



Защита конечных точек от сложных кибератак

Контроль рабочих станций сотрудников и серверов
с решением Endpoint Detection and Response (EDR)
для эффективной борьбы с целенаправленными атаками

Описание сервиса

Злоумышленники чаще всего начинают атаку на бизнес с заражения устройств сотрудников. Поэтому крайне важно выявлять и блокировать вредоносную активность именно на них. Однако базовые средства защиты рабочих мест — спам-фильтры, антивирусы и брандмауэры — обнаруживают только простые атаки. В случае сложной целевой атаки высока вероятность, что они не сработают.

Для противодействия комплексным угрозам Solar JSOC, крупнейший в России коммерческий центр противодействия кибератакам*, предлагает специализированную защиту конечных точек на базе решения класса **Endpoint Detection and Response (EDR)**. Сервис обеспечивает контроль рабочих станций и серверов в корпоративной сети, выявление вредоносной активности в режиме реального времени и оперативное реагирование на действия злоумышленников.

Решаемые задачи



Обнаружение следов присутствия злоумышленника в инфраструктуре



Больше информации об инциденте благодаря глубокой детализации журналов событий



Выявление атак на ранней стадии и локализация области распространения угрозы



Сокращение времени реагирования за счет автоматизации сбора доказательств

Для кого

Сервис подходит организациям, которые подписаны на услуги Solar JSOC по мониторингу и реагированию на инциденты ИБ, заинтересованы в эффективной защите конечных устройств от сложных атак и стремятся локализовать распространение угрозы в кратчайшие сроки.

Состав сервиса

круглосуточный мониторинг конечных точек

разработка и обновление сценариев выявления новых атак

выявление невидимых для базовых СЗИ угроз

информирование об инцидентах с ручной верификацией

автоматическое реагирование на инциденты или предоставление рекомендаций**

Почему Solar JSOC?

- Применение опыта крупнейшего коммерческого SOC в России в противодействии передовым киберугрозам
- Полный цикл экспертизы в управлении инцидентами
- Простое и централизованное управление расширенной защитой хостов без необходимости самостоятельной эксплуатации специализированных решений или поддержки opensource
- Собственная исследовательская лаборатория Solar JSOC CERT и ежедневно актуализируемая база знаний о новых атаках
- Круглосуточный мониторинг благодаря 6 филиалам в разных часовых поясах, где для решения сложных вопросов в любое время доступен бизнес-аналитик
- Наличие необходимых лицензий и сертификатов (ФСТЭК России, PCI DSS, ФСБ России)

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

**Список автоматических действий ограничен и согласовывается с заказчиком

Экономическая выгода и удобство

Сокращение затрат на внедрение и эксплуатацию решения



Экономия ресурсов внутренней службы ИБ заказчика



Сервис «под ключ», включая обогащение данными об актуальных угрозах из разных источников



Бесшовное масштабирование сервиса



Схема работы

Сервис функционирует на базе решения «Лаборатории Касперского» Kaspersky EDR и подключается как дополнение к базовой услуге Solar JSOC по мониторингу и реагированию на инциденты информационной безопасности. Возможно как использование ранее приобретенного заказчиком ПО (гибридная схема), так и предоставление в аренду лицензий и аппаратных мощностей для запуска из ядра Solar JSOC в облаке «Ростелеком» (облачная схема). Между инфраструктурой заказчика и облаком «Ростелеком» устанавливается защищенный канал связи.



Облачный вариант схемы

EDR автоматически собирает первичную информацию о событиях ИБ на рабочих местах и предоставляет подробную телеметрию. Эксперты Solar JSOC анализируют получаемую информацию, сопоставляют ее с данными Threat Intelligence из различных источников и при необходимости принимают меры реагирования и проводят расследование. Отчеты об инцидентах и данные расследования регулярно предоставляются клиенту.

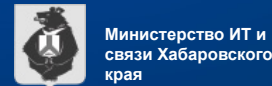
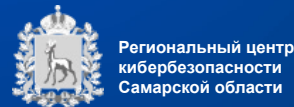
При необходимости в рамках сервиса можно подключить систему защиты от целевых атак **Kaspersky Anti Targeted Attack**, которая предоставляет возможности по обнаружению сложных угроз на сетевом уровне.

Узнать подробнее или заказать сервис:

solar@rt-solar.ru



Solar JSOC выбрали более 250 организаций



Сервисы кибербезопасности «Ростелекома»

Solar JSOC

Первый и крупнейший в России коммерческий центр противодействия кибератакам (MDR)

- Мониторинг и анализ инцидентов
- Комплексный контроль защищенности
- Расследование и реагирование на инциденты
- Анализ угроз и внешней обстановки
- Построение SOC и его частных процессов***
- 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)
- Защита от DDoS-атак (Anti-DDoS)
- Защита от продвинутых угроз (Sandbox)
- Регистрация и анализ событий ИБ (ERA)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)
- Контентная фильтрация (CF)

Решения Solar MSS

- Защита от фишинга и шифровальщиков
- Защита онлайн
- Единая сервисная модель для РОИБ

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

на рынке сервисов кибербезопасности

1300+

экспертов кибербезопасности

750+

организаций под защитой

24/7

обеспечение кибербезопасности

600+

реализованных проектов в год

160+ млрд

анализируемых событий ИБ в сутки