# SOC voor OT

You cannot protect what you don’t understand

**Nick Peeters & Tom Van Hoeydonck**
**10/10/2023**

Industrial Cyber Security

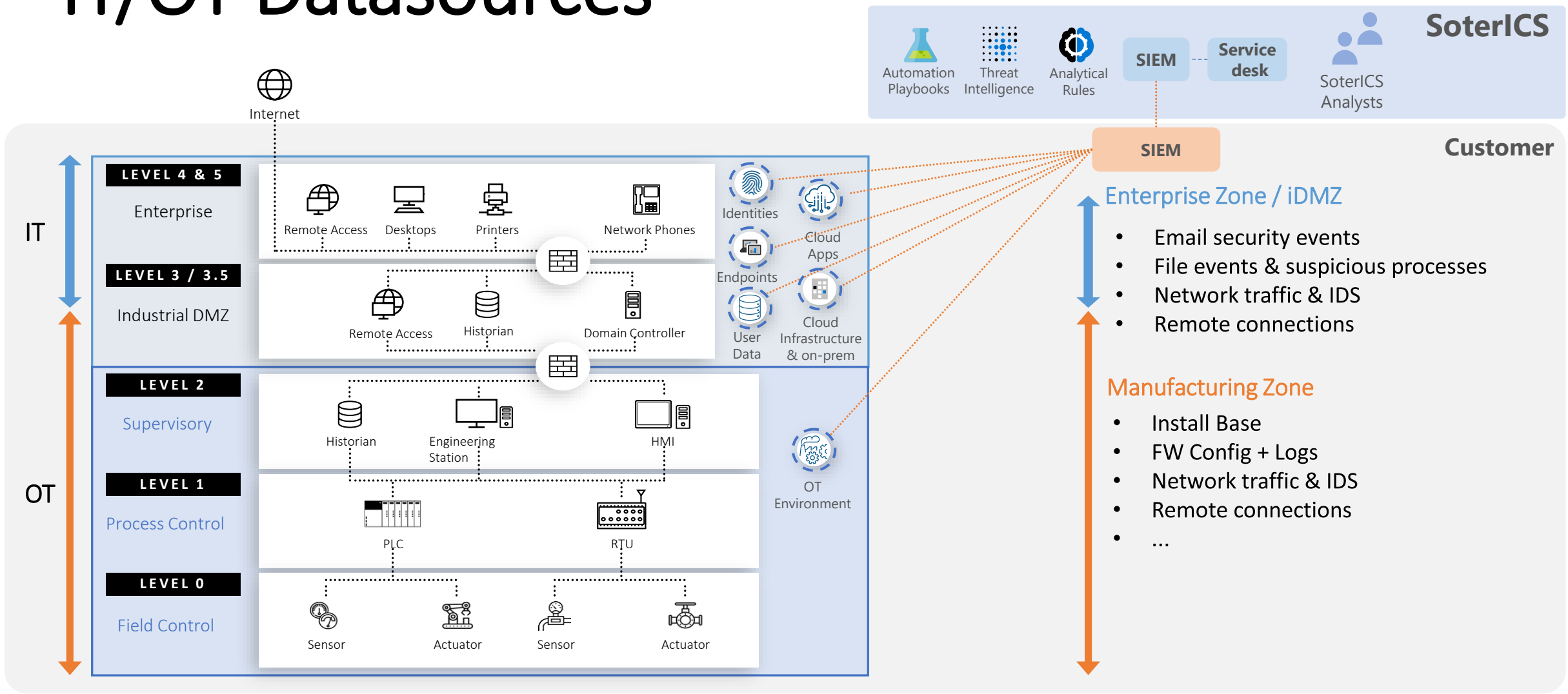
10 oktober 2023 | Congrescentrum 1931, den Bosch

soterics

# Wat is een SOC? - Gartner

- Een team dat 5/8 of 24/7 beschikbaar is om cyber incidenten te onderzoeken
- Preventief onderzoeken en mitigeren van cybersecurity dreigingen en incidenten
- Naleven van de cybersecurity bedrijfspolicy of wetgeving

# IT/OT Datasources




Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

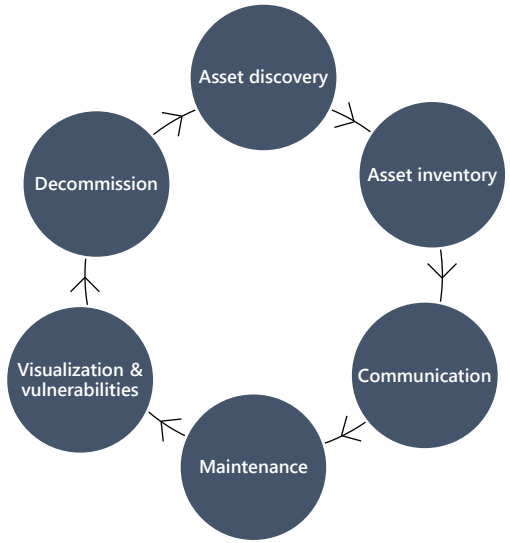
soterics

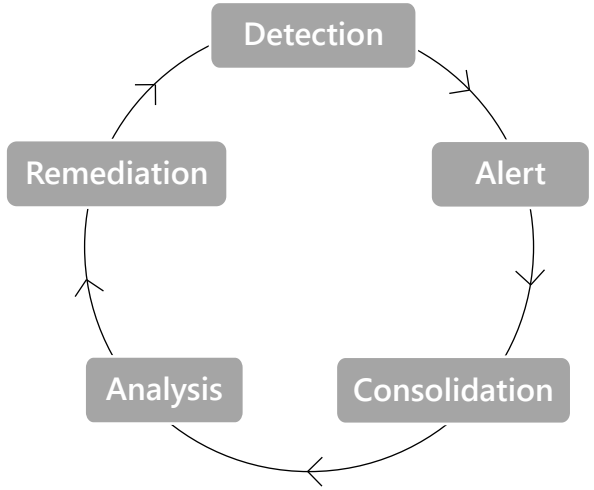
# Any fool can know. The point is to understand.

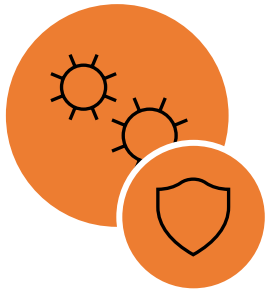
- Albert Einstein

# SecOps Teams Lifecycle

Visibility and profiling → Consolidated monitoring → Incident response → Security automation



OT/ICS

IT

OT/ICS

IT

Industrial Cyber Security

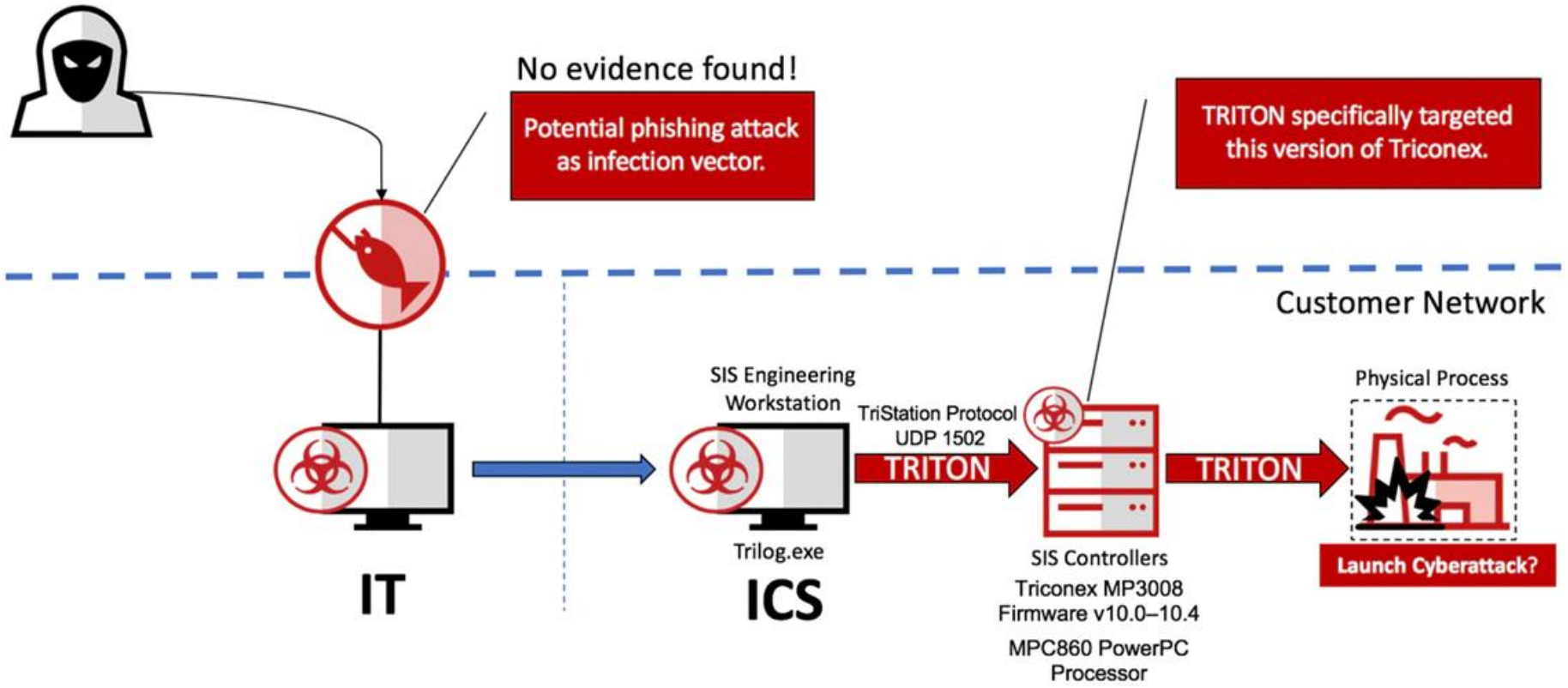
10 oktober 2023 | Congrescentrum 1931, den Bosch

soterics

# Lessons Learned from SOC Teams in OT

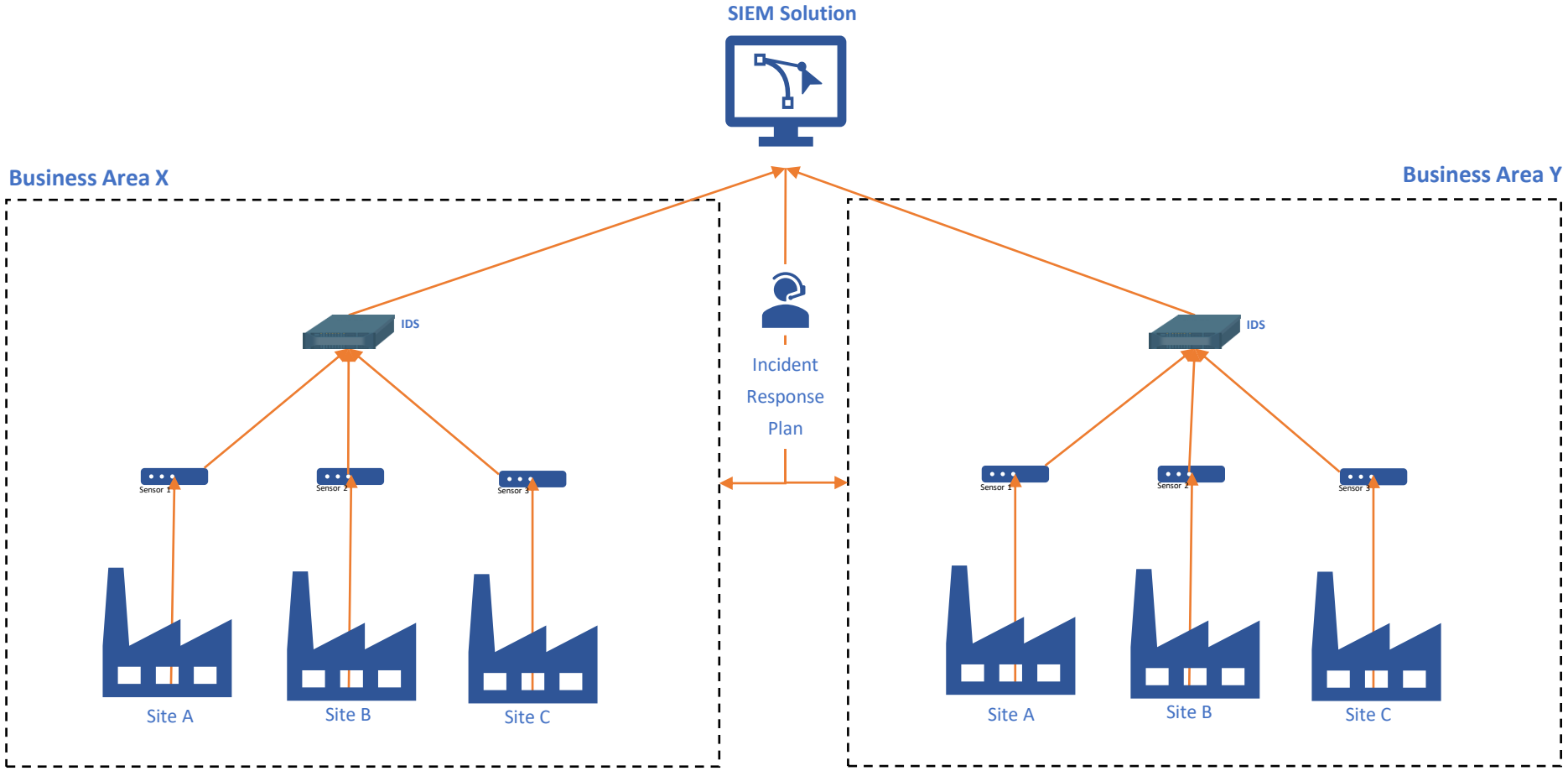
- [x] Unify OT/IT/IoT in het SOC
- [x] Volledige zichtbaarheid op de OT install base is cruciaal
- [x] Breng OT dichter bij SecOps

# Unify OT/IT/IoT in het SOC

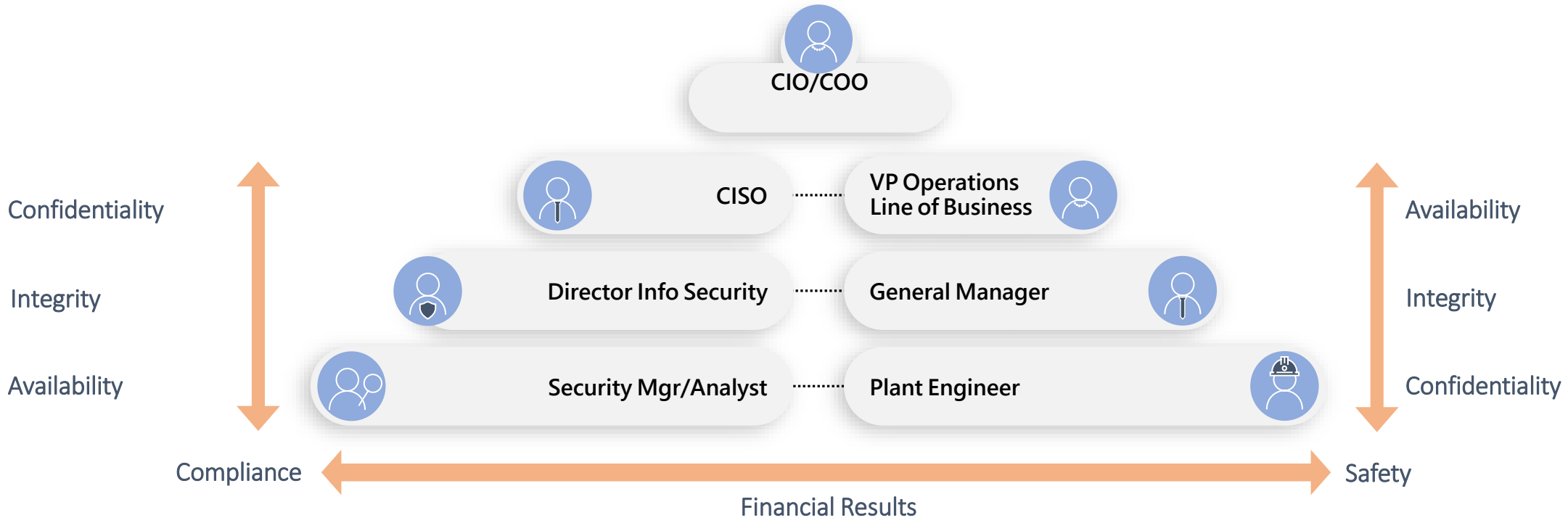



# Monitoring & Response

Volledige zichtbaarheid op de OT install base is cruciaal

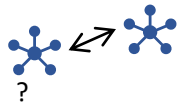



# Breng OT dichter bij SecOps



# Breng OT dichter bij SecOps

## Business Context is key!

| | | | | | |
|---|---|---|---|---|---|
| Internet Connectivity |  | Critical | Unauthorized Internet Connectivity | Policy Deviation | 22 hours ago | ✓ **Closed** |
| Device responsiveness |  | Major | Device Disconnected | Operational | 2 days ago | ✓ **Closed** |
| Malware alerting |  | Critical | Suspicion of Malware | Malware | 1 hour ago | ! **New** |
| Communication errors |  | Critical | Beckhoff AMS Command Failure | Policy Deviation | 5 days ago | ✓ **Closed** |

Showing 4 of 1267 alerts…

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

soterics

# Bigger Picture

servicenow | soterics

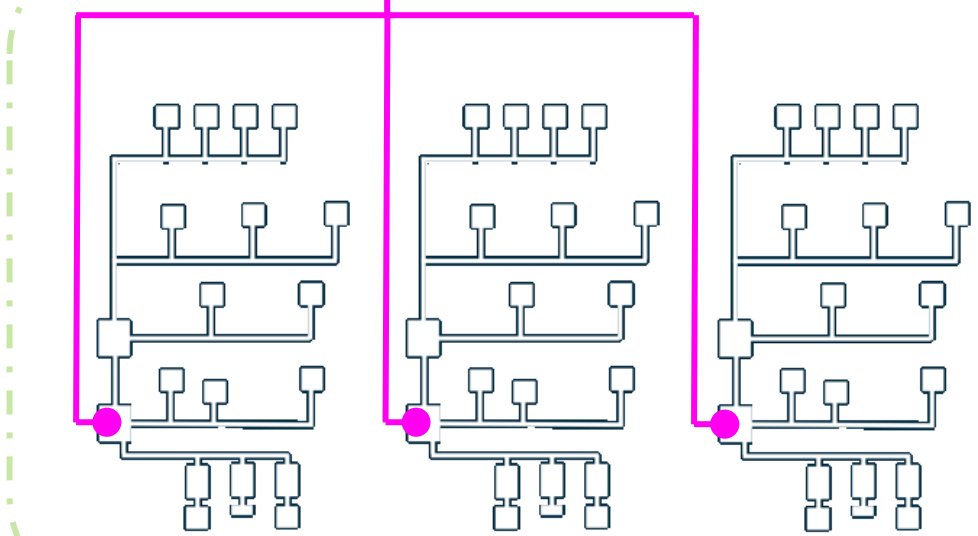
**OT SOC**

OTORIO | Microsoft | NOZOMI NETWORKS | WALLIX CYBERSECURITY SIMPLIFIED | CLAROTY | FORTINET

**Governance**
(Deviated from standards: IEC62443, NIST, ISO27k)

**Incident Response Planning**

**OT Security Society**
(Structure, Trainings, etc)



Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

soterics

# Get In Touch

**Nick Peeters**
**Consultancy Lead**

Nick.peeters@soterics.com
+324 78 96 10 64

**Tom Van Hoeydonck**
**Technical Lead**

Tom.van.hoeydonck@soterics.com
+324 77 32 28 65

# DEMO

soterics

*“Protecting the vulnerable in our digital society”*

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

soterics