SOC ПРЕМИУМ

Адаптивный сервис мониторинга угроз
для поддержки и расширения вашей ИБ-команды
в борьбе с кибератаками

ТАРИФ SOC ПРЕМИУМ ПОДОЙДЕТ ВАМ, ЕСЛИ:

01 Требуется больше данных

02 Есть необходимость в дополнительной команде

ПОГРУЖЕНИЕ В ИНФРАСТРУКТУРУ

Аналитик и сервис-менеджер непрерывно исследуют потребности клиента и особенности инфраструктуры, предлагая актуальные сценарии и доработку корреляционных правил.

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИБ

Расследуем инциденты вне зоны покрытия SIEM, сопровождаем процесс. Проводим углубленные технические расследования, предоставляем рекомендации по повышению устойчивости инфраструктуры клиента к повторению инцидента ИБ.

АДАПТАЦИЯ КОНТЕНТА

Интегрируем бизнес-системы клиента, ускоренно* подключаем нетиповые источники**, дорабатываем существующие сценарии** обнаружения инцидентов ИБ для адаптации корреляционной логики под инфраструктуру клиента, запускаем новые сценарии** по запросу клиента.

ВЫЯВЛЕНИЕ СКРЫТЫХ УГРОЗ

Вместе с клиентом эксперты ГК «Солар» выделяют критичные сегменты инфраструктуры, собирают профили активности, чтобы вовремя заметить скрытые угрозы, которые не обнаруживаются стандартными правилами детектирования. По запросу клиента производится анализ образцов вредоносного ПО.

* По сравнению с тарифом Классик
** Количество ограничено

SOLAR

W: RT-SOLAR.RU
E: INFO@RT-SOLAR.RU