LESSONS LEARNED

FROM SALT RIVER PROJECT'S DRAGOS DEPLOYMEN

DRAGOS

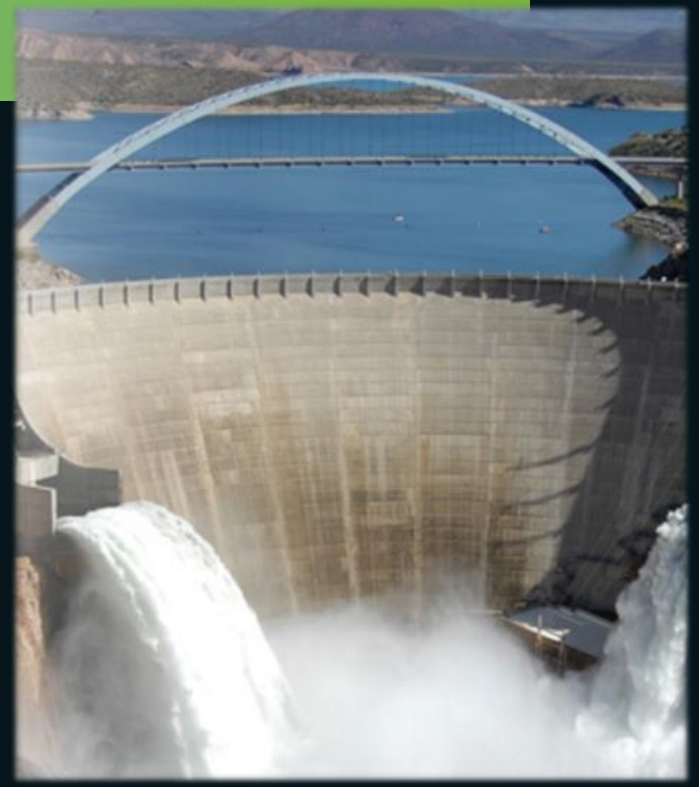
ABOUT US

SALT RIVER PROJECT'S CYBERSECURITY ARCHITECTS

MARK JOHNSON-BARBIER

BRENT HEYEN

ABOUT SRP



- FOUNDED 1903 (10 YEARS BEFORE AZ STATEHOOD)
- First multipurpose project under the National Reclamation act of 1902
- 5089 employees
- 1,074,952 customers
- 2,900 sq mile service area
- 375 sq mile water service area
- 13,000 sq mile watershed
- SALT RIVER VALLEY WATER USERS' ASSOCIATION
- 10 member board and 30 member council – elected by landowners
- Canals largely follow 500 miles of ditches built 400-1450AD by the Hohokam
- 2019 Water delivery: 785,126 acre-feet
- 8 dams and lakes
- SALT RIVER PROJECT AGRICULTURAL IMPROVEMENT AND POWER DISTRICT
- 14 member board and 30 member council – elected by landowners
- Generation Owner/Operator: 1 Nuclear, 12 Fossil, 8 hydro plants
- Generation: Biomass, Utility Solar, Wind, Geothermal, Rooftop Solar
- Transmission & Distribution
- Peak Power System: 7,615 MW
- Sustainable Portfolio 18.625% of retail requirements

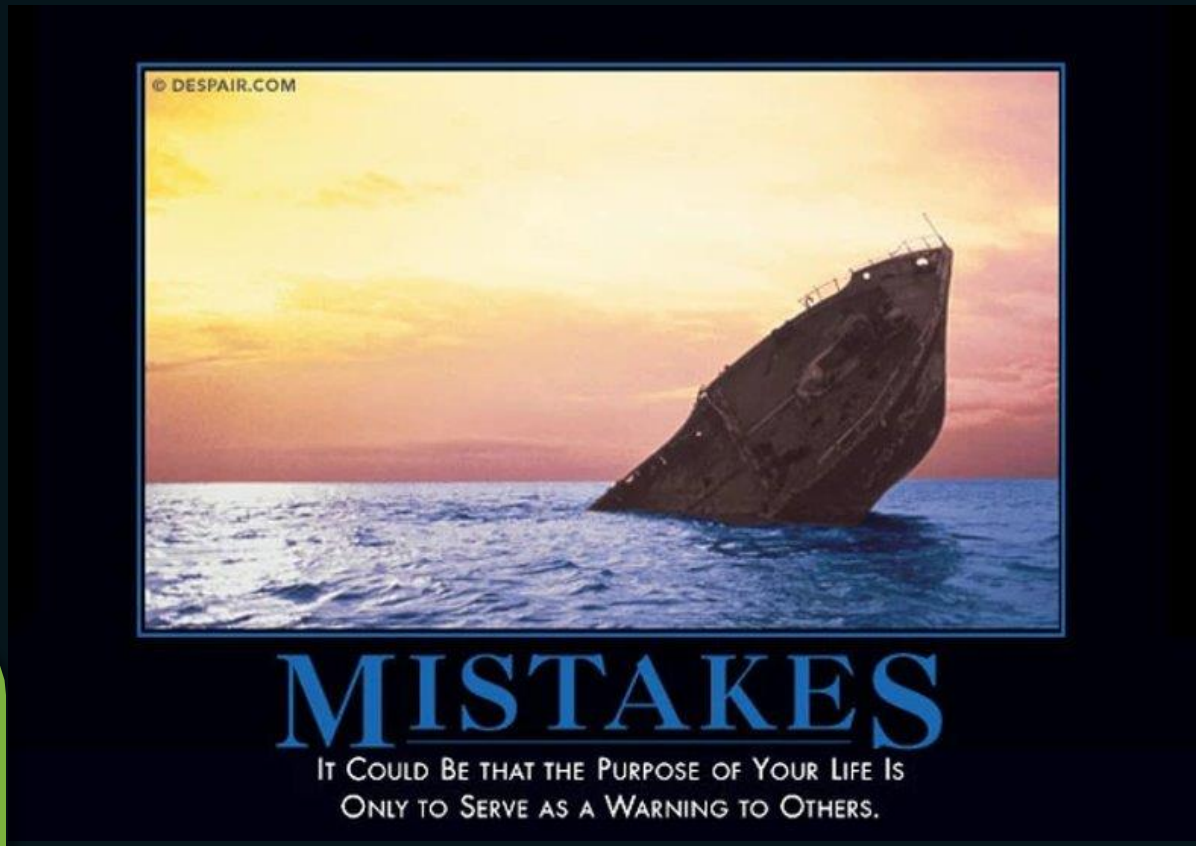
DISC 2020

AGENDA

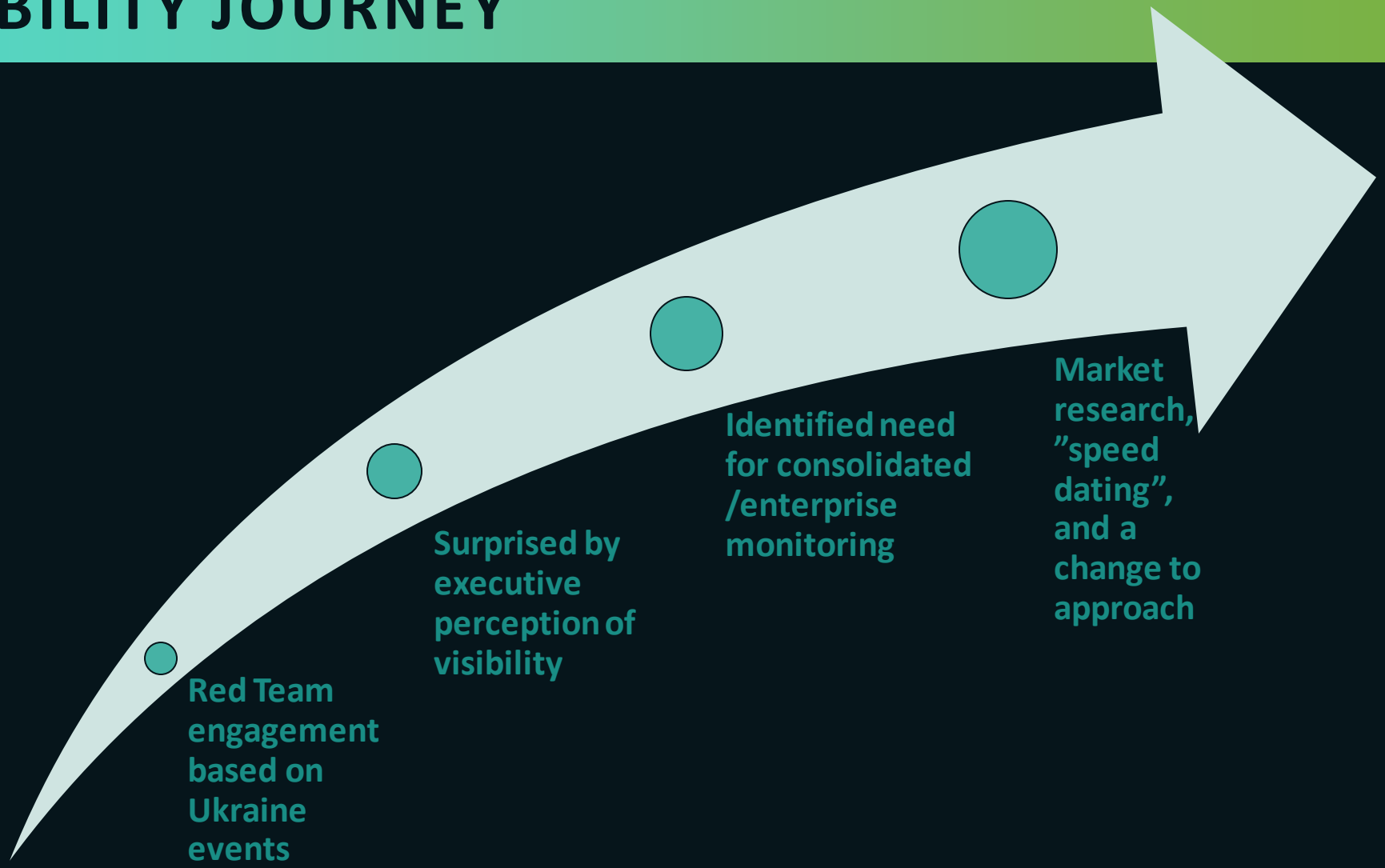
- OUR OT VISIBILITY JOURNEY
- WHAT WE'VE LEARNED:
- Politics
- Compliance
- Logistics/Coordination

POLL: How far are you on your OT visibility journey?

a) We have no visibility at all.
b) We have some visibility, but not centralized.
c) We are evaluating enterprise OT visibility products.
d) We are deploying an enterprise OT visibility solution.
e) We're done! We have it all!



OT VISIBILITY JOURNEY



OT VISIBILITY JOURNEY

- DRAGOS CUSTOMER FOR 3+ YEARS
- UTILIZED MANY SERVICES/PRODUCTS:
- WorldView Threat Intelligence
- **Dragos Platform** FOCUS OF THIS TALK
- Neighborhood Keeper
- Professional Services/IR Retainer
- FIRST-HAND EXPERIENCE WITH INTERACTIONS BETWEEN OFFERINGS

OT VISIBILITY JOURNEY

FROM

- Limited visibility
- Inconsistent and time-consuming monitoring & event handling
- Directive from Senior Management

TO

- Dragos Platform in Deployment
- Wins so far:
  - Asset verification
  - Identification of misconfigurations
  - Monitoring of vendor and remote access
  - Sleeping better at night!

+ WHAT HAVE WE LEARNED ABOUT DEPLOYING AN OT VISIBILITY SOLUTION?

POLITICS

LESSONS LEARNED - POLITICS

- TOP-DOWN SUPPORT
- Project backing
- Organizational change management
- Budget
  - Have extra available for unexpected costs
- Mediation (i.e. risk management)

LESSONS LEARNED - POLITICS

- INFORMATION AGGREGATION & SHARING
- A risk decision for your organization
- Eyes wide open: asset information, clear-text passwords, SNMP community strings, protocols/ports in use, etc.

+ Our opinion: A RISK TRADE-OFF
+ Central repository becomes a target
+ But only way to effectively search/correlate/detect off data
+ We believe the outcome is RISK REDUCTION for the ORGANZIATION

LESSONS LEARNED - POLITICS

- OT OUTREACH & ENGAGEMENT

SHOW UP & SHUT UP

- Listen & help
- Establish relationships
- BBQ & Donuts!

OT MANAGEMENT ROADSHOW

- Speak with management
- Address concerns and misunderstandings
- Don’t talk down!

EARLY ADOPTERS

- Find your security champions
- Deploy with them first
- Give them access

COMPLIANCE

LESSONS LEARNED - COMPLIANCE

- OT VISIBILITY PLATFORM CLASSIFICATION?
- NERC CIP: EACMS or Information Repository
  - **TALK TO YOUR COMPLIANCE PROGRAM TEAM!**
  - Understand your regulatory requirements

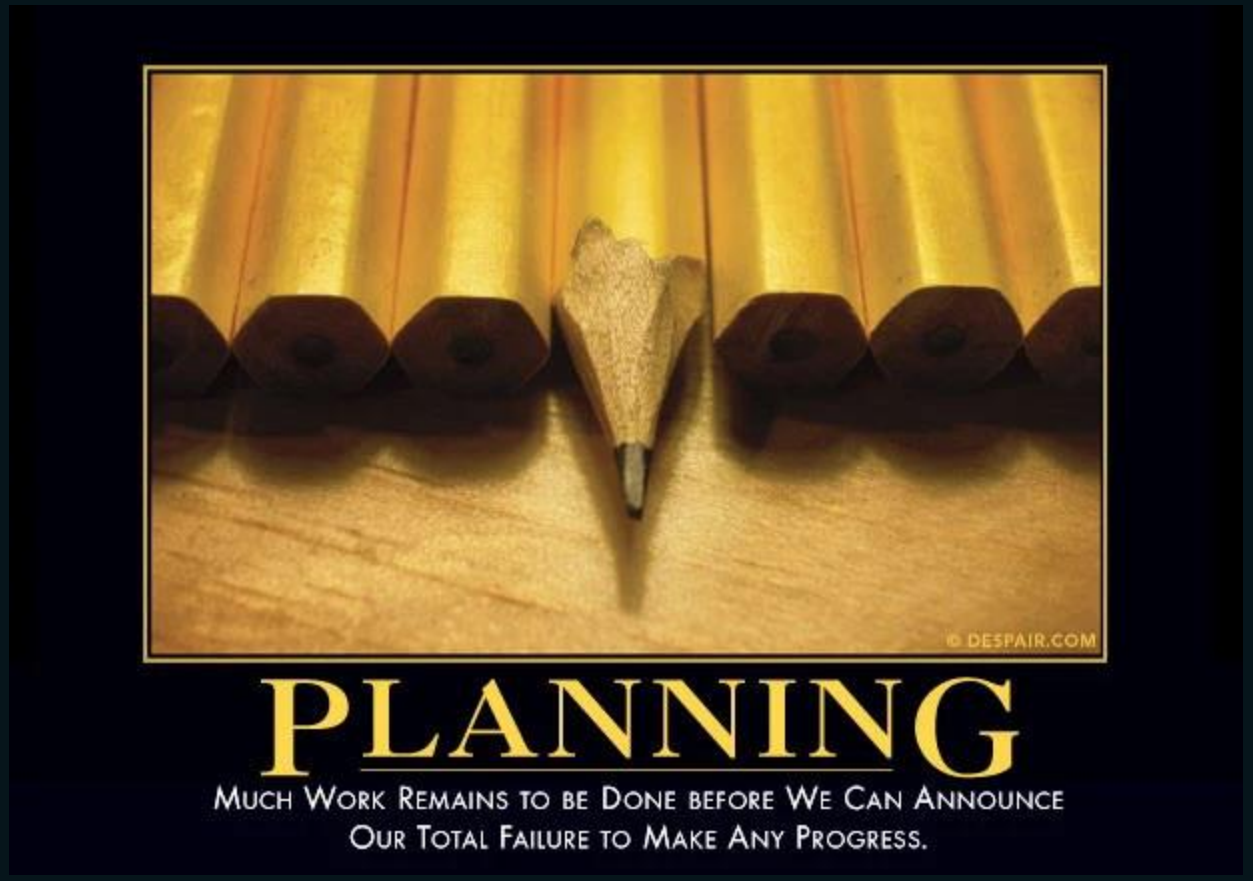
LESSONS LEARNED - COMPLIANCE

- DON'T FORGET YOUR CIP CHANGE CONTROLS!!
- Support compliance
- Build in lead time for changes
- Document
- Evidence

LOGISTICS / COORDINATION

LESSONS LEARNED - LOGISTICS/COORDINATION

- PROJECT MANAGEMENT
- We’re not project managers!
- Security doesn’t happen overnight
- Scope can change (new sites, retirements)



LESSONS LEARNED - LOGISTICS/COORDINATION

- OUTAGE & “NO TOUCH” WINDOWS
- Be aware!
  - Get your maintenance/outage schedules
  - Get the alerts concerning “no touch” windows
- Be helpful!
  - Is there anything you can do to help during these windows?

LESSONS LEARNED - LOGISTICS/COORDINATION

- WATCH FOR GOLDEN OPPORTUNITIES!

Major outages/upgrades are a GREAT time to get involved and move things along quickly!

LESSONS LEARNED - LOGISTICS/COORDINATION

- PREPARE FOR DEPLOYMENT
- Each site will be different!
- Gather as much info about a site as you can before you visit
- Documentation will be sketchy
  - Maturity level varies
- Expect the unexpected!

DEPLOYMENT NOTES

- Documentation to Gather Per Site:
  - Site contacts (management, technical)
  - Site address and map (geography)
  - Maintenance/Outage calendar
  - Network topology map (w/ physical locations of equipment if available)
  - Asset Inventory (w/ physical locations of equipment if available)
  - Vendor documentation

LESSONS LEARNED - LOGISTICS/COORDINATION

- SITE VISIT(S)
- Plan to visit more than once
- Initial visit should be about learning and listening
- Remember to build those relationships
- Goal 1: Important Asset Identification

DEPLOYMENT NOTES

- Asset Identification:
  - Important Network Equipment: Switches, Routers, Firewalls
    - Document: Name, location, make, model, port capacity, spanning capability, netflow capability, logging capability
  - Critical Hosts: HMI, Historian, Controllers, Engineering Workstations, Safety Instrumented Systems, Protection Relays, etc.
    - Document: Name, location, hardware type, OS, logging capability, network connectivity, IP address

LESSONS LEARNED - LOGISTICS/COORDINATION

- NETWORK DATA PLANNING
- SPAN, TAP or NetFlow

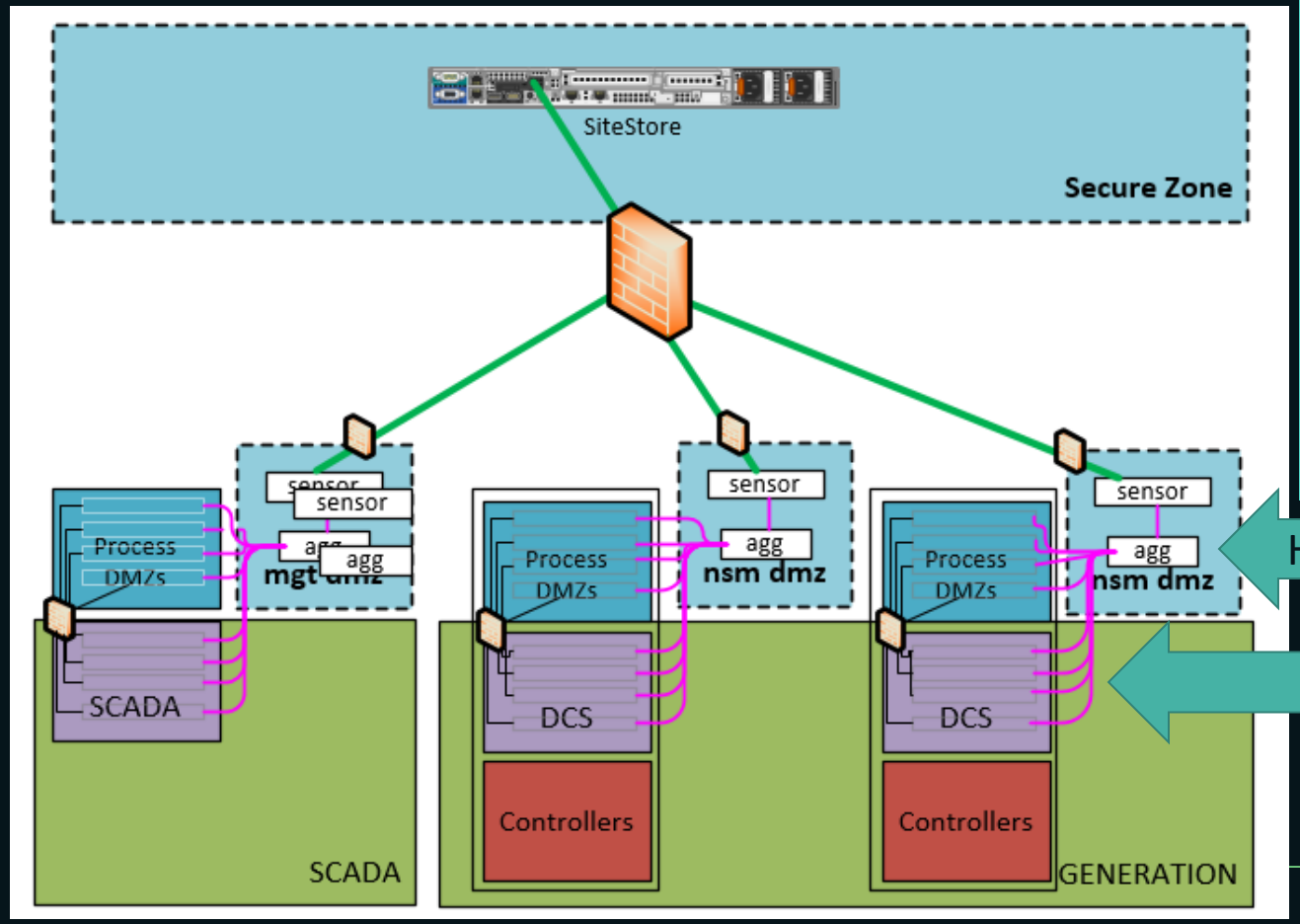
DEPLOYMENT NOTES

- Network Data Planning:
  - Questions to ask/answer:
    - How do configure port mirroring?
    - Can all traffic be mirrored?
    - Should all traffic be mirrored?
    - Physical output port available?
    - **Device has capacity (CPU)?**
    - Does the device need to be upgraded or swapped?
    - Connectivity path to get data to destination?
    - If TAP, where to install?

CAREFUL!

LESSONS LEARNED - LOGISTICS/COORDINATION

- NETWORK DATA PLANNING
- Aggregation



DEPLOYMENT NOTES

- Aggregation Planning
  - Questions to ask/answer:
    - Reduce number of sensors needed?
    - Available rack space?
    - Form factor requirements?
    - Power available?
    - Mounting brackets required?
    - Input and output connector types (fiber/copper)
    - Proximity and/or path to sensor ingest ports?

HAVE SOME OUTPUT PORTS AVAILABLE FOR NEW SENSORS

BRIGHT PINK CABLES! SERIOUSLY

LESSONS LEARNED - LOGISTICS/COORDINATION

- HOST DATA PLANNING
- Work with ICS vendors
  - They want to help!

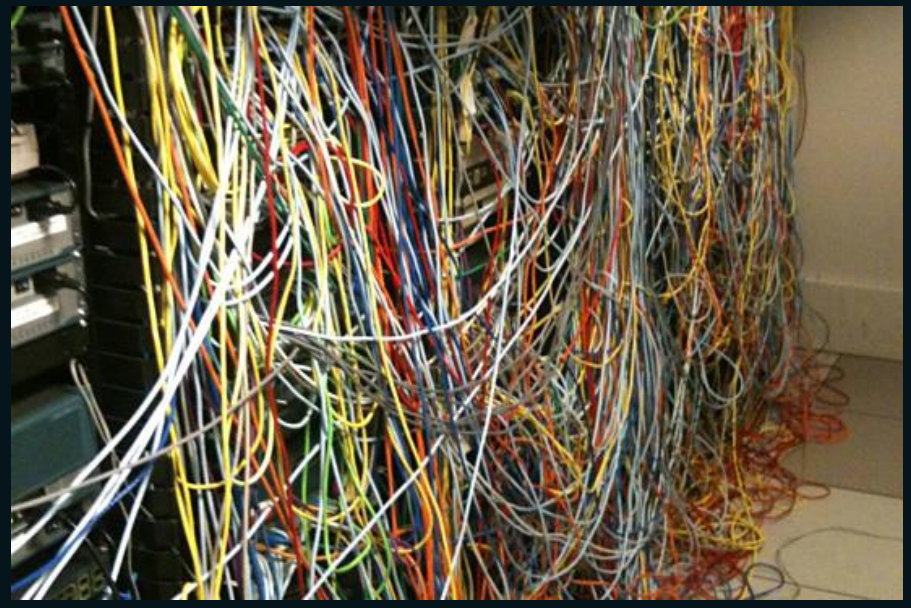
+ AND SUPPORT AGREEMENTS

DEPLOYMENT NOTES

- Host Data Planning
  - Questions to ask/answer:
    - Install agents (i.e. Sysmon, Forwarders)?
    - Adjust logging/audit levels?
    - How to configure syslog?
    - Send to central logging and then tee/forward to sensor?
    - Send direct to sensor (route to sensor)?

LESSONS LEARNED - LOGISTICS/COORDINATION

- SENSOR PLANNING
- Work with OT Visibility vendor on capacity and form factor options
  - Management NIC
  - Ingest NIC

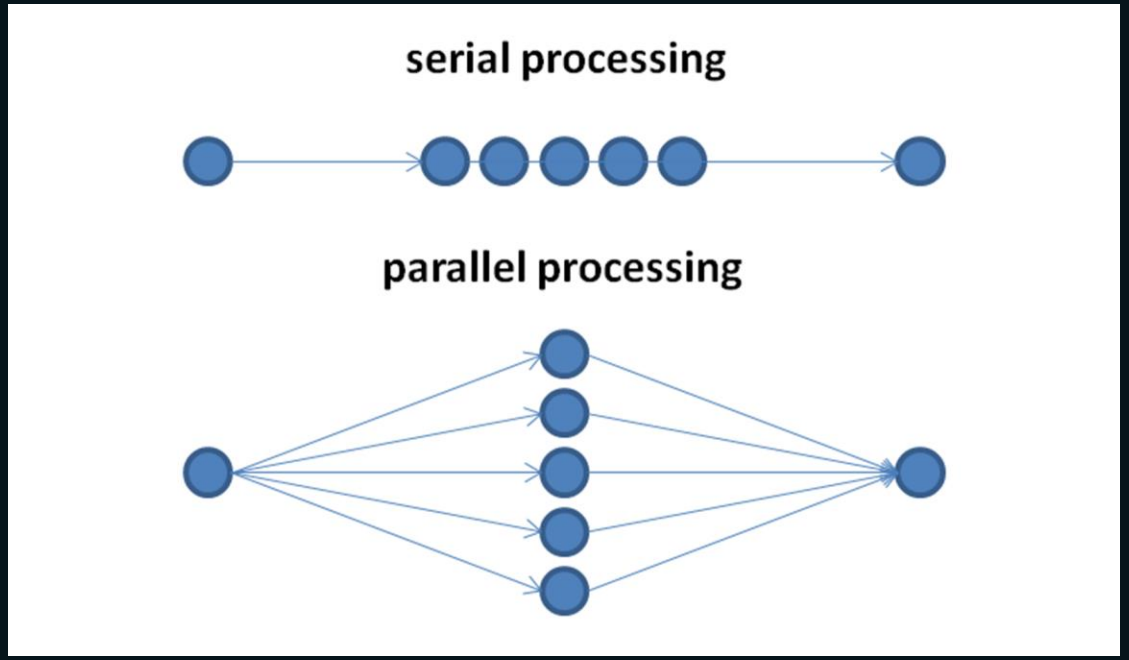


DEPLOYMENT NOTES

- Sensor Planning
  - Questions to ask/answer:
    - Estimated network capacity/bandwidth/throughput?
    - How many ingest NICs needed?
    - Form factor requirements: enterprise server, DIN rail, SEL3355, other?
    - Available rack space?
    - Power available?
    - Mounting brackets required?
    - Proximity to switch/firewall/aggregator?
    - Cable form factors (fiber/copper) and connector types?
    - Cable run requirements (management & ingest NICs)?

LESSONS LEARNED - LOGISTICS/COORDINATION

- PARALLEL PROCESSING OF MAJOR TASKS
- Site Planning
- Hardware ordering
- Site prep (Configs, Installs, Cable Runs)
- Sensor & Aggregator Installs
- Platform Configuration & Compliance



CONCLUSION

HOW TO USE THIS INFORMATION AFTER DISC

- PLAN FOR YOUR OT VISIBILITY JOURNEY
- Learn from us
  - Our mistakes
  - The questions we've learned to ask along the way
- Use this presentation as a launching point

RECOMMENDED RESOURCES ON THIS TOPIC

- US: FEEL FREE TO REACH OUT
- DRAGOS

THANK YOU

BRENT.HEYEN@SRPNET.COM
MARK.JOHNSON-BARBIER@SRPNET.COM
DRAGOS.COM

DRAGOS