DEFEATING INSIDER THREATS TO CRITICAL INFRASTRUCTURE

Chris Blask
Global Director Industrial Control Systems
Unisys
@chrisblask

Eric Knapp
Chief Engineer, Cyber Security Solutions and Technology
Honeywell
@twitter
The World is Changing for Industrial Enterprises

• Things are changing
  • Modern devices are smarter and better connected
  • Cost savings are driving adoption of new technologies
  • Challenging traditional approaches to security

• There will be winners and losers
  • Digital innovation provides competitive advantages
  • The risk is market viability in the coming years

• Successful change is hard
  • Planning, coordinating, policies, security
  • While increasing business effectiveness

• You need mature partners
  • Executive support
  • Execution support
  • Stability and reach
An ICS Security Primer

“OT is different than IT”

“The safety system will take care of us”

“We're safe behind an Air Gap”

“ICS predates security”

“We can't go offline long enough to upgrade”

“Hacking a control system requires specialized knowledge”

“Security by obscurity”
Even With The Best Intentions

1,000,000 GFLOPS

1,000 GFLOPS

40 GFLOPS

Modern Servers

Legacy Servers

“Air Gap”

Capability
The Recommended Solution

- **Strategy**
  - Have one

- **Standards**
  - Learn from them

- **Integration**
  - Embrace it

- **Digitalization**
  - Own it
SMX Example

- Moving to the cloud
  - Management says do it
  - Security team says absolutely not

- What Standards apply?
  - ISA-99/IEC 62443

- Integration of OT
  - Honeywell realized that with SMX needed a 62443 Zoned solution to isolate from customer networks

- Digitization of Solution
  - Own the entire solution
  - In this case end-to-end cryptographic zoning to achieve the first ISA-99 compatible cloud
We’ve Got an Industrial Cloud … Now What?
Questions?

christopher.blask@Unisys.com
eric.knapp@honeywell.com

Come see us at the ICS Village in the exposition area