SOC КЛАССИК

Проактивный мониторинг для лучшего понимания внешних воздействий на инфраструктуру

ТАРИФ SOC КЛАССИКПОДОЙДЕТ ВАМ, ЕСЛИ:

01 Нуждаетесь в дополнительных компетенциях

02 Испытываете дефицит квалифицированных кадров

КАСТОМИЗАЦИЯ ПОД ИНФРАСТРУКТУРУ

Подключаем нетиповые источники*, дорабатываем существующие сценарии* обнаружения инцидентов ИБ для адаптации корреляционной логики под инфраструктуру клиента, разрабатываем и запускаем новые сценарии* по запросу клиента. Своевременно отправляем очищенные и приоритизированные IOC'и по всей базе Solar JSOC.

МОНИТОРИНГ АНОМАЛИЙ

Запускаем сценарии профилирования* для выявления отклонений от профиля нормального поведения на критичных сегментах инфраструктуры. Проводим активный поиск скрытых киберугроз, не обнаруживаемых стандартным контентом. Проверяем гипотезы о киберугрозах.

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.

ВИЗУАЛИЗАЦИЯ МЕТРИК

Отслеживание в динамике метрик и показателей состояния информационной безопасности организации в режиме реального времени с помощью JSOC Security Dashboard.

* Зависит от количества eps

SOLAR

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