Подключение к сервисам Solar JSOC для АСУ ТП

Сервисы мониторинга, выявления и реагирования на угрозы для систем промышленной автоматизации

rt-solar.ru

rt.ru

Ростелеком
Солар

Проблематика

Кибератаки на промышленные активы и критическую информационную инфраструктуру — один из пяти основных глобальных рисков, озвученных на Всемирном экономическом форуме 2018 года в Давосе. Для предотвращения инцидентов и поддержки работоспособности инфраструктуры промышленных предприятий необходимо оперативно выявлять возможные киберугрозы и реагировать на них.

Риски для компаний с промышленной и критической информационной инфраструктурой

Информационная безопасность

- вирусное заражение
- несанкционированный доступ
- перехват управления технологическим процессом
- кража уникальных технологий производства

Невыполнение требований и претензии регуляторов

Приостановка деятельности

72%

обнаруженных уязвимостей АСУ ТП — высокого и критического уровней

28%

уязвимостей связаны с проблемами управления доступом

56%

предприятий с SCADA или ICS-системами заявили о кибератаках в 2017 году

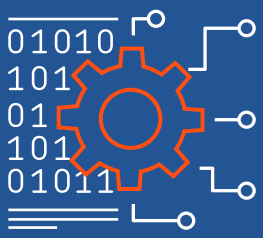
Данные: «Лаборатория кибербезопасности АСУ ТП» («Ростелеком-Солар», 2019) и Fortinet, 2018

Сложность самостоятельного мониторинга и анализа

Задачи мониторинга и анализа инцидентов ИБ можно решить, самостоятельно запустив отдельный промышленный центр мониторинга и реагирования на инциденты или направление в рамках уже работающего SOC. Такая работа затруднена рядом проблем:

- Перегруженный ИБ-отдел не успевает своевременно выявлять и анализировать возникающие инциденты
- Нехватка персонала с достаточными знаниями в АСУ и ИБ не позволяет круглосуточно контролировать состояние ИБ
- Необходимо привлекать дорогостоящих и редких экспертов, которые могли бы поддерживать сценарии выявления инцидентов в актуальном состоянии в условиях меняющегося промышленного и ИТ-ландшафта
- Трудно своевременно получать и качественно обрабатывать информацию о новых трендах и угрозах
- Создание промышленного SOC требует слишком много времени и зависит от работ по настройке и вводу в эксплуатацию собственной SIEM-системы

Уникальность



«Лаборатория кибербезопасности АСУ ТП» с это корпоративный центр компетенций для сбора, систематизации, распространения, приумножения знаний и лучших практик по обеспечению кибербезопасности систем промышленной автоматизации. Эксперты компании обладают реальным опытом разработки и внедрения проектов по защите АСУ ТП и являются одними из лидеров в рейтинге исследователей БДУ ФСТЭК России.

Решение

«Лаборатория кибербезопасности АСУ ТП» помогает подключиться к центру Solar JSOC и обеспечивает методологическое экспертное сопровождение всех работ. Solar JSOC — центр управления инцидентами информационной безопасности «Ростелеком-Солар» — предлагает услуги по управлению выявлением и реагированием для организаций промышленной и критической информационной инфраструктуры.

Преимущества

Сокращение времени реагирования на инциденты

Оперативный запуск услуги

Снижение зависимости от сотрудников

Оптимизация капитальных расходов на обеспечение мониторинга инцидентов ИБ

Получение эффективной пользы от вложений в лицензии SIEM

Обеспечение круглосуточной безопасности компании

«Лаборатория кибербезопасности АСУ ТП» совместно с Solar JSOC позволяет:

Реализовать требования № 187-ФЗ и Приказа ФСТЭК России № 31

Сократить возможный **ущерб** и негативные последствия от ИБ-инцидентов

Повысить устойчивость работы АСУ ТП

Автоматизировать и улучшить процесс управления инцидентами

Снизить совокупные **затраты** на управление инцидентами

Организовать круглосуточный мониторинг, выявление, разбор и оповещение об угрозах и инцидентах ИБ

Контролировать выполнение политик и стандартов в области ИБ и настроек средств защиты информации

Расследовать инциденты

Что получает заказчик

Установка системы мониторинга, адаптация и тестирование

Мониторинг инцидентов ИБ и реагирование

Экспертный и ретроспективный анализ событий ИБ

Доработка сценариев обнаружения

Регулярные информативные отчеты

Организация взаимодействия с НКЦКИ

Варианты подключения

Гибридное

В инфраструктуре заказчика развернута и настроена собственная SIEM-система

События от АСУ ТП поступают и обрабатываются в SIEM заказчика

Специалисты Solar JSOC подключаются к SIEM заказчика по защищенному каналу связи

Облачное

В инфраструктуре заказчика отсутствует собственная SIEM-система

События от АСУ ТП собираются и обрабатываются в облачном SIEM в ЦОД Solar JSOC

Передача событий из инфраструктуры заказчика по защищенному каналу связи

Узнать подробнее или заказать услугу presale@rt-solar.ru

Услуги «Ростелеком-Солар»

− Кибербезопасность АСУ ТП

- Приведение организации в соответствие с требованиями 187-ФЗ «О безопасности КИИ РФ»
- Подключение к сервисам Solar JSOC для АСУ ТП
- Выявление уязвимостей и НДВ в компонентах АСУ ТП и IIoT
- Построение киберзащищенных АСУ ТП
- Проведение киберучений
- Тестирование на проникновение АСУ ТП
- Комплексный анализ защищенности АСУ ТП

+ Интеграционные услуги

+ Соответствие требованиям

О компании

«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. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар».

Ростелеком Солар

info@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70

S.9.10.BR.ICS.SJ.01