Oil and Gas Infrastructure Resilience

Al Rivero, PE

ANG Consulting, LLC

CREDC PACIFIC Northwest Industry Workshop
Cybersecurity Research Needs - an Energy Sector Perspective

November 28th – 29th 2017

IoT: Connecting the Unconnected

50 Billion “Smart Objects”

Rapid Adoption Rate of Digital Infrastructure:

5X Faster Than Electricity and Telephony

World Population

TIMELINE

BILLIONS OF DEVICES

Inflection Point

2010 2015 2020

6.8 7.2 7.6
Converged, Managed Network

Operational Technology

- Traffic Control
- Telemetry
- Passenger Wi-fi
- Passenger Safety

- Trains
- Machine Parts
- Access Points
- Video Cameras

Information Technology

- ERP
- CRM
- VOIP
- Video

- PCs
- Smart-phones
- Data-Center
- Branch Offices
Shift in Architectural Philosophy

From

Closed Systems
(Little external interaction)

Proprietary Networks
(Usually layer 2 based)

Various Protocols
(Modbus, SCADA, BACnet, LON, HART)

Protocol Gateways
(Inherently complex, inefficient and fragmented networks)

To

Standardized Networks
(IP Based/ISO Stack)

Standardized Interfaces
(Wireless/Wired)

Geographically Distributed and Remote Edge Systems
(support for IP and non-IP)
Typical Oil and Gas Monitoring
Client Survey 21 Respondents

• Gaps in Technology
  • Slow to respond to threats
  • White Listing has many gaps in Industrial Networks
  • Struggling between White Listing and Black Listing
  • Current OS Environment Complexity (MS 72% and Lunix/Unix 28%)

• What Keeps you awake at night
  • 3rd Party connections (Vendors, Contractors, Maintenance)
  • Field Wireless Connection
  • Site Access (Controlling field access, Monitoring facilities, Drones becoming a major issue*)
  • MS Only AD Managed by third party
Client Survey 21 Respondents

• Needs for Closing the Gaps
  • Real White Listing solutions for IoT (Backend Network)
  • Real time scanning and blocking of 3rd party connections and threats
  • Faster Black Listing ID and role out capabilities
  • Skinny MS OS*, Lower patching

• Would industry be whiling to share in cost to develop
  • Most industry segments feel they invest in research through there, funded industry partners and vendors. But the progress has been slow

• What do you feel is needed to expedite the research
  • Most feel they have done everything possible except the trusted insider, not sure how to manage this threat.
  • No known real threat – not personal
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security