Защита в рамках цифровизации промышленных предприятий (АСУТП)

Гаращенко Дмитрий Владимирович
Начальник отдела информационной безопасности
АО «НПП «Исток» им. А.И. Шокина

Инциденты ИБ

Промышленный шпионаж

Злоупотребления служебными

Противодействие иностранным разведкам

Сетевые атаки на сетевое оборудование Общества

Не соблюдение требований по работе с материалами ограниченного доступа

Нарушение положения о работе в сети Интернет

Требования регуляторов по ИБ

Требования
к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса

Состав и содержание мер защиты информации для информационных систем управления производством должны соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17, и реализовываться на общесистемном, прикладном и сетевом уровнях, в том числе в виртуальной среде.

Автоматизированные системы управления
Приказ ФСТЭК №31

Государственные информационные системы
Приказ ФСТЭК №17

Изолированные станки это выход?

Как показывает практика бесконтрольная работа персонала эффективна на 60% от своего реального потенциала.
Данные с IOT платформы Winnum после их подключения к станкам потвердили эти цифры.
Требования бизнеса увеличение производительности и доходности.

Winnum®

Даже изолированный станок не защищен

Угрозы:

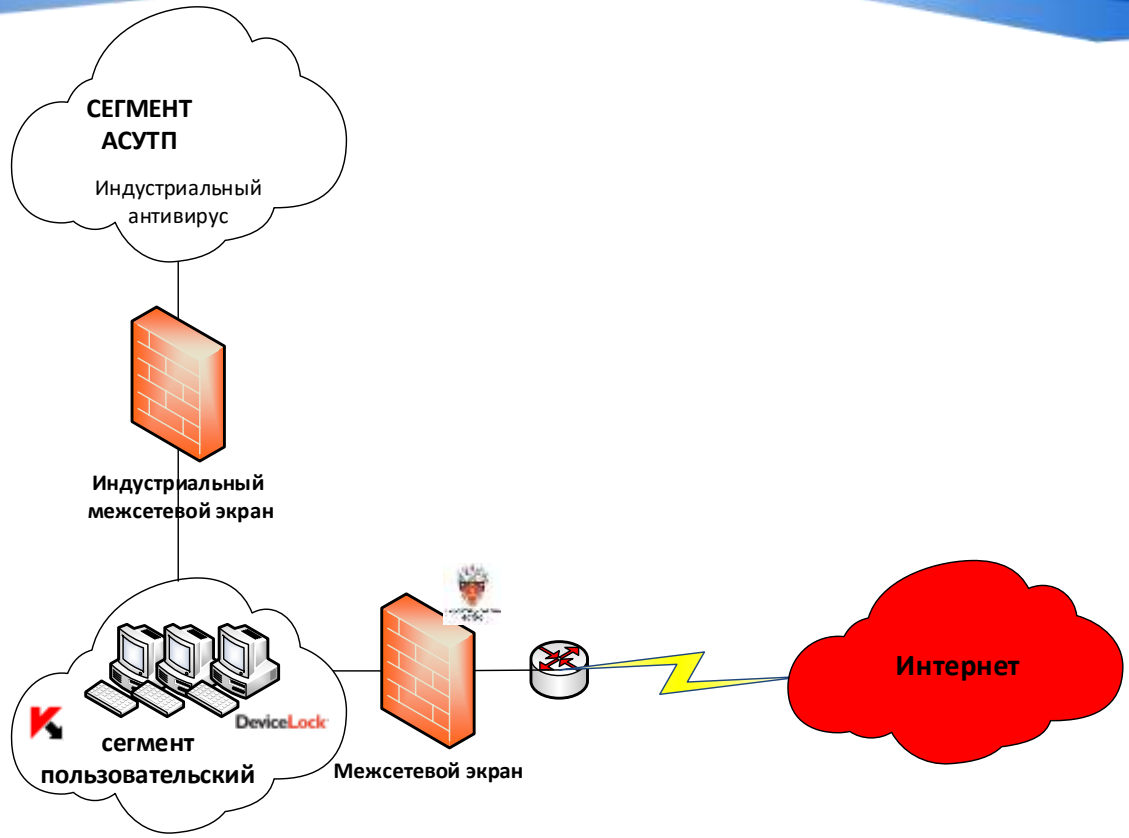
- Wifi есть в каждом телефоне, а прошивка зарубежных станков в качестве закладок позволяет подключаться и передавать данные о типе и количестве деталей.
- Техподдержка поставщиков оборудования
- Работник предприятия использующий зараженные носители

Мы все предусмотрели?

SIEM - есть

Индустриальный межсетевой экран - есть

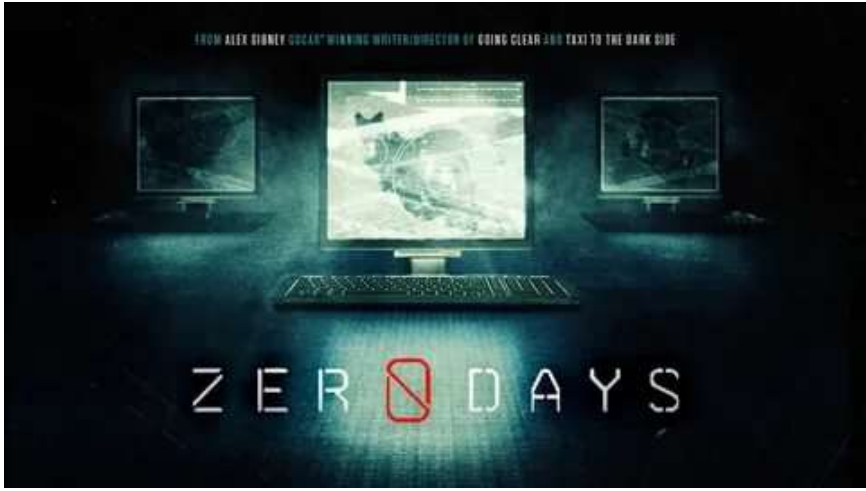
Индустриальный антивирус - есть



Атаки нулевого дня

Для защиты можно использовать традиционные антивирусные технологии, а также проактивные средства:

Sandboxing (песочницу);
анализ поведения;
эмуляцию кода;
эвристический анализ;
виртуализацию рабочего окружения.



Что нам ещё поможет ?

Искусственный интелект
Позволит определить отклонения от стандартных режимов работы АСУТП.

Ловушки
Платформы для создания распределенной инфраструктуры ложных целей (Distributed Deception Platform — DDP)

Искуственный интелект на помощь ИБ

Искусственный интелект идет на помощь SIEM в контроле за поведенческими аномалиями.

Увеличение периода обучения повышает эффективность определения инцидентов

Ловушки

Система LOKI от АВ «Софт» имитирует ИТ-инфраструктуру организации для инициализации взаимодействия с атакой киберпреступника, сбора информации о ней и проверки ее артефактов

Система THF от GroupIB осуществляет поиск обнаружения аномалий, скрытых тоннелей

Спасибо за внимание!