

# The BS is Certainly Deep

Sorting out hype from reality in industrial deep packet inspection technologies

Eric Byres P.Eng, ISA Fellow  
eric.byres@ics-secure.com



**ICS Secure**  
INDUSTRIAL SECURITY CONSULTANCY

# Today's Talk...

- **Review:** Understanding DPI
- **Issues:** What Can Possibly Go Wr0ng?
- **Solutions:** What Industry Really Needs

# **Review: Understanding DPI**

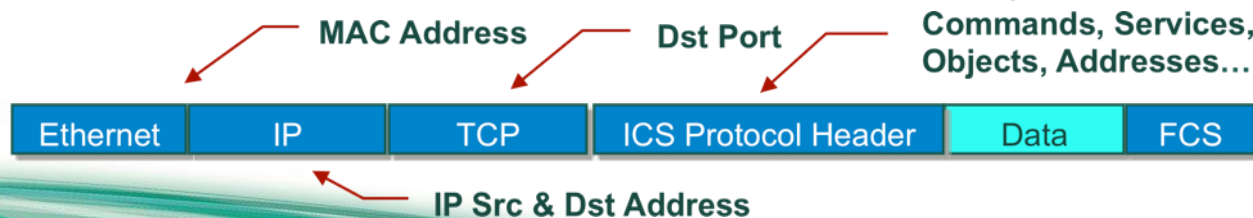
# Stateful Filtering of TCP/IP Traffic

- Originally most firewalls were designed to inspect and filter at the TCP/UDP and IP layers:
  - Source IP Address
  - Destination IP Address
  - Destination TCP Port Number
- The upper layers are NOT inspected



# Deep Packet Inspection

- DPI technologies were designed to inspect at both:
  - TCP/UDP and IP layers (just like a regular firewall)
  - Session, Presentation and Application layers
- **Ideally** can locate commands, services, objects addresses (and even data) in ICS traffic
- Used in firewalls, IDS/IPS, anomaly detect'n tools

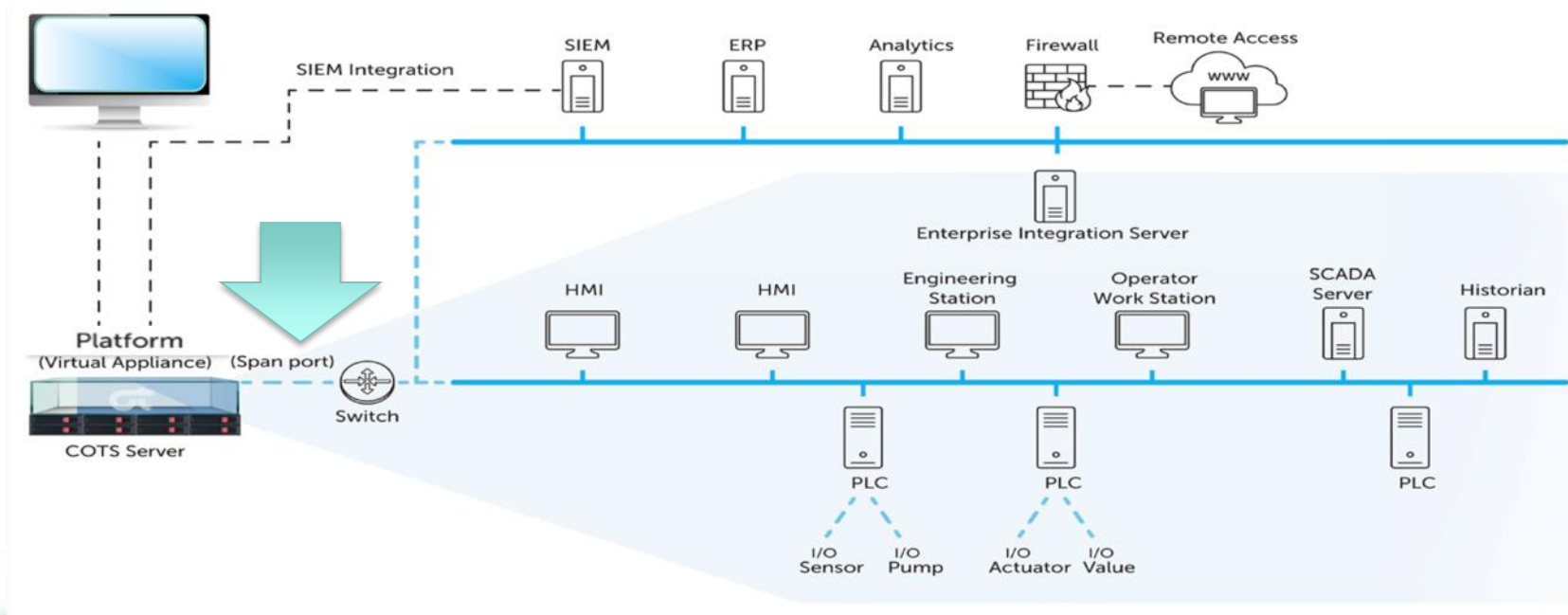


# Promises, Promises

- ***“Extreme Visibility:*** *[our product] dives deep into the network, uncovers hidden information, and generates actionable insights to secure and optimize even the most complex OT environments.”*

# Issues: What Can Possibly Go Wr0ng?

# Just plug it in!



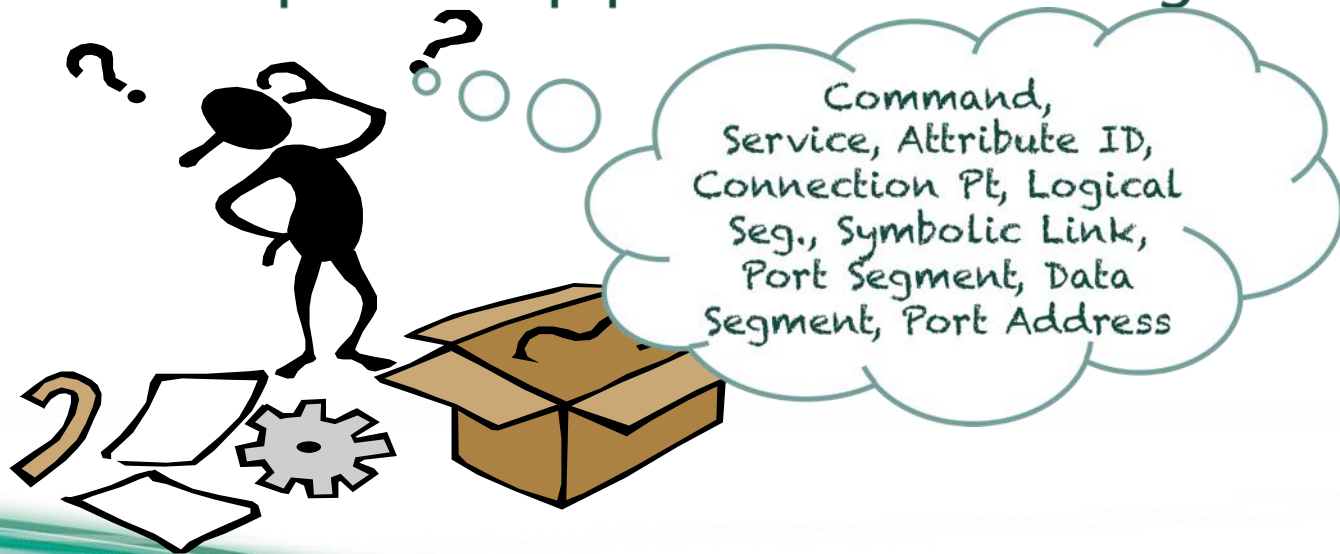


# Where did that Span Port go?



# “Complexity is the Enemy of Security”

- Few ICS engineers understand what is “on-the-wire”
- But some tools require deep protocol knowledge



# "Complexity is the Enemy of Security"

The diagram illustrates a complex security interface with various fields and labels. The labels are arranged in a grid-like fashion, with lines pointing to specific fields in the interface. The labels are:

- Class ID
- Member ID
- Service ID
- Connection Point
- Port Seg Number
- Data Segment Type
- CIP Service
- Instance ID
- Attribute ID
- Special
- Symbolic Segment
- Port Seg Address


The interface itself is a form with various fields and sections. The fields are:

- ClassID
- MemberID
- ServiceID
- Special
- ConnectionPoint
- Symbolic Link
- PortNumber
- Address
- Data Segment
- Match buffer

The sections are:

- Match class id on a CIP segment type logical.
- Match instance id on a CIP segment type logical.
- Match member id on a CIP segment type logical.
- Match attribute id on a CIP segment type logical.
- Match service id on a CIP segment type logical.
- Match special data on a CIP segment type logical.
- Match connection point on a CIP segment type logical.
- Match symbolic link on a CIP segment type symbolic.
- Match port number on a CIP segment type port.
- Match address on a CIP segment type port.
- Match data on a CIP segment type data.
- Match data with the provided content in hex.
- Match data starting from this offset.

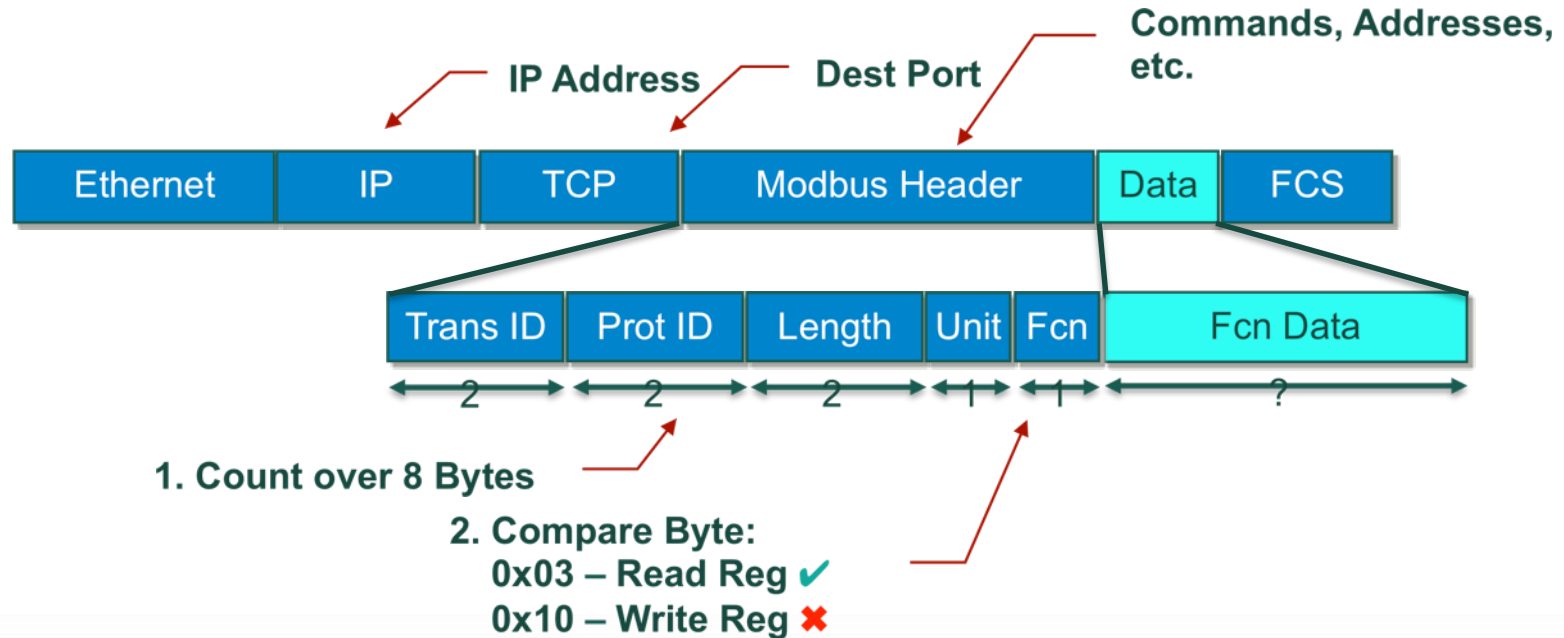
# ICS Protocols in the Real World

- Many ICS products do not comply with the published protocol specifications **yet they work**
  - DPI tools must work with real ICS products, not the protocol specification:
    - Must embed “special” cases for real-world functionality
    - Must allow user control over validation and state tracking to reduce false-positives
- 

# A Little Tailgating?

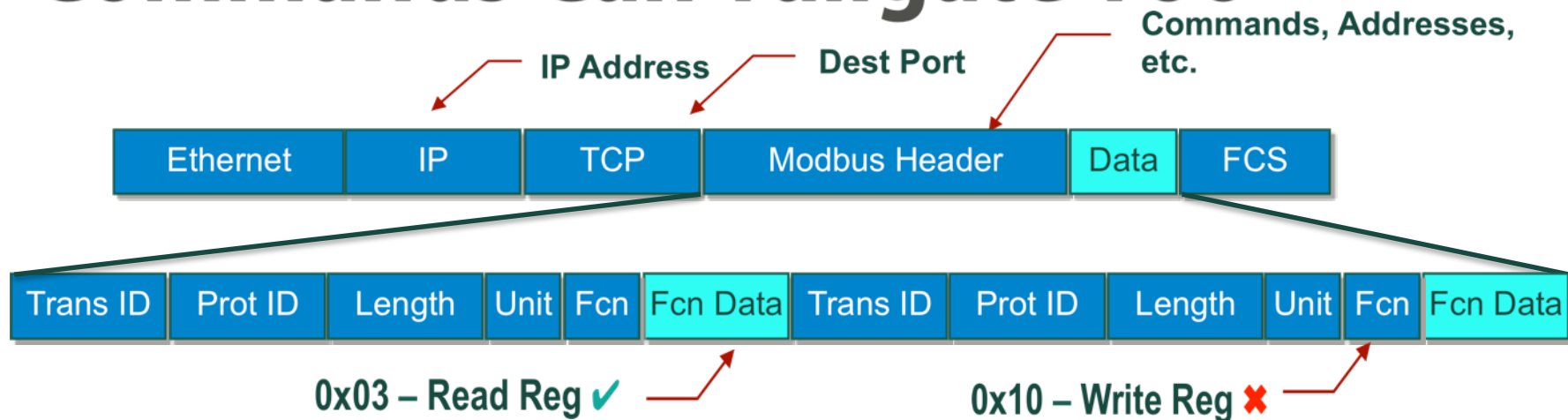


# A Simple Modbus DPI Read Filter





# Commands Can Tailgate Too



# Commands Can Tailgate Too

PipelineTestB.pcap

Apply a display filter ... < %>

No.	Time	Source	Destination	Protocol	Length	Info
5	0.085054	192.168.3.63	192.168.3.254	Modbus/TCP	309	Response: Trans: 6279; Unit: 0, Func: 3: Read
6	0.085110	192.168.3.254	192.168.3.63	Modbus/TCP	426	Query: Trans: 6403; Unit: 0, Func: 3: Read
7	0.086449	192.168.3.63	192.168.3.254	Modbus/TCP	309	Response: Trans: 6280; Unit: 0, Func: 3: Read
8	0.086483	192.168.3.254	192.168.3.63	Modbus/TCP	426	Query: Trans: 6404; Unit: 0, Func: 3: Read

Frame 6: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits)

- Ethernet II, Src: Dell\_cc:f7:12 (00:26:b9:cc:f7:12), Dst: Telemech\_07:6d:a7 (00:80:f4:07:6d:a7)
- Internet Protocol Version 4, Src: 192.168.3.254, Dst: 192.168.3.63
- Transmission Control Protocol, Src Port: 4364, Dst Port: 502, Seq: 13, Ack: 256, Len: 372
- Modbus/TCP
- Modbus
- Modbus/TCP
- Modbus
- Modbus/TCP
- Modbus
- Modbus/TCP
- Modbus
- Modbus/TCP
- Modbus
- Modbus/TCP
- ...

```

0040  00 7b 18 8f 00 00 00 06 00 03 03 d9 00 7b 18 93  .{.....{..
0050  00 00 00 06 00 03 05 c5 00 7b 18 97 00 00 00 06  .....{.....
0060  00 03 07 b1 00 7b 18 9b 00 00 00 06 00 03 09 9d  ....{.....
0070  00 7b 18 9f 00 00 00 06 00 03 0b 89 00 7b 18 a3  .{.....{..
0080  00 00 00 06 00 03 0d 75 00 7b 18 a7 00 00 00 06  .....u{.....
0090  00 03 0f 61 00 7b 18 ab 00 00 00 06 00 03 11 4d  ...a.{.....M
00a0  00 7b 18 af 00 00 00 06 00 03 13 39 00 7b 18 b3  .{......9...
    
```

Modbus/TCP (mbtcp), 12 bytes      Packets: 18889 · Displayed: 18889 (100.0%) · Load time: 0:0.164    Profile: Default



# Nested Commands and Services

- More sophisticated ICS protocols build in “Multiple Service” options
- Nothing forbids massive nesting of these “commands within commands”

```
[-] Common Industrial Protocol
  [+ Service: Multiple Service Packet (Request)
    Request Path Size: 2 (words)
  [-] Request Path: Message Router, Instance: 0x01
    [+ Path Segment: 0x20 (8-Bit Class Segment)
    [+ Path Segment: 0x24 (8-Bit Instance Segment)
  [-] Multiple Service Packet (Request)
    Number of Services: 33
    [-] Service Packet #1
      Offset: 68
      [+ Common Industrial Protocol
    [-] Service Packet #2
      Offset: 78
      [+ Common Industrial Protocol
      [-] CIP Class Generic
        [+ Command Specific Data
    [-] Service Packet #3
      Offset: 90
      [+ Common Industrial Protocol
      [-] CIP Class Generic
        [+ Command Specific Data
    [+ Service Packet #4
    [+ Service Packet #5
    [+ Service Packet #6
    [+ Service Packet #7
    [+ Service Packet #8
    [+ Service Packet #9
    [+ Service Packet #10
    [+ Service Packet #11
    [+ Service Packet #12
```

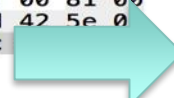

# A Little Over-Promising

- *“All The Data Needed About Your Environment:*
- *Asset Unique Descriptors:*
  - *IP Address, MAC Address*
  - *Equipment vendor*
  - *Equipment type (PLC, HMI, etc.)*
  - *Asset model number*
  - *Asset serial number*
  - *Firmware version*
  - *Physical data (rack slots)*
  - *And more...”*

# A Little Over-Promising

21.3843...	10.0.3.4	10.0.2.2	CIP CM	114	Unconnected Send: Identity - Get A
21.3959...	10.0.2.2	10.0.3.4	CIP	133	Success: Identity - Get Attributes
21.3964...	10.0.3.4	10.0.2.2	CIP CM	142	Connection Manager - Forward Open
21.4065...	10.0.2.2	10.0.3.4	CIP CM	124	Success: Connection Manager - Forw

- ▼ Attribute: 3 (Product Code)  
Product Code: 54
- ▼ Attribute: 4 (Revision)  
Major Revision: 17  
Minor Revision: 3
- ▼ Attribute: 5 (Status)  
▶ Status: 0xb060
- ▼ Attribute: 6 (Serial Number)  
Serial Number: 0x005e429d
- ▼ Attribute: 7 (Product Name)  
Product Name: 1756-L61/B LOGIX5561

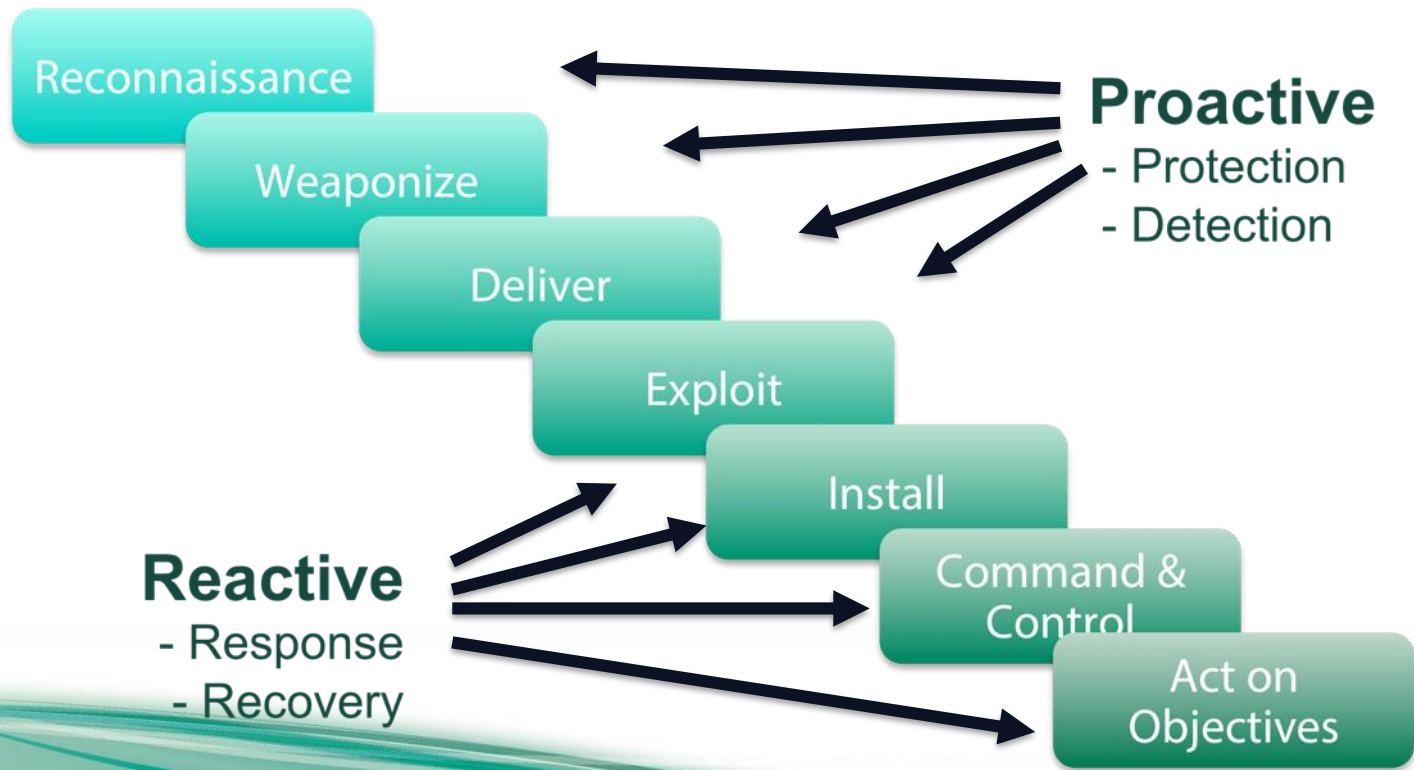


```
0000 00 d0 c9 b3 2a 5a 00 07 32 11 98 40 08 00 45 00 .....*Z.. 2..@..E.
0010 00 77 07 9a 00 00 3f 06 5a e2 0a 00 02 02 0a 00 .w....?. Z.....
0020 03 04 af 12 09 82 f4 ee 3f c4 92 5f 07 e6 50 18 ..... ?.._..P.
0030 42 1a fe 33 00 00 6f 00 37 00 00 18 02 17 00 00 B..3..o. 7.....
0040 00 00 64 30 0e 00 18 26 db 00 00 00 00 00 00 00 ..d0...& .....
0050 00 00 20 00 02 00 00 00 00 00 00 b2 00 27 00 81 00 .. ..... '
0060 00 00 01 00 0e 00 36 00 11 03 60 b0 9d 42 5e 00 .....6. ...B^
0070 14 31 37 35 36 2d 4c 36 31 2f 42 20 4c .....1756-L6 1/B LOGI
0080 58 35 35 36 31 .....X5561
```

Product Name (cip.id.product\_name), 20 bytes    Packets: 1640 · Displayed: 1640 (100.0%) · Load time: 0:0.33    Profile: Default

# **Solutions: What Industry Needs**

# High in the Kill-Chain



# 10 Simple Indicators That Matter

## (Modbus Example)

1. Modbus connections that are unexpected
2. Failed attempts to establish connection to TCP or UDP 502
3. Scans of TCP or UDP Port 502 in an Address Range
4. Function Code Scans against Modbus Slaves
5. Unexpected use of Vendor-specific Function Codes
6. Pipelining ADUs with a Variety of Function Codes
7. Serial Function Codes on Non-Serial Devices
8. Inconsistent Length Fields in **Replies**
9. Modbus Traffic above the DMZ
10. Modbus Traffic Using UDP



# Connecting the Dots

- Generating alert for every anomaly = **alarm overload**
- Look at Abnormal Situation Management Consortium (ASMC) alarm management requirements



# Getting Events to the Right People

- Deploying ICS security solutions **MUST** have the buy-in of the plant engineers
- What is the benefit to them?
- Most events will be caused configuration/process issues (not security issues)
- Does event info get to the right person **in a timely manner??**



# Making Events Actionable



# Making Events Actionable

- It's a CONTROL system
- Passive monitoring is nice but you must make **active** changes in response to events
- Usually you must do it quickly!

# Final Thoughts

- DPI solutions are not created equal (test your DPI)
- Start with key indicators (not what is easy)
- Start with anomalies at the top of the kill-chain
- Demand alarm/event correlation and management
- Make events actionable

**Done right, DPI is a powerful  
monitoring technology**

# Questions?

Eric Byres P.Eng, ISA Fellow  
eric.byres@ics-secure.com

