ETSI The Standards People

Security Conference

Beyond SBOM

Observability, Security Automation and Business Impact Analysis for Heterogenous, Programmable Infrastructures

Presented by: Piotr Zuraniewski (TNO, ETSI SAI delegate)

TNO innovation for life

ASOP THE AUTOMATED SECURITY OPERATIONS CONSORTIUM

17/10/2023

THE CHALLENGE

CYBERATTACKS:

CYBER SECURITY OPERATIONS:

THE ASOP PROJECT
Automatic Analysis & Response to Emerging Cyberthreats

- **Automated Security OPerations (ASOP)** is a Public Private Partnership
  - Multi-phased initiative lead by TNO
  - ASOP phase II (05'22 – 09'23) with commercial partners and support of Dutch government

- ASOP Architecture
  - Open
  - Interoperable & vendor-agnostic
  - Modular
  - Scalable

ASOP THE AUTOMATED SECURITY OPERATIONS CONSORTIUM

Partners

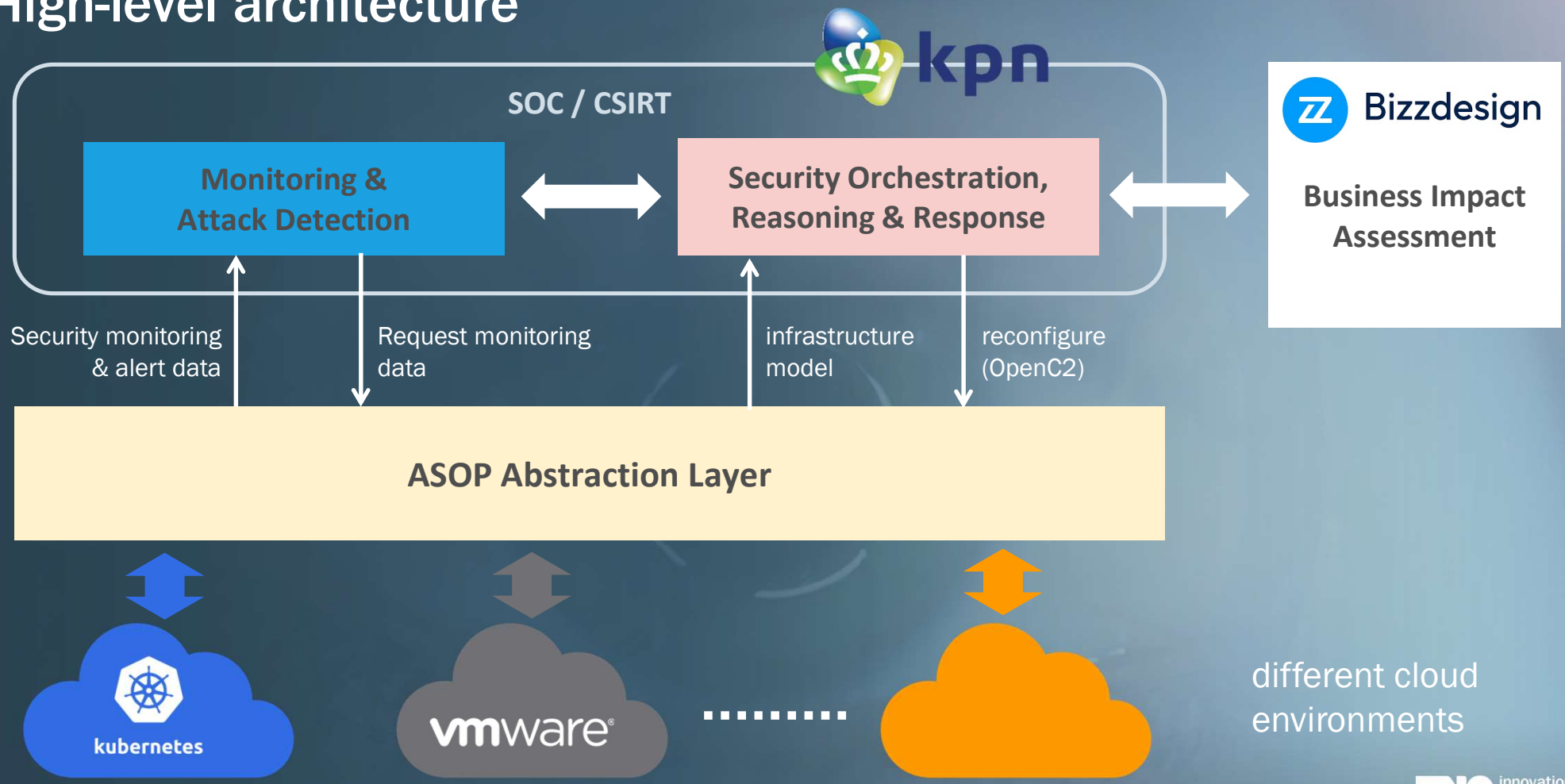
TNO innovation for life

Bizzdesign

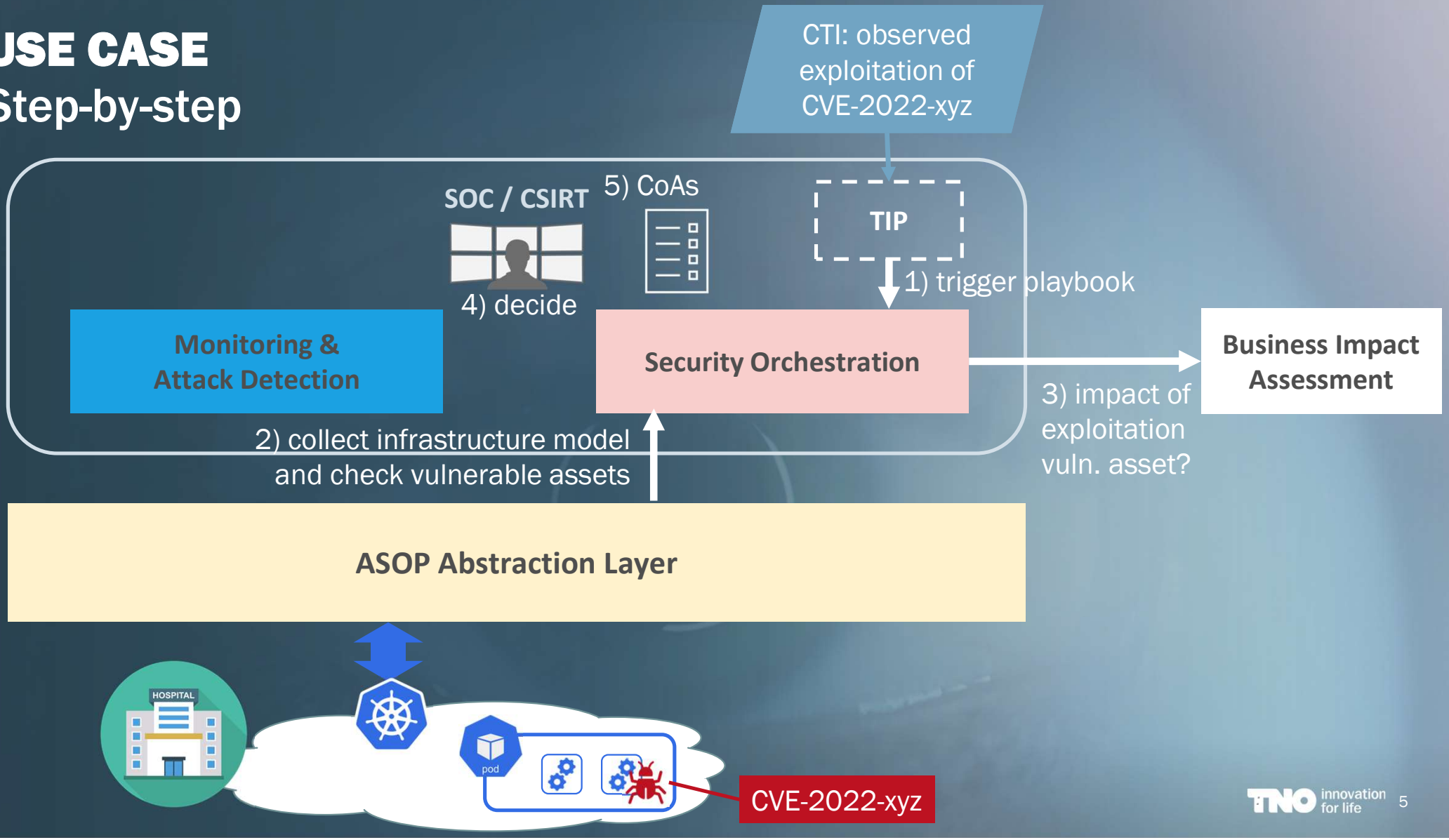
kpn

vmware

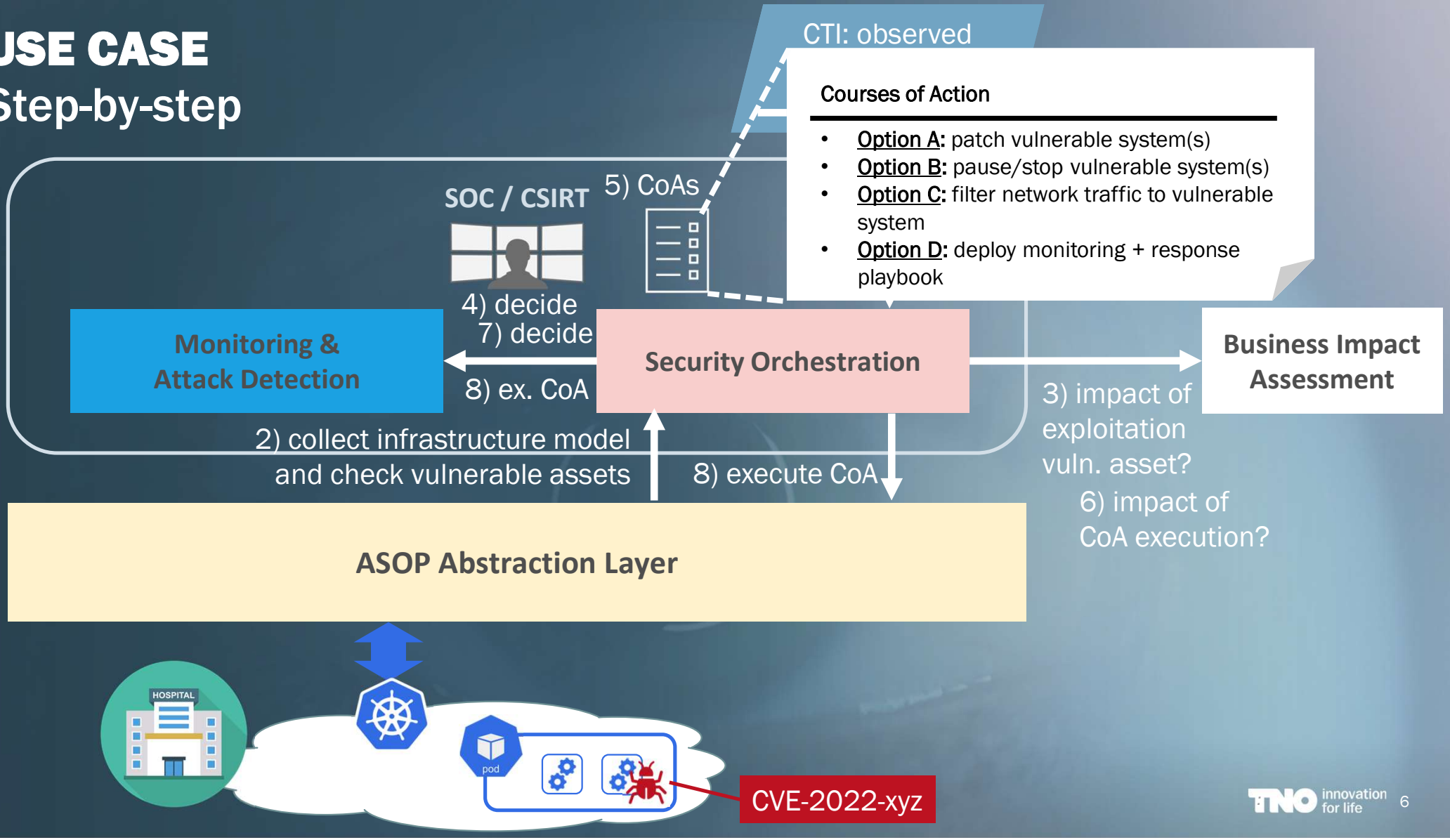
APPROACH
High-level architecture



USE CASE
Step-by-step



USE CASE
Step-by-step



ASOP
Main Innovations:

1. ASOP Abstraction Layer

focus of this presentation

2. Cloud agnostic Infrastructure Modelling — Innovation A
3. Dynamic Security Monitoring & Attack Detection capability
4. Security Orchestration
5. Dynamic Business Impact Assessment using enterprise architecture modelling — Innovation B

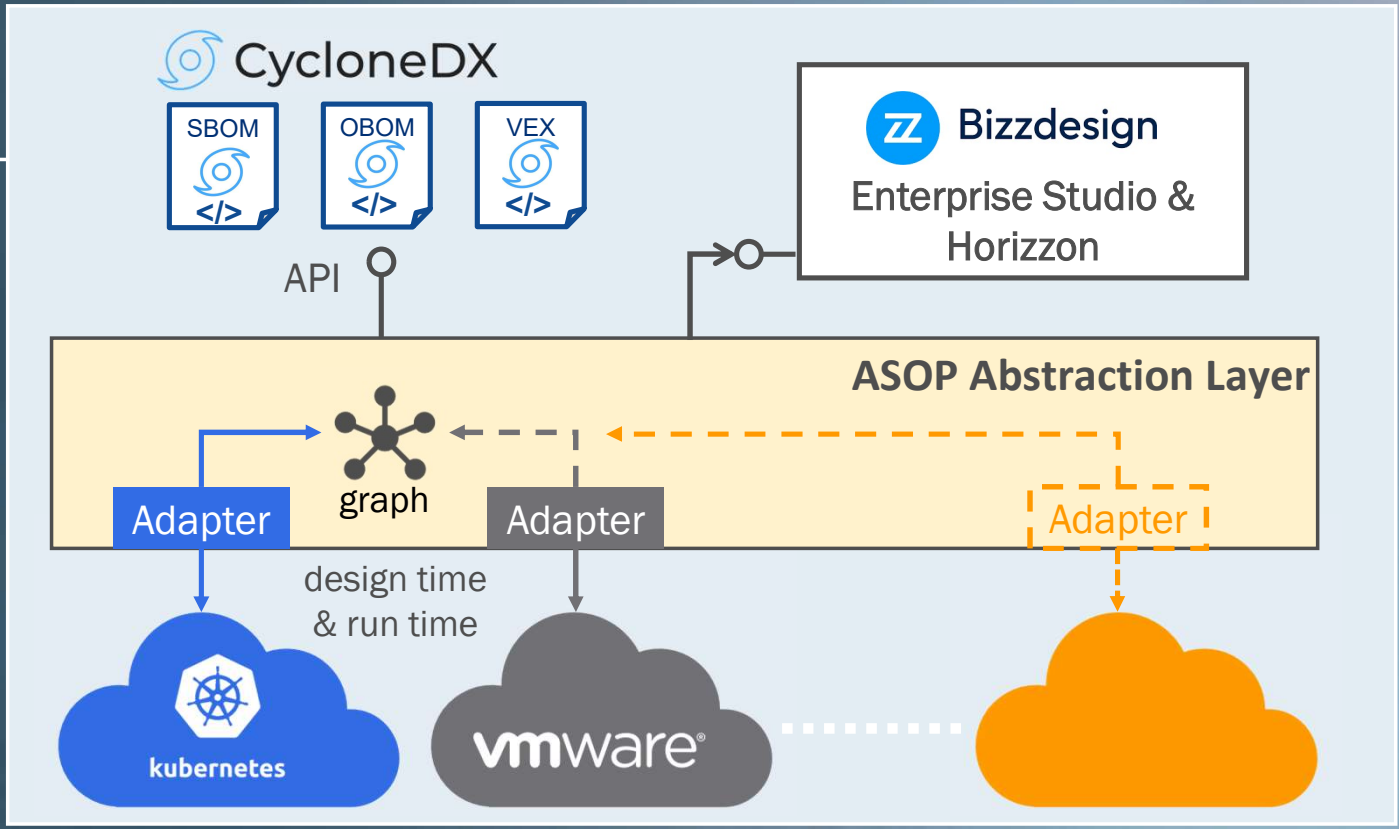
ASOP
Cloud Agnostic Infrastructure Modelling

1. What we need
2. What we did
3. What we learned

- Provide up-to-date accurate model of the infrastructure to security reasoning tools, e.g. business impact analysis module
- Machine readable model of the infrastructure, includes
  a) topology information (design time vs. run time, components that can be modelled – hardware, VM, containers),
  b) information on what software is running,
  c) information on what vulnerabilities are present,
  d) ability to express CoAs.
- Handle multiple (cloud based) data sources
- Standardised format

ASOP
Cloud Agnostic Infrastructure Modelling

1. What we need
2. What we did
3. What we learned



ASOP
Cloud Agnostic Infrastructure Modelling

OWASP CycloneDX is a full-stack Bill of Materials (BOM) standard that provides advanced supply chain capabilities for cyber risk reduction.

The specification supports:

- Software Bill of Materials (SBOM)
- Software-as-a-Service Bill of Materials (SaaSBOM)
- Hardware Bill of Materials (HBOM)
- Machine Learning Bill of Materials (ML-BOM)
- Manufacturing Bill of Materials (MBOM)
- Operations Bill of Materials (OBOM)
- Vulnerability Disclosure Reports (VDR)
- Vulnerability Exploitability eXchange (VEX)

Large support by vendors!

ASOP
Cloud Agnostic Infrastructure Modelling

1. What we need
2. What we did
3. What we learned

"beyond SBOM"

- It is possible to build and maintain Infrastructure Model, and make it available for security reasoning.
- Although, TNO focussed on K8s adapter, we plan to continue work with VMware to make the approach cloud agnostic.
- CycloneDX is promising as language to express and share cloud agnostic infrastructure models for security reasoning
  - needs to be **extended with** cloud service concepts (e.g. **services and relations between them**), and …
  - … with security concepts (e.g. actuators to link to OpenC2)
  - intermediate graph representation was needed

ASOP
Dynamic Business Impact Assessment

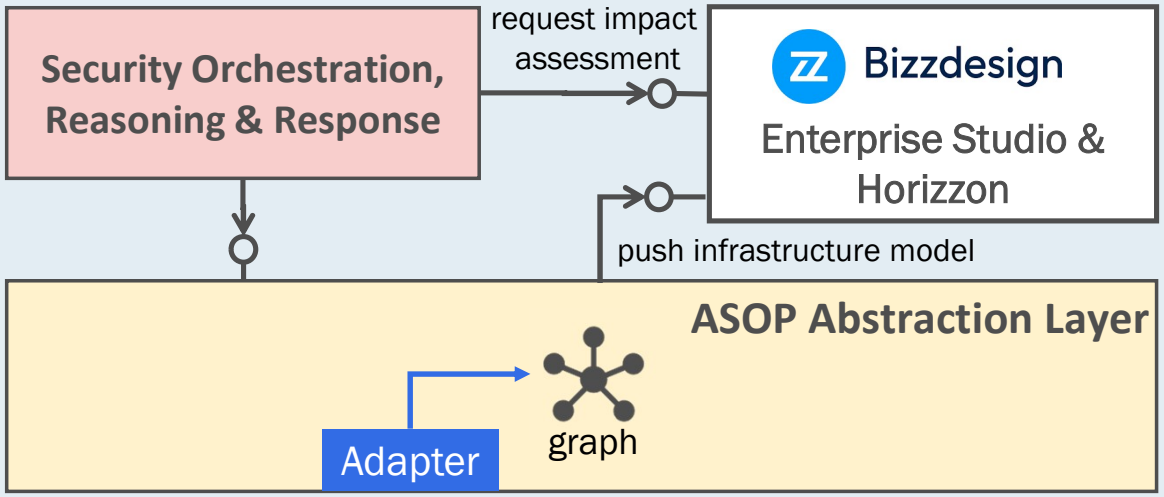
1. What we need
2. What we did
3. What we learned

- A service that provides current business impact information upon request for:
  - a compromised asset, and
  - a response action (e.g. filter traffic, isolate host)
- Open standard to represent information
  - Processing tools may be open or proprietary

ASOP
Dynamic Business Impact Assessment

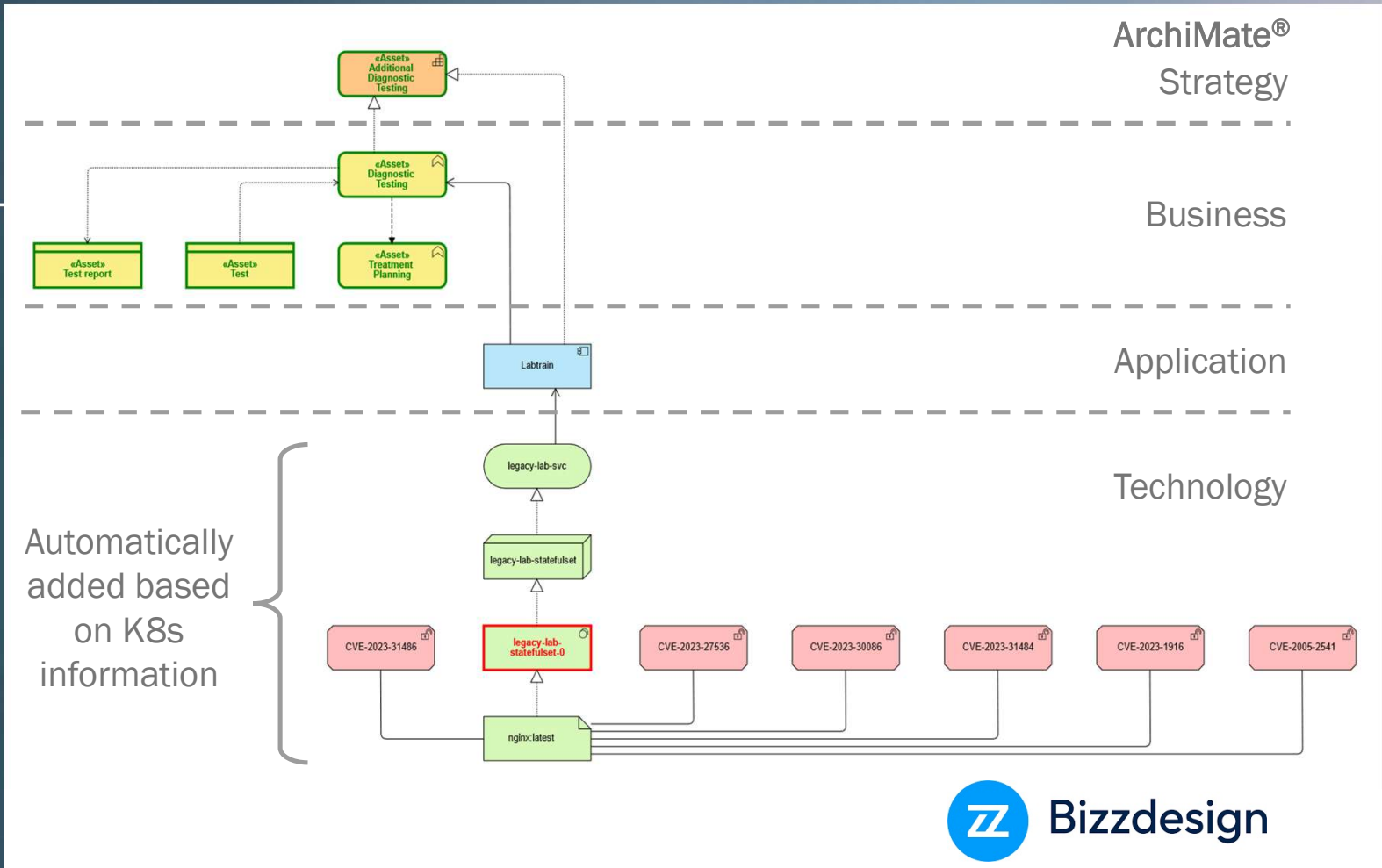
1. What we need
2. What we did
3. What we learned

- Adopted ZIRA v1.0 ArchiMate® model (The Open Group standard)
- Bizzdesign developed a method to calculate impact on business layer components due to compromise of CVE
- Provide API to request & collect business impact assessment



ASOP – Innovation B
Dynamic Business Impact Assessment

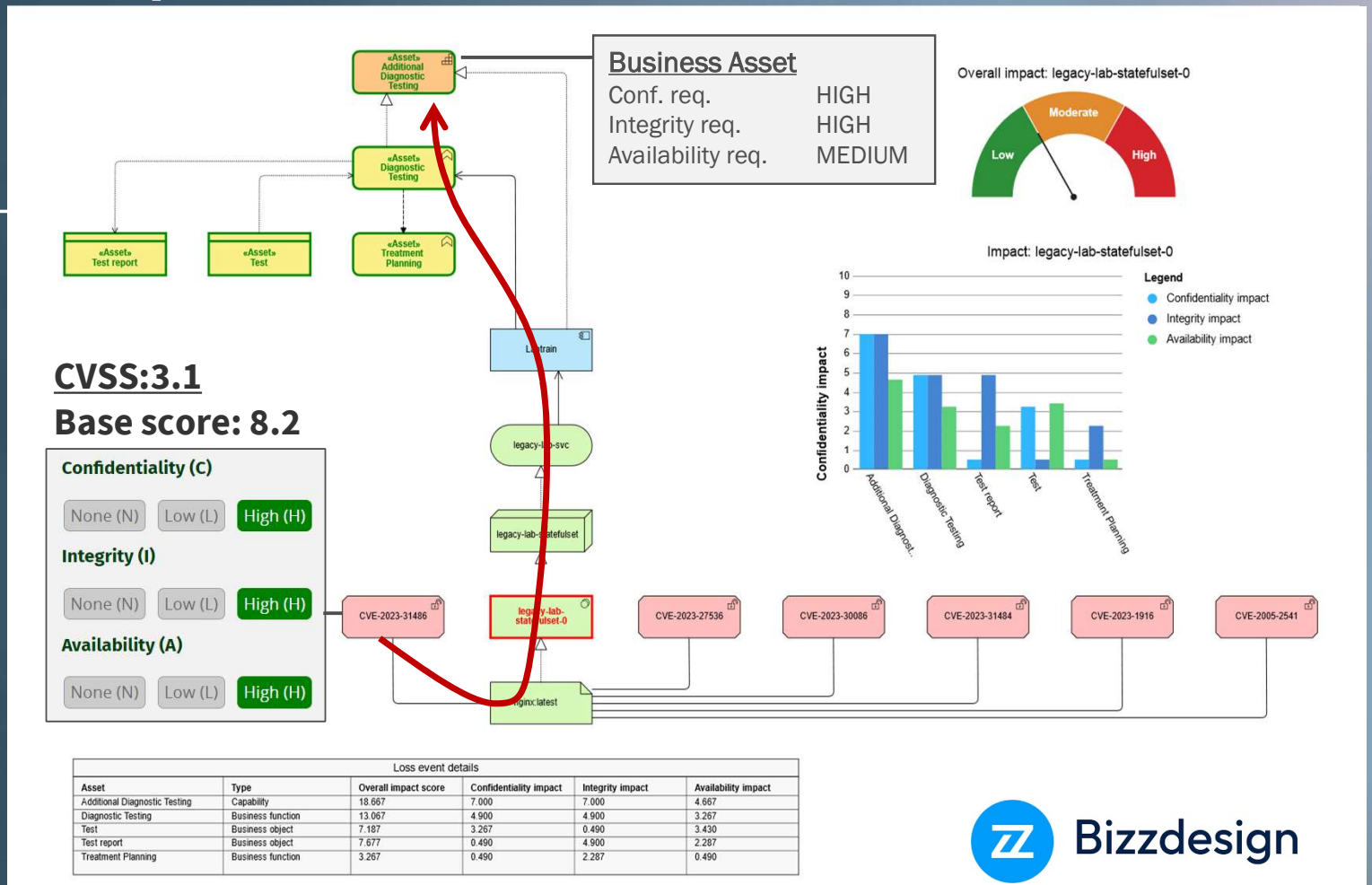
1. What we need
2. What we did
3. What we learned



Bizzdesign

ASOP
Dynamic Business Impact Assessment

1. What we need
2. What we did
3. What we learned



Loss event details

Asset	Type	Overall impact score	Confidentiality impact	Integrity impact	Availability impact
Additional Diagnostic Testing	Capability	18.667	7.000	7.000	4.667
Diagnostic Testing	Business function	13.067	4.900	4.900	3.267
Test	Business object	7.187	3.267	0.490	3.430
Test report	Business object	7.677	0.490	4.900	2.287
Treatment Planning	Business function	3.267	0.490	2.287	0.490

Bizzdesign

ASOP
Dynamic Business Impact Assessment

1. What we need
2. What we did
3. What we learned

- Impact assessment with ArchiMate® based Enterprise Architecture & Risk Management methodology by Bizzdesign is possible (note: different tools/methodologies are also allowed)
- Able to update infrastructure and link IT assets to application & business layer elements
- Requires ArchiMate® enterprise architecture models & assign business impact / security requirements.
- More research needed on dynamic business impact assessment
  - use current (temporal) business information
  - take interdependencies in to account
  - express impact on business/mission of a course of action

ASOP
Concluding Remarks and Next Steps

- Need for open, interoperable & vendor-agnostic, modular, scalable approach for security automation
- ASOP Phase III in preparation: towards operationalization with users
- Security reasoning on threat and attacks demand innovations like:
  - Support of various clouds
  - CoA execution: needs 100s plugins, use what is available + GenAI ?
  - Monitoring and detection (AI/ML and good old statistics)
  - Dynamic Real-Time Business Impact Assessment (even more AI…?)
- If employing AI, mind it may become target on its own (->ETSI SAI)

THANK YOU FOR ATTENTION

VISIT TNO BOOTH FOR LIVE DEMO!

TNO innovation for life

piotr.zuraniewski@tno.nl
frank.fransen@tno.nl
aditya.ganesh@tno.nl

TNO innovation for life

ASOP THE AUTOMATED SECURITY OPERATIONS CONSORTIUM

Partners

TNO innovation for life

Bizzdesign

kpn

vmware