Анализ сетевого трафика

Выявление сложных атак и сбор данных для расследования инцидентов с решением класса Network traffic analysis (NTA)

rt-solar.ru
rt.ru

Ростелеком

Описание сервиса

Корпоративная инфраструктура сегодня включает не только офисные компьютеры и серверы, но и личные устройства сотрудников, а рабочие данные хранятся как локально, так и у поставщиков услуг. Для сложной инфраструктуры недостаточно периметровых средств защиты или решений по контролю рабочих мест и шлюзов. Важно отслеживать вредоносную активность внутри корпоративной сети и оперативно выявлять зараженные объекты.

В этом поможет сервис анализа сетевого трафика от Solar JSOC — крупнейшего в России коммерческого центра мониторинга и реагирования на киберинциденты[1]. Сервис предполагает тщательную проверку периметрового и внутреннего сетевого трафика, а также хранение информации для расследований и ретроспективного анализа. Глубокая экспертиза Solar JSOC и собственная база знаний тактик, техник и процедур атакующих, а также методов реагирования на новейшие векторы атак гарантируют высокую эффективность сервиса.

Решаемые задачи

Расширение возможностей по выявлению сложных атак

Проверка гипотез Threat Hunting и выявление скрытых угроз

Помощь в расследовании атак и восстановлении их хронологии

Обнаружение утечек данных и нарушения политик безопасности

Для кого

Сервис подходит организациям, которые подписаны на услуги Solar JSOC и стремятся устранить «слепые зоны» в защите и охватить комплексным мониторингом всю инфраструктуру для выявления профессиональных кибергруппировок высокого уровня квалификации.

Возможности сервиса

- проверка, сбор и хранение всего сетевого трафика
- адаптация к новым угрозам и методам атак
- поиск скрытых каналов взаимодействия с управляющими серверами злоумышленников
- контроль соблюдения политики безопасности сотрудниками
- выявление аномалий

Почему Solar JSOC?

- Применение опыта крупнейшего SOC в России в противодействии передовым киберугрозам
- Разработка и регулярное пополнение базы сценариев выявления новых атак от центра технического расследования инцидентов Solar JSOC CERT
- Привлечение экспертов по реагированию для решения нетиповых инцидентов и оперативное предоставление рекомендаций по блокированию атаки
- Круглосуточный мониторинг благодаря 5 филиалам в разных часовых поясах, где в любое время суток доступен бизнес-аналитик для решения сложных вопросов
- Все необходимые лицензии и сертификаты (ФСТЭК России, PCI DSS, ФСБ России)

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

Преимущества

1

Эффективное выявление атак

- Оперативное выявление угроз, не детектируемых СЗИ уровня ОС
- Определение модифицированного или бесфайлового вредоносного ПО
- Выявление угроз в зашифрованном трафике

2

Помощь в анализе и расследовании

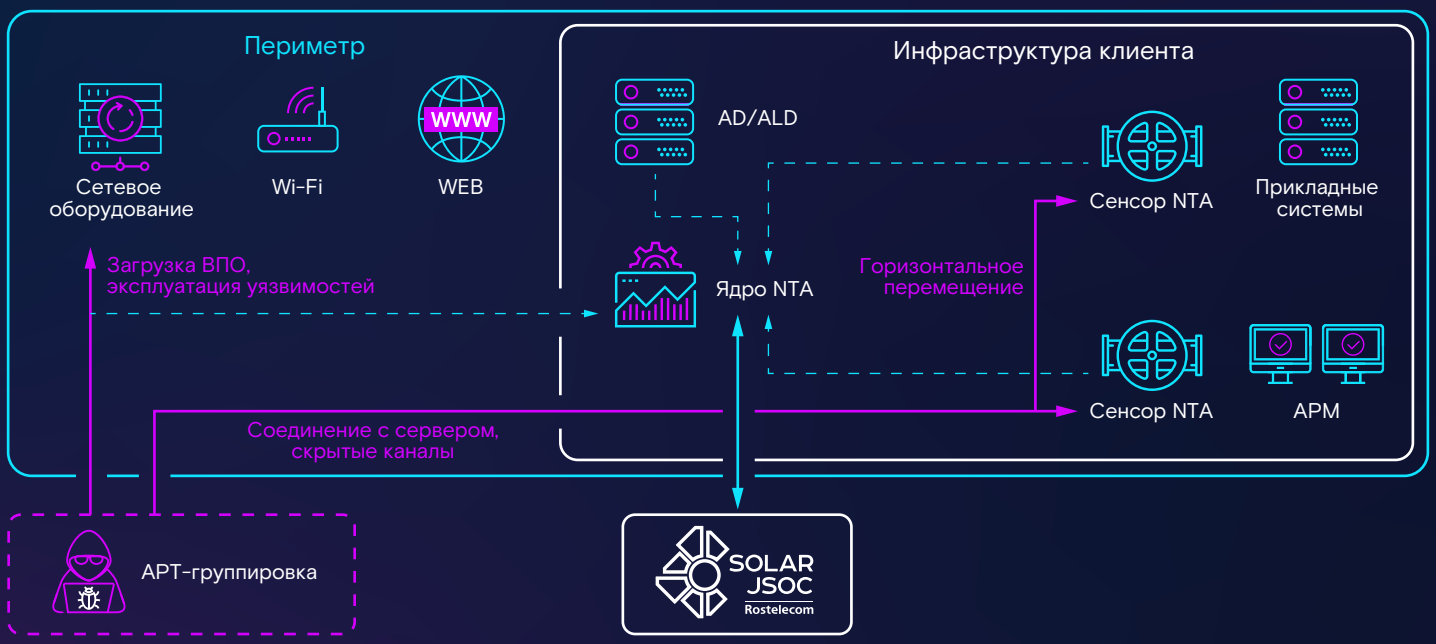
- Значительное расширение возможностей Threat Hunting и ретроспективного анализа по индикаторам компрометации
- Возможность найти атаку в прошлом
- Возможность понять контекст атаки

3

Экономическая выгода и удобство

- Снижение расходов на закупку лицензий и оборудования, управление платформой и ее настройку
- Получение уведомлений только верифицированных угроз с использованием комбинации ручных и автоматизированных методов обнаружения угроз
- Бесшовная интеграция с SIEM-системой и другими СЗИ

Схема работы



Захват сетевого трафика происходит на периметре и в инфраструктуре, что позволяет выявлять активность злоумышленника как при попытках проникновения в сеть, так и при развитии атаки внутри нее, например во время горизонтального перемещения или lateral movement. Обработка данных проходит в несколько этапов: проверка трафика по заданным правилам (свыше 5 тысяч), анализ и ручная верификация силами аналитиков Solar JSOC. Управление сервисом, обмен сообщениями по инцидентам, модернизация и обогащение контента, проведение расследований и предоставление рекомендаций по реагированию осуществляются экспертами Solar JSOC.

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

Варианты подключения

При выборе схемы подключения может быть использовано как имеющееся оборудование и лицензии NTA клиента, так и полное или частичное предоставление необходимых опций или мощностей.

Предоставление ПО	Предоставление мощностей для сенсора	Расположение ядра системы	Эксплуатация сервиса	
Нет*	–	В инфраструктуре клиента	+	гибридная схема
Да	–	В инфраструктуре клиента	+	
Да	–	В облаке ПАО «Ростелеком»	+	облачно-гибридная схема
Да	+	В облаке ПАО «Ростелеком»	+	

*Используется ПО клиента

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