Control System Cyber-Physical Security for Facilities

08/10/21

Ron@ronvictor.com

408-316-3982

TOPIC

Protect & Prevent Critical Cyber-Physical Infrastructure from Cyber Attacks

WHY

At least 1300 “known” severe critical infrastructure cyber incidents since 2005

1500 people dead

Over $70Billion in direct damages

Source: Information Technology (controlglobal.com)

IN ADDITION

Solar Winds, Colonial Pipeline, JBL Foods, Bay Area Water

……and a whole lot more

https://industrialcyber.co/article/hackers-see-big-bucks-in-ot-infrastructure-cloud-adoption-picks-up

CRITICAL INFRA HAS SIMILAR CYBER SECURITY VULNERABILITIES AS ENTERPRISE IT

Identity & Authentication

Who Is this person?

Can we verify that he actually is who he says he is?

Are his credentials secure

Trust & Authorization

Is he authorized to connect?

Who authorized him to connect?

What is he connecting to?

Was he supposed to connect to what he is connecting to?

Devices & Applications

Is his laptop/tablet secure?

What applications did he run?

Was he authorized to run those applications?

Are those applications patched?

Audit & Compliance

Which network is he using?

When did he log in?

When did he log out?

What changes did he make?

Do we have an audit log available?

…….and more

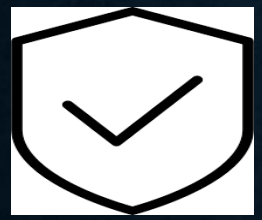
PROBLEM

Authentication

- Can we identify the service technician
- Can we identify the devices and systems
- Can we identify the network – public/private

Trust

- Can we trust the laptops, mobile and any other devices used for access
- Can we trust the applications and software used to access
- Can we trust the network – these applications are only allowed access from within my network



Authorization

- Does the person have sufficient privileges to access remote system
- Is access allowed during a particular time period?
- Can manager authorize certain actions before they are performed

Audit

- Can we find out who had access to my infrastructure ?
- Can we identify anomalous access ?
- Can the access and modification to system under use be logged

Compliance

- The Essential Critical Infrastructure Workers Guidance Version 4.0 ?
- Presidential Policy Directive 21 (PPD – 21)
- GDPR, NERC, NIST and others

PROBLEM AT SCALE

Thanks to 5G+IoT

WHY NOW? – THE PERFECT STORM!

Remote Workforce

Cloud Adoption by Critical Industrial Infrastructure (AI/ML)

Digital Transformation (IoT+5G adoption)

Connected EVERYTHING

Federal Govt. Mandates!!!

“I know from our perspective there’s certainly been a great increase over the past year or so in remote operations. For many of our customers, the increase in remote access and having secure control of remote access into plants is something that has jumped off the charts here and we expect that trend to continue.”

Paul Griswold
Chief Product Officer
Honeywell Connected Cybersecurity

https://industrialcyber.co/article/hackers-see-big-bucks-in-ot-infrastructure-cloud-adoption-picks-up

THE NEED

1. SECURE REMOTE ACCESS as-a-Service for Remote Workforce for Critical Industrial Infrastructure
   - Virtualization in the Cloud

2. SECURE EDGE COMPUTE infrastructure for DATA ACQUISITION for Cloud Adoption by Critical Industrial Infrastructure (AI/ML)
   - Virtualization at the Edge

A GDPR compliant architecture that meets both requirements

A PROPOSED SOLUTION

Air Gap
Authenticate
Isolate
Audit
Virtualize

Water Treatment Plant

Power Plant

Wind Farm

Solar Farm

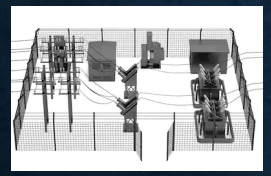
Transportation

Remote Workforce

Smart City

AI Driven
Operations Cloud
as a managed service

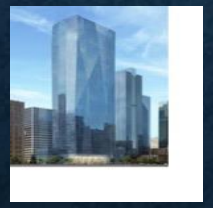
Data Lake



Substation

Refineries

Factories



Buildings

Frack Sites

Oil Rigs

Mines

A Single Uniform Secure Operations Cloud Platform for Ingress and Egress of People and Data from all Facilities

THE PROPOSED ARCHITECTURE

Third Party Vendor Clouds/Data Lakes

Remote Vendors

Enterprise Clouds/Data Lakes

Compliance Framework

App Zone (Windows/Containers)

Inventory Databases (User, Device, Applications)

Trust Inference

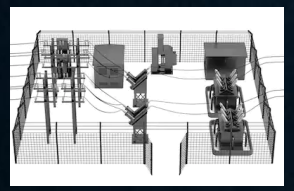
Overlay Routing

Access Control & Firewall

Access Proxies

Authentication & Single Sign-on

Cloud Infrastructure (AWS/Azure/GCP/VMware)

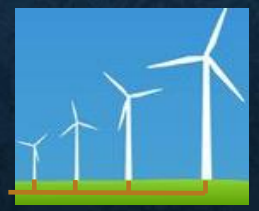


Substation

Power Plants

Factories

Buildings



Wind Farm

Oil Rigs

Mines

Refineries

Water Plant

Third Party Vendor Clouds/Data Lakes

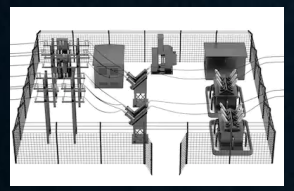
Remote Vendors

Enterprise Clouds/Data Lakes

Edge Orchestration + Third Party App Store

Operations Cloud

Network (SDN, Routing, PHY)	**Security** (Segment, Firewall, Isolate)	**Virtualization** (Third Party Containers)
Secure Managed OS		
COTS Hardware / VM (VMWare)		

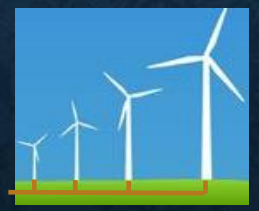


Substation

Power Plants

Factories

Buildings



Wind Farm

Oil Rigs

Mines

Refineries

Water Plant

Enclave Manager

Controller

Enterprise Clouds/ Data Lakes

Remote Workers

Operations Cloud Tenants

Access & Admin Portal

Access Control

Firewall/Proxy

Compliance

3rd party SaaS Gateways

App Virtualization

Identity

OPERATIONS CLOUD ENCLAVES

Machine Edge

Edge SDK

Smart Edge

Edge Appliance (COTS)

Network Edge

Edge Container

Azure Stack Edge / AWS Outpost / Google Anthos

Facility Infrastructure and IoT Devices

Enclave Manager

Controller

Remote Workers

OPERATION CLOUD TENANTS

Access & Admin Portal

Access Control

Firewall/Proxy

Compliance

3rd party SaaS Gateways

App Virtualization

Identity

VDIs

SCADA

Control Servers

Legacy Windows

OPERATIONS CLOUD ENCLAVE

Enterprise Clouds/ Data Lakes

Machine Edge

Edge SDK

Smart Edge

Edge Appliance (COTS)

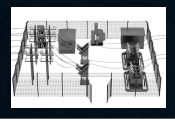

Network Edge

Edge Container

Azure Stack Edge / AWS Outpost / Google Anthos

Fieldbus · HART · EtherNet/IP · EtherCAT · PROFINET · LonWorks · OBD2 · CAN bus · Modbus · BACnet · OPC UA

Industrial Infrastructure and IoT Devices









THANK YOU

RON@RONVICTOR.COM
408-316-3982