

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: TECH-W02

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

Galina Antova

Co-Founder
Claroty
@GalinaAntova



#RSAC



RSA® Conference 2019

The Clean Slate Strategy

(aka “thank you, IT-OT Asymmetry”)



CLAROTY
Clarity for OT Networks

RSA® Conference 2019



- 
1. What you're learned in ITSEC will not serve our mission in securing OT networks
 2. We don't have time to close the gap step-by-step, we have to leap-frog

You've Been Investing in IT Security for Decades

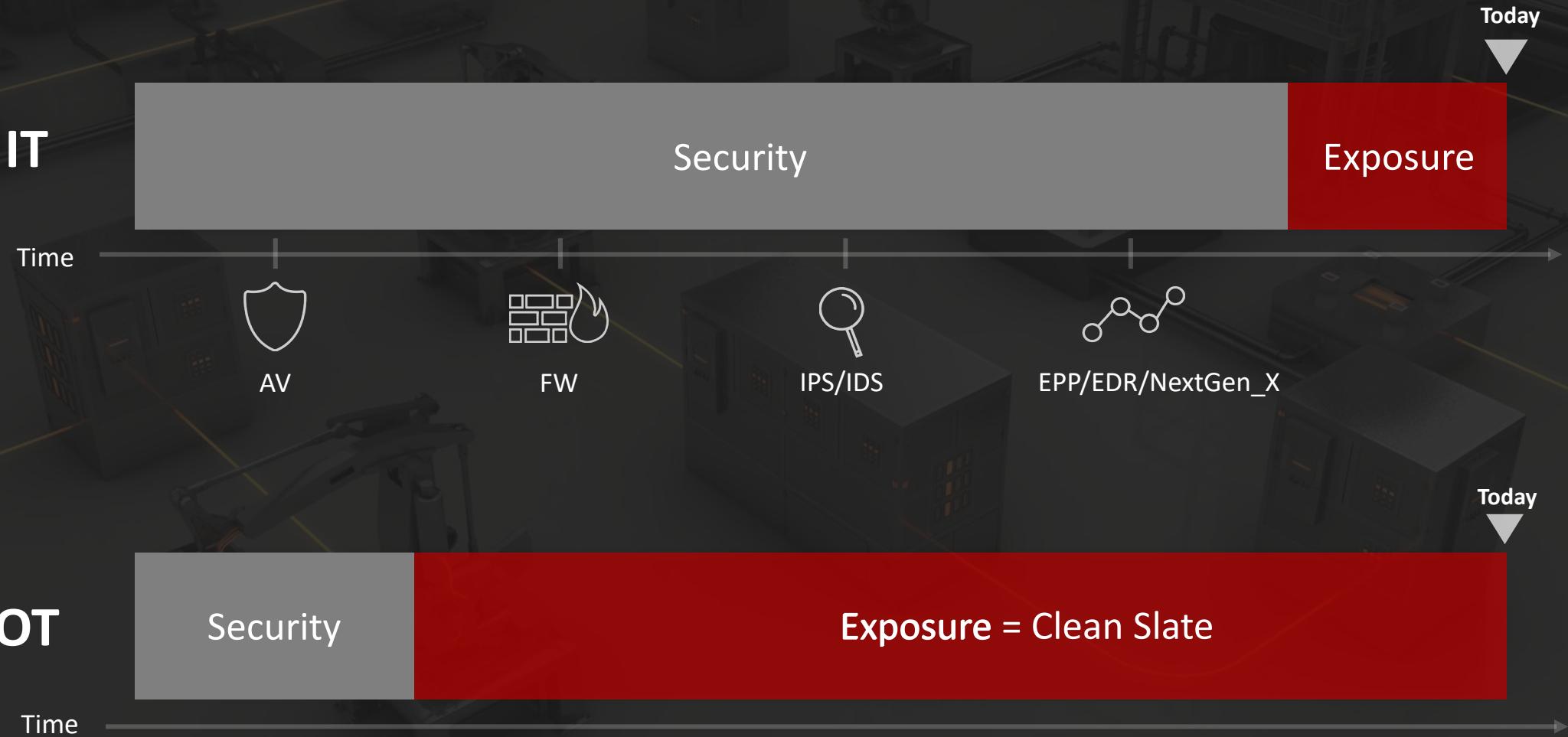
3. Some of the daunting challenges in ITSEC are remarkably simple in OT



CLAROTY
Clarity for OT Networks

RSA Conference 2019

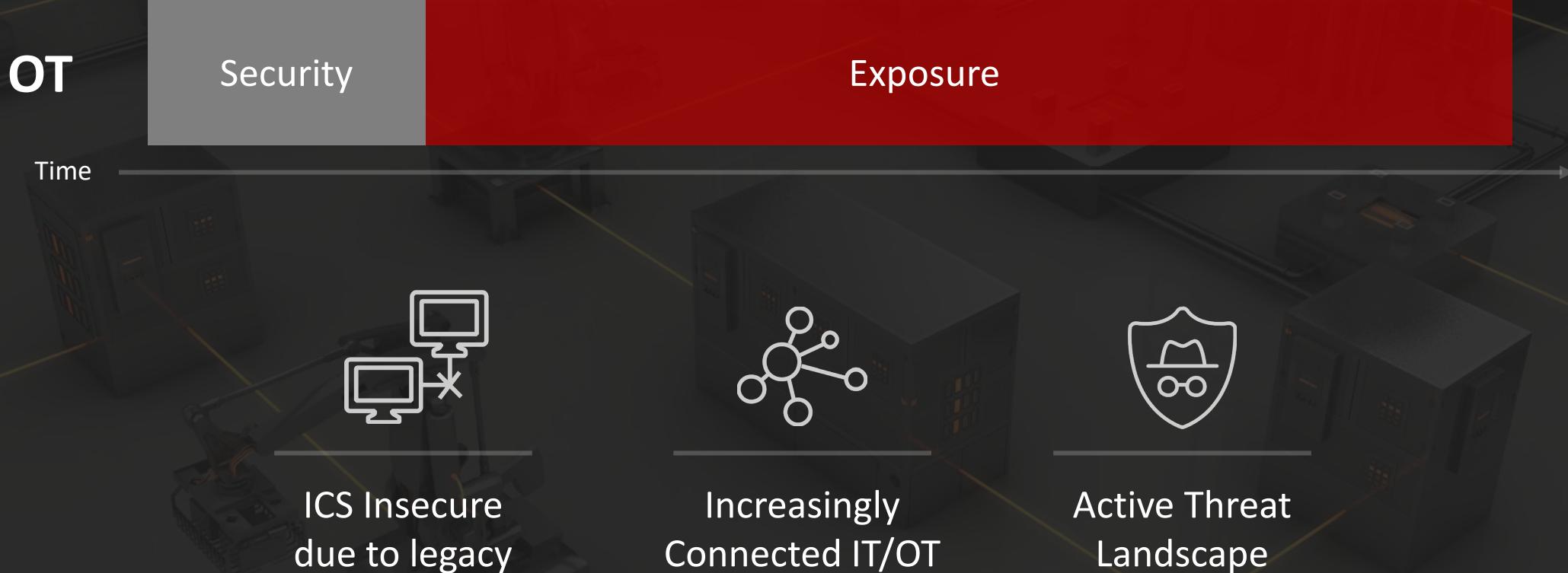
The IT-OT Asymmetry



CLAROTY
Clarity for OT Networks

RSA Conference 2019

The Perfect Storm

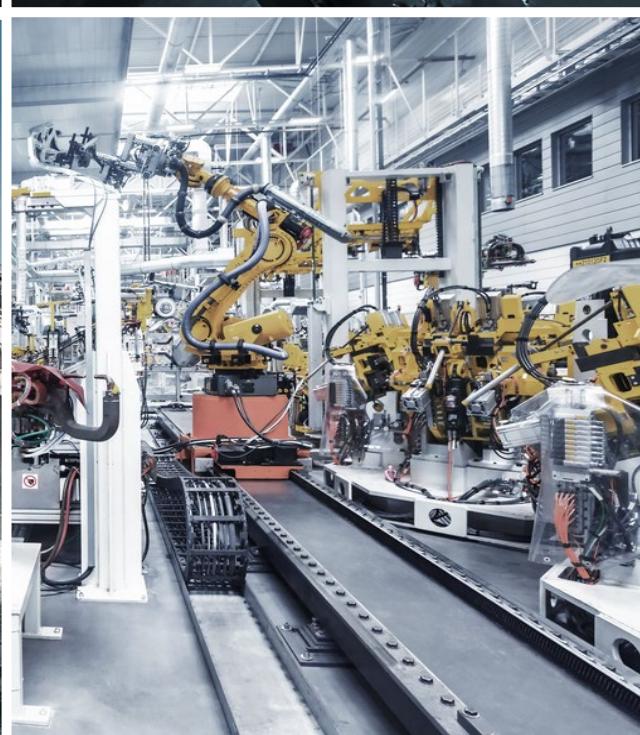
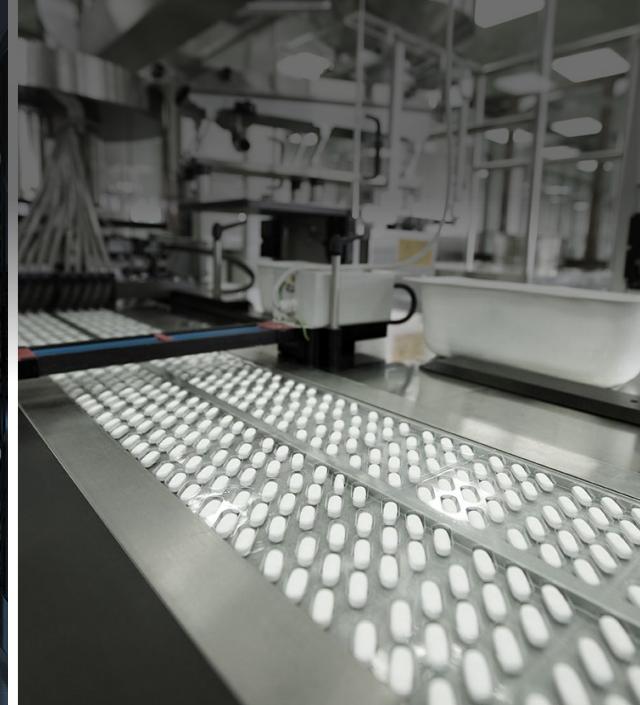
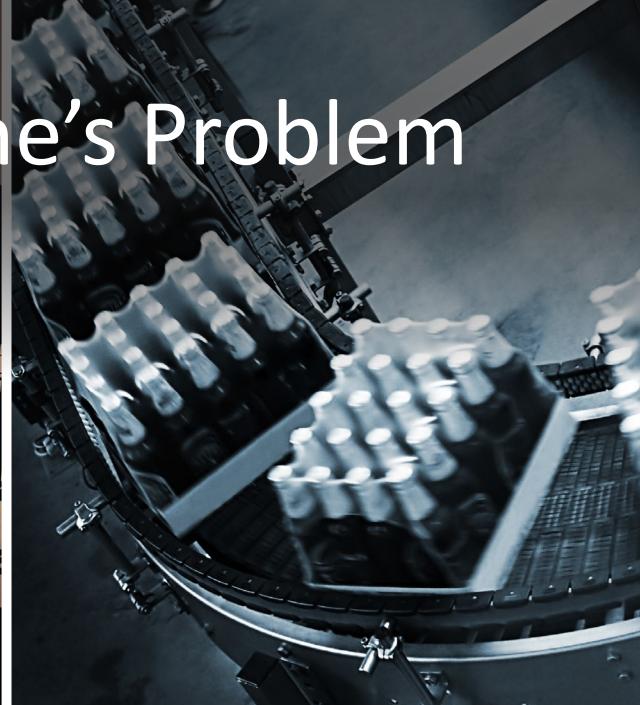




CLAROTY
Clarity for OT Networks

RSA® Conference 2019

OT is Everyone's Problem





Making the Impossible Jump



CLAROTY
Clarity for OT Networks

The background of the slide is a photograph of a large industrial facility, likely a chemical plant or refinery. The scene is dominated by numerous large, shiny, metallic pipes of various sizes and orientations, some with valves and fittings. The lighting is dramatic, with strong highlights and shadows on the curved surfaces of the pipes, creating a sense of depth and complexity. The overall atmosphere is one of a complex, high-stakes industrial environment.

RSA® Conference 2019

Where Do
We Even Start?



CLAROTY
Clarity for OT Networks

RSA® Conference 2019

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?



CLAROTY
Clarity for OT Networks

RSA Conference 2019

RSA®Conference2019

Lessons Learned

A photograph showing several oil pump jacks operating in a field. The pumps are silhouetted against a sky filled with scattered clouds. The sun is low on the horizon, creating a warm glow and long shadows.

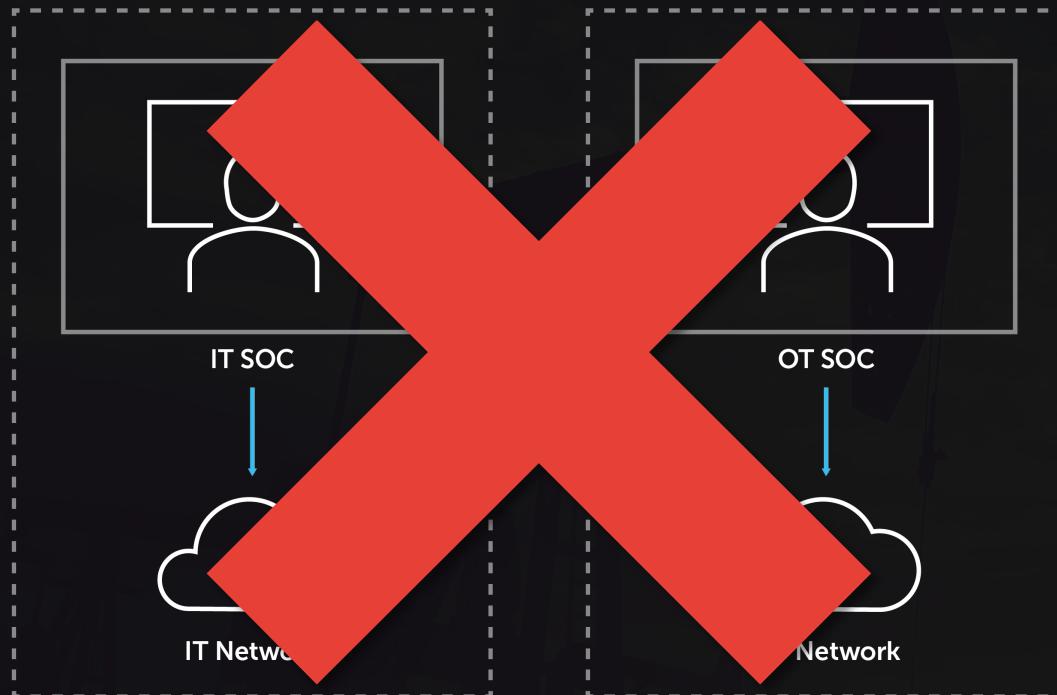
Case Study #1



CLAROTY
Clarity for OT Networks

RSA Conference 2019

Case Study #1



- Highly sophisticated ITSEC teams, initially wanted to create a separate OT SOC
- 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

A photograph showing several industrial oil or gas pump jacks operating in a field. The pumps are silhouetted against a bright, cloudy sky, with sunlight reflecting off the clouds. The scene is industrial and suggests a focus on existing resources.

Use What You Already Have

Lesson Learned #1

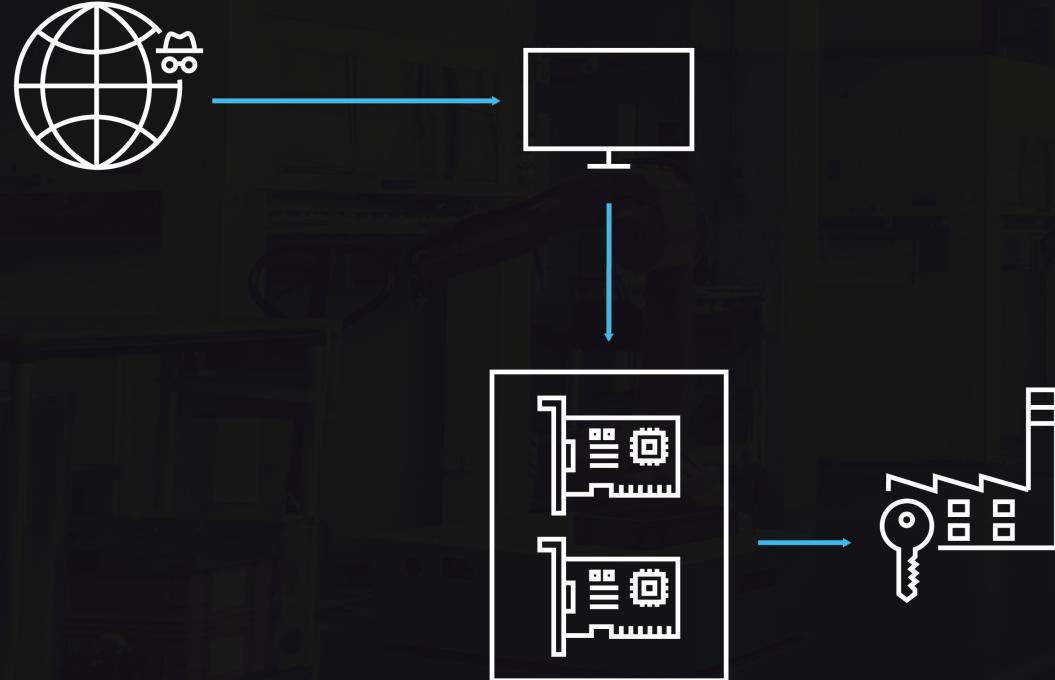
Case Study #2



CLAROTY
Clarity for OT Networks

RSA® Conference 2019

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

RSA® Conference 2019



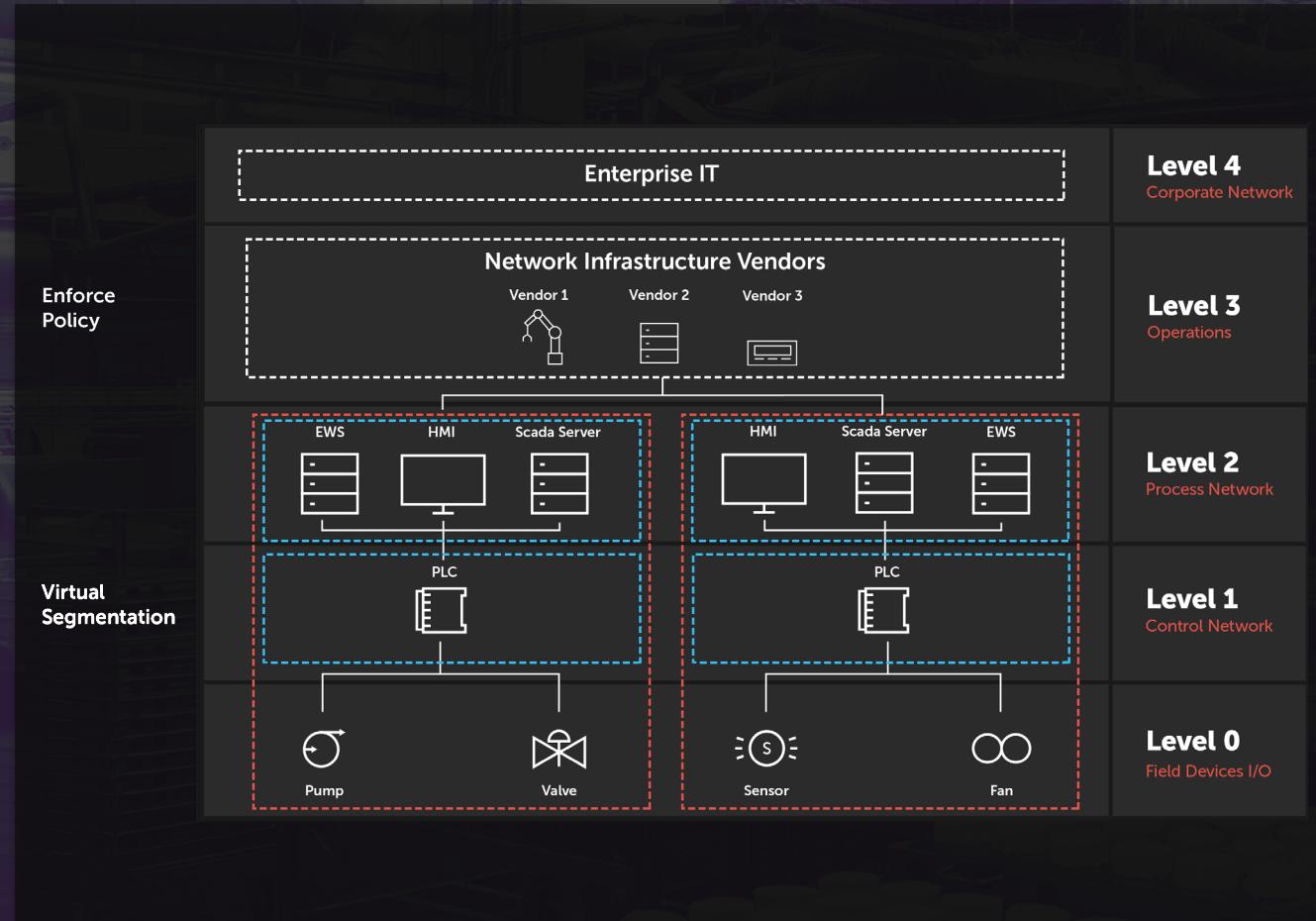
Case Study #3



CLAROTY
Clarity for OT Networks

RSA® Conference 2019

Case Study #3

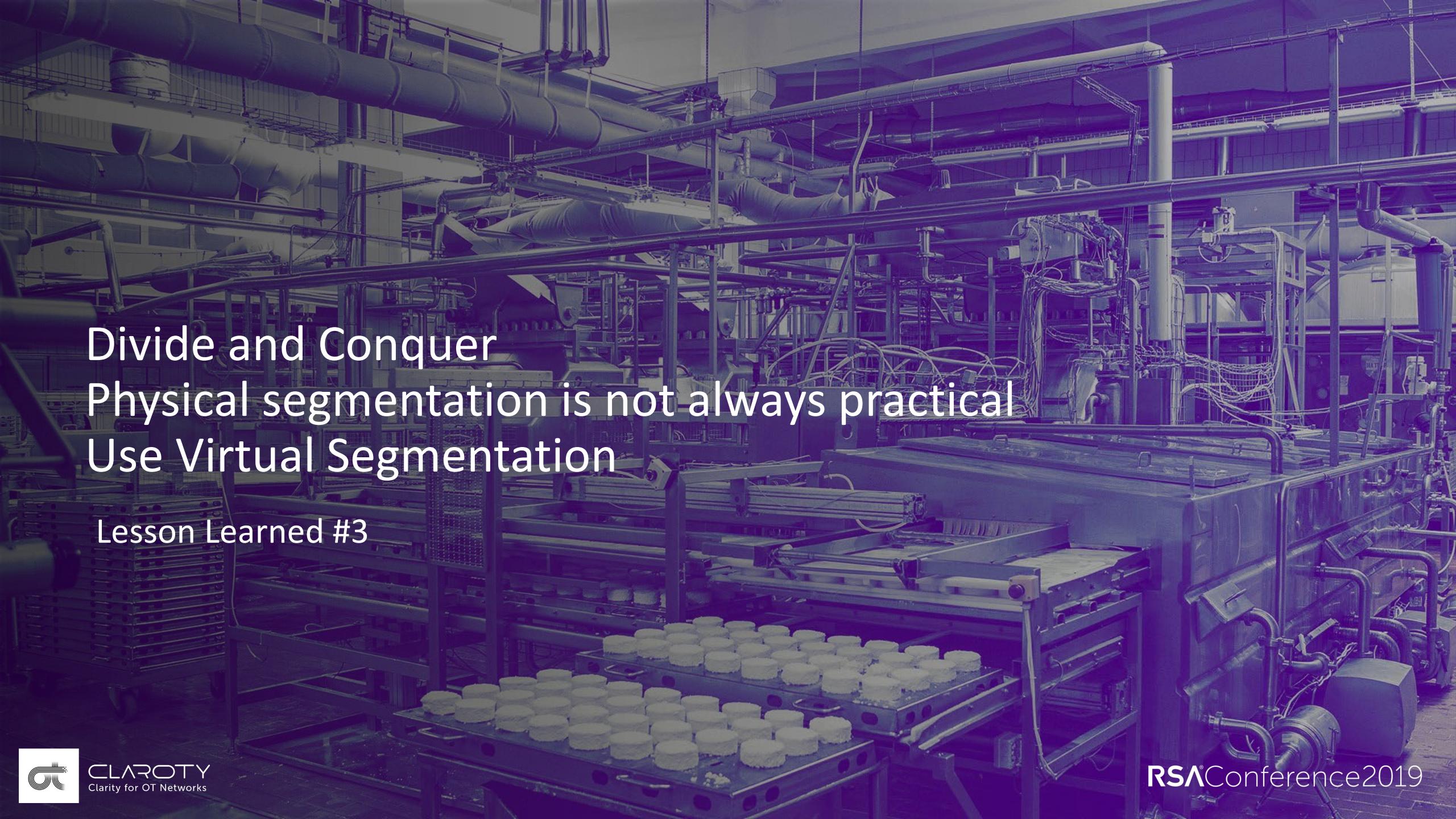


- Large manufacturing operation, initiated a physical segmentation project (Level 2 and below)
- Impractical to achieve – cost, downtime, personnel
- Virtual zones provide what's needed (alert, not block) without the downtime
- Enforcement policy implemented at a higher level
- Doesn't apply to every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



CLAROTY
Clarity for OT Networks

RSA® Conference 2019



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

Lesson Learned #3



CLAROTY
Clarity for OT Networks

RSA® Conference 2019

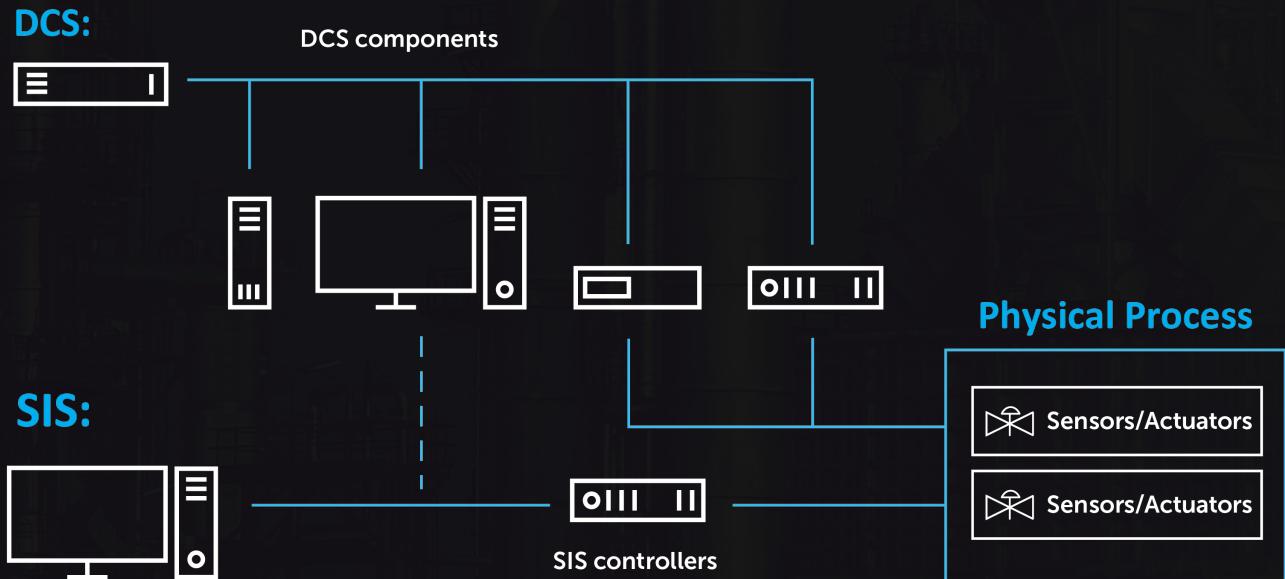
Case Study #4



CLAROTY
Clarity for OT Networks

RSA® Conference 2019

Case Study #4



- Known case of Triton, lessons apply to any critical infrastructure network
- Attackers in the network for months; ICS network a black box, no ability to identify movement
- Changing programming of Safety Instrumented System (SIS) is a different category of alert
- Measure everything through lenses of potential impact – that will inform prioritization

A large, complex industrial facility, likely a refinery or chemical plant, with numerous tall metal structures, pipes, and walkways against a clear sky.

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

Lesson Learned #4



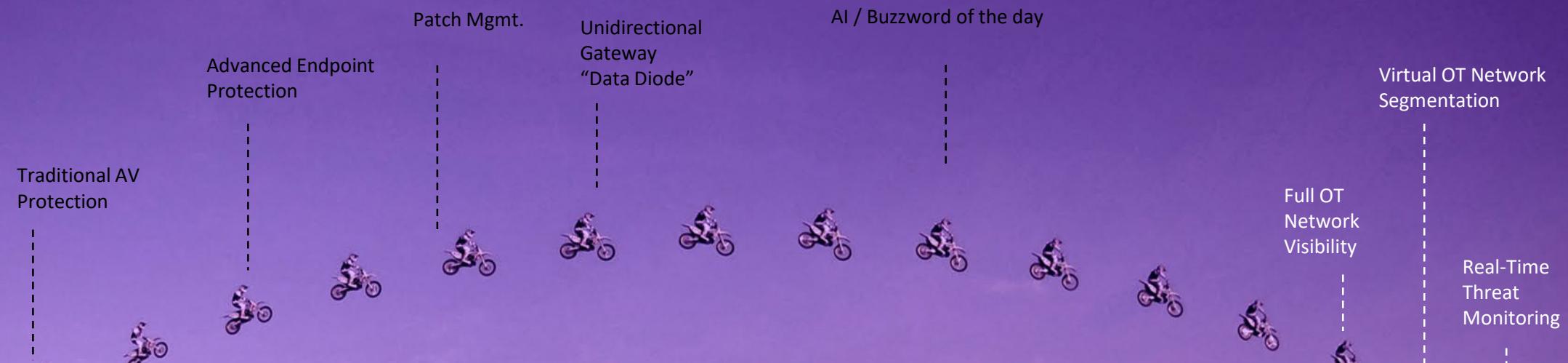
CLAROTY
Clarity for OT Networks

RSA Conference 2019

RSA®Conference2019

Ultimately, It's All About
Investing Smart

Prioritize Measures Based on the Highest ROI



CLAROTY
Clarity for OT Networks

RSA Conference 2019

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
- The only way to efficiently detect manipulation of 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
- Vitaly 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

RSA® Conference 2019

Thank you!

Questions?



CLAROTY
Clarity for OT Networks

RSA® Conference 2019