# Oil & Gas Infosec 101

DEF CON 21

DC101

# whoami && id

- 18 years in IT/Infosec
- Family business
- Worked in Oil & Gas (O&G) last 8 years
- Along the way
  - Pen testing local and federal gov’t
  - <REDACTED>

# What’s the big deal?

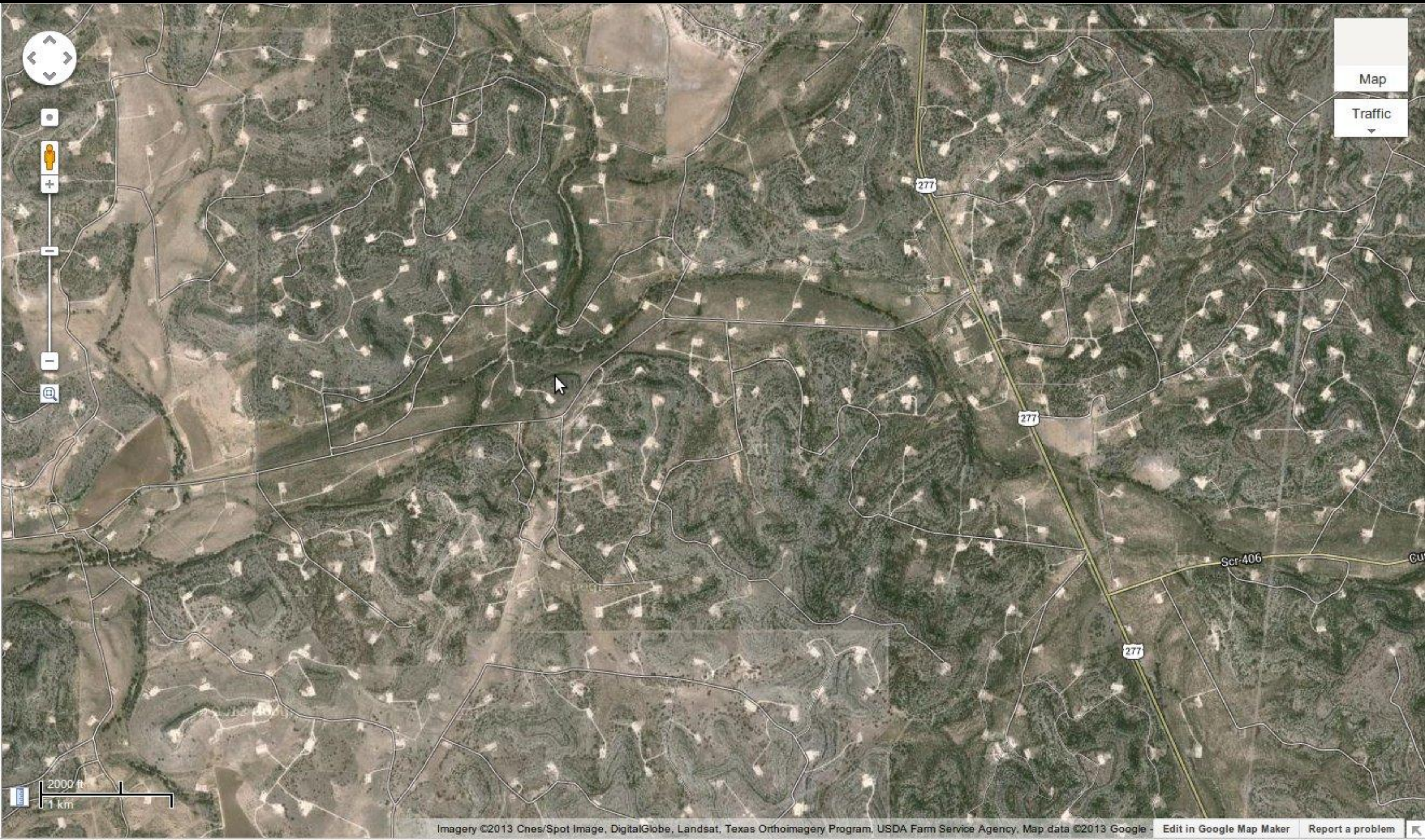
Oil & Gas is overlooked

- Ever-increasing target
- Legacy components & security issues
- **Whether you care about attack or defense, O&G is an area of which you need to be aware**

# Media Notes

- “Cyber attack targets gas pipeline companies” – 05/08/12 [1]
  - Spear phishing
  - DHS asked operators to let attackers remain
- “Aramo Says Cyberattack Was Aimed At Production” – 12/09/12 [2]
  - 30,000 workstations impacted
  - Intended to disrupt O&G production
  - Began on non Internet-connected workstation

# The energy industry needs help to catch up!



Imagery ©2013 Cnes/Spot Image, DigitalGlobe, Landsat, Texas Orthoimagery Program, USDA Farm Service Agency, Map data ©2013 Google -

# What is this?

# Location challenges

- Remote Locations – Fields, Pipelines
- Often little infrastructure
- Comms vary
  - Serial
  - Microwave
  - Licensed/unlicensed radio
  - 802.11/16 wireless

# Location challenges

- Traditional IT form factor may not work
- Need secure assets in insecure locations
- Rarely “one size fits all”

# Technical challenges

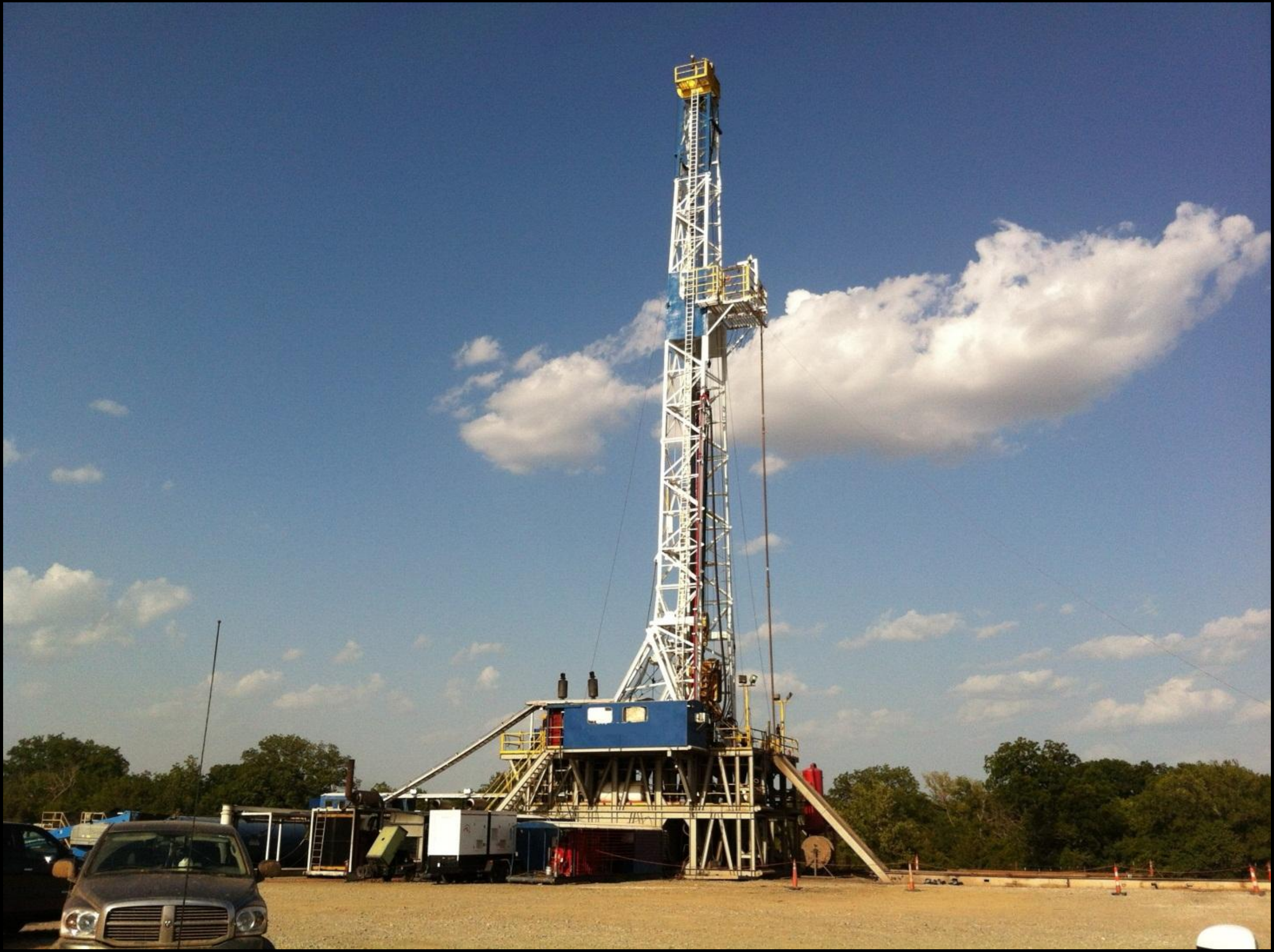
- Often have older equipment
- Patches? We don’t need no…
- Integrating dissimilar networks
- Field equipment – “Where’s the RJ45?”

# Low-hanging fruit

- Lots of default passwords
- Closed policy/default deny at boundaries
- Least privilege

# SCADA

- RTU, PLC, HMI, wtf?
- Defense in depth needs different approach
- Understand your data flows



# What’s this?

# Know your business

- Understand your specific business
  - Upstream – Exploration & Production (E&P)
    - Finding and getting product out of ground
    - Wells, rigs, gathering systems, etc
  - Midstream – Pipelines & Transport
  - Downstream
    - Refining
    - Marketing/selling
- Recommendations need to make business sense

# Know your business

- Talk to business users/managers
  - Understand their specific concerns
  - Where security needs to be applied
  - You are interested in helping, not just saying “no”
- You’re not going to win every battle
  - While security is always a compromise, **don’t compromise on security**
  - Functionality can trump security

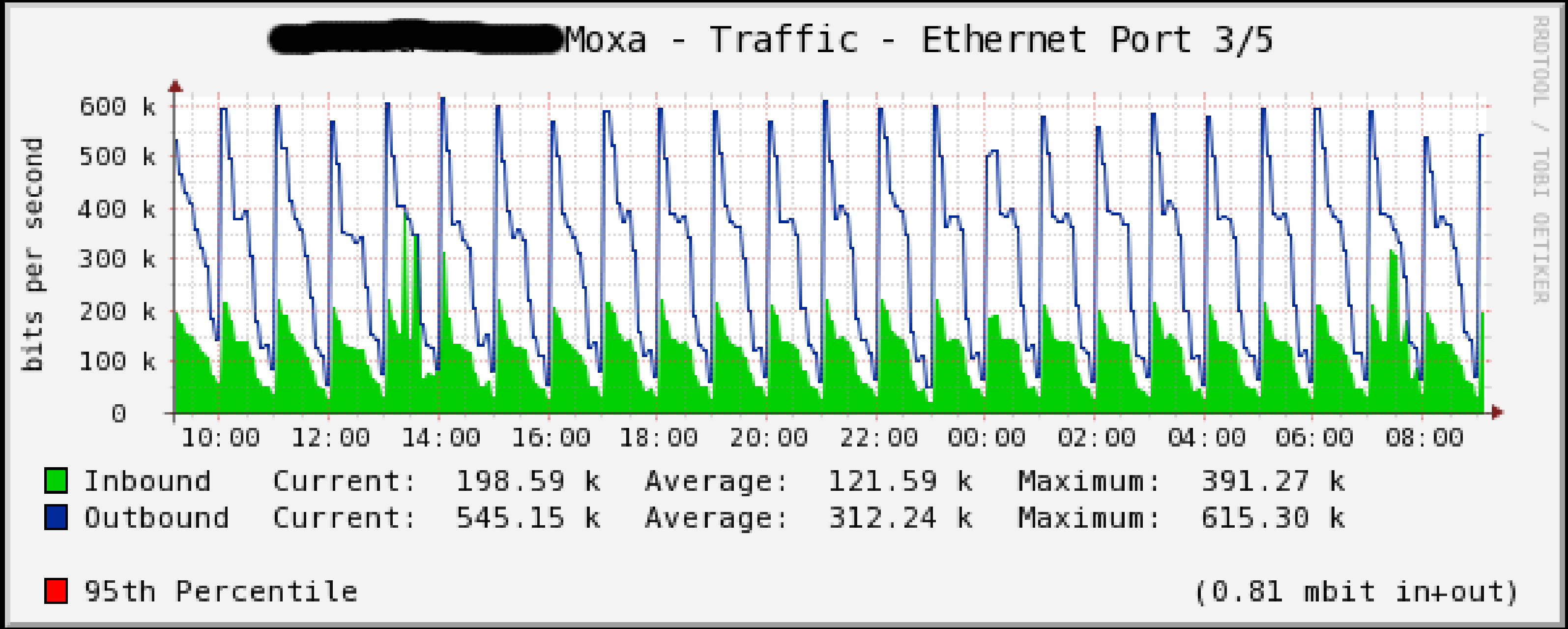
# Know the tech

- Use free/cheap Network IDS (Snort & Quickdraw sigs)
- Characterize your data flows & place accordingly
  - Data-to-data (Historians)
  - User-to-data (HMI, Viz apps)

# Know the tech

- Start scanning/profiling
  - Nessus has SCADA plugins
  - Wireshark can decode DNP3 and Modbus
  - Cacti is flexible and free
- Talk to the engineers & field hands
- Poke/prod/study surplus or test equipment

# Know yourself

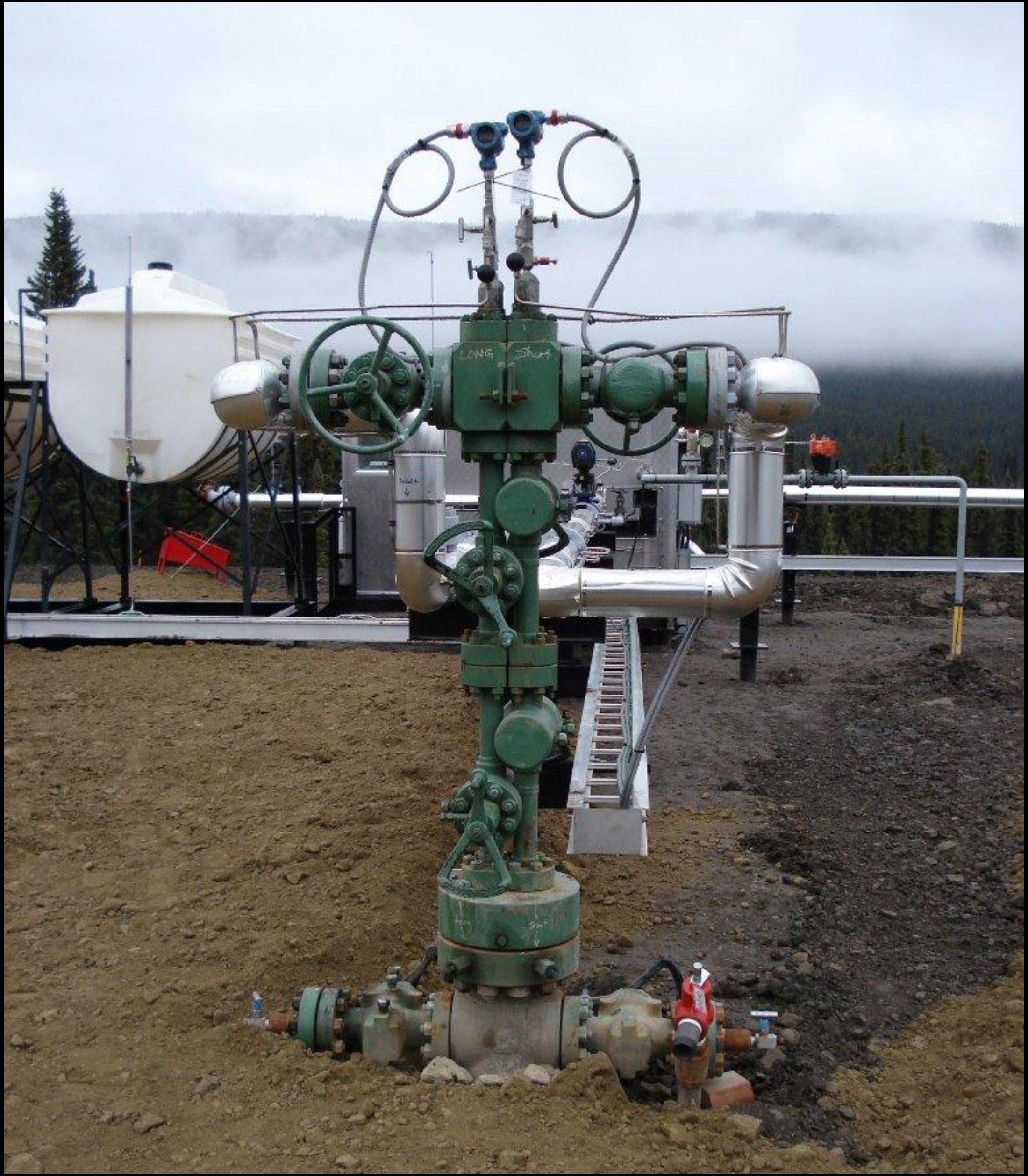


[redacted]Moxa - Traffic - Ethernet Port 3/5

```
🟩 Inbound    Current:  198.59 k   Average:  121.59 k   Maximum:  391.27 k
🟦 Outbound   Current:  545.15 k   Average:  312.24 k   Maximum:  615.30 k

🟥 95th Percentile                                    (0.81 mbit in+out)
```

- Patterns are your friend!



# What's this?

# Final thoughts

- Proper infosec can save time, money, and lives
- Can’t be 100% secure, rapid response & containment is crucial

- Questions?

# References

- [1] Kelly, S. (2012, May 8). Cyber attack targets gas pipeline companies. Retrieved 7/2/2013, from CNN website, http://security.blogs.cnn.com/2012/05/08/cyber-attack-targets-gas-pipeline-companies/
- [2] Reuters (2012, December 9). Aramco Says Cyberattack Was Aimed At Production. Retrieved 7/2/2013, from The New York Times website, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0
- Slide 5 – Smokey the Bear (Public Domain) – http://en.wikipedia.org/wiki/File:Smokey3.jpg
- Slide 12 – Drilling Rig – Copyright Aaron Bayles
- Slide 18 – Wellhead (Public Domain) – http://commons.wikimedia.org/wiki/File:Wellhead-dual_completion.jpg