DRAGOS

5 Lessons for Integrating OT Threat Intelligence

Sergio Caltagirone
Dragos VP, Threat Intelligence
@cnoanalysis

Dragos

The Dragos Platform

- ICS monitoring software for comprehensive asset identification, threat detection, and response.

Dragos WorldView

- In-depth situational awareness of the threat landscape via actionable insights and intelligence reports.

ICS Security Services

- Expert guidance to combat and respond to adversaries via incident response, proactive services, and training.

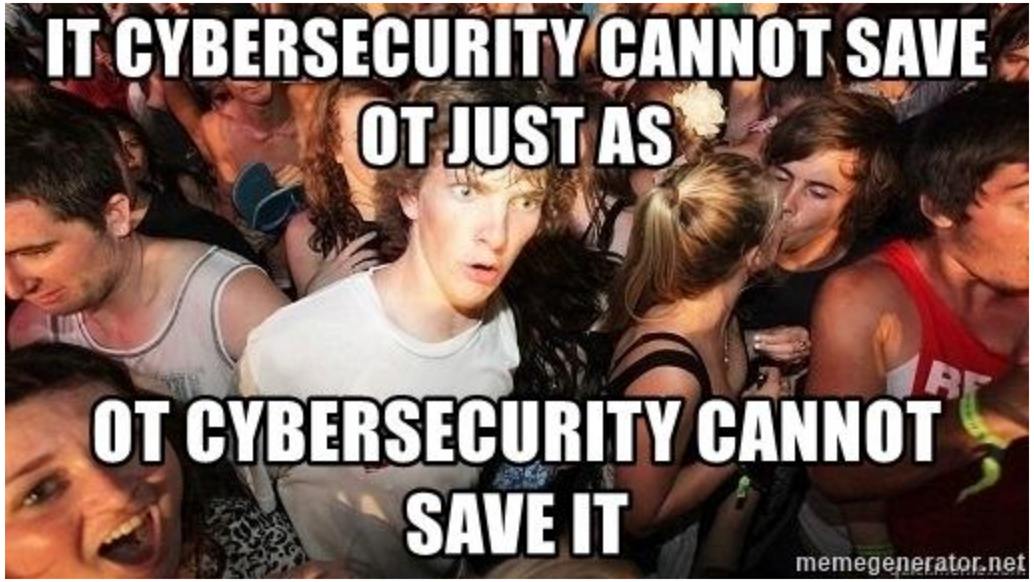
We Have to Work Together

Operations be like

Infosec be like

Lesson 1: IT + OT

- It's not either/or, it's **both**
- Most (but not all) OT threats start within IT environments
- Don't make the mistake: "protects IT protects OT" – because you need detection, intelligence, and defense in-depth across both environments


IT CYBERSECURITY CANNOT SAVE OT JUST AS
OT CYBERSECURITY CANNOT SAVE IT
memegenerator.net

Lesson 1: IT + OT is Necessary

Recommendations

- Build personal relationships with operators and plant managers by helping them find interest **relevant** items.

- Deliver value one OT thing ***monthly*** through 1:1 communications – don’t use “FW:FW::FW:::FW:::MUST READ” – pick one thing, make it count, don’t use more than 15 minutes

Lesson 2: Understand Operations

Relevance, Relevance, Relevance

The #1 killer of intel: irrelevant intel that wastes time or clutters inboxes

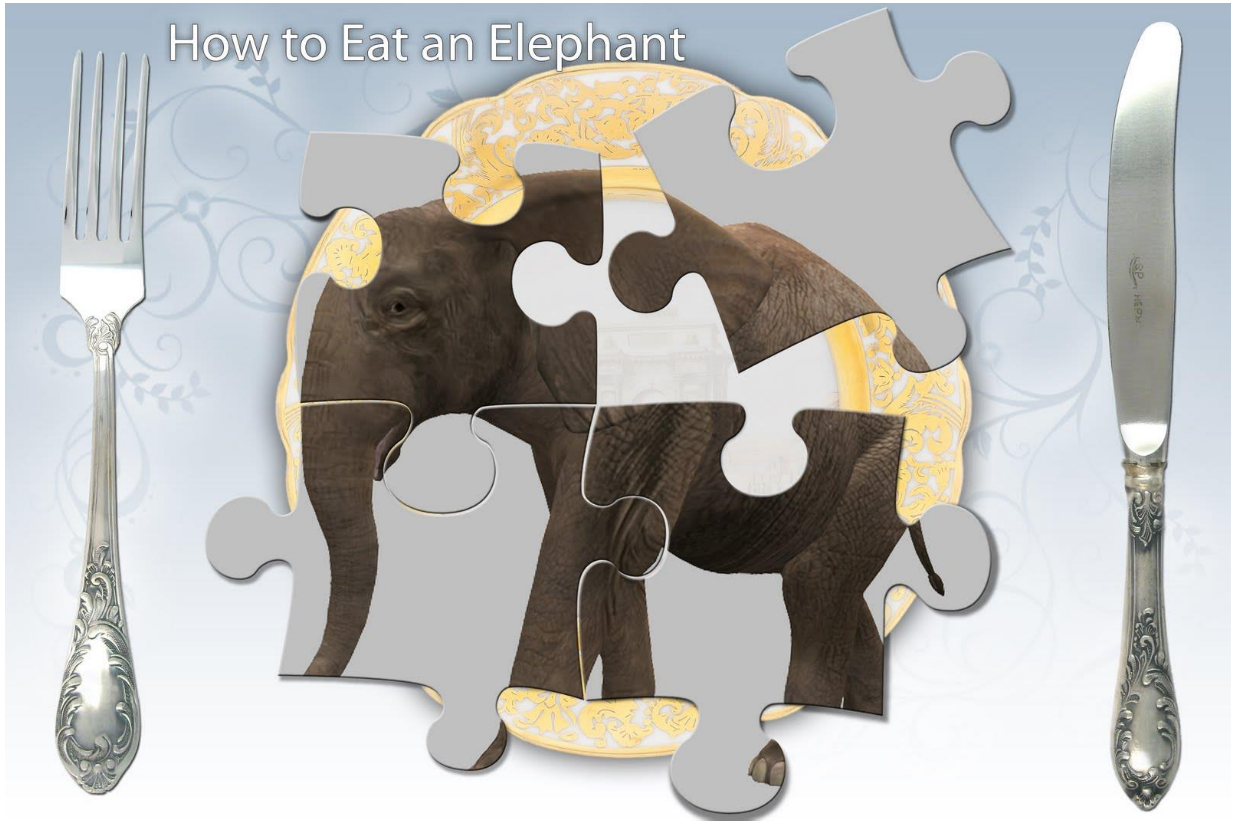
- Ops timeframes
  - E.g., Plant planned maintenance cycles
- Controlling entity
  - Who controls what
- Technology/assets
- Soft fail vs Hard fail

Success in dealing with people depends on sympathetic grasp of the other person's viewpoint.

Dale Carnegie

Lesson 3: Start Small

- Start at the OT edge instead of going straight to controlling layers or safety systems
- GET TO THE BASICS
    - Compliance, Vulnerability management, etc.



Lesson 3: Start Small

Recommendations

- Start at the OT edge! Edge monitoring is usually easier and quicker, usually requires fewer people involved.

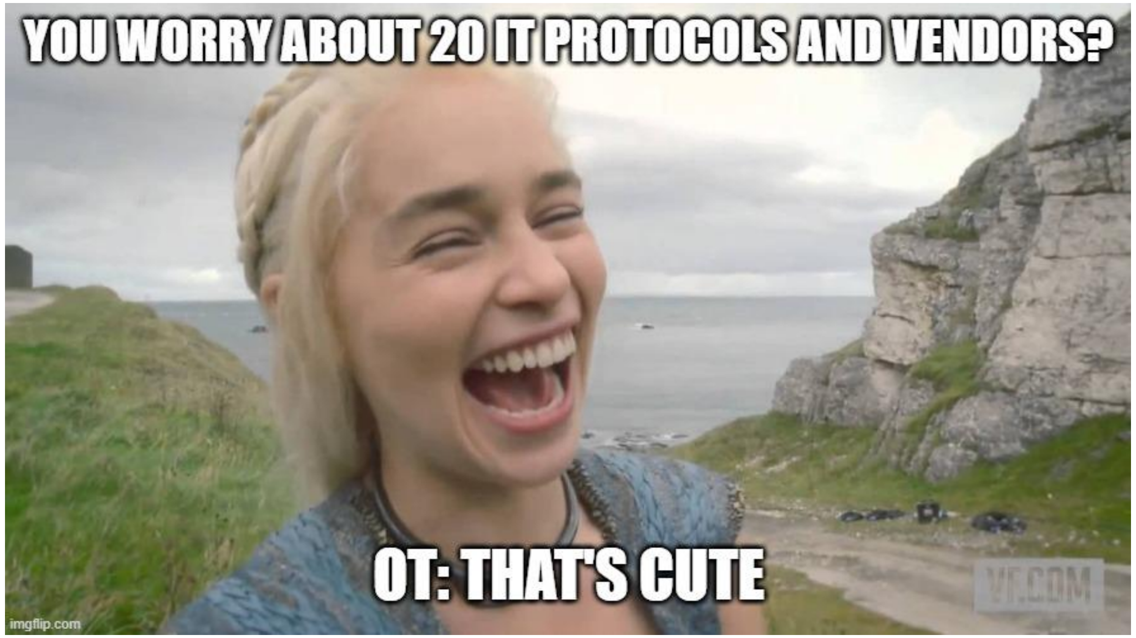
BUT – this isn't straight forward. **IT is not OT**. If you deploy ICS/OT IOCs or OT behavioral detection into an IT on the edge you'll have a higher FP rate. *This is a start not an optimal solution.* You may have some **pain** in the beginning. Eventually you need **ICS-specific** intel inside OT.

- Your risk register and compliance lawyers are your friends. Understand what they need to know to better manage the broader OT risks based on intelligence of the threat landscape.

Lesson 4: Get Specific in your Industry and Geo

OT intel IS NOT "OT intel"

- The space of OT/ICS is GIGANTIC
  - Hundreds of vendors, hundreds of protocols, each plant is unique
- You've got to specialize in your specific needs

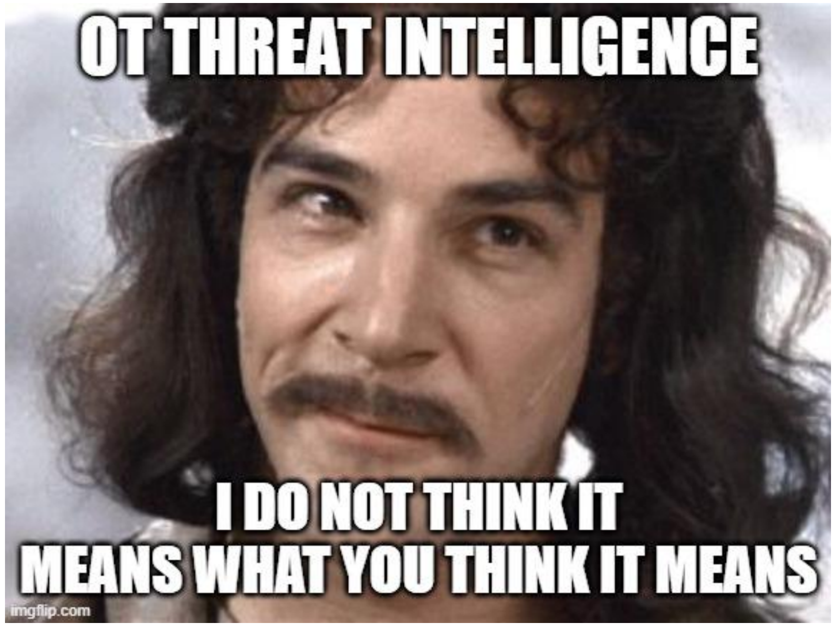


Lesson 5: It's All About the Fundamentals

The Hardest Part

- Fight your trained habit to worry about all the threats and protect against *all the things*
- Use threat intelligence to push for better cybersecurity visibility in OT environments
- This will serve you better and longer than protection against any single threat

>> Threat intelligence can get you there! Use it in business risk cases!



Lesson 5: It's All About the Fundamentals

Recommendations

- Use Threat Intelligence to drive fundamental OT cybersecurity change
  - Better visibility
  - Better cyber threat assessments during plant engineering
  - Better risk assessments
  - Better incident response
- For each OT threat, ask:
  - If that happened to us, would we see it?
  - Would we be able to tell the difference between a 'cyber attack' and an operational outage?
  - Would we have the right visibility to bring our operations back online safely knowing the environment was secure again?

Conclusion

Lessons

1. IT + OT is Necessary
2. Understand Ops
3. Start Small
4. Get Specific in "Which OT"
5. Exploit Intelligence To Achieve the Fundamentals

Recommendations

1. Build IT-OT relationships
2. Start at the edge
3. Relevance is key
4. Breakdown the world more than "OT" or "ICS"
5. Use OT threat intelligence to deliver effective business risk cases which drive fundamental improvements, like visibility

Questions?

Sergio Caltagirone
Dragos VP, Threat Intelligence
@cnoanalysis