ASSESSING [INDUSTRIAL CYBERSECURITY] ASSESSMENTS

Why most of industrial cybersecurity assessments are wrong?

Samuel Linares (@infosecmanblog)  
Europe & Latin America OT Security Lead
WHO IS ACCENTURE OT SECURITY?

EXTENDING SKILLS THROUGH ACQUISITIONS:
• Cimation
• FusionX
• Maglan
• Evopro
• ATAN
• Omnetric (Accenture / Siemens Joint Venture)
• Schlumberger Business consulting
• Investment in Joint Industry initiatives and Acquisitions is continuing throughout 2018/2019

PARTICIPATING IN INDUSTRY STANDARDS CREATION:
• Accenture team members are contributing authors to ANSI/ISA 62443-3
• Accenture is an active member of the Information Security Forum
• Accenture is a participant, collaborator, and contributor to the multi-industry initiative Risk Management Process

BUILDING ASSETS TO COMMODITIZE & INDUSTRIALIZE SERVICES
• Accenture Tech Labs for Security R&D (Technology radar, new solution scanning, incubation & innovation)
• Risk Assessment as a service
• Industrialized deployment services
• ICS Threat & Vulnerability Controls Database, etc.

CONSULTING EXPERTISE
6000+ Security practitioners worldwide
1000+ Plant Operation professionals

200+ OT Security Professionals
600+ Global Industrial Cyber Security Professional (GICSP) certified employees

ALLIANCES & JOINT INITIATIVES

Copyright © 2019 Accenture. All rights reserved.
assess:  [something]

1. Evaluate or estimate the nature, ability, or quality of.

   1.1. Calculate or estimate the price or value of.

   1.2. Set the value of a tax, fine, etc., for (a person or property) at a specified level.
[something]?
Industrial Cybersecurity
Industrial Cybersecurity
Industrial Cybersecurity

8 years, $3.5 billion, 30 years

Design
- 4 million man hours
- 50,000 design drawings

Construction
- 20 million man hours
- 66,000 tons in weight
- 6000 valves
- 250 km of piping
- 225 km of cabling

Operation
- Evolution of Processes, People and Technologies
- 30 years
- $3.5 billion
- 209 years
- 10,000 workers
Industrial Cybersecurity

What?

Where?

When?

Why?

Who?

How?
What?

(Activities)

MATURITY

TECHNICAL

RISK

TESTING

Active  Passive
Where?

(Libels)

- National
- Sector
- Entity/Organization
- Process
- System
- Network
- Device
When?

(Phases)

**PLAN**
- Conceptual Design
- Initial Specifications

**DESIGN**
- Front-end Engineering Design
- Detail Design
- Procurement and Acquisition

**BUILD**
- Provision (FAT, iFAT)
- Execution (SAT)

**OPERATE**
- Operation and Maintenance

Evaluate cybersecurity and develop initial specifications

Develop reference architecture, detail cybersecurity specifications and procurement support

Conduct cybersecurity tests during FAT, iFAT and SAT

Manage and operate industrial cybersecurity
Why?
(Reasons)

What?

Where?

When?
Who? (Stakeholders)

CONSULTANTS

CYBER VENDORS

INDUSTRIAL VENDORS

EPCs

SYSTEM INTEGRATORS
How?

Time to think about SUCCESS
CAPABILITIES
EXPERIENCE
THANK YOU

SAMUEL LINARES
Samuel.Linares@Accenture.com
@infosecmanblog