RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: TECH-W02

Getting Practical with Addressing Risks in OT Networks: Where to Start?

Galina Antova

Co-Founder
Claroty
@GalinaAntova

RSAConference2019

The Clean Slate Strategy

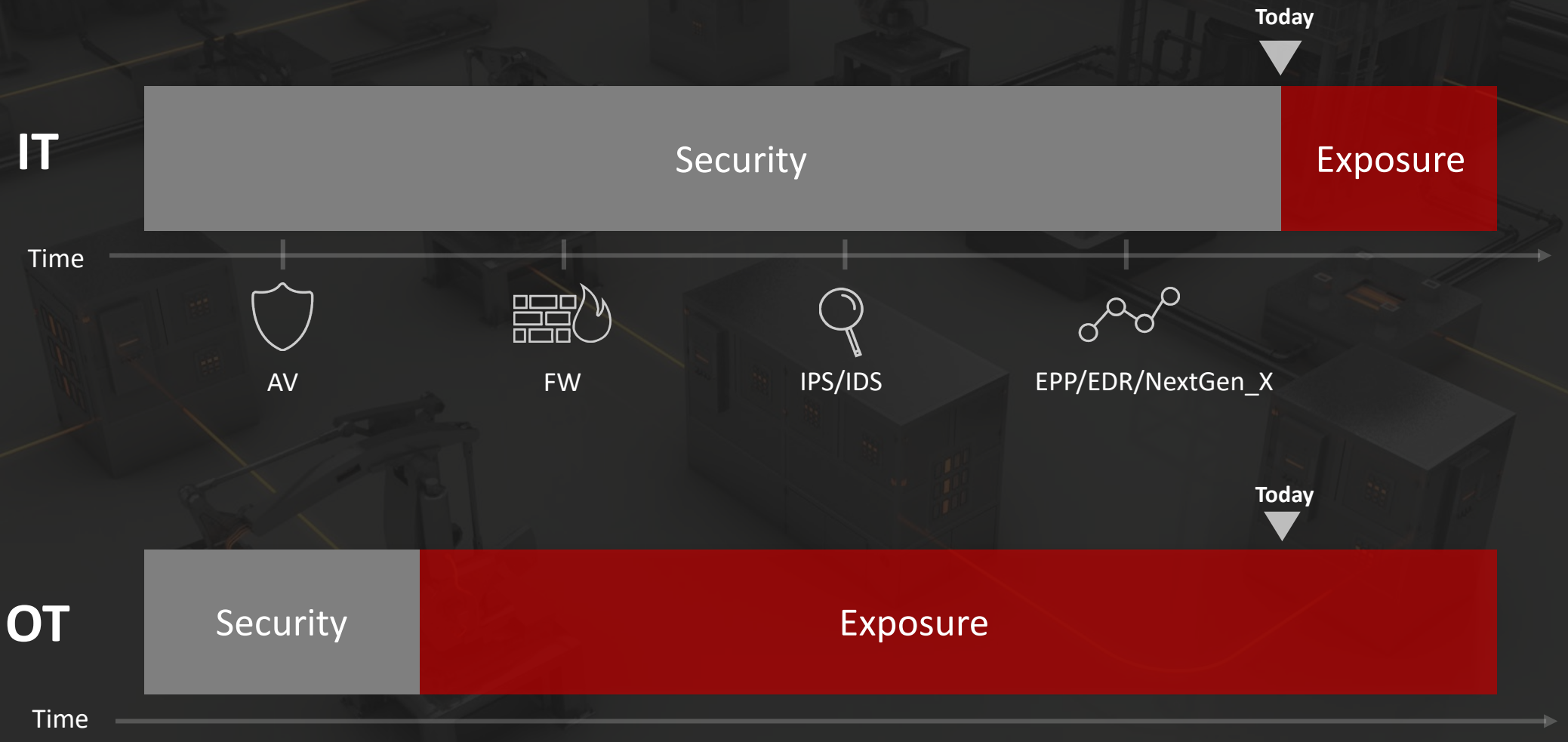
(aka "thank you, IT-OT Asymmetry")

CLAROTY
Clarity for OT Networks

RSAConference2019

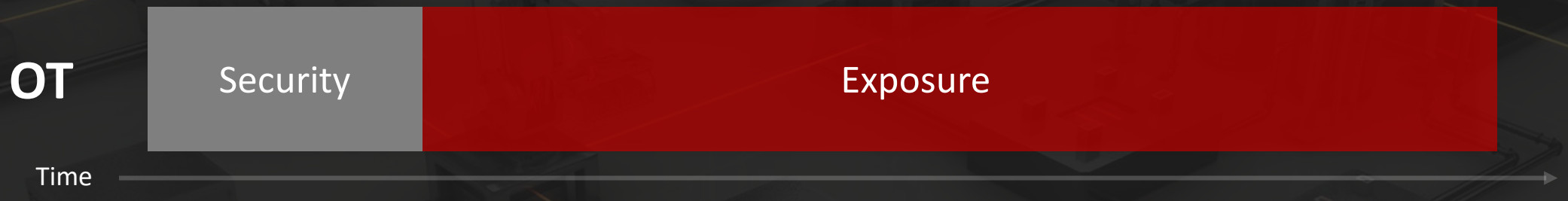

1. What you're learned in ITSEC will not serve our mission in securing OT networks
2. We don't have time to build the wall, we have to leap-frog
You've Been Investing
3. Some of the daunting challenges in ITSEC are remarkably simplify in OT
in IT Security for Decades

The IT-OT Asymmetry



It’s Challenging for a Reason

The Perfect Storm

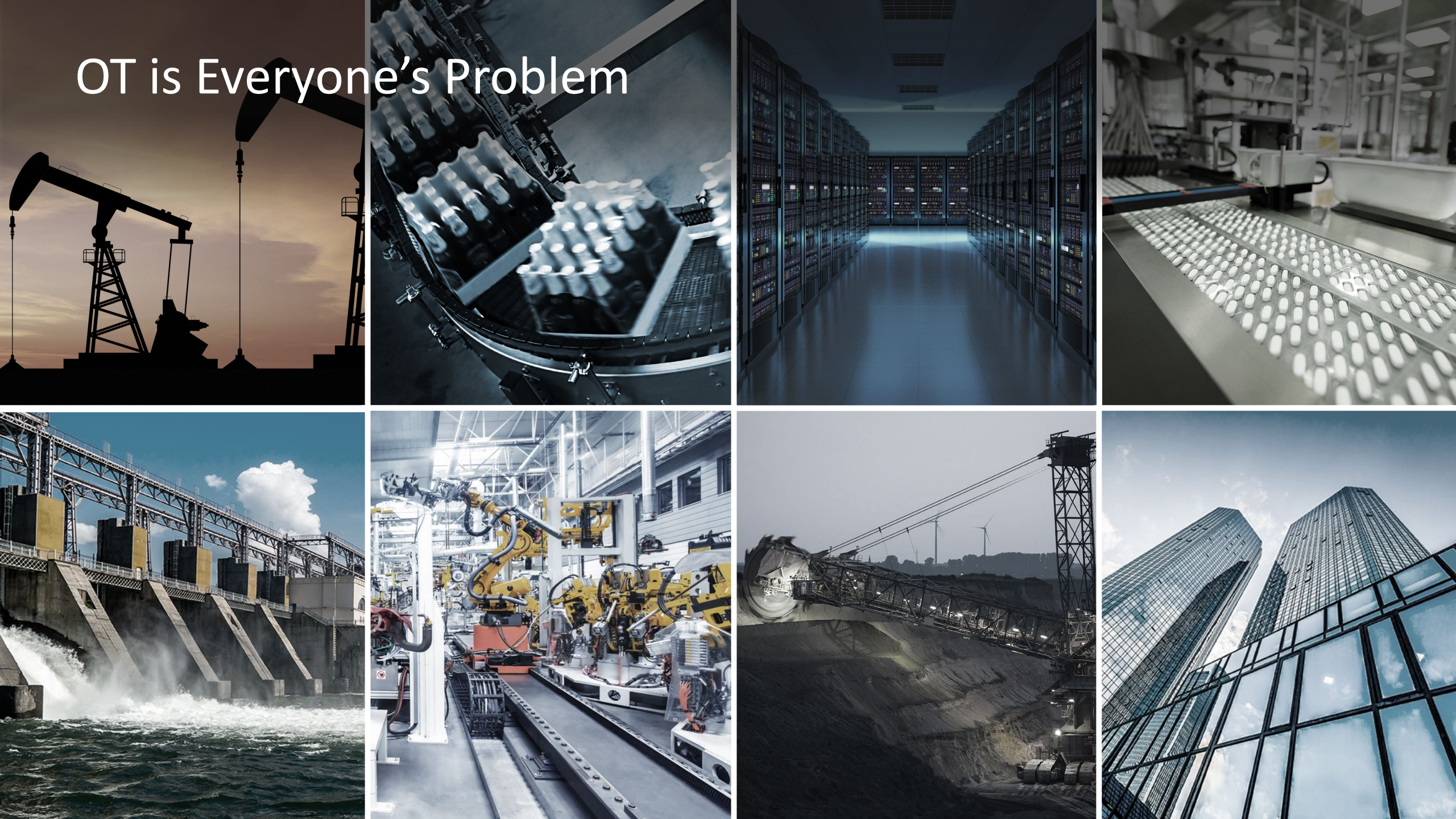


ICS Insecure due to legacy

Increasingly Connected IT/OT

Active Threat Landscape

OT is Everyone's Problem



Making the Impossible Jump


RSAConference2019
Where Do
We Even Start?
CLAROTY
Clarity for OT Networks
RSAConference2019

Get Management On-Board

90% it's already a boardroom issue

F500 Companies already have an OT strategy

For most, OT is a **Top 5** priority

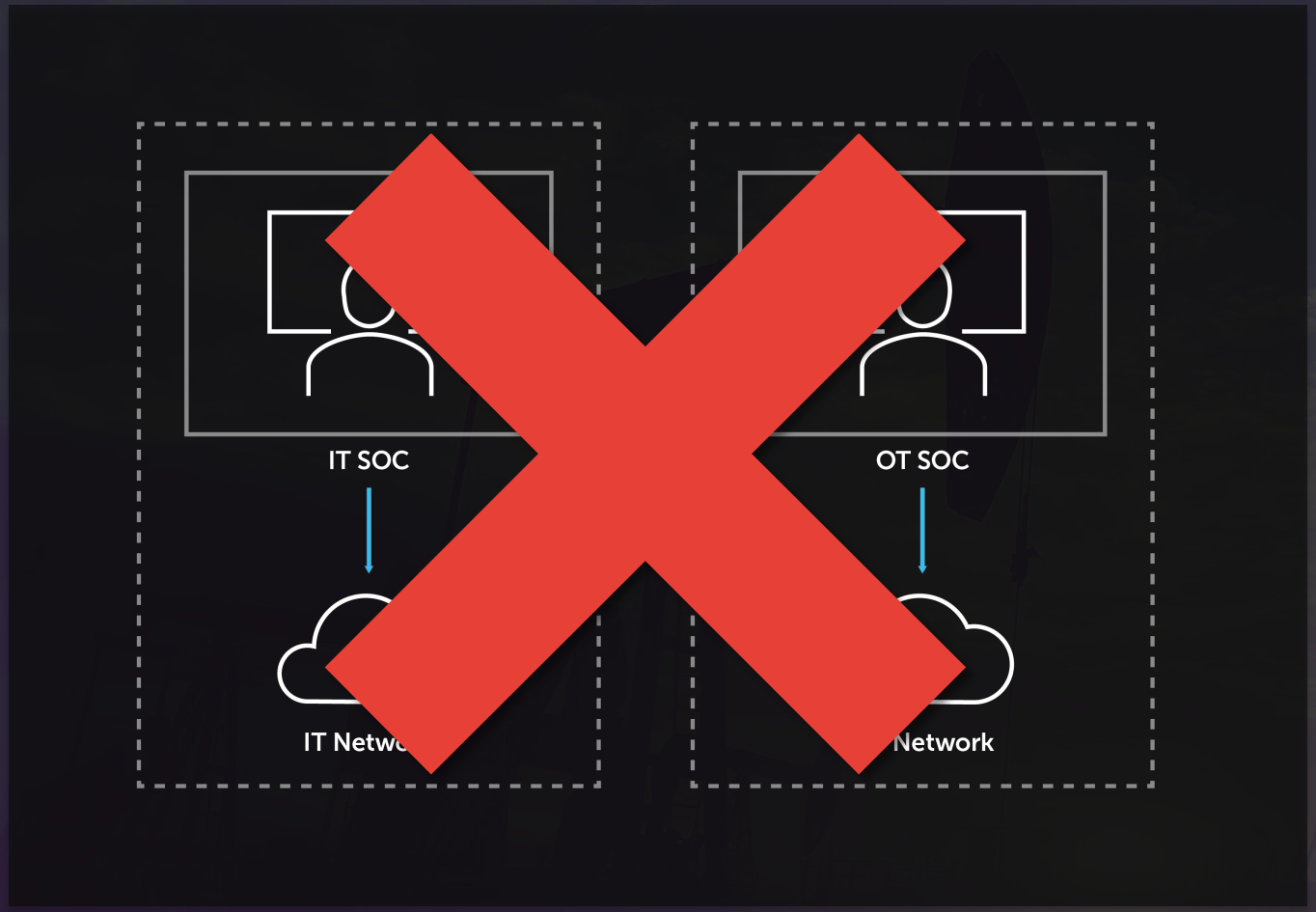
All started with an **assessment**:
how big is the OT gap?

RSAConference2019

Lessons Learned

Case Study #1

Case Study #1



- Energy company, highly sophisticated in ITSEC , initially wanted to recreate the process for OT SEC
- Conclusion reached: Impractical and not cost-effective across tech stack, people, process
- Invest in best practices that leverage existing infrastructure
- Leverage technology to ”translate” niche domains

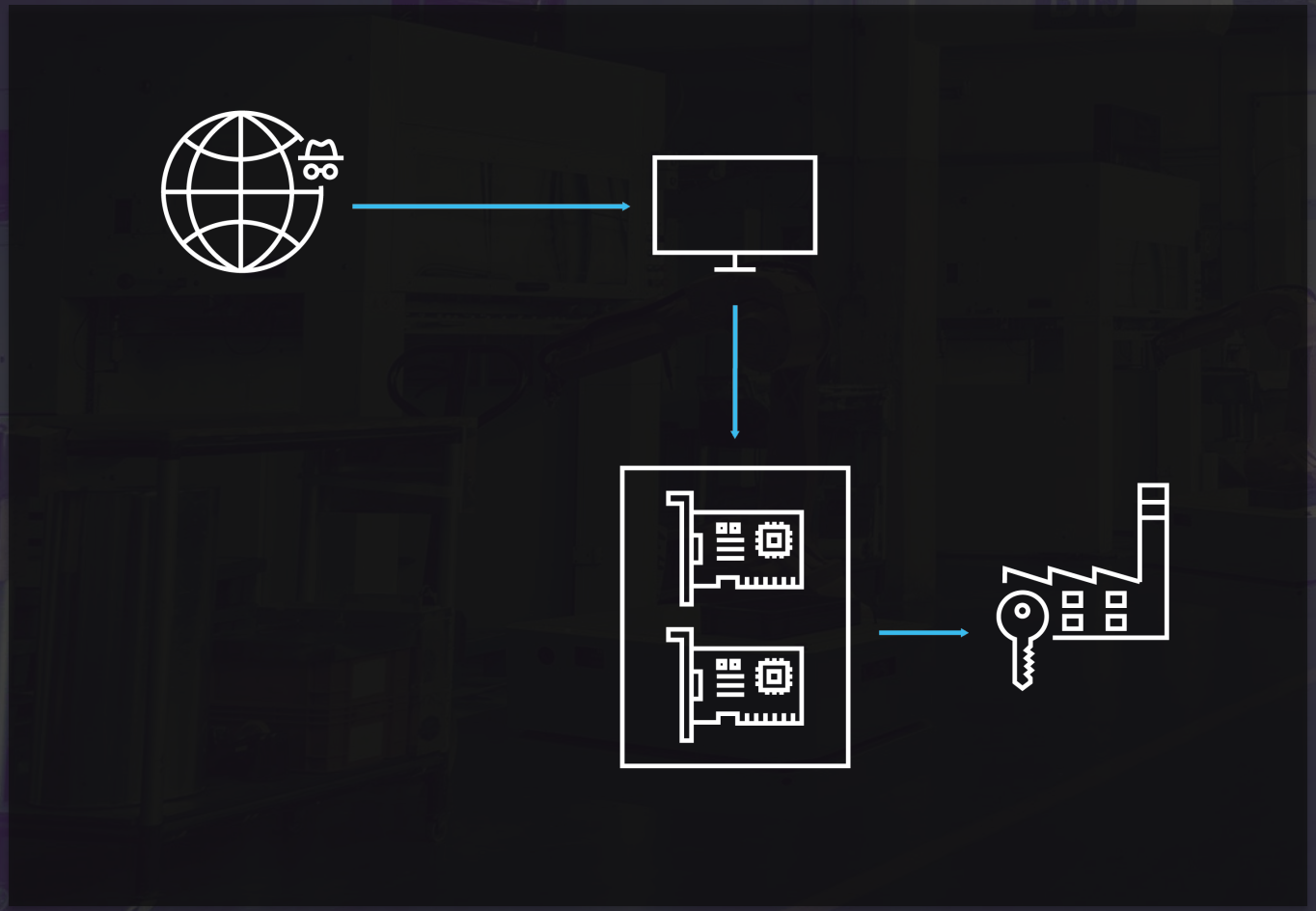
Use What You Already Have

Use What You Already Have

Lesson Learned #1

Case Study #2

Case Study #2



- Connectivity is needed and when not provided, people get creative
- OT network was a black box – no way to identify lateral movement
- No visibility into potential attack vectors
- No way to identify abnormal process-related behavior from the network

Visibility First. It's the Investment with the Highest RoI

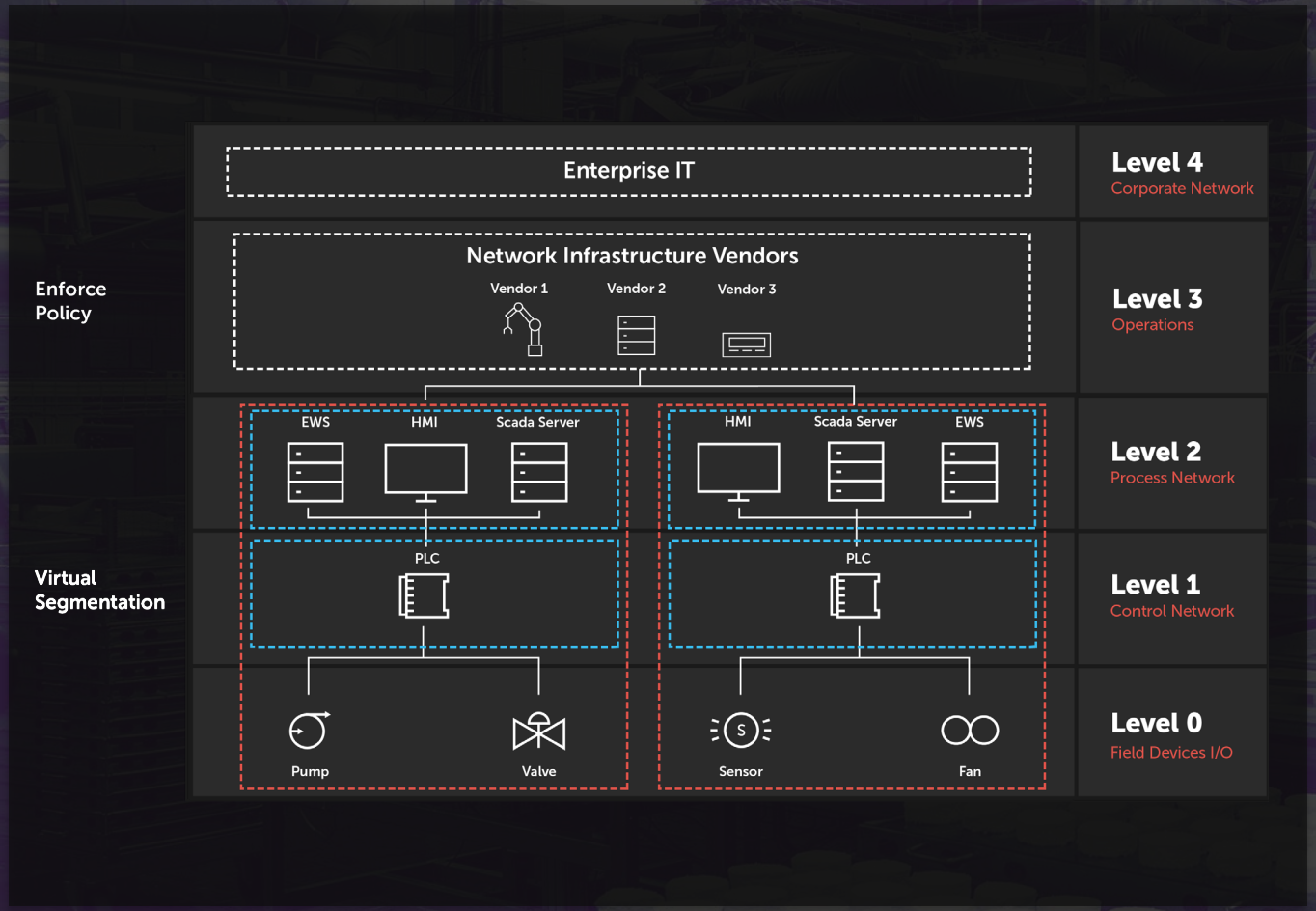
Lesson Learned #2

CLAROTY
Clarity for OT Networks

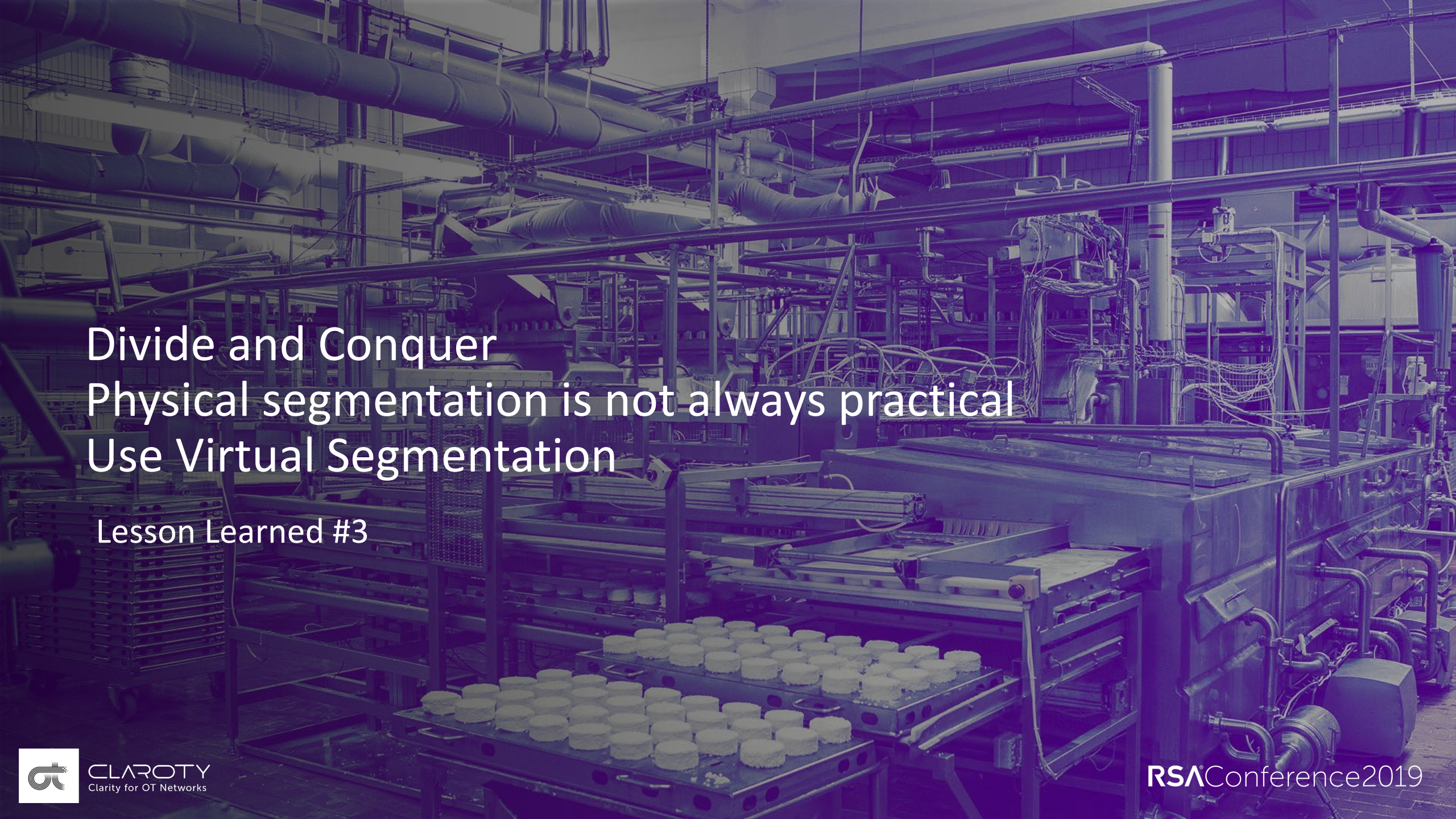
RSAConference2019


Case Study #3

Case Study #3



- Large manufacturing operation, initiated a physical segmentation project (Level 2 and below)
- Impractical to achieve – cost, downtime, personnel
- Virtual zones provide what's needed (alert, not block) without the downtime
- Enforcement policy implemented at a higher level
- Doesn't apply to every industry segment

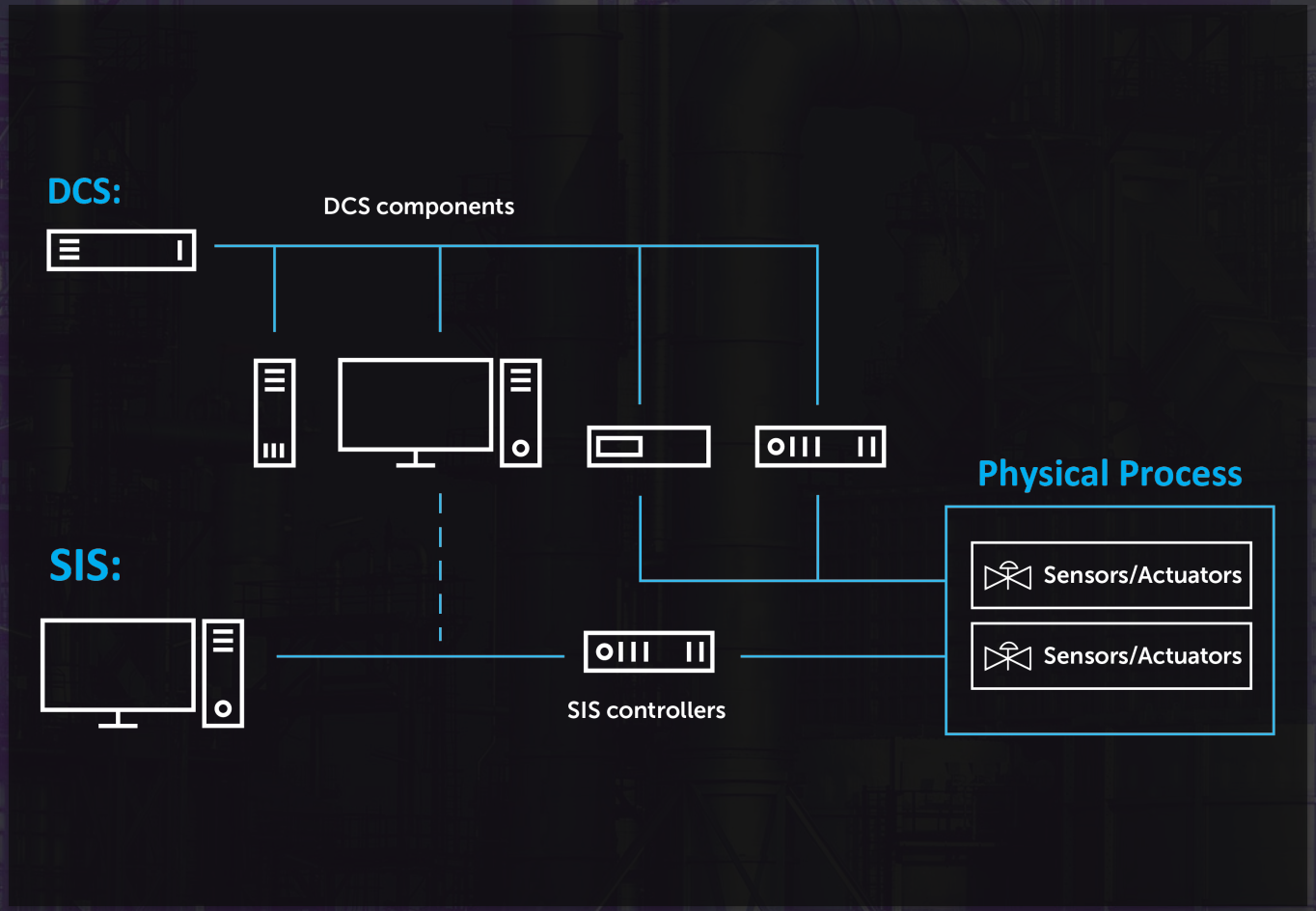


Divide and Conquer
Physical segmentation is not always practical
Use Virtual Segmentation

Lesson Learned #3


Case Study #4

Case Study #4



- Known case of Triton, applies to any critical infrastructure network
- No physical segmentation, no virtual segmentation
- Changing programing of Safety Instrumented System (SIS) is a different category of alert
- Measure everything through lenses of potential impact – that will inform prioritization

Prioritize Based on Risk
Understand the real risk based on OT-Specific Threat Monitoring

Lesson Learned #4

CLAROTY
Clarity for OT Networks

RSAConference2019

RSAConference2019

Ultimately, It's All About Investing Smart

Prioritize Measures Based on the Highest ROI

In Summary

Best Visibility Yields Better Security:

- See and monitor nested devices that others cannot see
- Expedite alert triage with OT-related details for improved risk-based decisions
- Efficiently respond to threats with OT-specific context your existing SOC team can understand and act on
- Pinpoint the vulnerable devices in your OT network by identifying firmware versions, model

Ability to Detect Targeted OT Attacks

- Detect attacks Triton-style (0-Day) – without requiring signatures or
- The only way to efficiently detect hackers manipulating your data is by automatically monitoring which device allows altering specific tags

Ability to Prevent Attacks

- Eliminate a key OT attack vector – unmanaged remote access by employees and contractors
- Vitally segment OT network for early detection of likely malicious task
- Enable network segmentation - understand your current segmentation, assess weak points, and building mitigation plan

Improved TCO

- Integrated platform and integration with your technology stack reduces deployment and operational costs
- Capabilities that have no impact on existing headcount, process, and technology

“Apply” Slide – What you can do immediately

Establish clear ownership

- Communicate who owns OT network security
- Budget allocations and project timelines

Assess the current status

- Understand the true extent of the exposure
- Discover the blind spots and quantify the implications

“Apply” Slide – What you can do in the next 6-9 months

- Goal is to optimize Total Cost of Ownership (TCO)
  - Leverage existing technology stack
  - Plug and play with existing processes
  - Min impact on teams/habits
- Transform Opacity into Transparency
  - Leverage all available methods to get to 100% visibility: passive monitoring, active querying, config files dissection, etc.
- Enable network segmentation - understand your current segmentation, assess weak points, and building mitigation plan
  - Implement virtual segmentation for lower levels of the OT network
  - Leverage implementations with existing network infrastructure to implement policy and alert-based segmentation
- Deploy threat detection technology
  - Contextual OT-specific tech with the ability to detect the full spectrum of OT-relevant threats

RSAConference2019

Thank you!

Questions?