



Solar JSOC

Первый и крупнейший в России коммерческий центр противодействия кибератакам

Непрерывная защита крупных государственных и коммерческих организаций от угроз любого уровня сложности

▶ rt-solar.ru
▶ rt.ru

 **Ростелеком**
Солар

Если вас еще не взломали – это не значит, что вы в безопасности

Независимо от размера и отрасли, каждая организация является мишенью для киберпреступников. В одном случае она может оказаться конечной целью, в другом – промежуточным звеном для атаки на партнерскую сеть.

Государственные организации, КИИ, объекты промышленности, нефтегазовой отрасли, энергетики, банковский сектор – все структуры находятся под угрозой сложных и технологичных атак.

+28%

рост числа
событий
ИБ в сутки

+20%

рост доли
критических
инцидентов

+30%

рост атак на получение
контроля над
инфраструктурой
организации

x2

рост атак
через подрядчиков
на объекты КИИ

Данные: Solar JSOC 2021 г.



Если вы крупный бизнес и киберриски высоки, то стоит играть на опережение

Пока компании продвигались по пути цифровизации, в сети многих из них накопились давние заражения вредоносным софтом.

Вирус или обнаруженная уязвимость в любой момент могут быть переданы профессиональной группировке, противостоять которой – сложная задача.



Узнайте больше

о разработанной экспертами «Ростелеком-Солар» модели уровней злоумышленников и определите, какой тип наиболее опасен для вашей организации

Защитим вашу инфраструктуру

Solar JSOC компании ПАО «Ростелеком» – первый и крупнейший в России коммерческий центр противодействия кибератакам, действующий по модели MDR (Managed Detection and Response).

С 2012 года мы несем ответственность за защищенность организаций из самых разных сфер экономики и стоим на страже цифровых границ государства, реализуя сложные проекты национальной безопасности.

#1

на рынке SOC

400+

экспертов
кибербезопасности

250+

клиентов

160+

млрд анализируемых
событий ИБ в сутки

ПРЕДОТВРАЩАЕМ

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

ВЫЯВЛЯЕМ

- ▶ Расширенные возможности мониторинга и анализа событий информационной безопасности 24/7, противодействие атакам на ранней стадии

РЕАГИРУЕМ

- ▶ Оперативное техническое расследование, ликвидация последствий и устранение причин возникновения инцидентов

КОНСУЛЬТИРУЕМ И РЕАЛИЗУЕМ ПРОЕКТЫ

- ▶ Помощь в создании и совершенствовании центров управления информационной безопасностью (SOC)

Сервис-подход MDR в основе работы Solar JSOC подразумевает:

- непрерывное совершенствование экспертизы в области противодействия сложным киберугрозам
- сочетание сильных технологий и навыков для расширения возможностей обнаружения
- глубокую аналитику и разведку угроз
- полноценное реагирование 24/7 за счет распределенной системы 6 филиалов по всей территории страны



Комплексный подход – формула защиты от сложных киберугроз

За целевыми и APT-атаками стоят злоумышленники высочайшей квалификации, действующие максимально скрытно. Для защиты от их действий требуется применение решений, выходящих за пределы типового мониторинга на основе SIEM.

В основе эффективности сервисов и услуг Solar JSOC – адаптивный и комплексный подход

Мы используем расширенные возможности по выявлению и анализу инцидентов на конечных точках и в сетевом трафике, а также уделяем большое внимание изучению деятельности злоумышленников, оперативному реагированию и контролю обстановки за пределами организации. Получаемые данные обогащают наш опыт и знания о противодействии злоумышленникам.



ЭКСПЕРТИЗА В ОБЛАСТИ ЗНАНИЙ О ТЕХНИКАХ, ТАКТИКАХ И ИНСТРУМЕНТАРИИ ЗЛОУМЫШЛЕННИКОВ

Собственная исследовательская лаборатория Solar JSOC CERT ежедневно актуализирует уникальную базу индикаторов и знаний о новых угрозах за счет мониторинга и анализа инфраструктур 250+ клиентов, а также коммерческих подписок, информационных обменов и развернутой сети сенсоров и ханипотов «Ростелеком-Солар».



Узнайте больше

о Solar JSOC CERT и опыте противодействия злоумышленникам

Наши преимущества

► ЗАЩИТА ОТ АТАК ЛЮБОГО УРОВНЯ СЛОЖНОСТИ

Применение опыта крупнейшего коммерческого SOC в России в противодействии передовым киберугрозам. Полный цикл экспертизы в управлении инцидентами и реальный опыт противодействия злоумышленникам продвинутых уровней

► ЭКОНОМИЧЕСКАЯ ВЫГОДА И УДОБСТВО

Сокращение затрат на внедрение и эксплуатацию решений. Устранение проблемы «кадрового голода». Сервисы «под ключ», в том числе обогащение данными об угрозах и предоставление экспертного контента

► КРУПНЕЙШАЯ БАЗА ОБ УГРОЗАХ

Собственная лаборатория Solar JSOC CERT и ежедневно обновляемая база знаний о новых атаках. Доступ к экспертной интерпретации рисков и консультациям по смягчению последствий – знаниям, которые так трудно построить и сохранить внутри типовой службы ИБ

► УРОВЕНЬ СЕРВИСА

Выделенная команда из сервис-менеджера и аналитика-эксперта. Не заваливаем лавиной оповещений, освобождаем от рутинных операций. Исполнение SLA составляет 99,5%. 10 минут на выявление и 30 минут на реагирование

► ИСТОРИИ УСПЕХА ВО ВСЕХ ОТРАСЛЯХ

Отработанные процессы выявления и реагирования на кибератаки у 190+ организаций из всех отраслей экономики России. Разработка специализированных сценариев и применение отраслевых индикаторов компрометации, в том числе для АСУ ТП

► НАСТОЯЩИЕ 24*7, А НЕ ДЕЖУРНЫЕ СМЕНЫ

Круглосуточный мониторинг осуществляется благодаря 6 филиалам в разных часовых поясах. Для решения сложных инцидентов в любое время доступен бизнес-аналитик, а не только дежурный инженер 1-й линии

► ПРОЗРАЧНОСТЬ

Удобная отчетность и визуализация данных о работе сервиса. Обеспечение как сквозными регламентами взаимодействия, так и инструментами ручной и автоматизированной отчетности по состоянию сервиса, уровню угрозы и критичности атак

► ГЛУБОКАЯ ЭКСПЕРТИЗА

Вместо распыления ресурсов на многовендорные решения – фокусировка на ключевых технологиях, позволяющая развить уникальную экспертизу и контент для выявления и противодействия киберугрозам

Экосистема сервисов



МОНИТОРИНГ И АНАЛИЗ ИНЦИДЕНТОВ

Комплекс услуг по выявлению внешних и внутренних инцидентов обеспечивает непрерывную защиту организации от кибератак любого уровня сложности. В дополнение к базовой услуге мониторинга инцидентов ИБ заказчику доступны расширения в виде сервисов защиты конечных точек от сложных кибератак (EDR) и анализа сетевого трафика (NTA).



Выявление угроз на ранней стадии



Обнаружение сложных атак



Защита в режиме 24/7/365



Выделенная сервисная команда

КОМПЛЕКСНЫЙ КОНТРОЛЬ ЗАЩИЩЕННОСТИ

Комплекс работ позволяет выявить слабые места в защите ИТ-инфраструктуры, провести анализ рисков и построить стратегию по предотвращению вторжений. Перечень услуг включает в себя пентест, анализ защищенности, социотехническое исследование, Red Teaming. На любом этапе развития информационной безопасности заказчику доступны решения по укреплению защиты: от поиска и приоритизации устранения уязвимостей до тренировки собственной команды SOC по отражению APT-атак.



Анализ и оценка защищенности



Выявление критичных уязвимостей



Подробные отчеты и рекомендации



Повышение навыков ИТ-, ИБ-служб заказчика

РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

Команда специалистов Solar JSOC обладает опытом и всеми необходимыми средствами для оперативного реагирования на инциденты и минимизации последствий реализованных атак. В рамках расследования осуществляется поиск, получение и анализ цифровых доказательств по инциденту ИБ. По итогам формируется отчет с результатами проведенного анализа, а также рекомендациями для предотвращения подобных инцидентов в будущем.



Выделенная команда быстрого реагирования



Сохранение технических работ в тайне от преступников



Сохранение непрерывности бизнес-процессов



Рекомендации по адаптации системы защиты



АНАЛИЗ УГРОЗ И ВНЕШНЕЙ ОБСТАНОВКИ

В основе эффективности сервисов Solar JSOC лежат данные киберразведки и глубокий анализ техник и тактик злоумышленников. Наша база Threat Intelligence ежедневно пополняется – как собственными силами, так и по коммерческим подпискам ведущих вендоров. Мониторинг даркнета помогает выявить факты утечек данных, продажи компрометирующей информации или формирования заказов на организацию. Получаемые данные в сочетании с внутренней экспертизой по выявлению и противодействию кибератакам гарантируют надежную защиту от комплексных угроз.



Собственная база
Threat Intelligence



Снижение
киберрисков



Исследование даркнета
и киберразведка



Предотвращение
кибератак



ПОСТРОЕНИЕ SOC И КОНСАЛТИНГ

Опыт построения SOC для компаний из разных отраслей и проекты федерального масштаба позволили Solar JSOC накопить уникальную экспертизу, привлечение которой значительно ускоряет работу над собственным центром противодействия кибератакам и делает процесс максимально эффективным. В рамках услуг по построению и консалтингу эксперты Solar JSOC оценивают особенности компании и помогают в принятии правильных решений на каждом этапе – от создания макета будущего SOC до внедрения новых решений и сопровождения после завершения проекта. А также создают у заказчика центр компетенций – фактически собственную копию Solar JSOC.



Отлаженная
методология
работы SOC



Структура
организации
контента SIEM



Практико-
ориентированное
обучение



Подключение
к мониторингу Solar
JSOC на период
построения



Подробная информация

о сервисах и услугах центра противодействия
кибератакам Solar JSOC

Отзывы клиентов



«Для финансовой компании, которая обслуживает клиентов в режиме 24/7, информационная безопасность – один из ключевых приоритетов. Круглосуточный мониторинг инцидентов и реагирование на них – это критические процессы для онлайн-банкинга, а значит, и для бизнеса. Поэтому мы приняли решение о сотрудничестве с Solar JSOC по данному направлению».

АО «Тинькофф Банк»



«Продемонстрированное качество услуги позволяет сравнивать Solar JSOC с ведущими европейскими провайдерами услуг кибербезопасности с точки зрения экспертизы специалистов и выстроенных процессов. Мы отмечаем существенное повышение уровня защищенности инфраструктуры от внешних киберугроз и готовы рекомендовать Solar JSOC как качественный сервис ИБ».

ООО «Леруа Мерлен Восток»



«Несмотря на существенную разницу в часовых поясах, сотрудники Solar JSOC вместе с нашими специалистами оперативно адаптировали профили мониторинга и защиты, что позволило нам противостоять попыткам проникновения и компрометации нашей инфраструктуры».

Министерство ИТ и связи Хабаровского края



«Важным фактором для нас стала готовность Solar JSOC делать сложную и глубокую адаптацию сервиса под наши потребности и внутренние задачи. В результате нам удалось построить эффективное взаимодействие, практически избавившись от ложных срабатываний и минимизировав нагрузку на нашу команду реагирования».

ПАО «Юнипро»

Партнеры

R-Vision



kaspersky



positive technologies

Сотрудничество



ФСТЭК



Аналитика



Эксперты «Ростелеком-Солар»

регулярно публикуют аналитические отчеты и исследования в области информационной безопасности.

Скачайте отчет по интересующему направлению

Филиалы Solar JSOC и ПАО «Ростелеком»



Узнать подробнее или заказать сервис

solar@rt-solar.ru



Solar JSOC

Первый и крупнейший в России коммерческий центр противодействия кибератакам

- Мониторинг и анализ инцидентов
- Комплексный контроль защищенности
- Расследование и реагирование на инциденты
- Анализ угроз и внешней обстановки
- Построение SOC и консалтинг

*В том числе центров ГосСОПКА

Solar MSS

Крупнейшая в России экосистема сервисов кибербезопасности по подписке

Сервисы Solar MSS

- Защита от сетевых угроз (UTM)
- Защита веб-приложений (WAF)
- Защита электронной почты (SEG)
- Мониторинг трафика и защита от DDoS-атак (Anti-DDoS)
- Защита от продвинутых угроз (Sandbox)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками кибербезопасности (SA)
- Контроль уязвимостей (VM)

Решения Solar MSS

- Защита от фишинга и шифровальщиков
- Защита онлайн-ресурсов

О компании

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



rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70