
Spinae
Cybersecurity in OT & IT

Bridging OT and IT

A practical, risk-based approach to industrial cybersecurity

2025-10-07 – BE-CYBER

Stijn Boussemaere, Co-Founder of Spinae

T: +32 9 396 35 35 – E: info@spinae.be
https://www.linkedin.com/in/stijnboussemaere/

Who is from the **IT** world?

Spinae

CYBER SECURITY COALITION.be

Who is from the **OT** world?

Spinae

CYBER SECURITY COALITION.be

Who is from both the **IT** & the **OT** world?

Spinae

CYBER SECURITY COALITION.be

M&S' slow recovery from cyberattack puts it at risk of lasting damage

By **James Davey** and **Sarah Young**

May 19, 2025 5:12 PM GMT+2 · Updated May 19, 2025

Spinae

CYBER SECURITY COALITION.be

M&S' slow recovery from cyberattack puts it at risk of lasting damage

By James Davey and Sarah Young

May 19, 2025 5:12 PM GMT+2 · Updated May 19, 2025

'Elevated' risk of hackers targeting UK drinking water, says credit agency

Moody's warning over hacking's effect on debts may bolster water utilities' plans to hike bills to cover needed investments

Integrated systems and smart meters make utility firms more vulnerable to cyber attackers targeting our water supply. Photograph: Rui Vieira/PA

Spinae

CYBER SECURITY COALITION.be

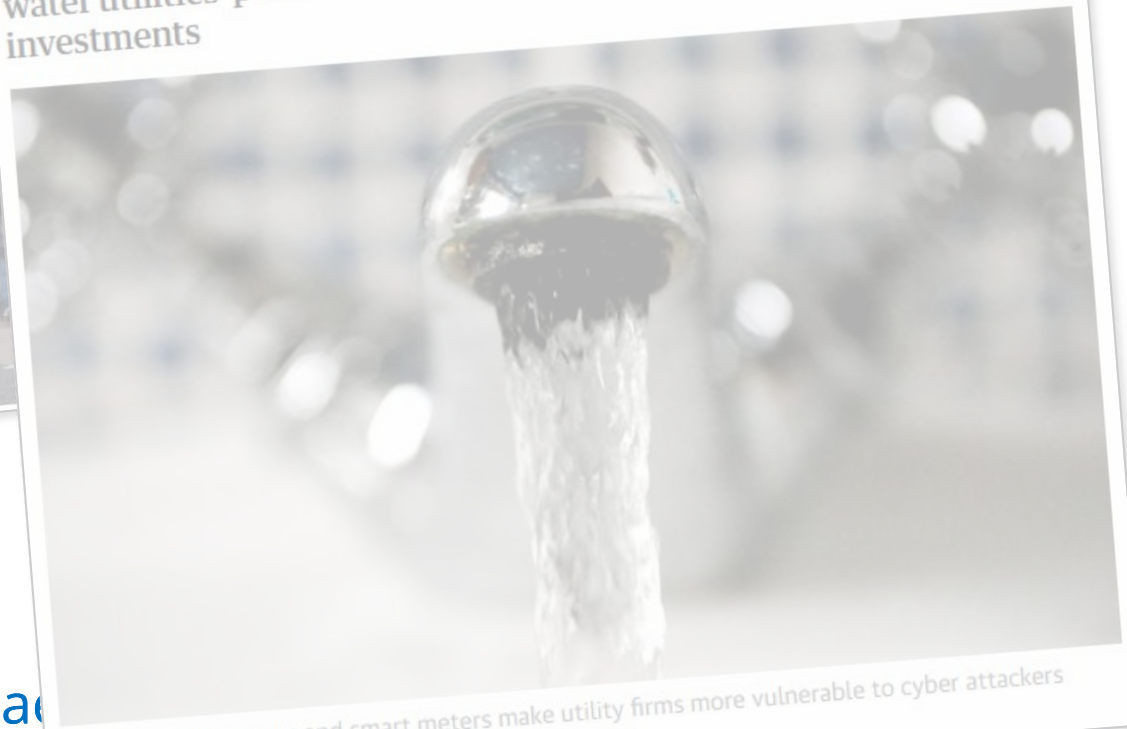
M&S' slow recovery from cyberattack puts it at risk of lasting damage

By James Davey and Sarah Young

May 19, 2025 5:12 PM GMT+2 · Updated May 19, 2025

'Elevated' risk of hackers targeting UK drinking water, says credit agency

Moody's warning over hacking's effect on debts may bolster water utilities' plans to hike bills to cover needed investments



Integrated systems and smart meters make utility firms more vulnerable to cyber attackers targeting our water supply. Photograph: Rui Vieira/PA

Risk of undersea cable attacks backed by Russia and China likely to rise, report warns

Spate of incidents in Baltic Sea and around Taiwan are harbinger for further disruptive activity, cybersecurity firm says

Submarine cables account for 99% of the world's intercontinental data traffic. Photograph: Mint Images/Getty Images/Mint Images RF

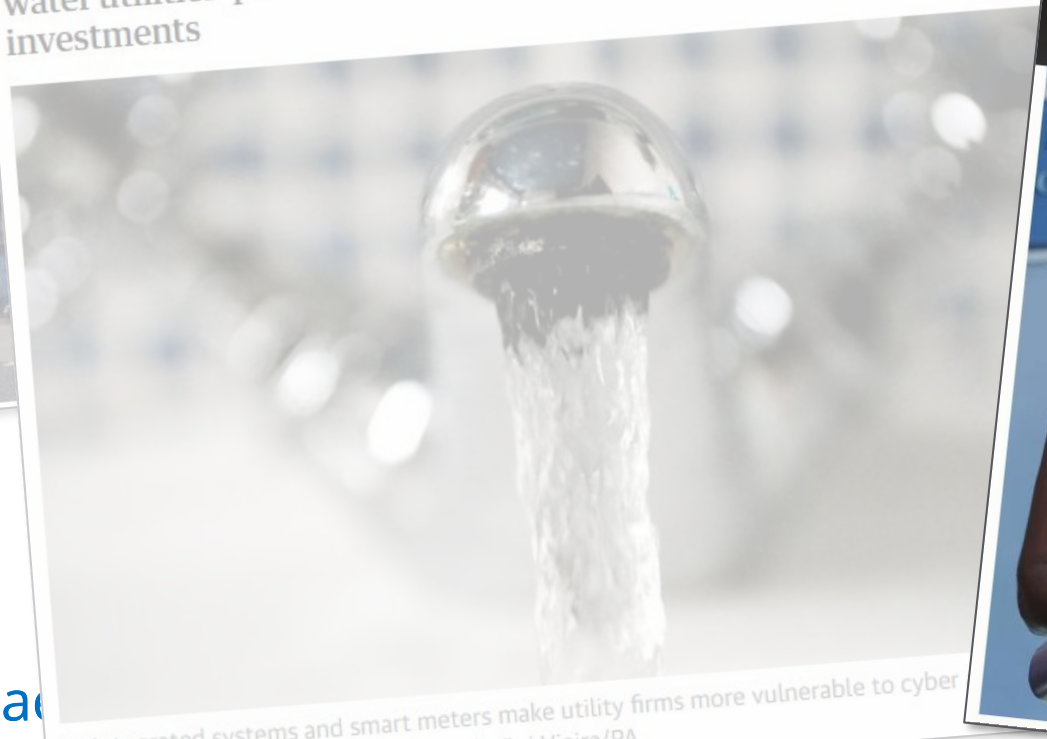
M&S' slow recovery from cyberattack puts it at risk of lasting damage

By James Davey and Sarah Young

May 19, 2025 5:12 PM GMT+2 · Updated May 19, 2025

'Elevated' risk of hackers targeting UK drinking water, says credit agency

Moody's warning over hacking's effect on debts may bolster water utilities' plans to hike bills to cover needed investments



Integrated systems and smart meters make utility firms more vulnerable to cyber targeting our water supply. Photograph: Rui Vieira/PA

Risk of undersea cable attacks backed by Russia and China likely to rise, report warns

Spate of incidents in Baltic Sea and around Taiwan are harbinger for further disruptive activity, cybersecurity firm says

New labels will help people pick devices less at risk of hacking

Standards / Frameworks / Directives / Legislation requiring risk-based approach

NIS2 Network & Information Systems Directive

NIST CSF

Cyber Resilience Act

IEC

ISA/IEC 62443

CIS Controls

Centre for Internet Security

Information Security Management System ISO 27001 Certified

ISO 27001

CyberFundamentals Framework

Spinae

CYBER SECURITY COALITION.be

But what is RISK?

"the effect of uncertainty on objectives"

a deviation from what is expected

cybersec: the potential that threats exploit vulnerabilities that lead to harm

Spinae

CYBER SECURITY COALITION.be


Ok, nice theory,
but what can I
do in practice?

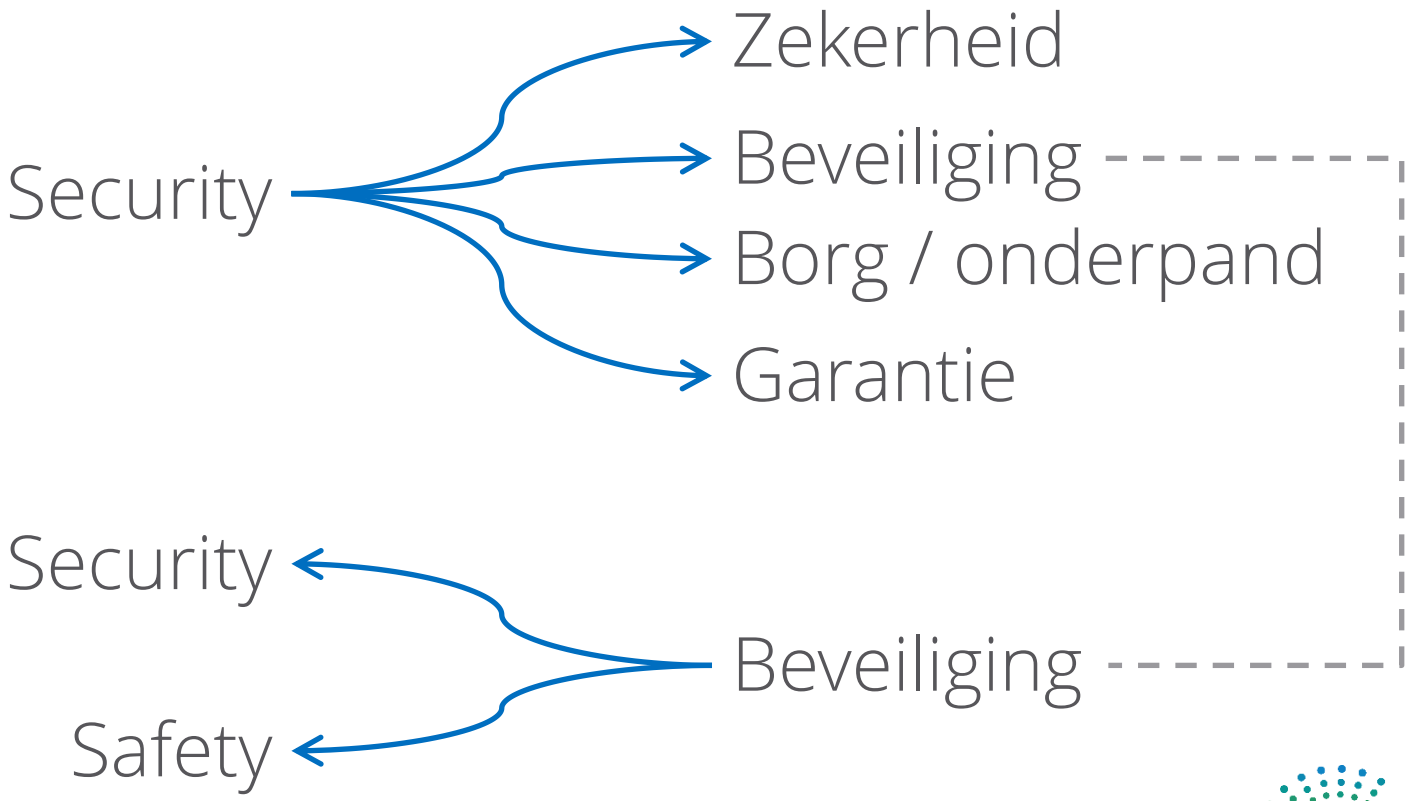
Language confusion

Spinae

CYBER SECURITY COALITION.be

Language confusion

English 🤜🤛 Dutch



Spinae

CYBER SECURITY COALITION.be

Language confusion

IT 👎 👉 OT

Spinae

CYBER SECURITY COALITION.be


Encryption,
MFA, SASE
Production,
OEE, Throughput
IT
OT

Create common language for risk

1

- Risk = Likelihood x Impact
- Risk = Probability x Consequence
- Risk = Threat x Vulnerability x Consequence

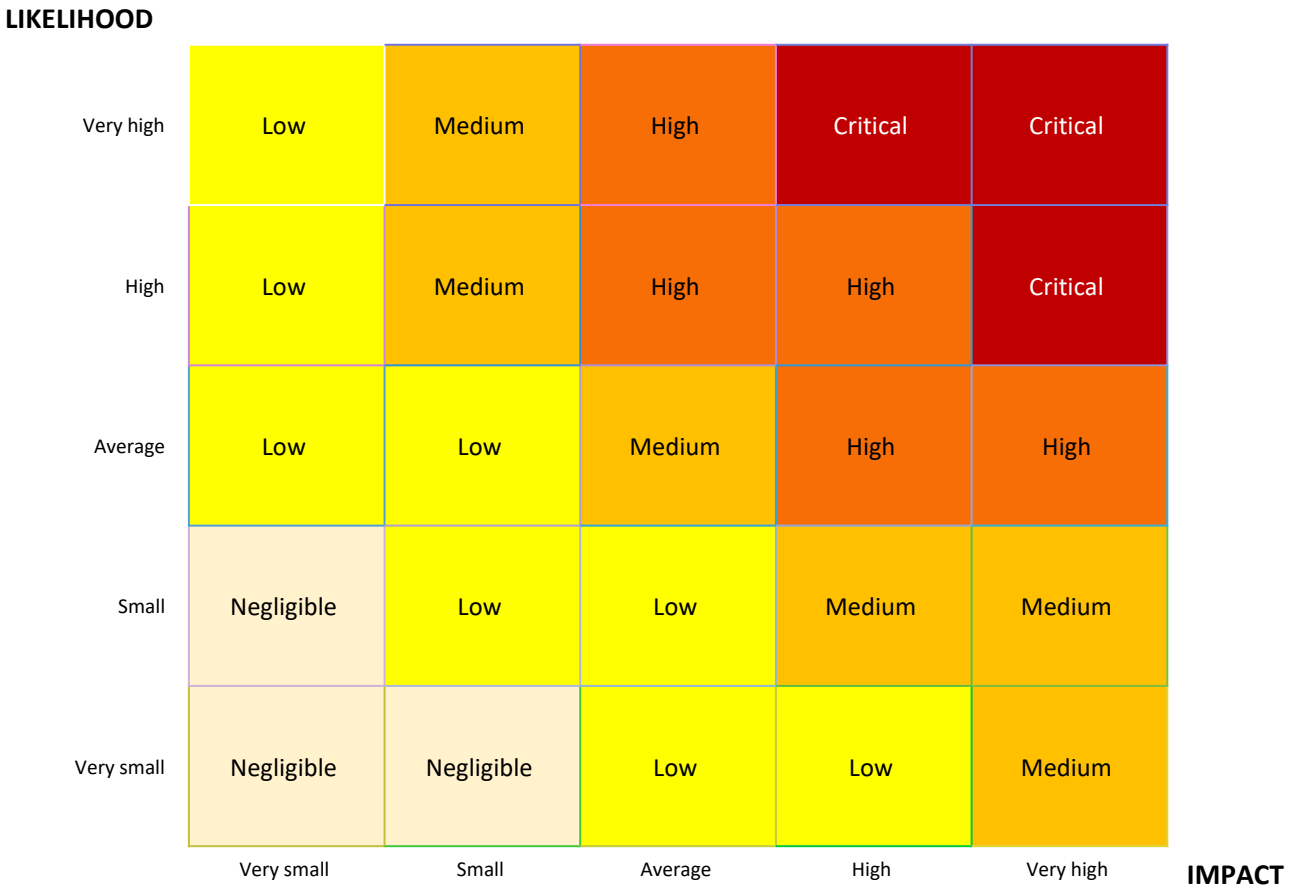
Whatever works
Pick one
Stick to that choice

- Already some form of formal risk management in the company? → align with that
  - Same number of levels of likelihood
  - Same number of levels of impact
  - Same wording

Spinae

CYBER SECURITY COALITION.be

- Risk = Likelihood x Impact



Spinae

CYBER SECURITY COALITION.be

Impact scales

Very high	- Complete production unplanned downtime of one or more production sites > 24 hours - Impact on large number of customers, potential customer loss - Significant threat to employee safety - Significant compromise/loss/unauthorized access to sensitive or confidential information (including PII)
High	- Complete production unplanned downtime of one production site > 8 hours - Impact on large number of customers, potential customer loss - Threat to employee safety - Significant compromise/loss/unauthorized access to sensitive or confidential information (including PII)
Average	...
Small	...
Very small	...

Spinae

CYBER SECURITY COALITION.be

Likelihood scales

Example

- Almost certain
  - Once or multiple times a year or expected to happen within 1 year
- Probable
  - Once every 2 years or expected to happen within 2 years
- Improbable
  - Once every 5 years or expected to happen within 5 years
- Exceptional
  - Once every 10 years or expected to happen within 10 years

Risk Management Policy

Common language established

Putting it in practice

2 examples

Spinae

CYBER SECURITY COALITION.be

Context

Example 1

- Multinational production company
- Headquarter in BE
  - Main datacenter in HQ (2 datarooms, redundancy, …)
- 30+ production sites
  - Some more important than others
- Standardized on Siemens PLCs & HMIs

Spinae

CYBER SECURITY COALITION.be

Situation

Example 1

- Backup of PLC programs and configurations using Octoplant*
- Suggestion: we want to consolidate the backups from all production facilities into our HQ datacenter
- Motivation: cost saving
- Required reflex: would this introduce additional cyber risks? If so: what are those and what is the risk level?

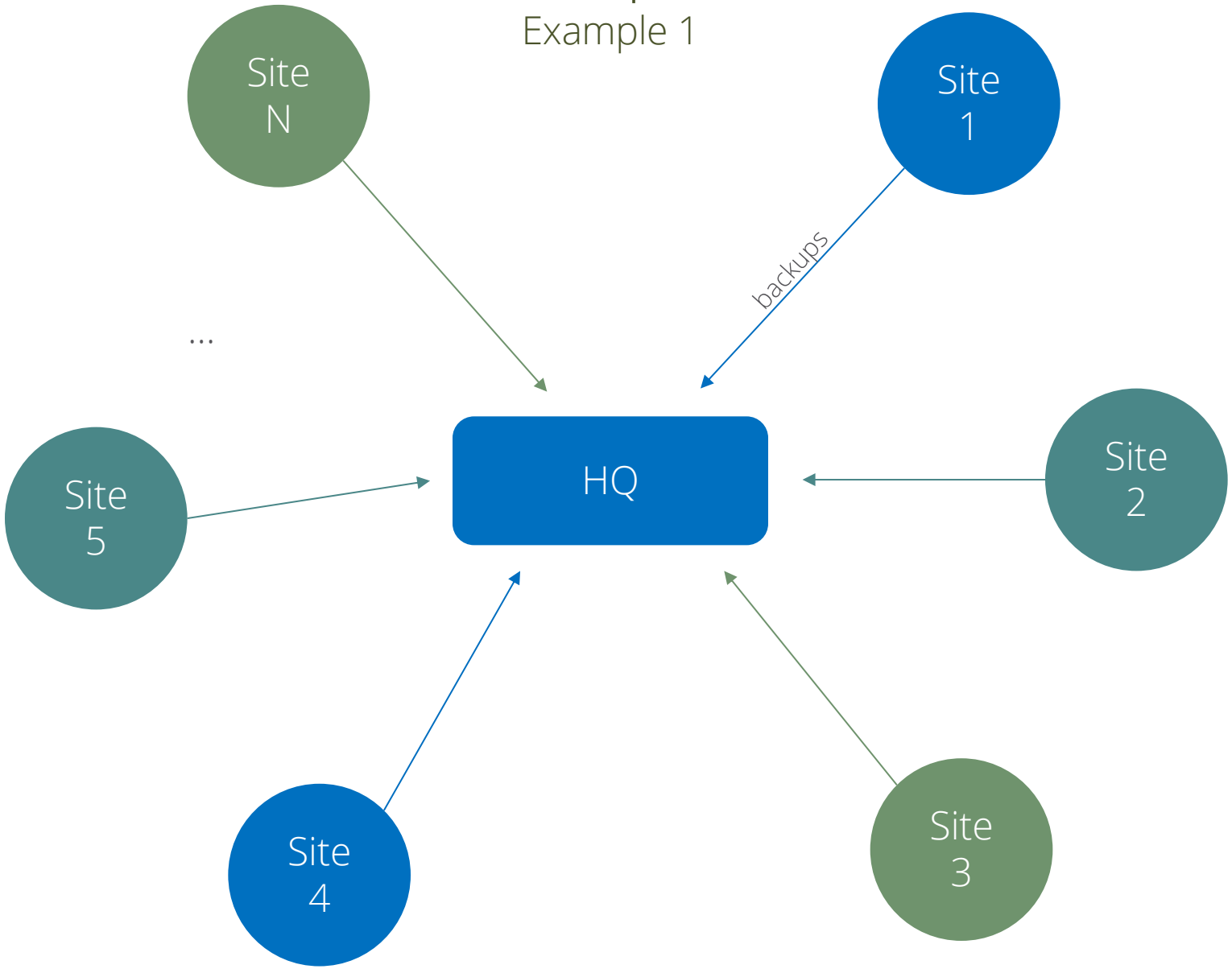
Spinae

*Spinae is vendor independent.
We have no affiliations with any of the brands or technologies used in these examples.

CYBER SECURITY COALITION.be

Conceptual

Example 1

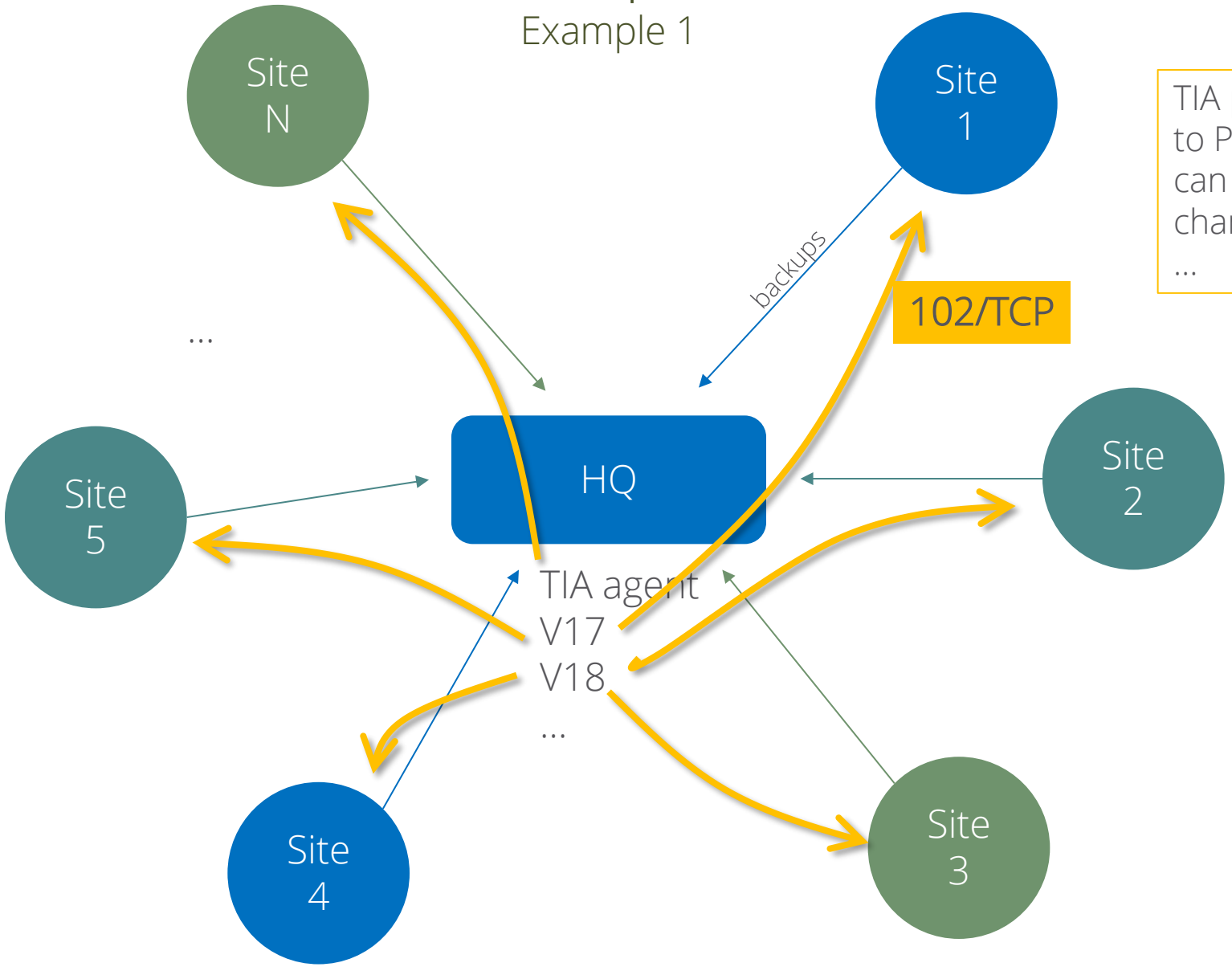


Spinae

CYBER SECURITY COALITION.be

Conceptual

Example 1



TIA portal with access to PLC over 102/TCP can change running state, change program, ...


What if this central backup system gets compromised? Or a human error (an “oops”) happens?

Risk-based approach in practice

In general

- Describe the risk
  - Describe the situation
  - Explain why it could happen
- Assess the impact
  - What could happen? What would be the worst-case situation resulting from this?
- Assess the likelihood
  - What are the chances that this would happen?

Spinae

CYBER SECURITY COALITION.be

Risk-based approach in practice

Example 1

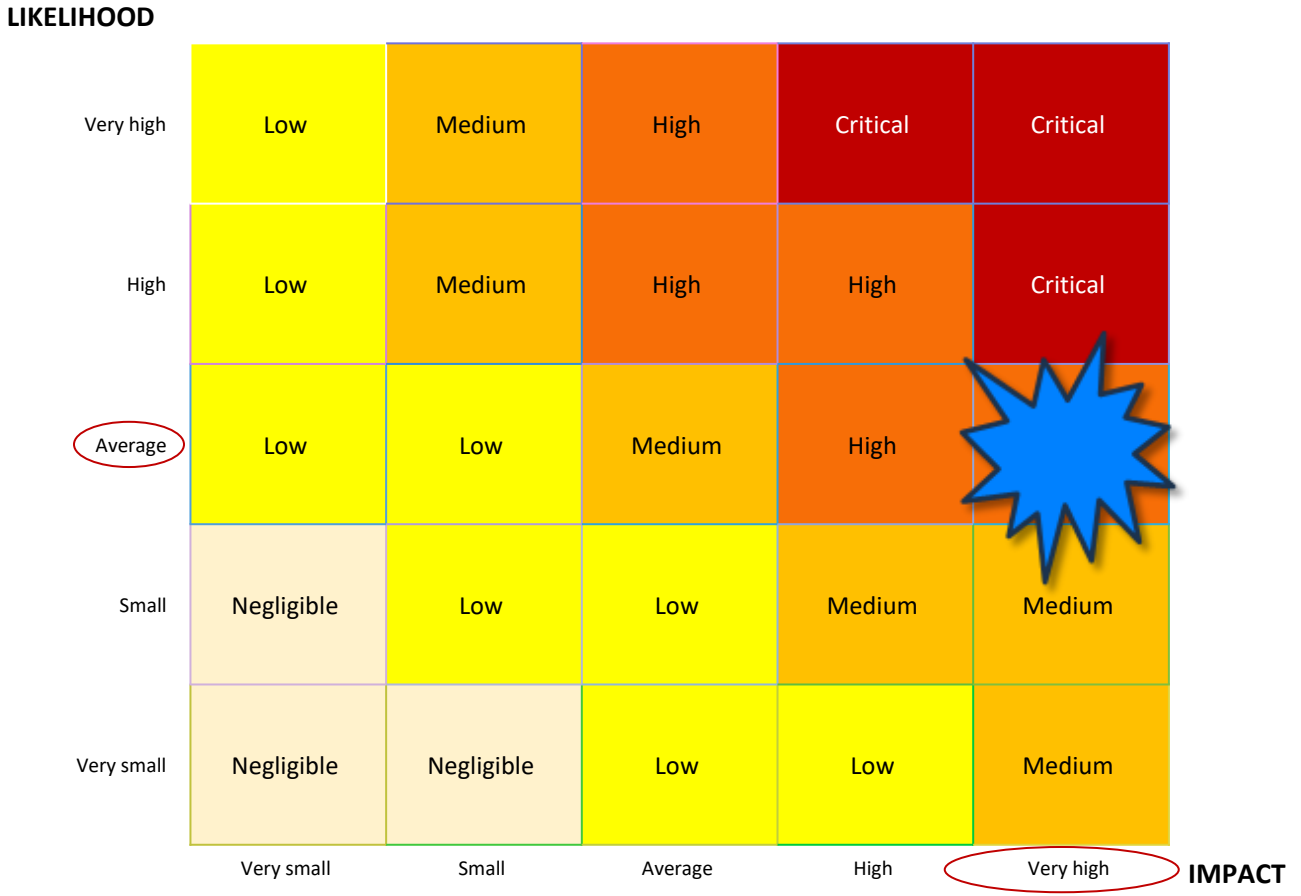
- Describe the risk
  - For the backup systems to work, they need to have network access to ALL PLCs of ALL production sites. The software required to create the backups also allows operation of the PLCs. This includes changing the running state and the programming of the PLCs.
  - Due to human error, misconfiguration, or a cyberattack, the programming or running state of ALL PLCs at ALL production sites could be modified. This could lead to the shutdown or malfunctioning of ALL production lines at ALL sites.
- Assess the impact
  - Very high
- Assess the likelihood
  - Average

Spinae

CYBER SECURITY COALITION.be

Risk-based approach in practice

Example 1



Spinae

CYBER SECURITY COALITION.be

Risk-based approach in practice

Example 1

- Describe the risk
  - For the backup systems to work, they need to have network access to ALL PLCs of ALL production sites. The software required to create the backups also allows operation of the PLCs. This includes changing the running state and the programming of the PLCs.
  - Due to human error, misconfiguration, or a cyberattack, the programming or running state of ALL PLCs at ALL production sites could be modified. This could lead to the shutdown or malfunctioning of ALL production lines at ALL sites.

- Assess the impact
  - Very high
- Assess the likelihood
  - Average

Risk Level = **High**

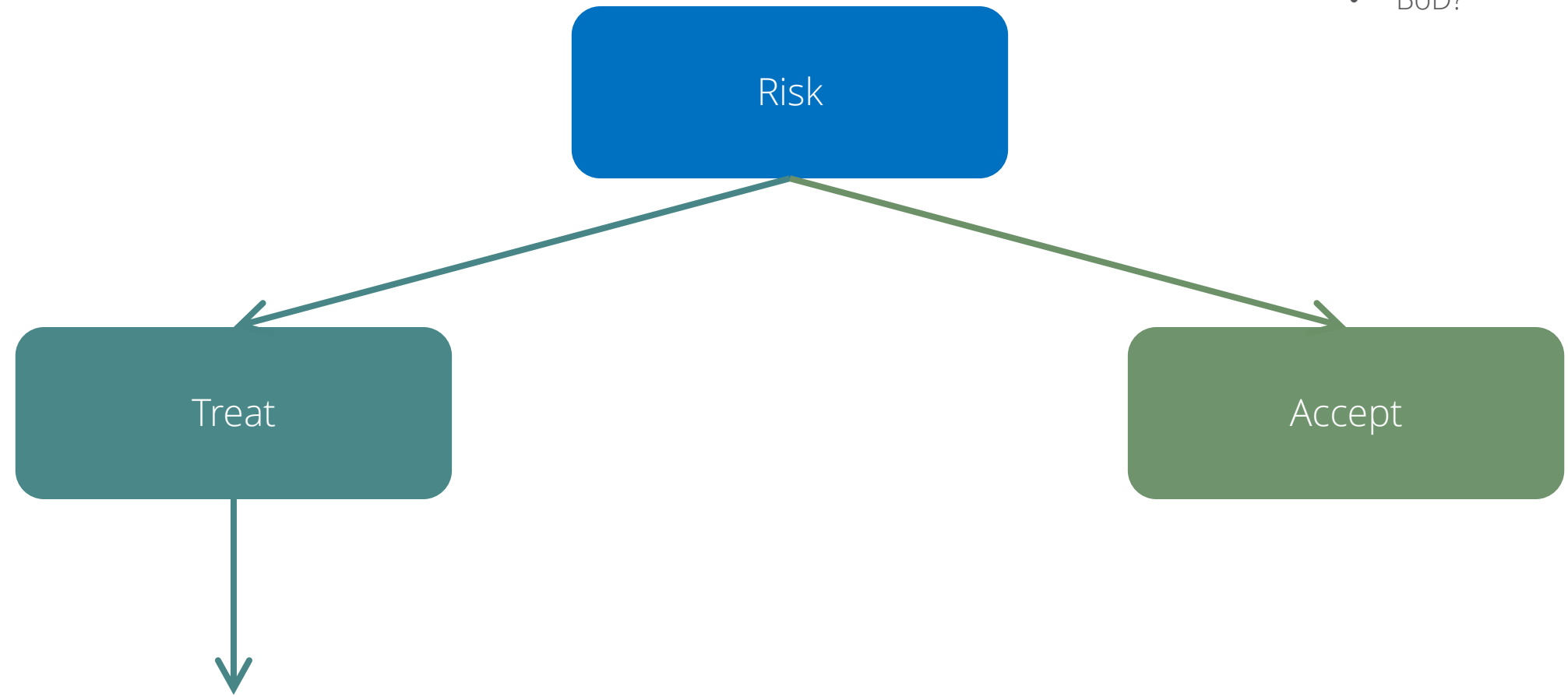
Spinae

CYBER SECURITY COALITION.be

Decide on risk

Risk owner

Depending on impact:
- Plant manager?
- Business Unit manager?
- BoD?



Spinae

CYBER SECURITY COALITION.be

Who has remote access possibilities into production?

Spinae

CYBER SECURITY COALITION.be

Context

Example 2

- Any type of production company where remote access into production is required
  - Basically : every production company

Spinae

CYBER SECURITY COALITION.be

Situation

Example 2

- Supplier / vendor delivers machine. Included with ‘the machine’ is an industrial remote access gateway
  - Examples: ewon, ixon, … *
- This is very convenient for the supplier / vendor
  - Remote support
  - Remote maintenance
  - …
- This might also introduce cyber risks

Spinae

*Spinae is vendor independent.
We have no affiliations with any of the brands or technologies used in these examples.

CYBER SECURITY COALITION.be

Risk-based approach in practice

Example 2

- Describe the risk
  - Hidden backdoor into our factory network
  - Supplier gateway as a stepping stone into our wider networks
  - Blind spot in our security monitoring

- Assess the impact
  - High
    - Unplanned production downtime in 1 factory, depending on type of machine or production line the Industrial Remote Access Gateway is placed in and how important that machine is in the production flow.

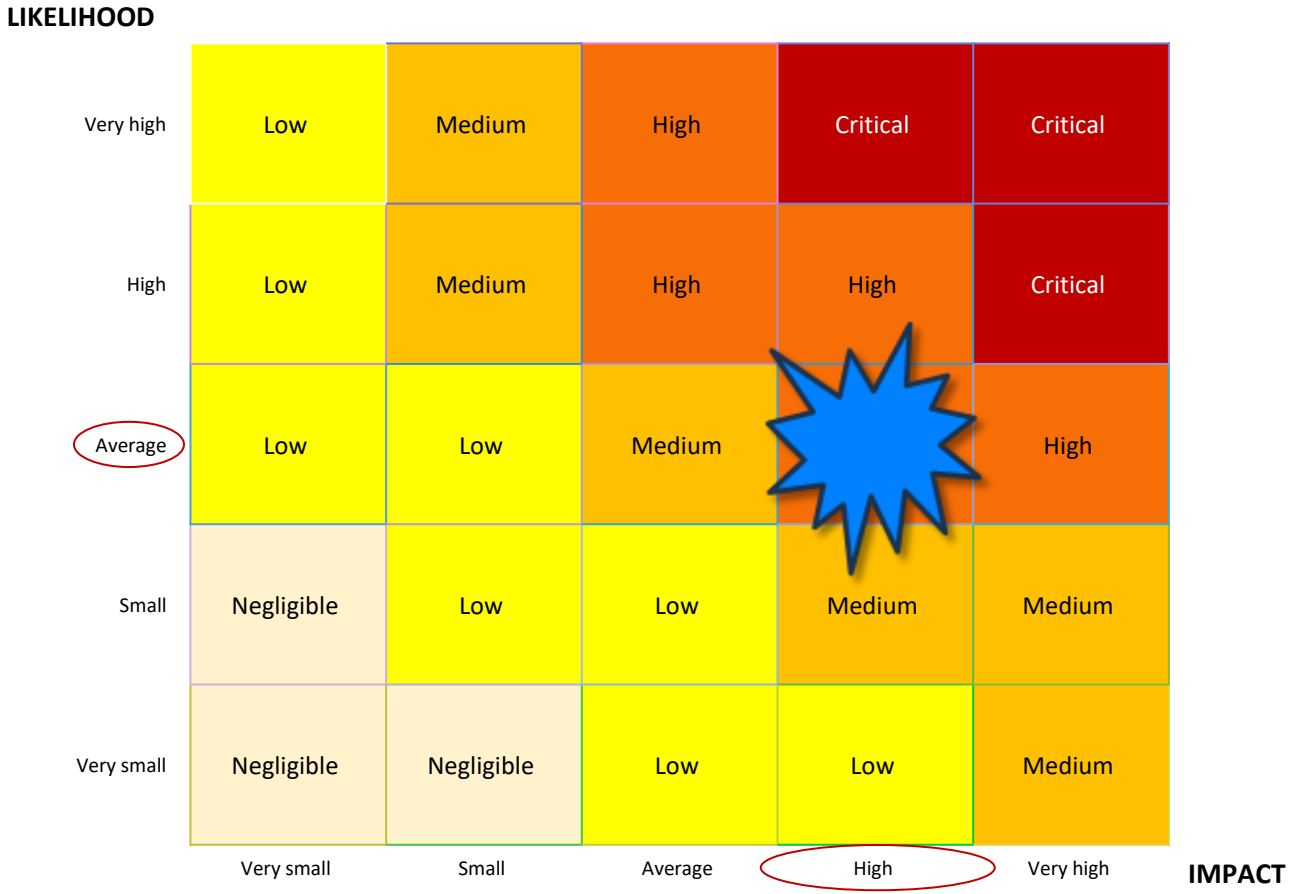
- Assess the likelihood
  - Average
    - The likelihood that a cyberattack leads to unplanned downtime, is estimated to be 'Small'.
    - The likelihood that a human error from the supplier that placed the Industrial Remote Access Gateway leads to unplanned downtime, is estimated to be 'Average'.
    - The estimated likelihood of the risk is therefor estimated to be 'Average'.

Spinae

CYBER SECURITY COALITION.be

Risk-based approach in practice

Example 1



Spinae

CYBER SECURITY COALITION.be

Regulatory requirements

Example 2

- *Assumption: you fall under NIS2 Important and follow CyberFundamentals*

PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

Remote maintenance shall only occur after prior approval, monitoring to avoid unauthorised access, and approval of the outcome of the maintenance activities as described in approved processes or procedures.

The organization shall make sure that strong authenticators, record keeping, and session termination for remote maintenance is implemented.

Allowing eWon or similar devices with 4G connection violates:
- Prior approval
- Monitoring
- Record keeping

Allowing eWon or similar devices with 4G connection could allow for the following requirements, but we do not have those under control, meaning this could be changed without us knowing:
- Strong authentication
- Session termination

It is not possible to meet the PR.MA-2 requirement of the (belgian) NIS2 legislation when eWon or similar devices with 4G connectivity are present

Unless specific additional compensating measures are carried out

Spinae

CYBER SECURITY COALITION.be

In summary

- What is risk?
- Create a common language, avoid speech confusion → Risk Management Policy
- Make it repeatable
- Use it in very practical situations
- Document your risk assessments
- Make sure decision makers will understand the risk: they must decide
- 2 examples
  - Centralized backups of PLC programs and settings
  - Industrial Remote Access Gateways with 4G connectivity

Spinae

CYBER SECURITY COALITION.be

Time for questions

Spinae
Cyber security in OT & IT

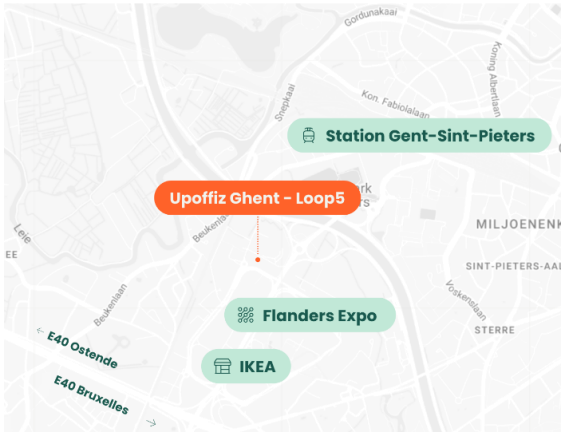
Stijn Boussemaere
Co-Founder
E: info@spinae.be – T: +32 9 396 35 35
https://spinae.be
https://www.linkedin.com/in/stijnboussemaere/

It's our mission to make the digital world a safer place

By empowering organisations to secure their critical assets, products and services

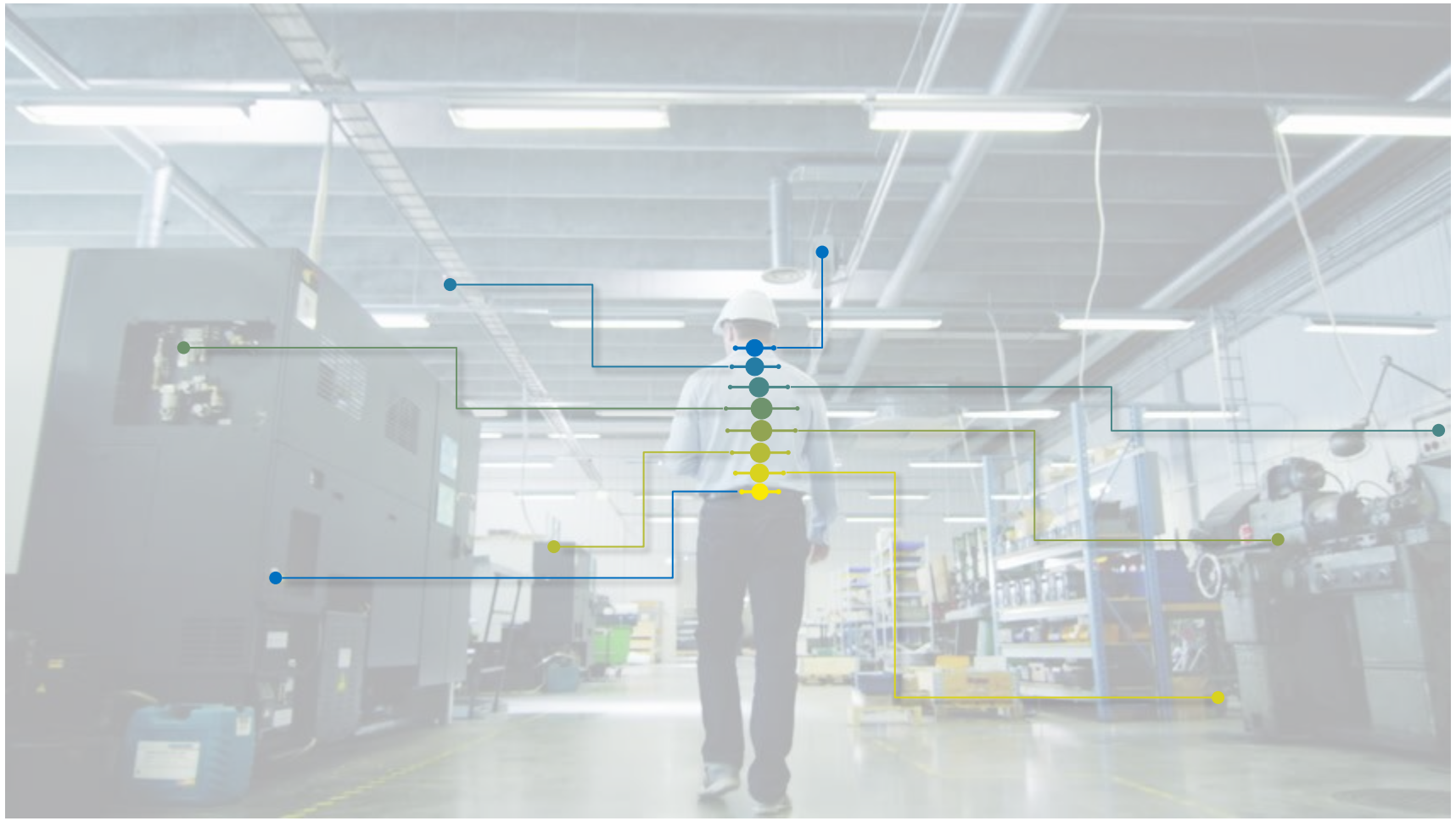
Key facts & figures

- °2019
- 100⁺ customers with DMU in Benelux
- Continual growth & improvements
- 14 co-workers
- Driven by focus, quality and integrity
- Sustainable relationships, mobility, offiz, ...



Cyber Security in OT & IT

We've got your back



Spinae

CYBER SECURITY COALITION.be