ТГК-2 защищает промышленную сеть с помощью Kaspersky Industrial CyberSecurity

ТГК-2, одна из крупнейших теплоэнергетических компаний Северо-Западного и Центрального федеральных округов России, внедрила решение для мониторинга и контроля в рамках промышленной сети — KICS for Networks. На очереди — внедрение KICS for Nodes и пилотирование SIEM-системы Kaspersky Unified Monitoring and Analysis Platform.

kaspersky

Предыстория

01.

В ТГК-2 выбрали решение Kaspersky Industrial CyberSecurity for Networks по ряду причин.

Kaspersky Industrial CyberSecurity for Networks понятно и просто интегрируется в промышленную сеть по сравнению с решениями конкурентов и соответствует ряду требований заказчика:

- поддерживает широкий список проприетарных протоколов, используемых в ТГК-2
- сертифицировано ФСТЭК России
- интегрируется с KICS for Nodes
- удобно управляется из единой консоли KSC.

Так как сенсоры подключаются в системе «на горячую», без долгой настройки, это обеспечило оперативное внедрение систем. Кроме того, быстрому развёртыванию решения в инфраструктуре способствовала всесторонняя поддержка со стороны экспертов «Лаборатории Касперского».

ТГК-2:

- **Одна из 14 ТГК России (Территориальные генерирующие компании)**
- **Включает крупнейшие генерирующие предприятия пяти регионов: Архангельской, Вологодской, Костромской, Новгородской и Ярославской областей**
- **В Ярославле, Костроме и Архангельске за ТГК-2 закреплен статус единой теплоснабжающей организации (ЕТО)**
- **Всего в городах деятельности компании проживает более 2 700 000 человек.**
- **В 2014 году ТГК-2 вышла на международный рынок электроэнергии, завершив сделку, посредством которой компания установила контроль над электростанцией комбинированного цикла ПГУ «ТЕ-ТО АД Скопье» мощностью 220 МВт в г. Скопье (Республика Македония).**

Решение

02.

KICS for Networks — это решение, позволяющее реализовать сценарии инвентаризации устройств и сетевых коммуникаций, пассивного выявления атак и аномалий в трафике промышленной сети, а также инспекции промышленных протоколов для контроля команд и параметров технологического процесса.

Kaspersky Industrial CyberSecurity «Лаборатории Касперского», в состав которого входит внедрённый в ТГК-2 KICS for Networks, — это целая экосистема специализированных продуктов и сервисов, призванная обеспечить кибербезопасность промышленных организаций. Продукты в составе этой экосистемы помогают реализовать комплексный подход к кибербезопасности на всех уровнях, начиная с анализа защищённости и тренингов для сотрудников и заканчивая передовыми технологиями защиты АСУ ТП и реагированием на инциденты. В основе KICS лежат многолетний опыт в области кибербезопасности, глубокое понимание природы уязвимостей информационных систем и тесное сотрудничество с международными и российскими регуляторами в области требований к защите.

KICS for Networks выявляет аномалии и вторжения в АСУ ТП на ранних этапах и обеспечивает необходимые контрмеры для предотвращения ущерба технологическому оборудованию. Возможности продукта не зависят от используемой аппаратной платформы, поэтому клиенты не ограничены в выборе поставщиков для своей инфраструктуры. Интерфейс KICS for Networks включает консоль управления, данные которой обновляются в режиме реального времени, и карту сети, что позволяет с комфортом работать с устройствами предприятия и отслеживать события безопасности.

Продукты в составе предложения для заказчика:

- **KICS for Networks** — решение для мониторинга промышленных сетей, подключаемое пассивно к сети АСУ ТП в виде программного обеспечения или виртуального устройства.
- **Kaspersky Industrial CyberSecurity for Nodes** — решение для защиты конечных узлов промышленной среды, предлагаемое в виде ПО для компьютеров на базе Windows и Linux.
- **Kaspersky Security Center** — решение для централизованного управления безопасностью. Оно обеспечивает простоту контроля и прозрачность не только для промышленных уровней инфраструктуры на множестве объектов, но и для окружающих корпоративных сетей.
- **Kaspersky Unified Monitoring and Analysis Platform** — SIEM-система, которая собирает и производит корреляцию событий ИБ, упрощая их обработку специалистами службы информационной безопасности.

Результат и отзывы

03.

Для защиты непрерывности промышленных процессов от существующих и будущих угроз и создана экосистема промышленной кибербезопасности Kaspersky Industrial CyberSecurity.

«Мы успешно сотрудничаем с „Лабораторией Касперского“ с 2008 года. Наши рабочие станции защищены решением Kaspersky Security для бизнеса, а теперь мы развиваем систему защиты наших промышленных компонентов с помощью специализированных индустриальных решений. В первую очередь они удобно интегрируются с нашими системами. К тому же приятно развивать отношения с партнёром, в качестве продуктов и экспертизе специалистов которого мы могли убедиться за эти годы», — Александр Суворов, начальник отдела информационной безопасности ПАО «ТГК-2».

Несмотря на то что промышленные системы изначально создаются по высоким стандартам безопасности, этого оказывается недостаточно для полноценной защиты от современных цифровых угроз. Согласно исследованию Kaspersky ICS CERT, в 2020 году доля промышленных компьютеров, на которых были обнаружены вредоносные объекты, достигла 38,6 %. Банковский троянец или программа-вымогатель, случайно попавшие в автоматизированные системы управления технологическим процессом (АСУ ТП) с помощью заражённого флеш-накопителя или фишингового письма, могут серьёзно навредить бизнесу. И хотя случайные заражения происходят не так часто, очевидно, что задавшийся целью киберпреступник также может проникнуть в промышленную сеть и нанести ощутимый ущерб производственным процессам, дорогостоящему оборудованию или украсть ценную информацию.

Преимущества KICS

- **Обнаружение устройств: пассивная идентификация и учёт устройств в промышленной сети**
- **Deep Packet inspection (DPI): анализ телеметрии технологических процессов практически в режиме реального времени**
- **Контроль целостности сети: обнаружение несанкционированных хостов и потоков в сети**
- **Система обнаружения вторжений: оповещения о вредоносной активности в сети**
- **Контроль команд: проверка команд, передаваемых по промышленным протоколам**
- **Поддержка внешних систем: обнаружение угроз внешними системами благодаря интеграции через API**
- **Использование машинного обучения для обнаружения аномалий (MLAD): позволяет выявлять аномалии в цифровых и физических процессах с помощью телеметрии в режиме реального времени и обработки исторических данных (рекуррентная нейронная сеть)**
- **Обнаружение уязвимостей: обновляемая база уязвимостей промышленного оборудования.**

Узнать больше о продуктах Kaspersky Industrial CyberSecurity →