INCIDENTRON.EU

LSEC - Wim Stoffelen
19.05.2026

ONE INCIDENT, ONE WORKFLOW

WHEN 1 INCIDENT TRIGGERS MULTIPLE OBLIGATIONS

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

INCIDENTRON

- European initiative focused on simplifying and improving cyber incident reporting, coordination, and cross-regulatory compliance under EU frameworks (NIS2, DORA, GDPR, CRA)
- Support for Implementation of EU legislaton on Cybersecurity and National Cybersecurity Strategies

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

WE ARE NOT:

- ☒ Another reporting portal
- ☒ Another SEP – Single Entry Point
- ☒ Another layer of complexity

'We're not another destination. We help navigate the journey.'

WE ARE:

- ☑ Decision-making intelligence
- ☑ Workflow orchestration
- ☑ Operational guidance

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

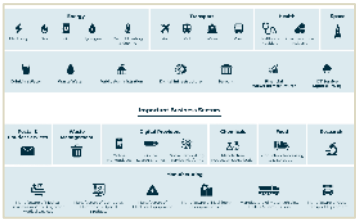
This project is financed by Co-funded by the European Union ECCC


SUCCESS
What authorities see here
WORK
What entities do here
INCIDENT
Report (-s)
Timeline & content
Routing
Treshold
Scope
PER EACH FRAMEWORK
INCIDENTRON.EU

MAIN STAKEHOLDERS

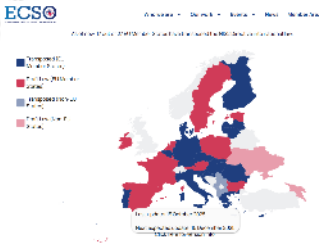
End users

Cut complexity. Stay compliant. Focus on response & recovery, cover compliance



EU & Member States

Better insights. Better coordination. A stronger Europe



Authorities, CSIRTs

Better collaboration. Cleaner reports. Faster insights. Less burden

Competent Authority

NATIONAL CSIRT

Sectoral CSIRTs

Cyber Industry

Turn complexity into Business. Offer compliance assurance, build new products

Cybersecurity and compliance solution/service providers

MSSP

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

The Partners

INCIDENTRON, the partnership : Who's Who?

NRD Cyber Security	itml innovation applied	S2 GRUPO	CDEX
incibe_	circl	TIMELEX	LSEC
ECSO EUROPEAN CYBER SECURITY ORGANISATION	Nocode-X	VUB ARTIFICIAL INTELLIGENCE RESEARCH GROUP	

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

How did we get here?

Inside the Storm: What Entities Are Really Facing

They want to know....

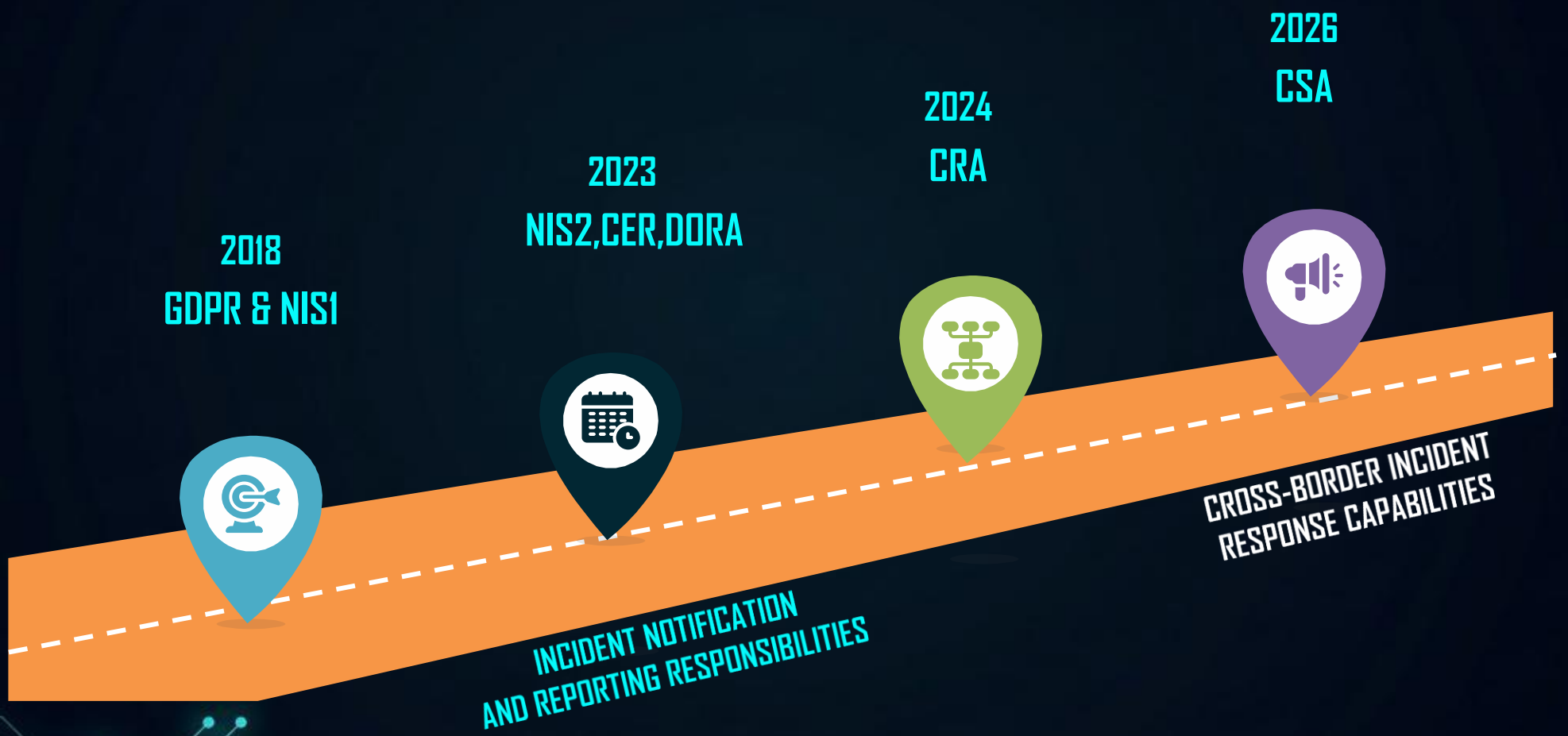
"It took us 6 months together with advisory from one of the Big 4 to determine if we even were an essential entity under NIS2 " - CISO (anonymous)

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

EU Regulations <-> Incidents



INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

THEY ALL MAKE SENSE...IN ISOLATION

	SCOPE	EXAMPLE TRESHOLD	ROUTING
NIS2 — CYBER	• Severe disruption • Financial loss • Damage to other natural or legal persons	Complete outage >30 min, or avg DNS response time >10 sec for >1 hour.	National CSIRT, SECTORAL CSIRT, Competent Authority
GDPR — PRIVACY	• Data breach • Risk to rights/freedoms of individuals	Information critical for personal safety or physical/psychological conditions = DPC + 3	DPA
DORA — DIGITAL RESILIENCE	• ICT-related incident affecting financial services	Affected transactions >10 % of daily average number of transactions carried out	NCA

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

WHERE IT GETS COMPLICATED

More then just 'NIS2' Entity

1. Essential Entity (NIS2)
2. Critical Entity (CER)
3. Medical Device User / Operator (MDR)
4. IVD Operator / Diagnostic Provider (IVDR)
5. Data Controller (GDPR)
6. National Health Sector Regulated Entity (national health & safety law)
7. Potential Victim of Cybercrime (criminal reporting under national law)
8. User of Products with Digital Elements (voluntary disclosure under CRA)

They want to know....

1. **What framework** (-s) apply to my incident?
2. **When** must I report? (threshold)
3. **When** must I report? (deadlines)
4. **Where** must I report? (member states)
5. **Who** should I report to? (authorities)
6. **What** should be in the report (s!)?
7. **How** do I submit the report?

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

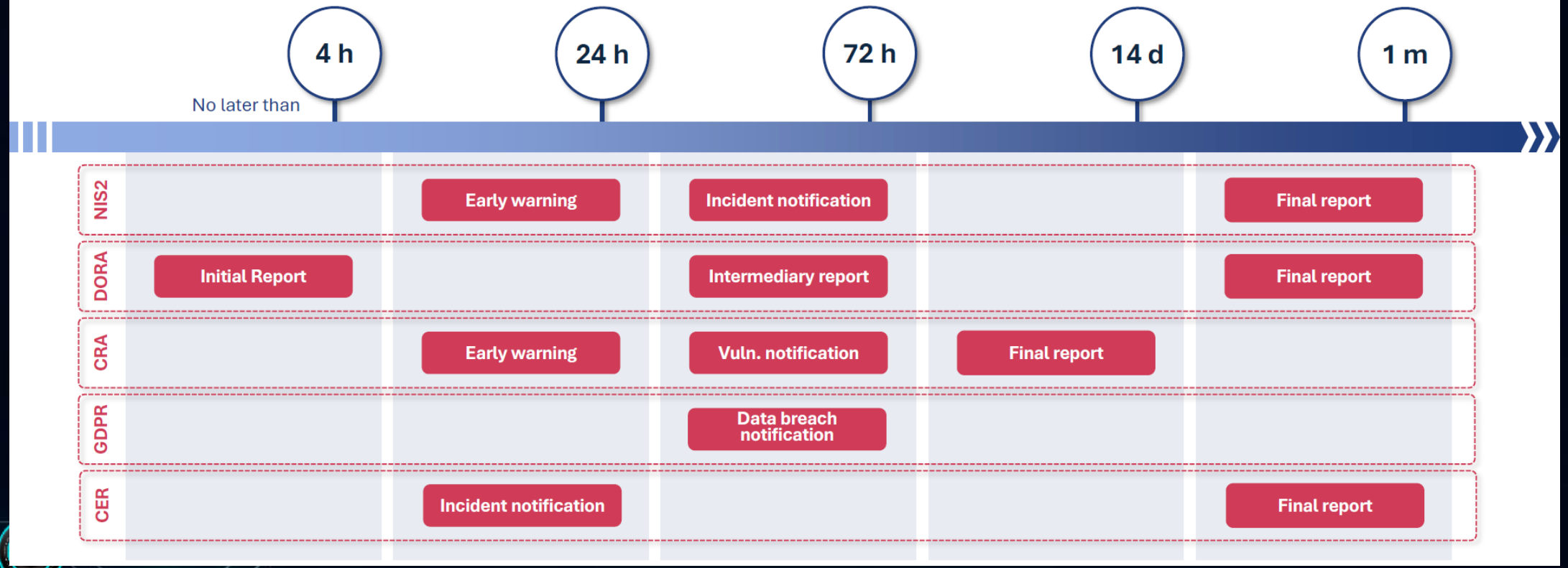
This project is financed by Co-funded by the European Union ECCC

THEN

Incident Reporting Complexities

When to Report

Illustrative



INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

ON TOP OF THAT

One incident.
Multiple legal clocks

FROM?:

- 'Becoming aware'
- 'Reasonable certainty of significant incident'
- 'Classification as major ICT incident...unless ;)'

FINAL REPORT?:

- 'One month from the date and time of awareness'
- 'One month from submission of the intermediate report
- 'Does not require an official final report'

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

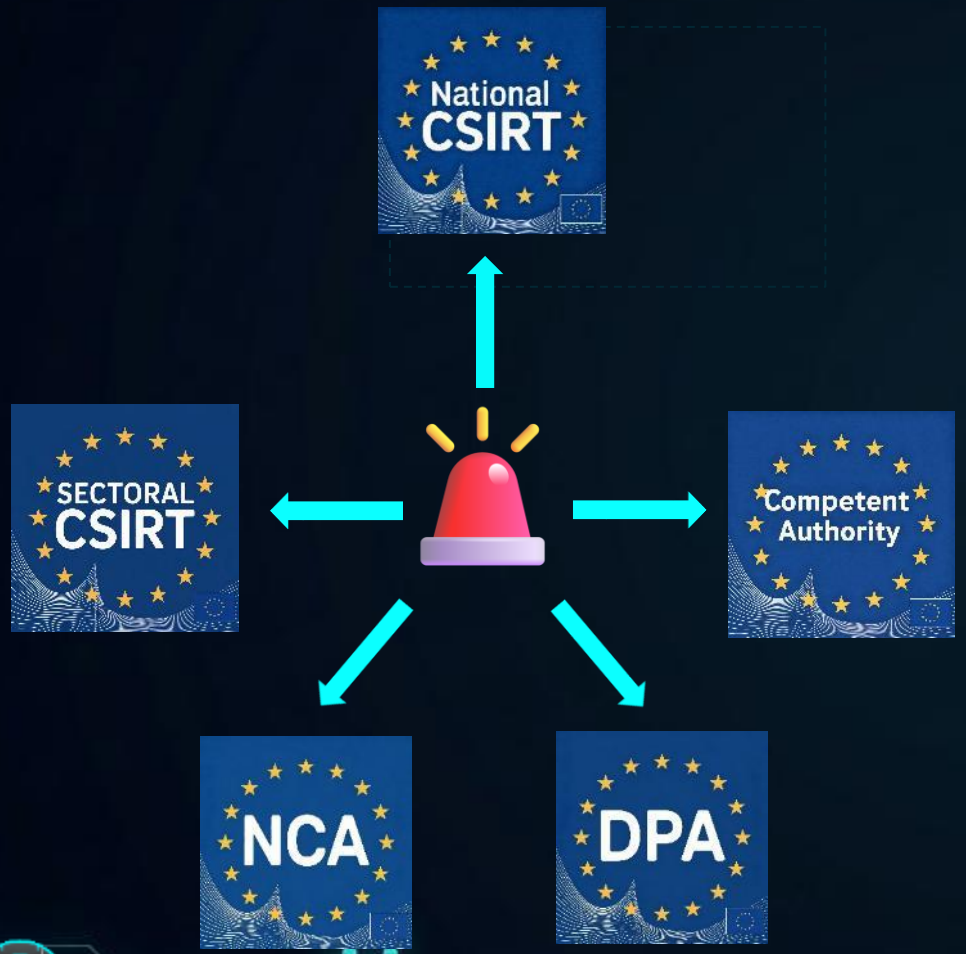
HAPPY WEEKEND! -> for some <TIME STAMPING 101>

Exception applies.... but not for all

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

THE ROUTING CHALLENGE



Routing complexity

- Which framework?
- What authority?
- What member state?
- Parallel reporting?

Diverging expectations

- Different reporting content
- Different thresholds
- Different formats

Technical fragmentation

- Portals
- Emails
- Templates
- National systems

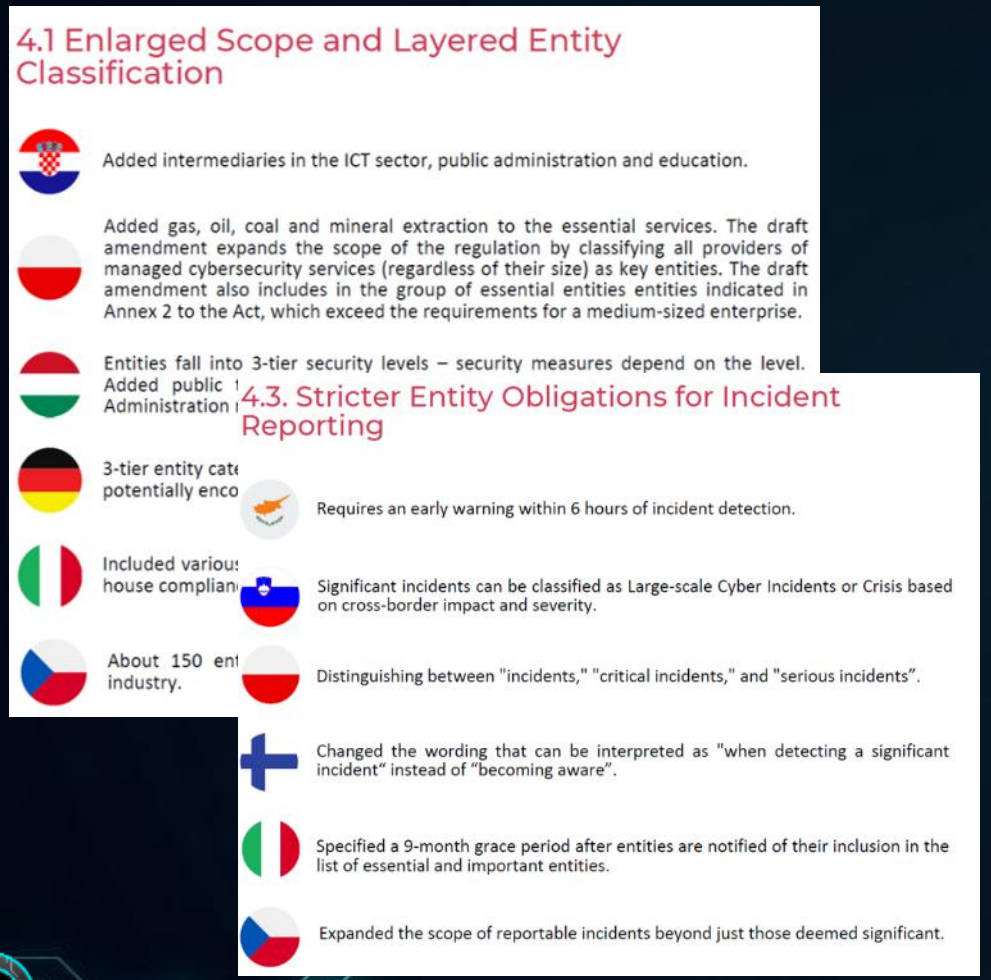
"Organizations do not report to 'Europe'. They report into fragmented operational ecosystems."

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE ECCC

NATIONAL TRANSPOSITIONS



Reporting triggers

- "Becoming aware"
- "Detection"
- National variations

Entity scope

- Additional sectors
- Categorisation models
- National expansions

Incident classification

- Significant
- Serious
- Critical
- Large-scale

"Harmonized legislation does not guarantee harmonized operations."

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE ECCC

TODAYS REALITY

One Incident

Frameworks

- NIS2
- DORA
- GDPR
- CRA
- .....

Authorities

- CSIRTs
- Sectoral
- DPAs
- National bodies
- Cross border

Operational differences

- Different timelines
- Different formats
- Different languages
- Different definitions

Cross border complexity

- Different Member States
- Different transpositions
- Different obligations

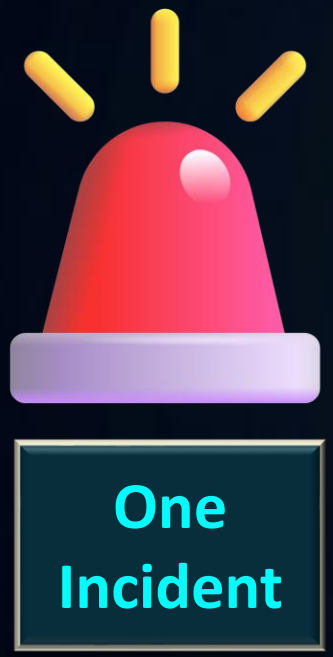
"The same operational event becomes multiple disconnected reporting processes."

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

ONE INCIDENT, ONE WORKFLOW



Today:

- Administrative burden
- Cross-border uncertainty
- Parallel reporting
- Operational distraction

Tomorrow?:

- Incident reporting = incident: A single operational event
- Organizations focus on response, cover compliance
- Authorities receive consistent information

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

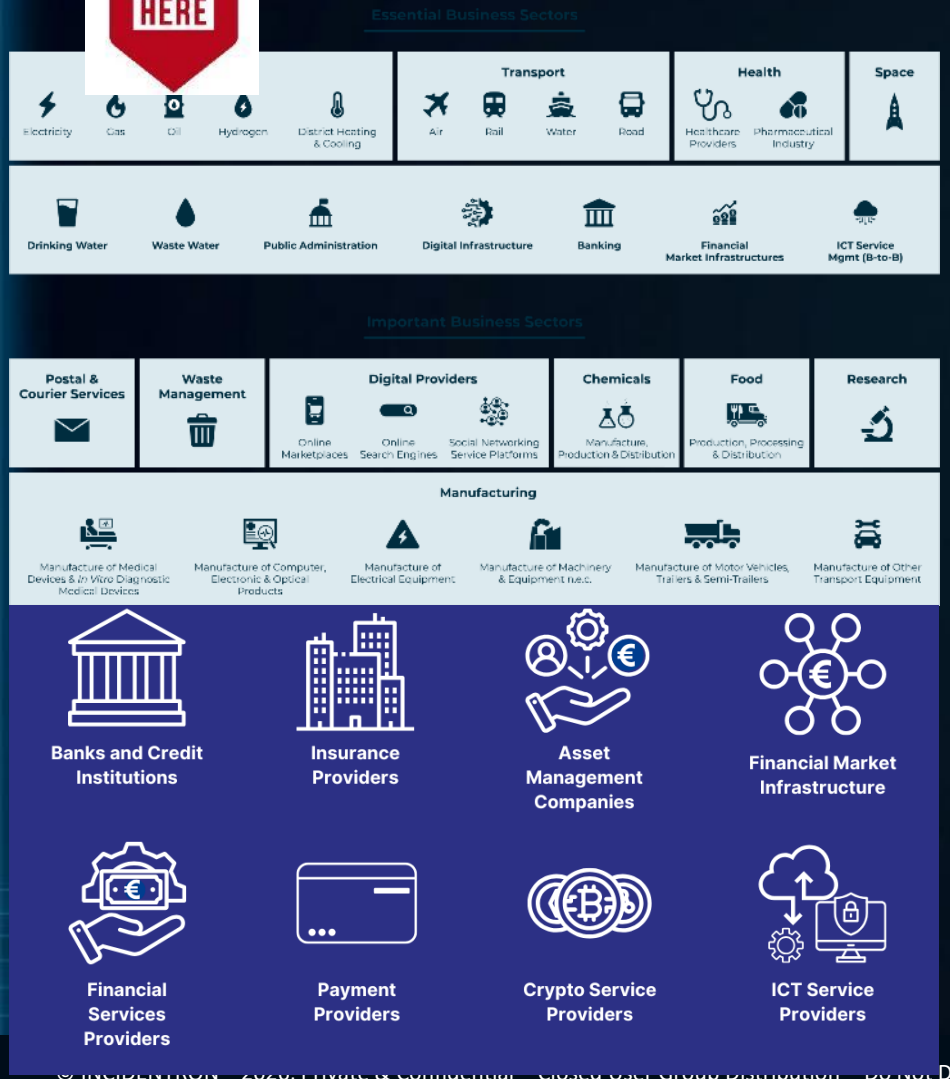
This project is financed by

Co-funded by the European Union

ECCC

THE MINDSHIFT: DON'T START FROM THE FRAMEWORK

START HERE



THEN HERE

Must be reported under..?

NIS2 CER DORA GDPR

Caused by PDE?

CRA

Other 'obligations'?

PSD2 EU-MDR 2020/561 EU-IVDR

National CSIRT

SECTORAL CSIRT

Competent Authority

enisa

Data Subjects

SCOPE TO MANAGE, DESIGN TO SCALE

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by

THE GOOD NEWS

Legal fragmentation

- ✕ Different frameworks
- ✕ Different authorities
- ✕ Different legal language
- ✕ Different implementations

Similar logic

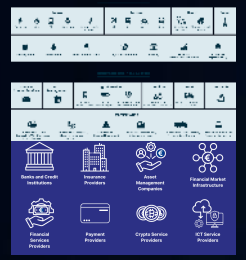
- framework and scope mapping;
- threshold assessment;
- authority routing;
- phased reporting and timeline management;
- mandatory reporting content and evidence.

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

INCIDENTRON IN 1 PICTURE



NIS2 CER DORA GDPR

Entity onboarding → **Connection & Ingestion** → **Taxonomy engine** → **Assessment and Decision Engine** → **Review Report** → **Orchestration & Reporting**

- Entity intake
- Incident awareness
- Incident qualification
- Threshold & severity assessment
- Authority & Channel determination
- Notification phases & timelines
- Mandatory content & evidence
- Submission, follow-up & supervision

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

INCIDENTRON

Streamlined Multi-Framework Reporting

NIS2, DORA, GDPR, CRA and future frameworks
Reduced fragmentation and administrative burden

1

CRA & Responsible Disclosure

Supplier coordination
PDE responsible disclosure
Market surveillance support

2

INCIDENTRON FOUDATION

Opensource framework, architecture, platform

INCIDENTRON.EU

Preparedness & Collaboration

Threat intelligence
Lessons learned
Cyber ranges & exercises
LEA collaboration

3

Open European Ecosystem

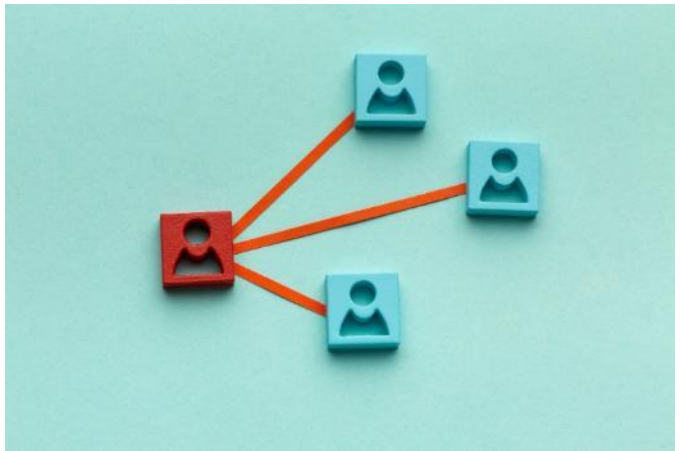
Open-source framework
Developer ecosystem
Reusable taxonomy & components

4

THE RESULTS

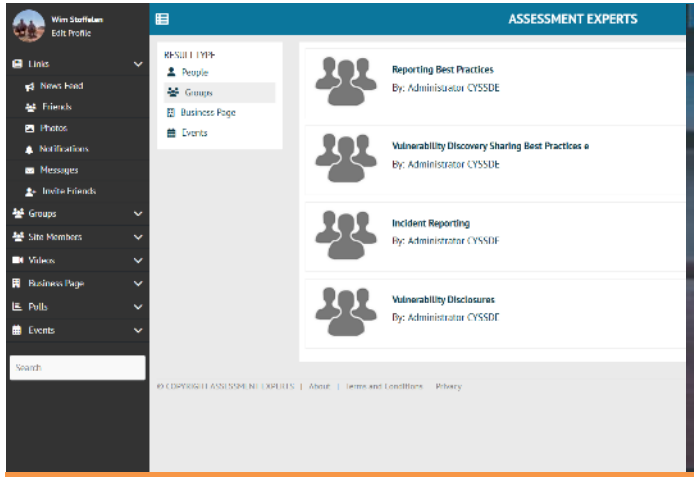
1 decision making model for multi-regulatory, cross-border incident reporting

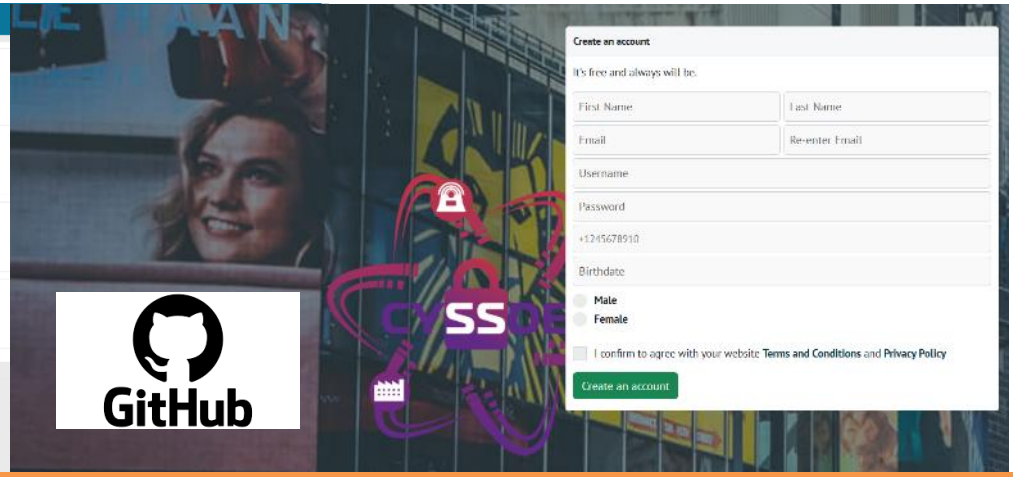
1 opensource framework and architecture



10 pilot use cases: Tested on an end-to-end platform with end users, MSSPs, CSIRTs

40 white papers, research, decision trees, etc.





Opensource INCIDENTRON community enabling collaboration between developers, MSSPs, end users, authorities and policy actors to support adoption, innovation and long-term sustainability of the framework.

5 Cyber Range excercises driven by real life scenarios

BASELINE REQUIREMENTS TO MAKE THIS WORK

- Correct translation of law into workflows
- Scalable, adaptable to changes
- Clear operational & business value
- Seamless integration, automation-ready
- Aligned with authority expectations

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

1. LEGAL ANALYSIS THAT STICKS, SCALES & ADAPTS

- **Entity- & incident-centric**
  Start from the incident and affected entity, not from isolated frameworks
- **Common operational logic**
- **EU Baseline + national overlays**
  Reusable EU core with Member State, sectoral and authority-specific deviations
- **Granular threshold model**
  Uses the most operationally mature criteria (e.g. NIS2 IR 2024/2690) as scalable superset logic

✓ Reusable across different Member States, sectors & frameworks)

✓ Capable of evolving ("moving target" mitigation)

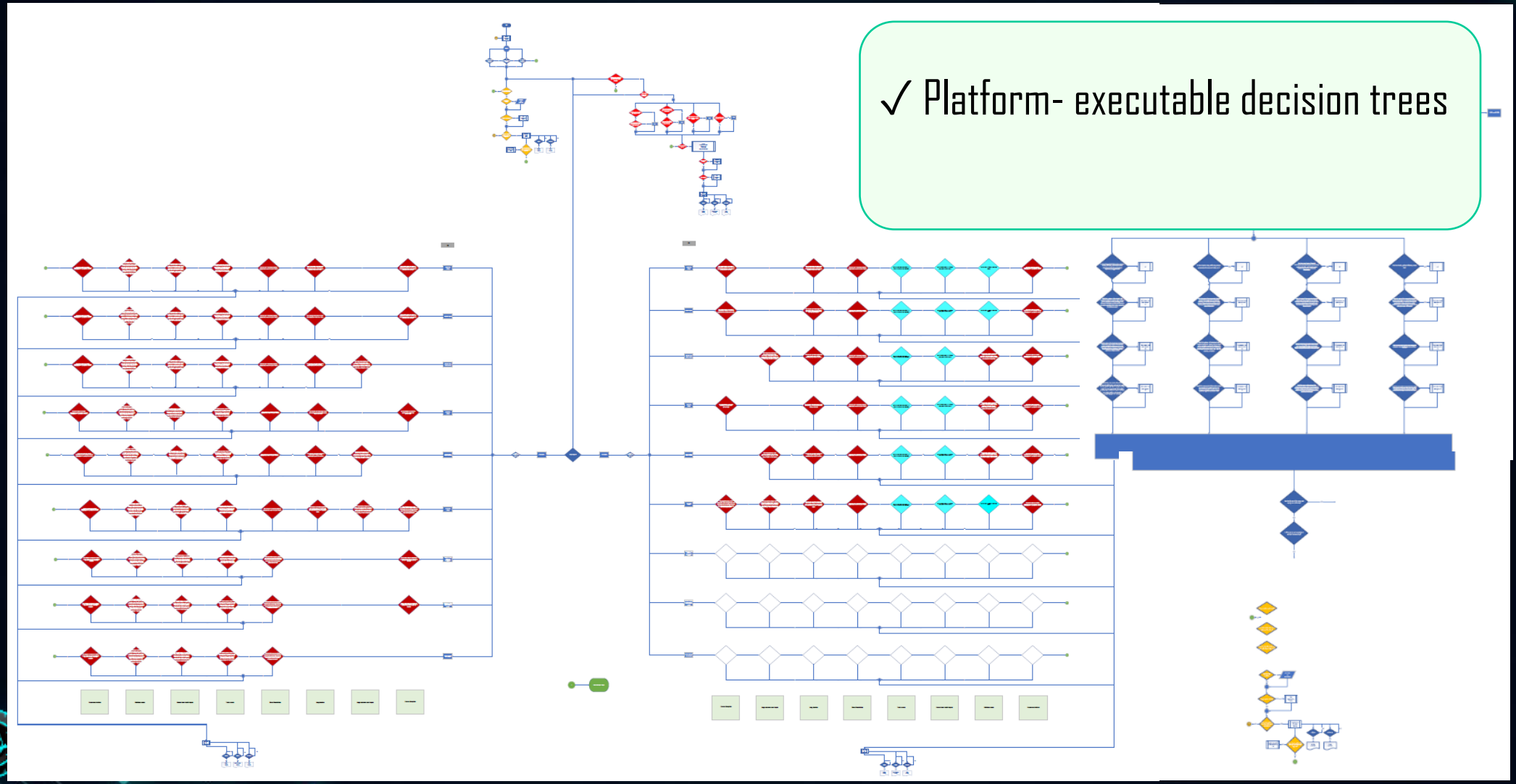
✓ Scalable beyond mandatory reporting obligations

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

2. FROM LEGAL ANALYSIS TO DECISION LOGIC



INCIDENTRON.EU

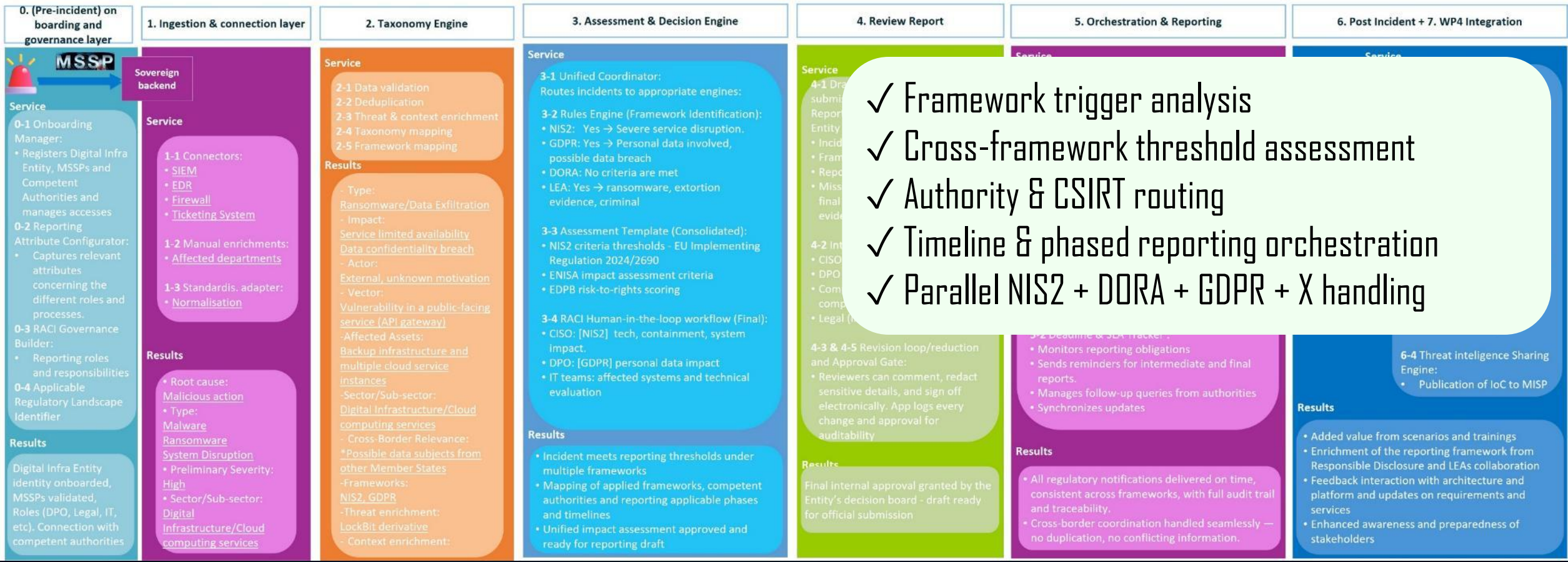
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by

Co-funded by the European Union

ECCC

3. FROM DECISION LOGIC TO DECISION ENGINE



- ✓ Framework trigger analysis
- ✓ Cross-framework threshold assessment
- ✓ Authority & CSIRT routing
- ✓ Timeline & phased reporting orchestration
- ✓ Parallel NIS2 + DORA + GDPR + X handling

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

4. VALIDATED THROUGH SCENARIOS

Provisional

INCIDENTRON – Digital Infrastructure scenario validation (BE)	
Reference scenario	D2.1 §11.1.4 – Belgian cloud computing services provider – ransomware (multi-stage)
Validation scope	Digital Infrastructure (NIS2, Annex I) – Country scope: Belgium; cross-cuts to NIS2 generic, GDPR, DORA where relevant
Author	ECSO – INCIDENTRON
Attack chain	Exploitation of an exposed API gateway vulnerability → IAM abuse → Lateral spread → Exfiltration → Backup ransomware
Impact (assumed)	Limited availability for ~6% of EU users for ~1.5 hours; 15,000 GDPR data subjects affected; suspected malicious unauthorised access confirmed; data integrity/confidentiality compromised
Hard triggers met	EU 2024/2690 Art. 7 (cloud): >5% EU users + >1h limited availability; malicious unauthorised access; data compromise. GDPR Art. 33 personal data breach. NIS2 Art. 23 significance criteria met.
Triggered frameworks	NIS2 + EU Implementing Reg. 2024/2690; Belgian NIS2 Law + CCB Royal Decree; GDPR (ENISA severity); (DORA only relevant if organization is also financial-entity - out of scope here).

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

5. CO-CREATED WITH STAKEHOLDERS (M1-M6)

- 11 events, 635 stakeholders
- Presentation @ Joint TF-CSIRT & FIRST Regional Symposium Europe (159)
- Launch event in Brussels (60)
- 2 closed CISO workshops (30)
- NCC, CSIRT, Authority closed workshop (43)
- INCIDENTRON - MISP Training (CIRCL)
- NISDUC: 2x workshops

INCIDENTRON KEY MILSTONES

- **08/2026: Opensource taxonomy published**
- 10/2026: Core Framework Prototype
- **11/2026: Start of integration and pilots**
- **11/2026: Public repository launched**
- 06/2027: Minimum Viable Product (MVP) Release
- 08/2028: Pilot integration report

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

JOIN US @NISDUC TODAY/ TOMORROW:

Register at the reception desk

Breakout session C - Day 1

13:30	15:00	**INCIDENTRON workshop aimed at authorities and CSIRTs**

Breakout session C - Day 2

13:00	15:00	**INCIDENTRON workshop aimed at NIS2-subjected entities**

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC

NOT THE END

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

More information, slides and follow-up

www.incidentron.eu

www.lsec.eu

project@incidentron.eu
Wim Stoffelen
wim@incidentron.eu
+32 622 04 0562

INCIDENTRON.EU

This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101249201.

This project is financed by Co-funded by the European Union ECCC