



Ростелеком



Solar JSOC

**Крупнейший коммерческий центр мониторинга и
реагирования на инциденты кибербезопасности в России**

▶ rt-solar.ru

▶ rt.ru

Solar JSOC

Solar JSOC компании ПАО «Ростелеком» — первый и крупнейший в России коммерческий центр мониторинга и реагирования на инциденты кибербезопасности (SOC), действующий по модели MDR (Managed Detection and Response).

Сервисы Solar JSOC позволяют эффективно противодействовать кибератакам, устранять причины возникновения инцидентов, а также оперативно принимать превентивные меры для снижения последствий потенциальных угроз.

Мониторинг, реагирование и анализ инцидентов ИБ

Эксплуатация систем ИБ и реагирование на атаки

Техническое расследование инцидентов ИБ

Комплексный контроль защищенности

Сервисы ГосСОПКА

Построение SOC или его частных процессов

Главные преимущества Solar JSOC — самая большая команда экспертов кибербезопасности, отработанные процессы и техническая инфраструктура, а также налаженные взаимоотношения со ФСТЭК России, НКЦКИ (ФСБ России) и ФинЦЕРТ Банка России.

Архитектура сервисов Solar JSOC



Партнеры



POSITIVE TECHNOLOGIES



Сотрудничество



БАНК РОССИИ

ФИНЦЕРТ

Сервисная модель

Экономия и эффективность

Снижение стоимости владения
Совокупная стоимость владения сервисами дешевле покупки, внедрения и последующей поддержки ИБ-решений.

Устранение дефицита кадров
Отсутствие необходимости создания отдела из высококвалифицированных ИБ-специалистов.

Экономия
Снижение затрат на оборудование и персонал, перевод капитальных издержек в операционные.

Профессиональная команда
Настройка, обслуживание и разбор инцидентов безопасности лучшими специалистами отрасли.

Технологичность и надежность

Доступность
Защита и мониторинг 24 часа в сутки без перерывов и выходных.

Надежность
Эксплуатация распределенной отказоустойчивой инфраструктуры.

Гибкость
Простая масштабируемость и быстрое изменение параметров услуги.

Скорость
Быстрое подключение к сервисам и оперативное реагирование на инциденты.

Соблюдение законодательства

Соответствие требованиям
Выполнение требований законодательства и регуляторов РФ.

Подходящие средства защиты
Эксплуатация сертифицированных решений лидирующих вендоров.

Лицензии регуляторов
Компания является лицензиатом ФСТЭК России, ФСБ России и Минобороны России.

Отслеживание изменений
Меры защиты всегда соответствуют всем новым законам и регламентам.

Преимущества Solar JSOC

Масштаб

Кибербезопасность обеспечивают 190+ специалистов в 4 филиалах. Налажено взаимодействие с ключевыми вузами страны

Компетенции

Мониторинг и реагирование обеспечивают эксперты, компетентные во всех сферах кибербезопасности

Опыт

Отработанные процессы, 100+ клиентов, истории успеха во всех отраслях экономики России

Уровень сервиса

Каждому клиенту выделяется свой сервис-менеджер и аналитик-эксперт. Исполнение SLA составляет 99,5%

Технологичность

Solar JSOC использует технологии и индикаторы компрометации от лидеров рынка кибербезопасности

Экосистемность

Все сервисы взаимосвязаны и обеспечивают комплексную защиту от актуальных киберугроз

Независимость от вендоров

Применение SIEM нескольких вендоров, в том числе из России, дает свободу выбора и гарантию бесперебойной работы

Сотрудничество с регуляторами

Налажено взаимодействие со ФСТЭК России, НКЦКИ (ФСБ России) и ФинЦЕРТ Банка России

Лидер экспертного сообщества

Активный обмен знаниями и навыками в рамках ключевых экспертных мероприятий и сообществ

Solar JSOC в цифрах

№1

на рынке SOC в России

190+

экспертов кибербезопасности

50+

клиентов из топ-100 российского бизнеса

72+

млрд анализируемых событий ИБ в сутки

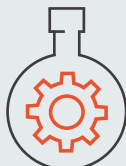
Сервисы Solar JSOC

Мониторинг, реагирование и анализ инцидентов ИБ

При подключении к Solar JSOC заказчику выделяется свой сервис-менеджер и аналитик-эксперт. Это обеспечивает понимание особенностей инфраструктуры клиента, внимание к деталям и максимальную скорость реагирования на подозрительные инциденты. В случае кибератаки клиент получает полное детальное описание инцидента, его возможных последствий и мер противодействия.



Подключение
за 2 недели



Отработанные методики
реагирования



Защита в режиме
24/7/365



Выделенная
сервисная команда

Эксплуатация систем ИБ и реагирование на атаки

Собственные системы кибербезопасности клиента и SaaS-системы Solar JSOC могут использоваться как единый инструмент защиты. Это позволяет оперативно заблокировать действия злоумышленника в инфраструктуре, а также снять с заказчика задачи настройки средств защиты и поиска дорогостоящих специалистов. В результате клиент может перейти от рутинных операций к достижению стратегических целей.



Экспертиза по всем
средствам защиты



SLA с четкими
параметрами



Защита в режиме
24/7/365



Выделенная
сервисная команда

Сервисы ГосСОПКА

Сервисы Solar JSOC позволяют выстроить процесс обмена данными с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), сбора информации для отчетности, организовать мониторинг инцидентов и реагирование, а также обеспечить контроль защищенности инфраструктуры. Между «Ростелеком-Солар» и ФСБ России заключено соглашение о взаимодействии по предупреждению кибератак в рамках ГосСОПКА.



Запуск центра
ГосСОПКА за 2 месяца



Быстрое повышение
уровня защищенности



Приведение в
соответствие требованиям



Экспертиза
Solar JSOC

Комплексный контроль защищенности

Комплексный контроль защищенности позволяет выявить недостатки и уязвимости в ИТ-инфраструктуре, эксплуатация которых может привести к репутационным и финансовым потерям, утечке конфиденциальных данных и замечаниям со стороны регуляторов. Работы проводятся как вручную, так и при помощи автоматизированных средств, что обеспечивает охват всех ИТ-систем компании. По результатам работ клиенту предоставляется отчет с рекомендациями по устранению уязвимостей и повышению уровня защищенности.



Тестирование
на проникновение



Разведка на основе
открытых источников



Социотехнические
исследования



Инструментальное
сканирование

Техническое расследование инцидентов ИБ

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



Выделенная
команда быстрого
реагирования



Корреляция
данных из разных
источников



Сохранение
непрерывности
бизнес-процессов



Рекомендации
по адаптации
системы защиты

Построение SOC или его частных процессов

Solar JSOC может значительно облегчить и ускорить создание собственного SOC клиента, построив его в рамках гибридного подхода. Он подразумевает совмещение услуг классической интеграции с защитой по сервисной модели. В процессе создания SOC инфраструктура заказчика подключается к Solar JSOC, что позволяет настроить SIEM-систему, отработать ключевые процессы SOC, а также нанять и обучить команду будущих сотрудников SOC. Это дает возможность в разы сократить сроки получения первого результата, одновременно повышая качество реализованного проекта.



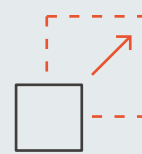
Запуск SOC заказчика
за 1-2 месяца



Передача
процессов и опыта



Обучение
на реальных данных



Защита на время
создания SOC

Отзывы клиентов



Тинькофф Банк

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

АО «Тинькофф Банк»



«Продemonстрированное 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»



«В случае выявления инцидентов в инфраструктуре специалисты Solar JSOC вне зависимости от времени суток в самые короткие сроки связываются со специалистами ГК "Содружество", предлагая полное и информативное описание деталей события, его возможных последствий и мер противодействия».

ГК «Содружество»



«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»



«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 связи и ИТ Хабаровского края



«Наши партнеры из IT Energy и "Ростелеком-Солар" подтвердили свой профессионализм, в крайне сжатые сроки запустив сложный технологический сервис по мониторингу и реагированию на инциденты ИБ в инфраструктуре ПАО "ФСК ЕЭС"».

ПАО «ФСК ЕЭС»



«Коллеги из Solar JSOC оперативно передают нам значимую информацию об угрозах и попытках атак, которая транслируется в НКЦКИ и на основании которой можем принимать взвешенные решения по защите».

Центр информационных технологий
Волгоградской области



«В случае выявления инцидентов в инфраструктуре специалисты Solar JSOC, вне зависимости от времени суток, в самые короткие сроки предлагают полное и информативное описание деталей событий, их возможные последствия и меры противодействия».

Росфинмониторинг

Аналитика

Команда Solar JSOC постоянно работает над улучшением объема и качества собираемой и анализируемой информации. Высокое качество и актуальность аналитики обеспечивают:



- информационный обмен о киберугрозах с ФинЦЕРТ Банка России и ГосСОПКА ФСБ России
- опыт отражения атак на клиентов из различных сегментов экономики с помощью экосистемы сервисов Solar MSS
- более 50 крупных коммерческих и государственных организаций федерального уровня
- налаженные процессы сбора и анализа информации на основе открытых источников

Филиалы Solar JSOC и ПАО «Ростелеком»



Узнать подробнее или заказать сервис

presale@rt-solar.ru



Сервисы кибербезопасности «Ростелекома»

Solar MSS — кибербезопасность как сервис

- Защита от сетевых угроз (UTM)
- Защита веб-приложений (WAF)
- Защита электронной почты (SEG)
- Защита от DDoS-атак (Anti-DDoS)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)



Solar JSOC — сервисы мониторинга и реагирования

- Мониторинг, реагирование и анализ инцидентов ИБ
- Контроль защищенности и управление уязвимостями
- Техническое расследование инцидентов
- Эксплуатация систем ИБ и реагирование на атаки
- Сервисы ГосСОПКА

*Единая платформа сервисов кибербезопасности

