Kaspersky Industrial Cybersecurity Conference 2023

Формирование ИБ-защиты в организации через призму IT

Владислав Тен

kaspersky

О заводе

Атырауский нефтеперерабатывающий завод (ТОО «АНПЗ») — один из трёх ведущих нефтеперерабатывающих заводов Казахстана.

- Проектная мощность переработки - 5,5 млн тонн в год
- Производство свыше 20 наименований товарных нефтепродуктов
- Производство нефтехимической продукции - 629 тыс. тонн

Инфраструктура предприятия. Сеть

Проблематика технологической сети

- «Устаревшее» оборудование и ПО
- Несовместимость ПО с новыми решениями
- Участившиеся атаки на технологические сети

Выбор решения

1. Этап выбора решения

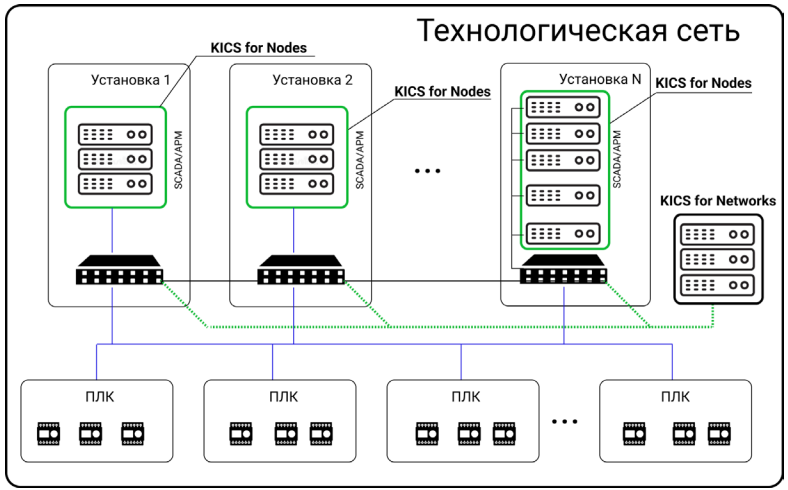
Критерии выбора решений:

- Решения должно «закрывать» и конечные рабочие станции и анализировать промышленный трафик
- Унификация с корпоративным решением
- Должен быть сертификат соответствия СТ РК.

Kaspersky Industrial CyberSecurity

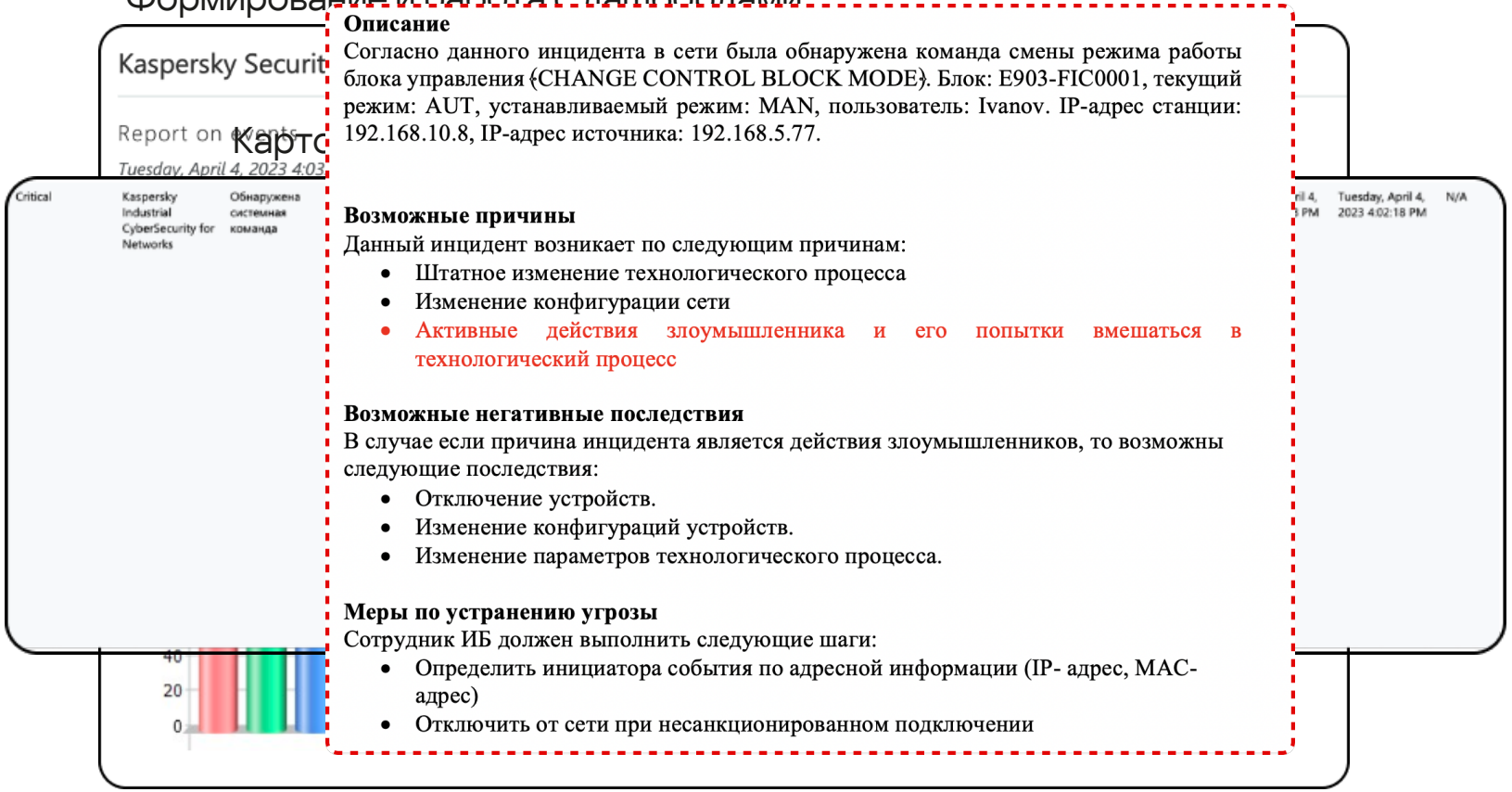
2. Внедрение

- Предпроектное исследование
- Монтаж, пуско-наладка
- Ввод в эксплуатацию
- Подготовка кадров



Эксплуатация и первые детекты

Формирование и работа с дашбордами



Описание

Согласно данного инцидента в сети была обнаружена команда смены режима работы блока управления (CHANGE CONTROL BLOCK MODE). Блок: E903-FIC0001, текущий режим: AUT, устанавливаемый режим: MAN, пользователь: Ivanov. IP-адрес станции: 192.168.10.8, IP-адрес источника: 192.168.5.77.

Возможные причины

Данный инцидент возникает по следующим причинам:

- Штатное изменение технологического процесса
- Изменение конфигурации сети
- Активные действия злоумышленника и его попытки вмешаться в технологический процесс

Возможные негативные последствия

В случае если причина инцидента является действия злоумышленников, то возможны следующие последствия:

- Отключение устройств.
- Изменение конфигураций устройств.
- Изменение параметров технологического процесса.

Меры по устранению угрозы

Сотрудник ИБ должен выполнить следующие шаги:

- Определить инициатора события по адресной информации (IP- адрес, MAC-адрес)
- Отключить от сети при несанкционированном подключении

Спасибо!