



Защита промышленных сетей на Пермском заводе «Машиностроитель»

Пермский завод «Машиностроитель» — крупное машиностроительное предприятие, история которого насчитывает более 55 лет. Завод входит в структуру военно-промышленных корпораций «Тактическое ракетное вооружение» и «НПО машиностроения» и производит авиационное оборудование, узлы авиационных двигателей, дозировочные системы и насосы и другие виды продукции. Сегменты предприятия являются объектами КИИ.

ЦЕЛЬ ПРОЕКТА

Система анализа сетевого трафика и обнаружения вторжений была необходима для обеспечения бесперебойной работы промышленных процессов. Деятельность Пермского завода «Машиностроитель» критически важна для государства и национальной безопасности: он обеспечивает обороноспособность страны, стимулирует научно-технический прогресс и экономическое развитие региона.

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

- Значительно улучшена видимость промышленной сети: появилось понимание, как используются устройства и приложения, и как они взаимодействуют друг с другом
- Обнаружены уязвимости в промышленных системах, которые ранее оставались незамеченными
- Решение помогло выявить и остановить несколько попыток злоумышленников получить доступ к промышленным системам предприятия
- Сокращено время реагирования на инциденты ИБ за счет оперативного получения необходимой информации

В качестве решения был внедрен комплекс

UDV DATAPK Industrial Kit, обеспечивающий:

- Глубокий анализ сетевого трафика, регистрацию событий информационной безопасности и их анализ в контексте технологических процессов
- Обнаружение аномалий сетевой активности в режиме реального времени
- Защиту промышленных сетей и эффективное выявление угроз, характерных для АСУ ТП

UDV DATAPK Industrial Kit — комплексное решение для обеспечения ИБ АСУ ТП, выполняющее анализ сетевого трафика и обнаружение вторжений, управление конфигурациями, уязвимостями и внешними событиями

Решение позволяет быстро начать реагировать на угрозы без негативного влияния на защищаемые системы, обеспечивает видимость ландшафта АСУ ТП, выявляет инциденты на ранних этапах и помогает выполнить требования регуляторов. UDV DATAPK Industrial Kit использует целостный подход в рамках единого решения, что позволяет оптимизировать расходы на защиту АСУ ТП.

ПРЕИМУЩЕСТВА

— Выполняет функции нескольких классов решений: системы обнаружения вторжений, средства управления событиями и средства анализа защищенности

— Создан специально для АСУ ТП и применяется для защиты значимых объектов КИИ РФ в металлургии, энергетике, нефтегазовом секторе, химической промышленности и на производствах

— Использует безагентный подход, что позволяет осуществлять мониторинг без влияния на защищаемые системы

— Сертифицирован ФСТЭК России по требованиям профиля защиты СОВ уровня сети, уровнем доверия в соответствии с Приказом №76 от 2 июня 2020 г.



Константин Селезнёв

Специалист по защите информации отдела по противодействию иностранным техническим разведкам и технической защите информации АО «Пермский завод «Машиностроитель»

«Мы подошли к выбору решения для защиты наших объектов КИИ с особой тщательностью. Мы искали систему, которая не только соответствовала бы требованиям законодательства, в частности 187-ФЗ, но и обеспечивала бы глубокий анализ сетевого трафика в наших промышленных сетях (ICS/OT) и быстрое обнаружение аномалий и вторжений, а также была экономически целесообразна.

UDV DATAPK Industrial Kit безусловно является важным элементом нашей стратегии защиты объектов КИИ. Он обеспечивает нам глубокий анализ сетевого трафика, своевременное обнаружение вторжений и аномалий и позволяет оперативно реагировать на киберугрозы. Если вы ищете надежное и эффективное решение для защиты вашей промышленной сети и объектов КИИ, я рекомендую вам обратить внимание на DATAPK».



Федор Маслов

Менеджер продукта UDV DATAPK Industrial Kit

«Успешное внедрение UDV DATAPK Industrial Kit в таких значимых заказчиках, как Пермский завод «Машиностроитель», в очередной раз подчеркивает эффективность и надежность наших методов обеспечения комплексной кибербезопасности промышленных предприятий, объектов критической информационной инфраструктуры. Как разработчик ПО и эксперты по информационной безопасности, мы безусловно заинтересованы в предоставлении наших решений организациям из различных секторов экономики, а в текущих геополитических реалиях считаем своим долгом предоставление предприятиям ВПК проверенных временем инструментов для защиты от любых сложных киберугроз».