности 24/7, противодействие атакам на ранней стадии

Реагирование

Оперативное техническое расследование, ликвидация последствий и устранение причин возникновения инцидентов

Построение SOC и консалтинг

Помощь в создании и совершенствовании центров управления кибербезопасностью

№1
на рынке SOC в России

350+
экспертов по кибербезопасности

190+
клиентов из всех отраслей экономики

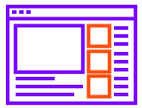
110+
млрд анализируемых событий в сутки

10 минут
на обнаружение кибератаки

30 минут
на реагирование и защиту

Ростелеком Солар

Экосистема сервисов Solar JSOC



Мониторинг инцидентов

- Мониторинг и анализ инцидентов
- Анализ сетевого трафика (NTA)
- Защита конечных точек (EDR)
- Мониторинг бизнес-систем
- Мониторинг АСУ ТП
- Сервисы ГосСОПКА

Комплексный контроль защищенности

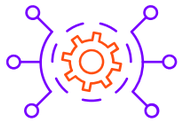
- Тестирование на проникновение
- Анализ защищенности
- Социотехническое исследование
- Assumed Breach
- Red Teaming
- Анализ рисков и обследование инфраструктуры
- Оценка зрелости технической защиты

Расследование и реагирование на инциденты

- Управление процессами реагирования на киберинциденты (IRP)
- Разработка плейбуков
- Incident Response
- Техническое расследование инцидентов

Анализ угроз и внешней обстановки

- Кибербразведка



Построение SOC и его частных процессов

- Построение SOC
- Консалтинг

Ростелеком Солар

Преимущества Solar JSOC

Защита от атак любого уровня сложности

- Полный цикл экспертизы в управлении инцидентами
- Реальный опыт противодействия злоумышленникам продвинутых уровней

Настоящие 24/7, а не дежурные смены

- 6 филиалов в разных часовых поясах
- Круглосуточная доступность бизнес-аналитика для решения сложных инцидентов, а не только инженера 1-й линии

Экономическая выгода и удобство

- Сокращение затрат, устранение «кадрового голода»
- Сценарии сотрудничества: сервисная и гибридная модели, помощь в построении SOC, консалтинг

Экспертиза и постоянное изучение новых угроз

- Собственная лаборатория Solar JSOC CERT и ежедневно обновляемая база знаний о новых атаках
- Доступ к экспертной интерпретации рисков и консультациям по смягчению последствий

Истории успеха во всех отраслях

- Отработанные процессы выявления и реагирования на кибератаки
- Специализированные сценарии и применение отраслевых индикаторов компрометации, в том числе для АСУ ТП

Уровень сервиса

- Выделенная команда из сервис-менеджера и аналитика-эксперта
- Исполнение SLA – 99,5%

Прозрачность

- Удобная отчетность и визуализация данных

Ростелеком Солар

Solar MSS – крупнейшая в России экосистема сервисов кибербезопасности по подписке

Solar MSS

Solar MSS – крупнейшая в России экосистема сервисов кибербезопасности по подписке. Сервисы защищают от всего спектра угроз и решают комплексные задачи кибербезопасности.

Эксперты «Ростелеком-Солар» осуществляют все работы с учетом специфики каждого региона, профиля и масштаба компании в режиме 24/7.

Разнообразие технологий в составе экосистемы и партнерство с ведущими поставщиками кибербезопасности позволяют предоставить клиентам широкий выбор вариантов сервисов и снизить санкционные риски.

Сервисы Solar MSS объединены в экосистему на трех уровнях:

Технологический

Обмен информацией между сервисами и создание общих политик безопасности

Пользовательский

Единая точка взаимодействия с клиентом и визуализации работы

Аналитический

Оценка эффективности решения комплексных задач

Ростелеком Солар

Экосистема сервисов и решений Solar MSS

Сервисы

Защита от конкретных угроз кибербезопасности

- Защита от сетевых угроз
- Защита электронной почты
- Контроль уязвимостей
- Защита от продвинутых угроз
- Управление навыками кибербезопасности
- Шифрование каналов связи – ГОСТ VPN
- Защита от DDoS-атак
- Защита веб-приложений
- Контентная фильтрация
- Регистрация и анализ событий кибербезопасности

Решения

Комплексные решения для защиты от целого спектра угроз с фокусом на бизнесе

- Защита от фишинга и шифровальщиков
- Защита онлайна

Ростелеком Солар

Преимущества Solar MSS

Просто

Оперативность
от 2 дней нужно для подключения сервисов и решений

70%
сервисов и решений экосистемы подключаются без вмешательства в инфраструктуру

Прозрачность
удобное управление и визуализация работы сервисов в личном кабинете

Выгодно

Гибкость
большое количество тарифов для разных потребностей клиентов

40%
средняя экономия на горизонте 5 лет в сравнении с классической моделью закупки и внедрения технологий

Комплексность
решение задач клиентов вместо обычного предоставления средств защиты в аренду

Надежно

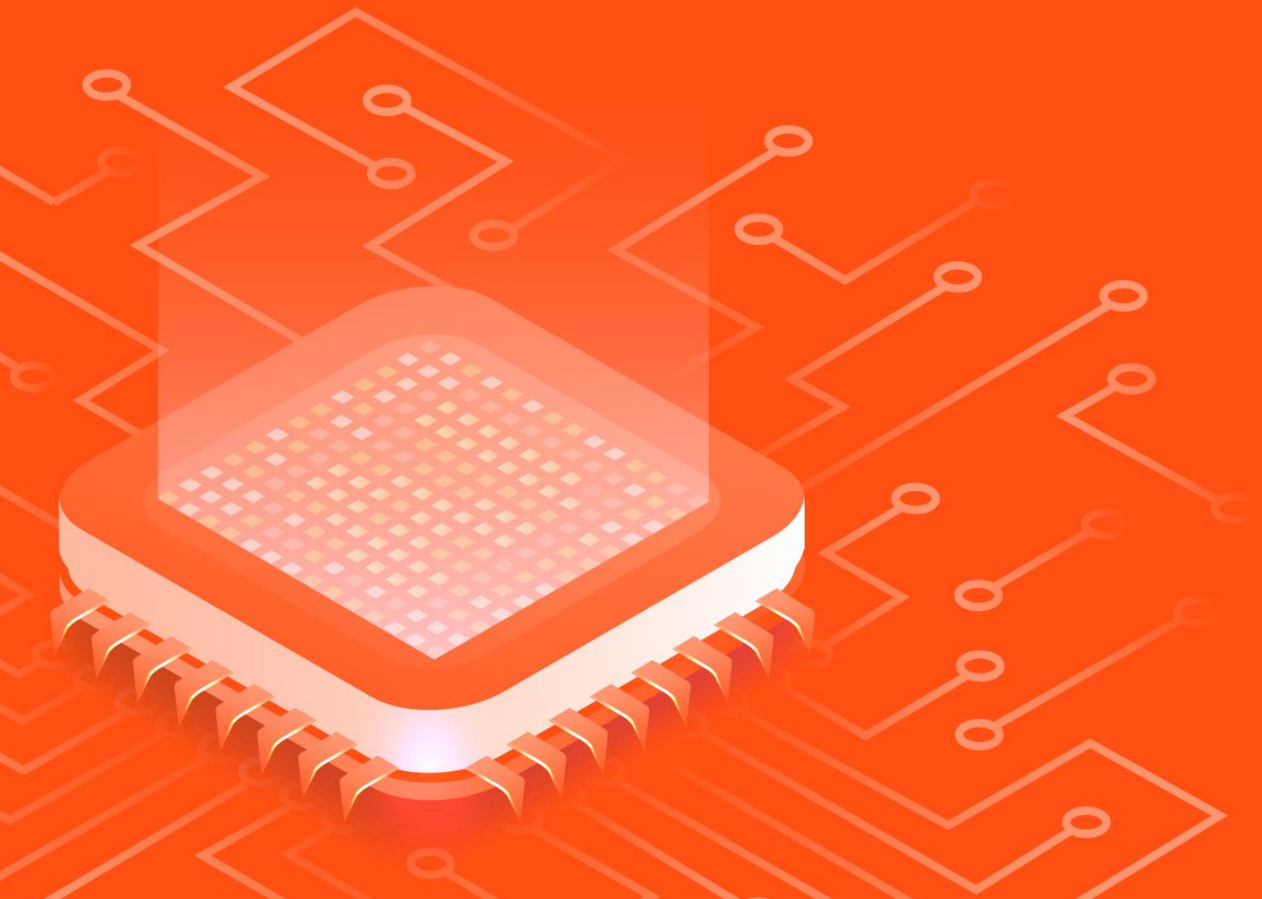
Ответственность
финансовая ответственность в рамках договорных обязательств

99,5%
стандартный гарантированный уровень оказания сервисов (Service Level Agreement, SLA)

Отказоустойчивость
12 500 стоек в современных ЦОД класса Tier III

Ростелеком Солар

Технологии



Ростелеком
Солар

Solar Dozor – система предотвращения утечек (DLP)

Solar
Dozor

Solar Dozor – система предотвращения утечек (DLP)

Блокирует утечки информации, выявляет аномалии в поведении пользователей и помогает обнаружить ранние признаки корпоративного мошенничества.

Решаемые задачи:

01 Предотвращение утечек информации

02 Проведение расследований по персоне или группе персон

03 Выявление ранних признаков корпоративного мошенничества и коррупции

04 Мониторинг групп особого контроля

05 Выявление признаков аномального поведения сотрудников

06 Контроль рабочего времени

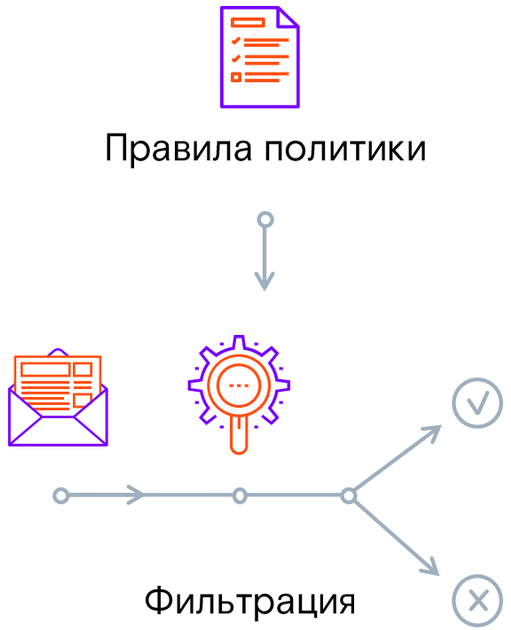
Ростелеком Солар

Принцип работы Solar Dozor 7

Перехват

- Корпоративная почта
- Веб-почта
- Печать
- Мессенджеры
- Публикации в сети
- Съемные носители
- Веб-запросы
- Файловые ресурсы

Фильрация



Анализ

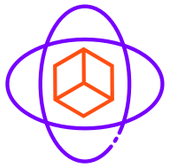
- Досье на персоны и группы
- Досье на информацию
- Аналитика и отчетность
- Анализ поведения пользователей
- Управление событиями и инцидентами
- Архив коммуникаций

Ростелеком Солар

Ключевые преимущества Solar Dozor

Высокая производительность

Держит нагрузку в 250 000+ пользователей



Единая технологическая платформа

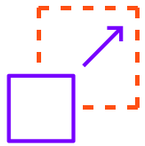
Полная интеграция модулей, единая консоль

Безопасность с фокусом на человеке

Единая концепция, лучшие Досье, UBA, ГрОК*

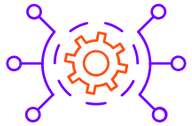
Лучшая геораспределенная DLP

Поддержка филиалов, единое управление



Масштабируемость

Как вертикальная, так и горизонтальная



Передовые технологии

Нейронные сверточные сети, UBA, VDI

Лучший краулер

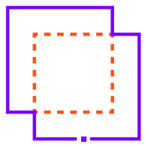
Построение карты сети, активный режим

Лучший долгосрочный архив

Хранение 1000+ ТБ данных сроком 10+ лет

Готов к импортозамещению

Российское ПО, лучший агент для Linux



Интеграция с Solar webProxy

Единое Досье, блокировка веб-доступа

*Мониторинг групп особого контроля

Ростелеком Солар

Solar webProxy – шлюз веб-безопасности (SWG)

Solar webProxy

Solar webProxy – шлюз веб-безопасности (SWG)

Контролирует доступ сотрудников и приложений к веб-ресурсам и защищает от вредоносного ПО и навязчивой рекламы, которые они могут содержать.

Решаемые задачи:

01 Контроль доступа сотрудников и приложений к веб-ресурсам

02 Контроль доступа удаленных сотрудников к корпоративным веб-ресурсам и OWA

03 Расшифровка HTTPS-трафика для его проверки другими СЗИ (DLP, AV и т. д.)

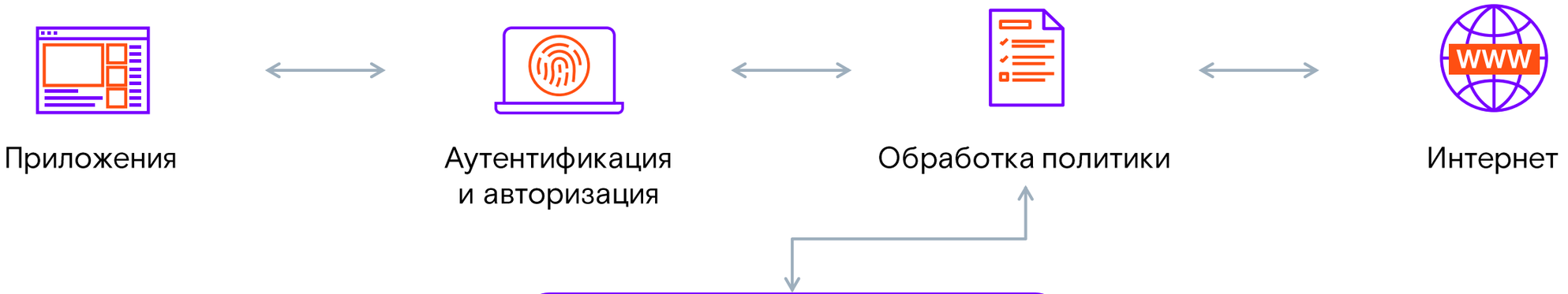
04 Проверка веб-трафика по ключевым словам для предотвращения утечек информации

05 Категоризация сайтов для защиты от вредоносного ПО и фишинга

06 Блокировка навязчивой рекламы

Ростелеком Солар

Общий принцип работы Solar webProxy



- Встроенным антивирусным модулем
- Любыми внешними системами по ICAP

- Источников соединений
- Назначений соединений: URL, категорий
- HTTP-заголовков: Referer, User-Agent
- Атрибутов файлов: имен, контрольных сумм
- Расписания действия политики

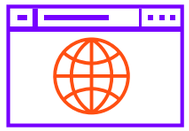
- Ключевых слов
- Типов получаемых и отправляемых файлов
- Размера получаемых и отправляемых данных
- Лимитов трафика

Ростелеком Солар

Ключевые преимущества Solar webProxy

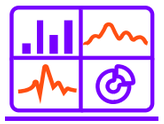
Высокая производительность

Держит нагрузку в 100 000+ пользователей



Веб-интерфейс

Единый, простой и удобный

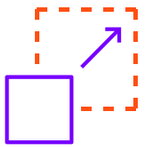


Встроенная система отчетов

Гибкая, наглядная и интерактивная

Гибкая аутентификация

По разным протоколам



Масштабируемость

Как вертикальная, так и горизонтальная

Минимальная стоимость

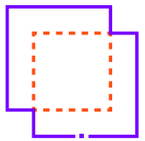
Мощные базовые функции, доступные цены

Собственный категоризатор

Который ежедневно обновляется

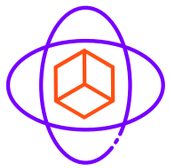
Политики фильтрации

Готовые, автоматически обновляемые



Интеграция с Solar Dozor

Единое Досье, блокировка веб-доступа



Виртуальное исполнение

Легко развернуть, легко обновлять

Ростелеком Солар

Solar addVisor – организационное развитие и оценка продуктивности труда (EPM)

Solar addVisor – организационное развитие и оценка продуктивности труда (EPM)

Помогает оптимизировать управление организацией, подразделением и сотрудниками.

Решаемые задачи:

01 Организация рабочих процессов

02 Повышение операционной эффективности организации

03 Оптимизация численности персонала

04 Обеспечение трудовой дисциплины

05 Категоризация сайтов для защиты от вредоносного ПО и фишинга

Ростелеком Солар

Общий принцип работы Solar addVisor

Ростелеком Солар

Ключевые преимущества Solar addVisor

Объективность

Применение математических моделей помогает сформировать единый подход к должностям и компетенциям, выявляя лидеров и ключевых сотрудников. Управлять организационной структурой становится проще

Фокус на главном

Вместо того чтобы концентрироваться на учете рабочего времени или выгорании сотрудников, Solar addVisor позволяет работать с причинами проблем — оценивать производительность труда и заниматься организационным развитием

Безопасность

Вся собранная информация хранится на серверах заказчика и не передается в облако, конфиденциальность личной переписки и персональных данных сохраняется, а экспертиза в области кибербезопасности позволяет разговаривать на одном языке со службой безопасности

Легкое внедрение

Solar addVisor не требует значительных ресурсов и времени на внедрение. Агенты для рабочих компьютеров сотрудников не нуждаются в большом объеме вычислительных ресурсов и не влияют на удобство работы

Ростелеком Солар

Solar inRights – управление правами доступа пользователей (IGA)

Solar inRights – управление правами доступа пользователей (IGA)

Помогает выстроить эффективные процедуры исполнения регламентов, а также профилактику и расследование инцидентов кибербезопасности в части управления правами доступа.

Решаемые задачи:

01 Исполнение регламентов управления доступом

02 Сокращение числа инцидентов, связанных с избыточными правами доступа

03 Управление жизненным циклом учетных записей и ролей

04 Снижение нагрузки на ИТ-специалистов и экспертов по кибербезопасности

05 Создание единого окна по обслуживанию пользователей

06 Быстрый аудит прав доступа к информационным системам

07 Эффективное расследование инцидентов, связанных с правами доступа

08 Снижение рисков кибербезопасности

Ростелеком Солар

Принцип работы Solar inRights

- Solar inRights получает данные о сотрудниках и организационно-штатной структуре из кадровой системы
- Solar inRights двусторонне интегрирован с целевыми системами с помощью программных коннекторов
- В Solar inRights автоматизируются процессы управления доступом и контроль
- Процессы могут исполняться полностью автоматически или требовать участия сотрудников для согласования
- Пользователи взаимодействуют с Solar inRights через веб-интерфейс

Ростелеком Солар

Ключевые преимущества Solar inRights

Понятный интерфейс

Интерфейс разработан экспертами по UI, клиенты признают его одним из самых удобных среди IdM-систем

Адаптация под нужды компании

Система легко кастомизируется под конкретные требования организации

Соответствие требованиям

Платформа Solar inRights имеет сертификат ФСТЭК и внесена в реестр российского ПО

Быстрое внедрение

5 недель – самый короткий проект внедрения продукта для организации в несколько тысяч сотрудников

Большая команда экспертов

Крупнейшая на российском рынке команда в сфере IdM, включающая архитекторов, аналитиков, разработчиков, тестировщиков и других специалистов

Мощная система провижининга

Управление не только учетными записями, но и смежными объектами, такими как папки, группы и т. д.

Ростелеком Солар

Solar appScreener – статический анализ безопасности приложений (SAST)

Solar appScreener – статический анализ безопасности приложений (SAST)

Проводит статический анализ безопасности информационных систем и приложений (SAST), проверяя как исходный код, так и исполняемые файлы.

Решаемые задачи:

Для экспертов по кибербезопасности

01 Самостоятельный анализ приложений на уязвимости без привлечения разработчиков

02 Снижение рисков кибербезопасности, получение подробных рекомендаций по настройке WAF

03 Контроль разработчиков приложений и компаний-подрядчиков, проверка унаследованного ПО

Для разработчиков

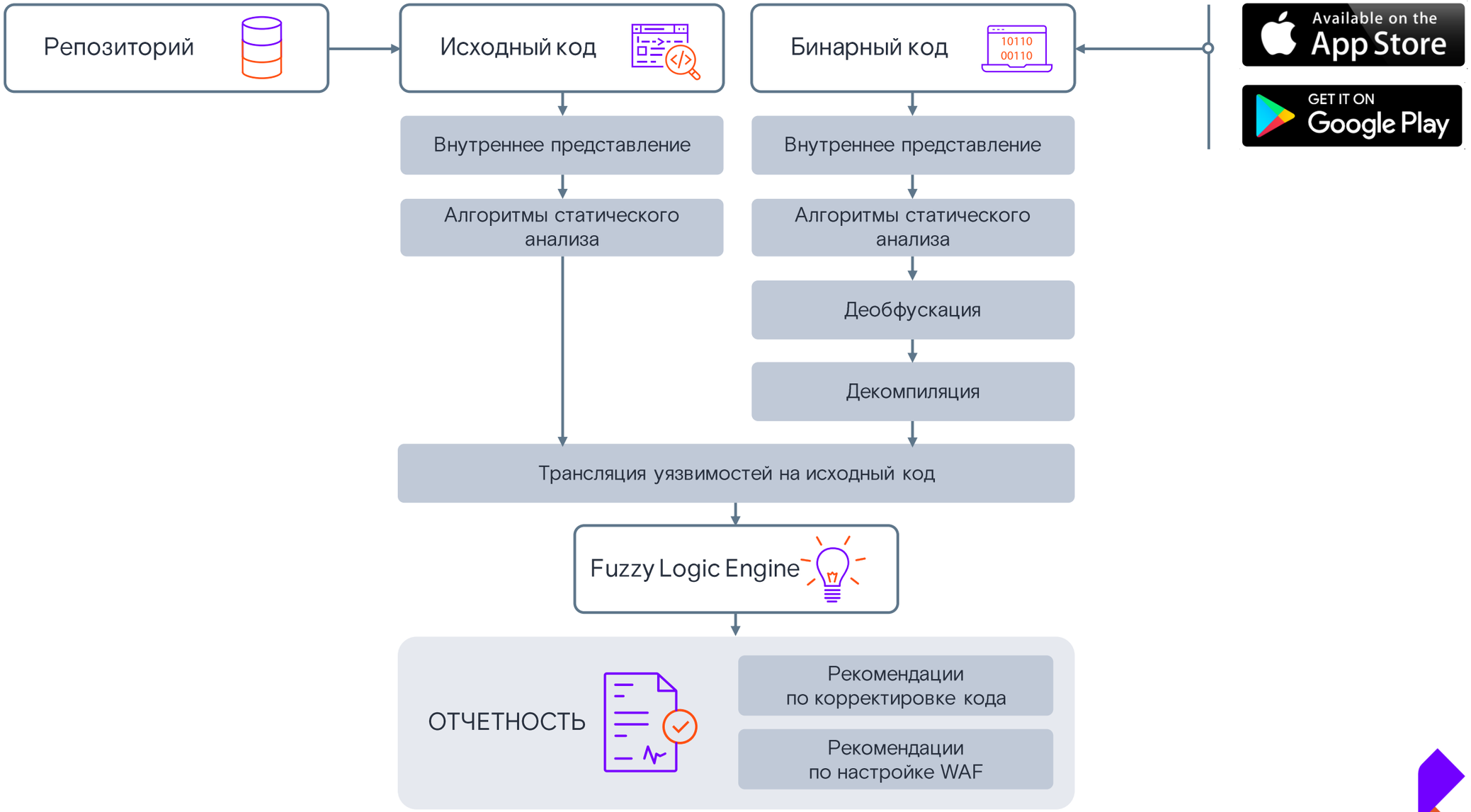
01 Раннее обнаружение и устранение уязвимостей до релиза приложения

02 Встраивание анализа кода в цикл безопасной разработки (Secure SDLC) и обеспечение DevSecOps

03 Повышение качества кода благодаря снижению числа уязвимостей в разрабатываемых приложениях

Ростелеком Солар

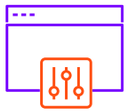
Принцип работы Solar appScreener



Ростелеком Солар

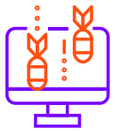
Ключевые преимущества Solar appScreener

Умеет работать без исходных кодов – можно получить исполняемый файл для анализа у системного администратора или использовать ссылку на приложение в Google Play или App Store



Не требует опыта разработки и рассчитан на службу кибербезопасности. Интерфейс отличается простотой, а сам анализ максимально автоматизирован

Единственный в мире анализатор кода с поддержкой 36 языков программирования



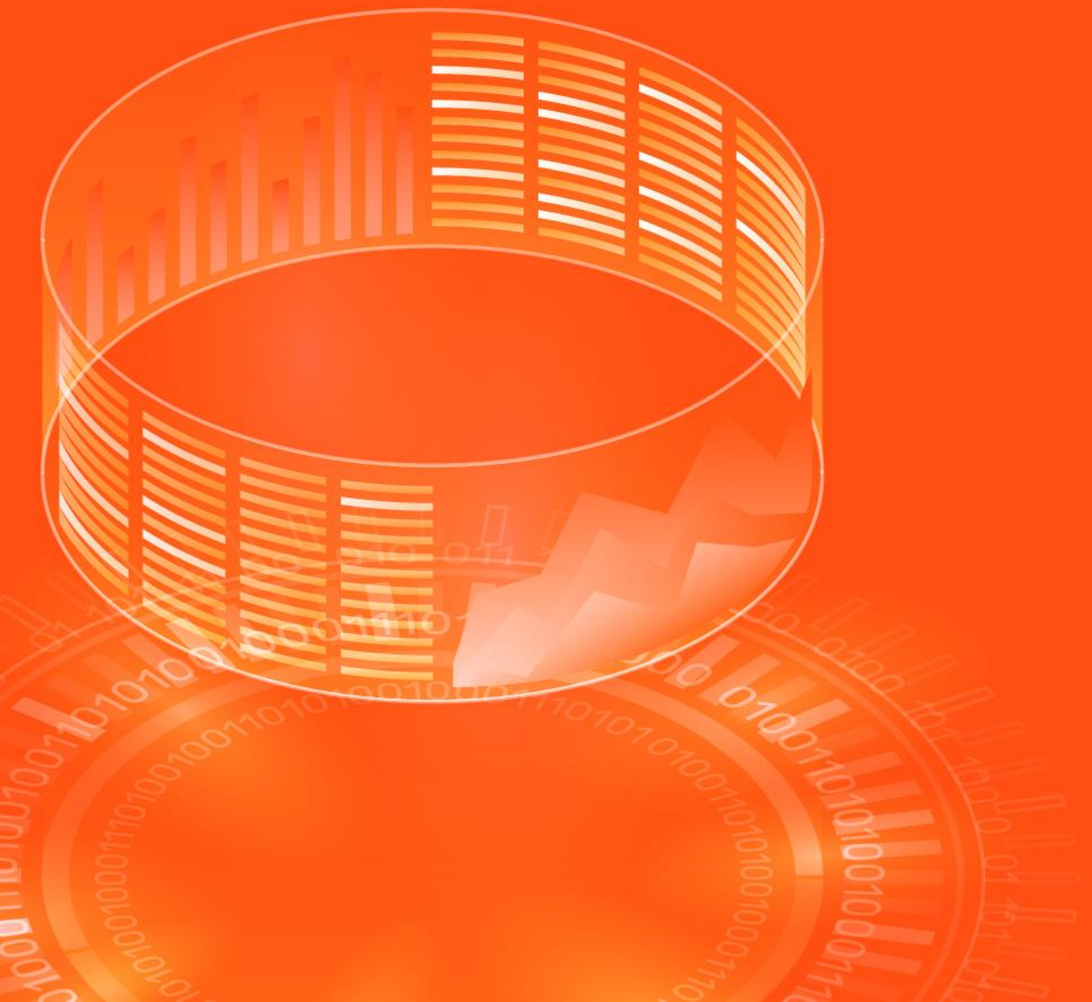
Минимизирует процент ложных срабатываний благодаря уникальной технологии Fuzzy Logic Engine

Дает подробные описания найденных уязвимостей и НДВ, а также рекомендации по настройке WAF

Отчеты могут формироваться в соответствии с классификацией уязвимостей по версии PCI DSS, БДУ ФСТЭК России, ОУД4, OWASP Top 10 и др.

Ростелеком Солар

Киберполигон



Ростелеком
Солар

Национальный киберполигон – повышение квалификации сотрудников отрасли кибербезопасности

Национа
киберполи

Национальный киберполигон

На киберполигоне эмулируется типовая инфраструктура выбранной отрасли, включая сетевую часть, конкретные сервисы, приложения, инструменты и т. д.

Это дает возможность:

- на практике освоить лучшие средства и методы защиты информации
- подготовиться к реальным актуальным атакам
- научиться защищаться от атак в реальном времени
- объективно оценить уровень знаний специалистов
- выявить и закрыть уязвимости инфраструктуры

На такой эмулированной площадке можно безопасно тренировать специалистов во время наиболее актуальных и деструктивных атак, отрабатывать навыки реагирования на инциденты, анализа защищенности, обнаружения компьютерных атак и защиты от них, работы в команде, оттачивать мастерство Blue- и Red-команд, а также рядовых специалистов по кибербезопасности.

Сервисы Национального киберполигона

Что это такое

Проект в рамках программы «Цифровая экономика», в ходе которого «Ростелеком-Солар» разработала свою платформу «Кибермир» для проведения киберучений.

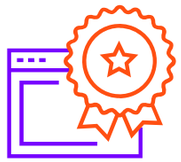
Платформа – это «виртуальная страна» с цифровыми двойниками реальных инфраструктур корпоративного, промышленного и финансового сегмента.

Сервисы Национального киберполигона

- Моделирование кризисных ситуаций
- Консалтинг
- Исследование защищенности
- Центр подготовки и сертификации
- Инфраструктурные решения

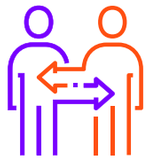
Ключевые преимущества Национального киберполигона

Концепция
виртуальной страны
с цифровыми предприятиями



Вендор
ИБ-продуктов в реестре
отечественного ПО

Воспроизведение в цифре одного
или нескольких регионов с сетью
предприятий



Обмен экспертизой
и уникальная база
актуальных угроз Solar JSOC

Научная и методологическая
база подготовки и проведения
киберучений, практическая
и отраслевая экспертиза

Типовой полигон
от 50 до 200 активов,
максимальный размер
полигона – 1500 активов

Ростелеком
Солар

Интеграция

Ростелеком
Солар

Solar Интеграция – комплексные решения по кибербезопасности

Solar Интеграц

Реализация комплексных проектов по кибербезопасности

«Ростелеком-Солар» предлагает комплексный подход к проектированию, созданию, сопровождению и развитию систем безопасности в соответствии с требованиями регуляторов, учитывая планы по цифровизации и масштабированию бизнеса.

Решаемые задачи:

1 Разработка стратегии развития кибербезопасности

для обеспечения непрерывности бизнеса и реализации планов развития компании

2 Создание защищенной цифровой среды

с использованием современных продуктов и решений по кибербезопасности и их дальнейшее сопровождение

3 Выстраивание процессов кибербезопасности

и обеспечение технической и организационной целостности при внедрении стека решений

4 Оптимизация расходов и повышение качества

выполнения проектов по кибербезопасности за счет привлечения единой команды профессионалов «Ростелеком-Солар»

Ростелеком Солар

Решения и услуги Solar Интеграция

Экспертный консалтинг и комплексный аудит

- Комплексный аудит
- Анализ и оценка рисков
- Разработка стратегии и политики кибербезопасности
- Выстраивание процессов кибербезопасности

Защита периметра и ИТ-инфраструктуры

- Защита сети
- Криптографическая защита каналов связи
- Шлюз безопасности
- Комплексная защита рабочих станций
- Защита от несанкционированного доступа
- Защита виртуализации
- Защита почты
- Защита от продвинутых угроз

Защита бизнес-приложений и данных

- Защита баз данных
- Защита данных на файловых хранилищах
- Шифрование дисков и носителей

Защита конечных станций и пользователей

- Защита рабочих станций и серверов от ВПО
- Продвинутая защита конечных станций
- Защищенный доступ с мобильных устройств

Защита онлайн-систем и веб-сервисов

- Защита от DDoS-атак
- Защита веб-приложений
- Анализ кода

Комплексный контроль защищенности

- Выявление и контроль уязвимостей
- Тестирование на проникновение

Управление доступом

- Управление правами доступа
- Многофакторная аутентификация
- Управление привилегированными пользователями

Управление кибербезопасностью

- Управление инцидентами
- Управление процессами
- Управление сетевой безопасностью

Кибербезопасность объектов КИИ и АСУ ТП

- Выполнение требований 187-ФЗ
- Обеспечение кибербезопасности АСУ ТП
- Мониторинг АСУ ТП
- Киберучения АСУ ТП

Обеспечение соответствия требованиям регуляторов

- Защита ПДн
- Защита ГИС
- Защита КИИ
- Защита финансовых организаций
- Защита КТ

Техническая поддержка и сопровождение 24/7

Ростелеком Солар

Ключевые преимущества Solar Интеграция

1 **Большой опыт реализации проектов федерального масштаба**

для государственных организаций и коммерческих компаний из разных отраслей

2 **Выполнение территориально распределенных проектов**

благодаря присутствию компании «Ростелеком-Солар» во всех регионах России

3 **Наличие собственной методологии управления проектами**

с учетом требований международных и российских стандартов корпоративного менеджмента

4 **Активное участие в экспертных группах регуляторов**

по разработке требований и методических документов

5 **Реализация проектов силами экспертов с разноплановым опытом**

необходимым для выполнения сложных и инновационных задач

6 **Выбор оптимальных средств защиты для решения конкретных задач**

из широкого перечня продуктов российских и зарубежных вендоров

Ростелеком Солар

Ростелеком
Солар

Центральный офис

125009, Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

solar@rt-solar.ru