15th OT Security Forum
29 May 2024

The Business-driven network segmentation

Johny Gasser

Business
CyberDefense

Agenda

I. Setting the scene
II. Most network segmentation projects fail…
III. What is the root cause?
IV. Why?
V. What can we do?

Setting the scene

Setting the scene
Time is running

40%+

of ransomware and wipers targeted the industrial sector, indicating that cybercriminals are focused on OT and the supply chain

4.76 days

On average, for new exploits identified, attacks occurred in 4.76 days after discovery. That's 43% faster than the prior period.

Source: Fortinet Global Threat Landscape Report 2023 H2

Unit42 (Palo Alto Networks) exposed 320 honeypot infrastructures hosted in the main hyperscalers cloud

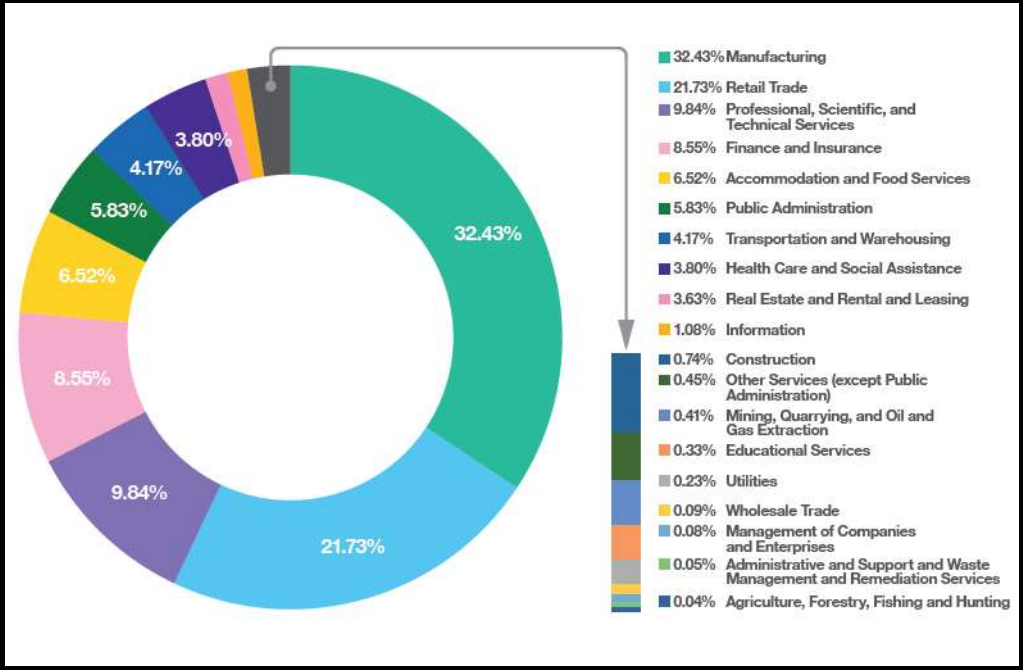
Findings

- **Researchers found that 80% of the 320 honeypots were compromised within 24 hours**
- **all of the honeypots were compromised within a week**
- The most attacked SSH honeypot was compromised 169 times in a single day.
- One threat actor compromised 96% of our 80 Postgres honeypots globally within 30 seconds.
- 85% of the attacker IPs were observed only on a single day.

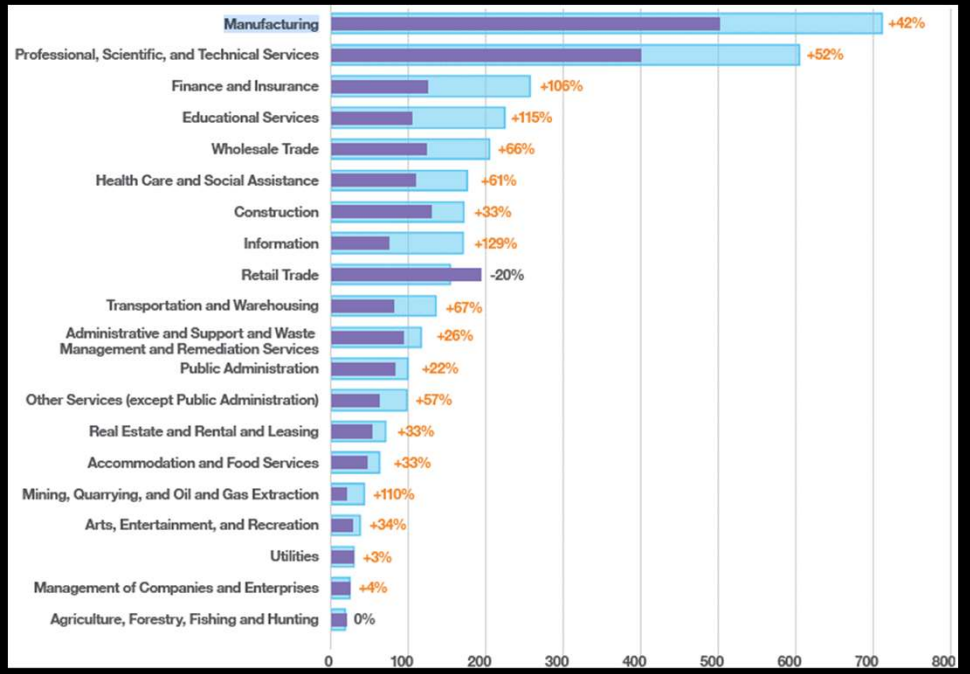
Source: https://unit42.paloaltonetworks.com/exposed-services-public-clouds/

Setting the scene
Manufacturing is the preferred target

Cyberincident split



Cyber-extorsion victims



Source: Orange CyberDefense Security Navigator 2024 - https://www.orangecyberdefense.com/ch/security-navigator

Schwartau concept
Time-based security

$$Et = Dt + Rt$$

Exposure time (Et): The time the resource, information, or organization is susceptible to attack or compromise.

Detection time (Dt): The time it takes for the vulnerability or the threat to be detected.

Reaction time (Rt): The time it takes for the individual, group, or organization to respond and eliminate or mediate the vulnerability or risk.

Most network segmentation fails to deliver the promises
What do Analysts say?

FORRESTER®

Most Microsegmentation Projects Fail

- Analysis paralysis
- Going too big too soon
- Lack of visibility
- Enforcement anxiety
- Lack of a nontechnical business driver

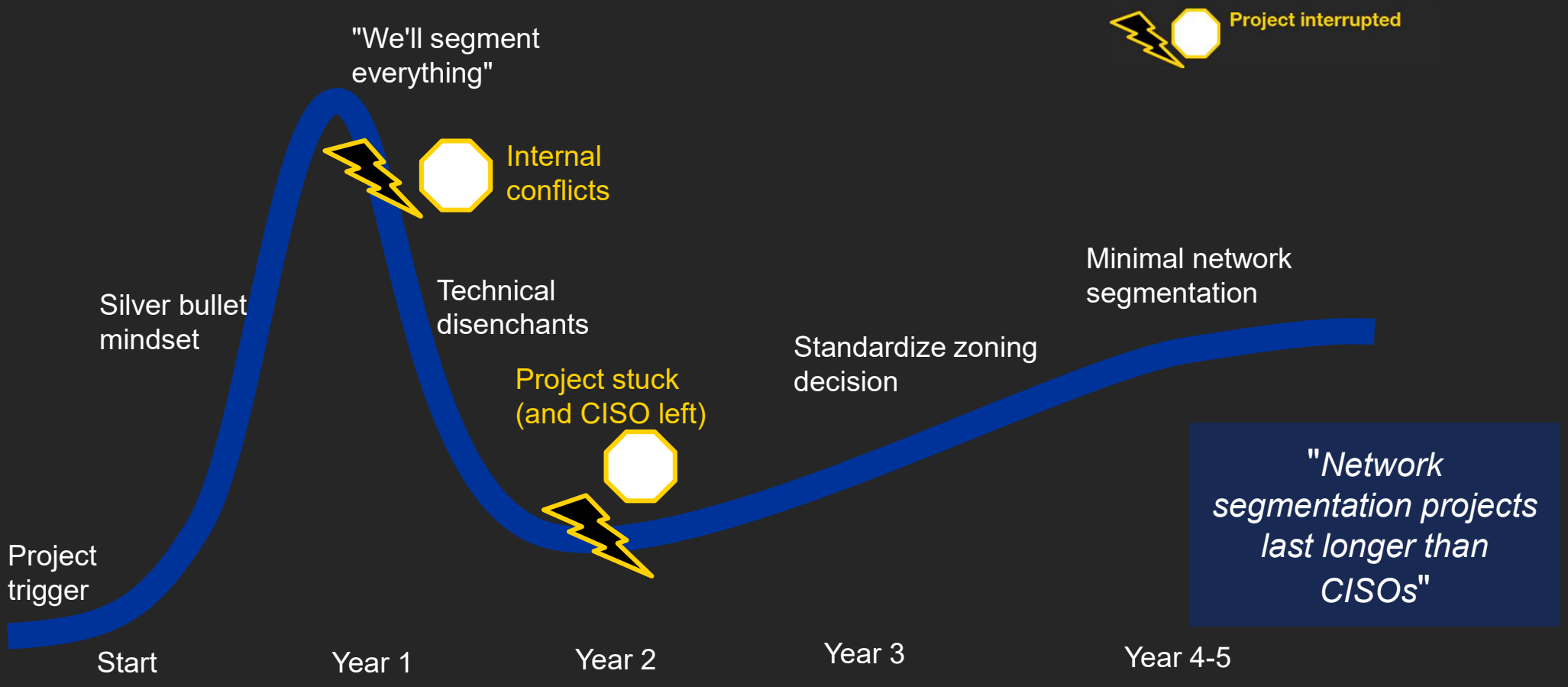
Source: Apply Zero Trust In The Network With These Best Practices For Microsegmentation

Gartner

- The failure rate for network segmentation projects is high, and most projects last longer than the average tenure of a CISO.
- “Broad scope” and “segment everything” mindsets will inevitably lead to a network segmentation project failure.
- Implementation constraints and “shiny new technology” driving the network segmentation strategy inevitably lead to suboptimal and inefficient architectures.

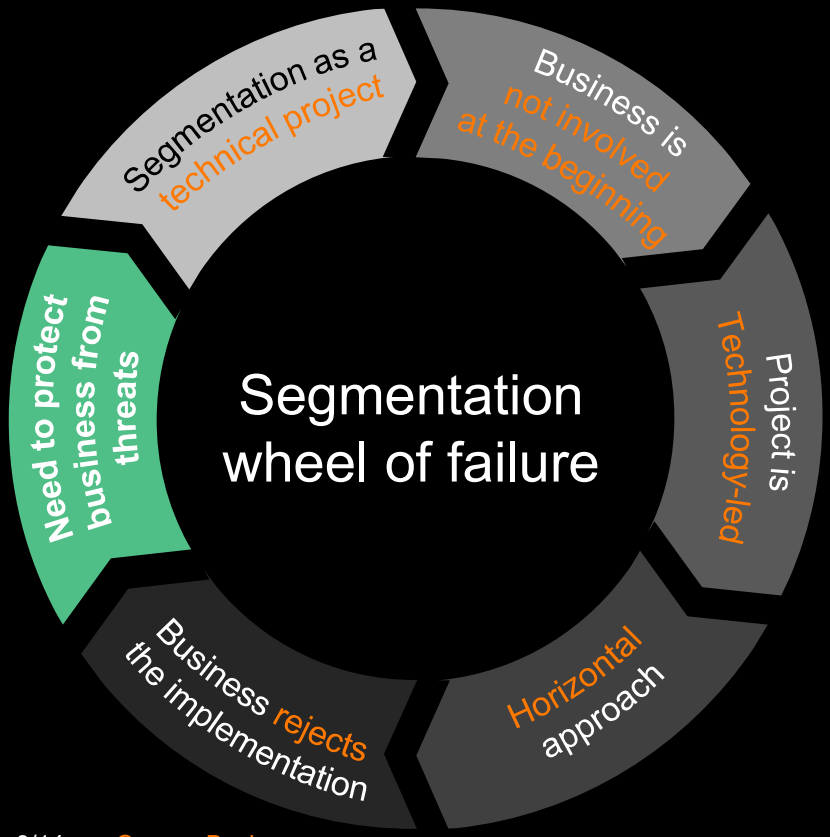
Source: The 6 Principles of Successful Network Segmentation Strategies

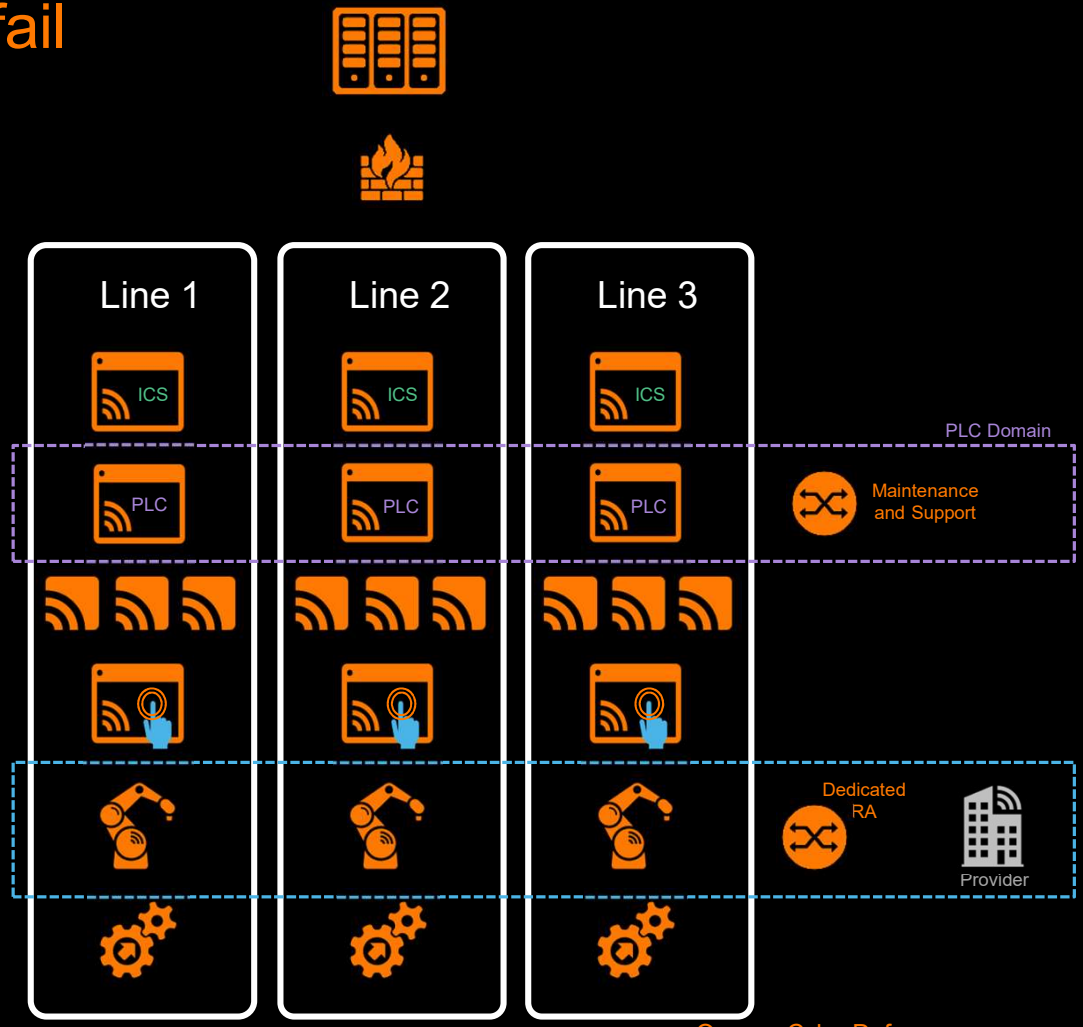
How Network Segmentation Projects Fail
According to Gartner



Source: https://blogs.gartner.com/andrew-lerner/2021/06/09/network-segmentation-is-still-hard/

Many network segmentation projects fail
Orange view

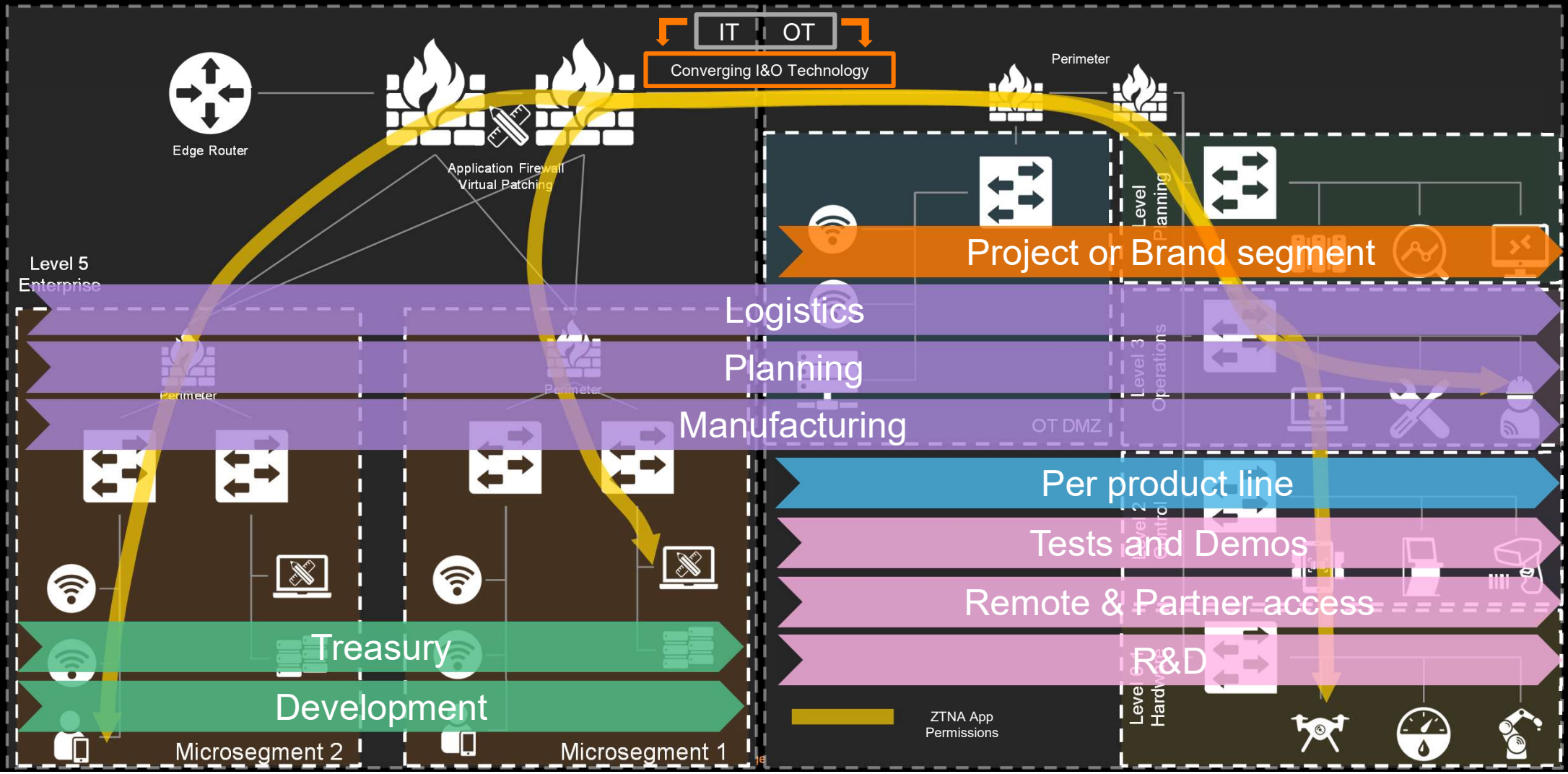




The Orange's analysis of the root causes

What if this mindset was applied in the air tansport industry?

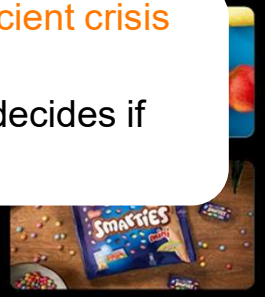
Segmentation
Business functions

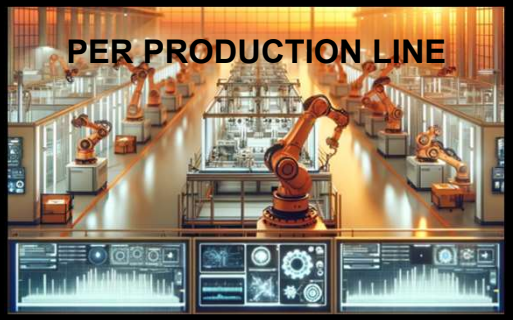


Forget the technical segmentation
Adopt the Business-driven segmentation

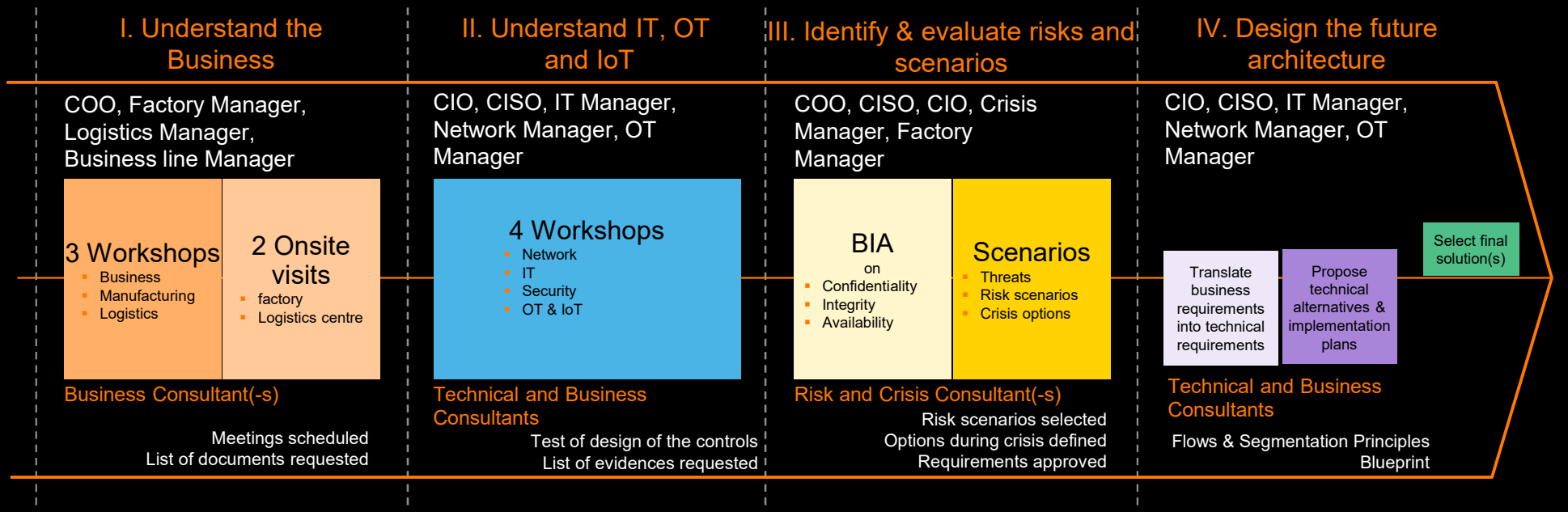
Expert tip for an efficient crisis management:

A single business owner decides if we isolate a segment





The Business-driven segmentation
The Orange's approach



Our advice for a successful network segmentation
The Top-5

1. The aim is to protect the Business, not IT/OT systems. So, understand the Business as the initial step
2. Identify IT/OT systems per Business process
3. Identify the risk scenarios (both technical and business) you would like to protect from
4. Gain trust from the Business and factory/operations managers by starting with a limited scope
5. The vendor/technology choice comes last

Multi-disciplinary

Involves the key stakeholders:

- Business representative
- Decisionmaker
- Business Risk Experts
- Security Management
- Security & IT Architects
- Security Operations
- IT
- OT

Questions?

Let's stay in touch

Johny GASSER

Strategist & Advisor

- Digital Business Risk Management
- Cyber Risk Management
- Business Cyber-Protection
- Cybersecurity
- Crisis Management

Key certificates

- Harvard graduated in cybersecurity
- CISM
- CISSP
- CRISC
- Enterprise Data Protection Officer
- and more

johny.gasser@orange.com

+41 78 694 99 94