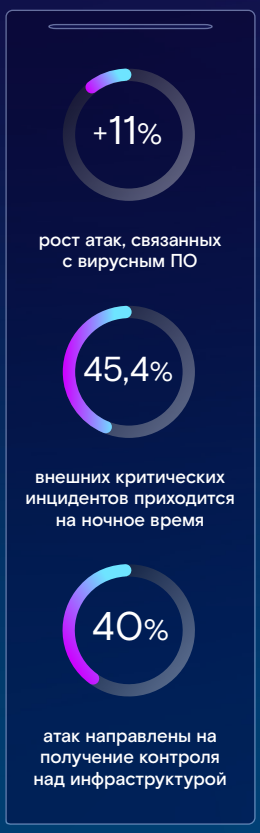
Сервис регистрации и анализа событий ИБ (ERA)

Доступное и надежное решение для государственных структур и среднего бизнеса по обнаружению массовых кибератак и выполнению требований 187-ФЗ

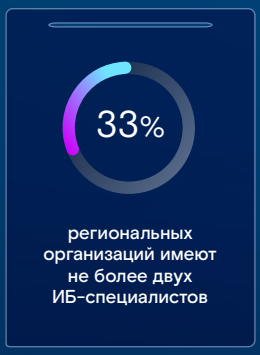
rt-solar.ru
rt.ru

Ростелеком

Описание сервиса



Данные Solar JSOC Security Report, 2019 г.



Данные внутреннего исследования МСБ «Ростелеком-Солар», 2020 г.

Организации, которые должны выполнять требования Федерального Закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации», испытывают трудности при реализации задач центров ГосСОПКА и соблюдения требований приказов ФСТЭК России. Выявление, реагирование и ликвидация последствий массовых кибератак собственными силами требуют значительных кадровых и бюджетных ресурсов. Отсутствие налаженного процесса противодействия кибератакам ставит под угрозу не только выполнение требований регуляторов, но и защищенность самой организации от действий злоумышленников.

Специально для государственных структур и среднего бизнеса компания «Ростелеком-Солар», входящая в ПАО «Ростелеком», разработала решение - сервис ERA (Event registration and analysis). Это доступный и надежный инструмент по обнаружению массовых кибератак, в том числе по требованиям ГосСОПКА.

Решаемые задачи

- Выполнение требований регуляторов для субъектов КИИ
- Реализация полного цикла задач центра ГосСОПКА «под ключ»
- Защита от массовых атак и киберэпидемий в режиме 24/7
- Снижение затрат на специалистов и закупку технологий
- Оперативное выявление уязвимостей инфраструктуры

Для кого?

Сервис ERA подходит организациям, которые:

- попадают под действие 187-ФЗ
- являются владельцами объектов КИИ в сферах госуправления, здравоохранения или науки
- располагают инфраструктурой до 500 активов[1] и до 400 пользователей
- имеют существенные кадровые и бюджетные ограничения по обеспечению информационной безопасности
- испытывают нехватку локальной экспертизы в выявлении и противодействии кибератакам

Возможности сервиса

Выполнение требований регуляторов

- сбор, хранение, обработка событий и выявление инцидентов согласно требованиям 187-ФЗ и приказа ФСТЭК России от 25.12.2017 № 239
- анализ актуальных для компании угроз и результатов устранения инцидентов
- предоставление рекомендаций по реагированию
- двухсторонний обмен с вышестоящим центром ГосСОПКА (при необходимости)

Защита от массовых кибератак

- раннее обнаружение массовых кибератак типа WannaCry и Petya
- обработка запросов по ретроспективному поиску событий
- оперативный анализ кибератак, реагирование и ликвидация последствий
- оповещение ответственных лиц заказчика
- обработка инцидентов не только с СЗИ заказчика, но и в рамках информационного обмена от НКЦКИ и ФинЦЕРТ ЦБ РФ
- минимизация рисков нарушения работы объектов КИИ из-за киберинцидентов

[1] Активы – вся активная инфраструктура заказчика (серверы, рабочие станции, СЗИ и сетевое оборудование)

Преимущества

Доступность
Отсутствие первоначальных затрат и выгодные тарифы.

Готовое решение «из коробки»
Сервис не требует настроек или эксплуатации со стороны заказчика.

Скорость
Получение высококлассного сервиса через месяц после подписания контракта вместо длительного строительства собственного центра.

Лицензии и сертификаты
Все необходимые лицензии и сертификаты (ФСТЭК России, PCI DSS, ФСБ России).

Чем ERA отличается от других сервисов?

1. **Высочайшая экспертиза**
   Обогащение сервиса экспертизой по выявлению массовых атак и новых уязвимостей из аналитического центра Solar JSOC — крупнейшего в России коммерческого центра мониторинга и реагирования на киберинциденты[2].

2. **Выявление инцидентов 24/7**
   Обеспечиваем круглосуточную работу за счет 5 филиалов на территории РФ с покрытием всех часовых поясов.

3. **Реальный опыт**
   Кейсы и референсы во всех отраслях, в том числе по ГосСОПКА.

Параметры сервиса

Базовые

Область защиты
Массовые кибератаки

Размер клиента
До 500 активов
До 400 пользователей

Минимальный срок подписки
От 6 месяцев

Длительность этапа подключения
1 месяц

Информационный обмен с НКЦКИ
Включено

Сценарии обнаружения
40+ унифицированных сценариев

Схемы предоставления сервиса
арендная (облачная/гибридная модели)
и
безарендная (SIEM заказчика)

Дополнительные возможности

Подключение инфраструктурных источников
Базовая инфраструктура заказчика + интеграция с другими сервисами экосистемы Solar MSS: SEG, UTM, Sandbox, SRW и другие

Выезд инженера
В течение 24 часов после получения запроса

Узнать подробнее или заказать сервис: presale@rt-solar.ru

[2] Anti-Malware. Сравнение услуг коммерческих SOC (Security Operations Center). Часть 1. 2019

Выгоды сервисной модели

- Просчитываемые ежемесячные платежи
- Устранение дефицита кадров
- Быстрое подключение
- Контроль работы сервиса 24/7
- Взаимодополняемые сервисы в рамках экосистемы
- Простая масштабируемость
- Личный кабинет с детальными отчетами
- Соответствие законодательству РФ

Сервисы кибербезопасности «Ростелекома»

Solar MSS
управляемые сервисы кибербезопасности

Экосистема управляемых сервисов кибербезопасности для комплексной защиты от массовых киберугроз (MSS)

- Регистрация и анализ событий ИБ (ERA)
- Защита от сетевых угроз (UTM)
- Защита электронной почты (SEG)
- Защита от продвинутых угроз (Sandbox)
- Защита веб-приложений (WAF)
- Защита от DDoS-атак (Anti-DDoS)
- Защищенная удаленная работа (SRW)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)
- Контентная фильтрация (CF)

Solar JSOC
экспертные сервисы кибербезопасности

Первый и крупнейший в России коммерческий центр мониторинга и реагирования на киберинциденты (SOC)

- Мониторинг, реагирование и анализ инцидентов ИБ
- Комплексный контроль защищенности: пентесты, Red Teaming, анализ защищенности, социотех
- Техническое расследование инцидентов ИБ
- Эксплуатация систем ИБ и реагирование на атаки
- Построение SOC и его частных процессов*
- Мониторинг АСУ ТП и субъектов КИИ (SOC OT)

*В том числе Центров ГосСОПКА

О компании «Ростелеком-Солар»

«Ростелеком-Солар», компания группы ПАО «Ростелеком», – национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью. В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ.

№1	700+	70+	24/7	400+	86+ млрд
на рынке сервисов кибербезопасности	экспертов кибербезопасности	клиентов из топ-100 российского бизнеса	обеспечение кибербезопасности	комплексных и сервисных проектов в год	анализируемых событий ИБ в сутки

Ростелеком

presale@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70