FORESCOUT

FORESCOUT EYEINSPECT www.forescout.com

МОНИТОРИНГ И ЗАЩИТА УСТРОЙСТВ В ПРОИЗВОДСТВЕННЫХ СЕТЯХ

Forescout eyeInspect защищает промышленные сети (OT и ICS) от широкого спектра киберугроз, предоставляет возможности как пассивного, так и активного обнаружения устройств для автоматической инвентаризации активов в режиме реального времени. Решение обеспечивает контроль угроз в производственных сетях на основе данных об их потенциальном влиянии на бизнес.

Задачи и проблемы:

- Ограниченная видимость АСУ ТП инфраструктуры или полное ее отсутствие
- Невозможность обнаружения уязвимостей в системах управления производством
- Переизбыток логов
- Усложненный процесс интеграции с SIEM и другими системами
- Медленный и дорогостоящий процесс обнаружения угроз и реакции на них
- Отсутствие карты сети и сведений о географическом местоположении устройств
- Ограниченная стратегия сегментации АСУ ТП сетей
- Невозможность детектирования и понимания информационных потоков
- Недостаточный уровень комплаенса и понимания корректности конфигурации оборудования
- Отсутствие актуальных инвентаризационных данных
- Неточное отслеживание данных о версиях ПО и моделях устройств

FORESCOUT

FORESCOUT EYEINSPECT www.forescout.com

Детектирование угроз АСУ ТП и построение базовой линии

Построение базовой линиии для устройств и групп устройств на основе базы данных индиаторов угроз

Оптимизированный анализ рисков для аналитиков АСУ ТП

Автоматическая агрегация тысяч алертов и миллионов логов в соответствии с уровнем риска и причинами

Выборочное активное сканирование сетей и групп устройств

Неинвазивное выборочное активное сканирование и составление полного профиля устройств

Простая масштабируемость (Enterprise Command Center)

Двухуровневая архитектура позволяет мониторить всю инфраструктуру независимо от распределенности

Ключевые возможности и преимущества:

- Тотальный мониторинг. Устранение слепых пятен, обнаружение новых и вредоносных устройств
- Подробная и точная инвентаризация активов в режиме реального времени
- Видимость устройств любого типа, включая HMI, SCADA, ПЛК, контроллеры, датчики, измерители и I/O
- Обнаружение известных и неизвестных киберугроз на основании тысяч индикаторов, специфичных для производственных сетей
- Выявление кибер- и операционных рисков, их приоритезация в соответствии с уровнем срочности и потенциального воздействия на бизнес
- Обнаружение устройств, не соответствующих комплаенс политикам, по всей сети
- Обнаружение изменений в сети, включая новые устройства, изменения в инфраструктуре и нерегулярную активность
- Построение реакций на предупреждения по заранее определенным автоматизированным рабочим процессам, правилам и действиям по исправлению
- Реакция на изменения статуса комплаенса на основании базовых показателей активов
- Контроль систем управления зданиями (BMS) и систем автоматизации зданий (BAS), включая HVAC и контроль доступа
- Мониторинг всей сетевой инфраструктуры, включая коммутаторы, маршрутизаторы, VPS, контроллеры и точки беспроводного доступа
- Визуализация предупреждений, ведение журналов и создание отчетов