ICONS

ICONS Zero Trust architecture

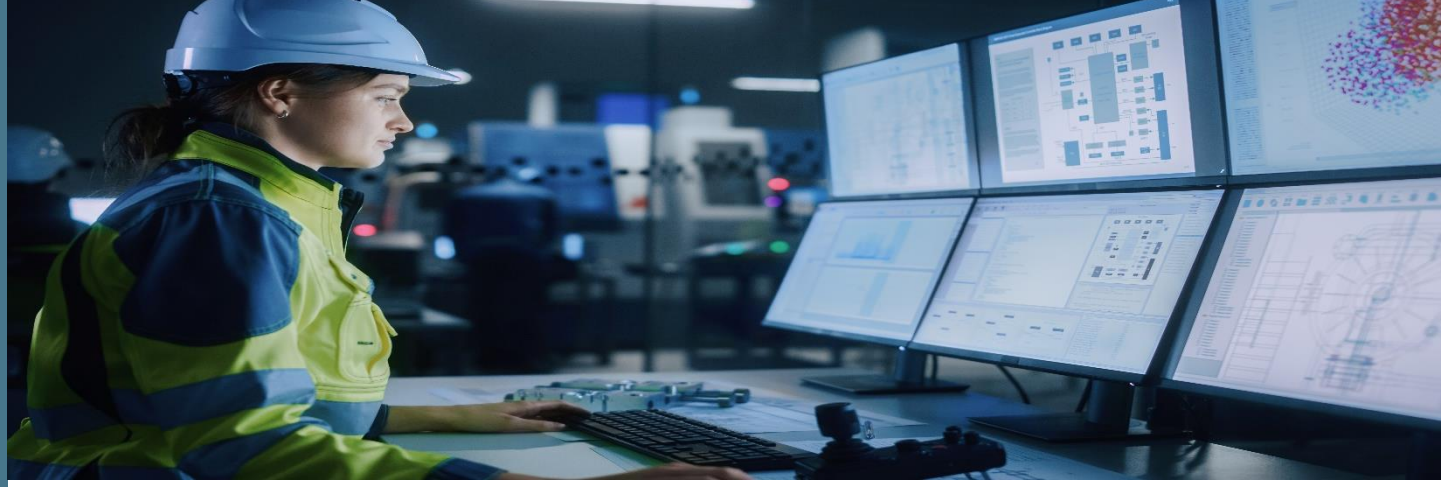
Cyber security i Operational Technology environment with ICONS - Industrial Compliance OT Network Security

Table of Contents

ICONS's Zero Trust Cyber Security architecture is based on ground-breaking design and technology, ICONS is divided into six phases where the network is analyzed, policies are drawn up, real-time monitoring both on the enterprise network and OT network. (PLC/Sensor)

ICONS incorporates disaster recovery into running firewall policies, which ensure locking down of critical systems mapped in phase 1 (DAAS), the policies also ensure that administrators can work unhindered and map how a cyber attack occurred and prevent further damage.

ICONS's Cyber Security architecture



Identifying your protect surface (DAAS)

Protection begins by identifying your protect surface, which is based on data, applications, assets, and services, commonly referenced by the acronym DAAS:

Data: Which data do you have to protect?

Applications: Which applications have sensitive information?

Assets: What are your most sensitive assets?

Services: Which services can a bad actor exploit in an attempt to interrupt normal IT operation?

Identifying data and traffic flow

Identify data flow and the traffic flow across a network determines how it should be protected. The company should document how specific resources interact and the interdependencies of the DAAS.

Architect a Zero Trust network

Since the Zero Trust network can be iteratively deployed with the existing systems and adopts a holistic approach, it can be customised around the

protect surface, once the protect surface is defined and the data/traffic flows is mapped, we can build a Zero Trust architecture starting with Fortigate

firewall as central policy server, with Micro and Nano network segmentation, we strengthen the protect surface and limit the lateral movement attack.

With Network Access Control (NAC) we continuously verify user and devices to ensure non profiled entities enter the network. ICONS also uses

Honeypots both in IT and OT networks.

Create Zero Trust policy for all users and devices

Create Zero Trust policy on our FortiGate, this documenting which resources should have access to others. Active Directory should be used as the primary container for users, groups etc.

The following questions should be answered:

Who should be accessing a resource?
What application is being used to access a resource inside the protected surface?
When is the resource being accessed?
Where is the packet destination?
Why is this packet trying to access this resource within the protect surface?
How is the packet accessing the protected surface via a specific application?

Implement real-time monitoring with SIEM

ICONS offers real-time monitoring of all devices in the Purdue model including in level 0 and 1.

To improve breakout time, when an attacker breaks into the system, compromises it, and then laterally moves to other systems.

ICONS's SIEM solution allows the security team to detect an intrusion faster, investigate and remediate the intrusion, and prevent further instances.

Implement disaster recovery within policy server

Disaster recovery firewall rules controls traffic flow when disaster happens, this rules is disabled by default and can be enabled automatic or manuel.

This rules allows intercommunication services between Active Directory and the central firewall, this allows critical functionality, it also allows administrators to investigate and document the attack, furthermore the rules isolate critical systems defined by the protect surface

Contact ICONS: