Welcome, I will tell you a bit about Security Enhancements for Network Segregation

Why is it important?

Cyber attacks are generally on the rise

Proportionally larger vs manufacturing

Late to the party, as often overlooked but now industry 4.0

Very long lifecycle

Why is OT – operational technology different from IT

the vendors and producers have not agreed on standard

Leading to hundreds of non-standard protocols

Simple machines expecting exact imput

Probing actively or changing packages can break

Short delays can have big consequences

One machine breaking can delay entire production for weeks

In this case, as it’s chemicals and medicinal products even worse

How did I go about the problem

Minimise exposure to outside communication

Minimaly invasive monitoring, no package inspection, just data flow

No extra monitoring software on systems

In detail?

Separation of networks

Canary servers that can be monitored

Log and historian servers become extra important

How to we get an overview?

The purdue model:Developed in the 1990s by Theodore J. Williams and members of the Purdue University Consortium for computer integrated manufacturing, the Purdue Enterprise Reference Architecture defines the different levels of critical infrastructure used in production lines. PERA was ahead of its time when it was introduced and, implemented correctly, could have achieved the air gap between industrial control systems (ICS) or operational technology ([OT](https://www.zscaler.com/resources/security-terms-glossary/what-is-ot-security)) and IT systems.

8 levels ->

Level 5 Enterprise Network/CLoud

XSOAR control Server

Elastic Log Server

Beyond Trust PAM

Level 4 Site Business and Logistics

SAP

DMZ (Not true DMZ as only one Firewall deployed)

Patch management

Application mirrors

Level 3 Manufacturing and Operations Control

Application Servers

Engineering workstations

Level 2 Area Supervisory Control

Factory Talk

Operator interfaces

Level 1 Basic Control

Batch Control

Safety control

Level 0 Process Control

Sensors Drivers, actuators, robots

We fill in the current situation

Quick go through

Logging/historian

Historian server is properitary database

Can understand factory talk and other such communication

Logs from windows etc directly to Elastic pool

Time is syncronised with timeserver

Removes issue where production devices not always able to keep time

Firewalls

1 by Corporate

2 by plant

Double control for all communication that goes to internet or corporate

Plant engineers get more autonomy in plant network

Jump server

Hardened Server with all security tools

Server team need extra permission for changes

Access is brokered through cloud solution not directly

All sessions are recorded

Canary server

Set up in manufacturing zone

Decoy servers, running same OS as other systems in plant whenever possible

Alarm if anything changes, plant engineers have access but strict instructions not to access

To verify account integrity

Outbound requests needed for

Batch orders,

system updates

effectivity boards

IP requests allowed on firewall level

Domain requests go over proxy server

Last we need to ensure that these are actually monitored

SOC team gets playbooks

XSoar for automated playbook

Infrastructure teams get necessary access to ESX hosts and network parts

And with that we have improved out security posture significantly, as we now have a good overwiev what is happening in our plants

Questions?