My Background

Started in IT in 1980

Started working with OT systems in 1998

Drilling, downhole, pipelines, refining and retail of petroleum products

Supported manufacturing systems

Support for Foothills Hospital ICU ward
What I will cover

- Similarities and differences – big picture
- Similarities and differences – DFIR
- What to ask
- Aligning with Processes
- Tools
- Communicating with Field Staff
ICS is different!

Pipeline IR

No it’s not!
Different

- Uptime and safety
- Physical interaction
- Blue team practices are new
- “Pre-cyber security” designs
- Less known protocols
- And when things go wrong...
They go really wrong!
The Same

- Limited number of breach scenarios
- Computers are still computers.
- Code is still code.
- Standards
- Time is money

Time is money
One Small Refinery

- $368.00 per minute
- $22,080.00 per hour
- $529,920.00 per day
What to ask Before you arrive

• What appears to have happened?
• What systems do you have?
• Do you have a firewall?
• Do you have any logging?
What to say when you get there

Safety orientation

Expect PPE

“Show me / Tell me about it.”
Processes

Identification
Collection
Preservation
Analysis
Reporting
Processes 2

- Interviewing
- Chain of custody
OT Processes

Event reconstruction

Config files
• Logs
  – Historian
  – OS
  – PLCs

- HMI
- Network
- RTUs
Acquisition tools

- Disk duplicators
- Memory acquisition
- Network based acquisition tool
- JTAG equipment
Some of the Gear
Field HMIs
Gear II

Operator HMI screen
Gear – III

AB 505C / Rockwell 1700 series
**Gear IV**

**Riverbead Flow Meter**

---

**General Description**

The Model 2204 Remote Terminal Unit (RTU) is an advanced intelligent electronic device that is used for data acquisition, local/remote control and simple to complex real-time processing of field or plant data. The compact Model 2204 RTU is designed for small to medium size sites. Up to 4 I/O modules can be field proven RTU software is available for a broad range of process applications such as gas/oil well and pipeline flow control, plant process control and electrical utility power distribution monitoring and control. The RTU has a Web interface for easy configuration from any standard PC, without the need for any custom software. Uses the stable open source Linux operating system.
• They are people, too
• Proud of their site
• Willing to share
• Expect them to question you.

Talking to Field Staff
Real Examples

• Rogue 3rd party
• German Steel factory
Questions?

- smokydbear.ca
- smokydbear@gmail.com
Special Thanks

• David Cowen
• Eric, Keith, Robert and Matt E.
THE WEBCAST WILL BEGIN SHORTLY