Kurt Callewaert
Business Line Director Cyber Security

capyx

Always bright,
better and beyond.

15 jaar CS

The Hackers are ready, are you ?

13 Mei 2025 Ronse


BL IT Modernization
BL AI & Cybersecurity
85 consultants
capyx
"Always bright, better and beyond"
Empower your business with seamless IT Modernization, fortify your future with cutting-edge Cybersecurity, and unlock potential with AI and Data-driven insights. Transform, protect, and innovate with our expertise. We're not just upgrading tech— we're revolutionizing possibilities.
www.capyx.be

capyx

capyx lux

Business Line AI & CS
Director : **Kurt Callewaert**

Project

NIS2
DORA
CRA
AI ACT
Cyber Resilience 360°

GenAI - LLM
Machine Learning

Research

People

CS GRC
CS Red Team
CS Bleu Team

Data Scientist
AI Engineer

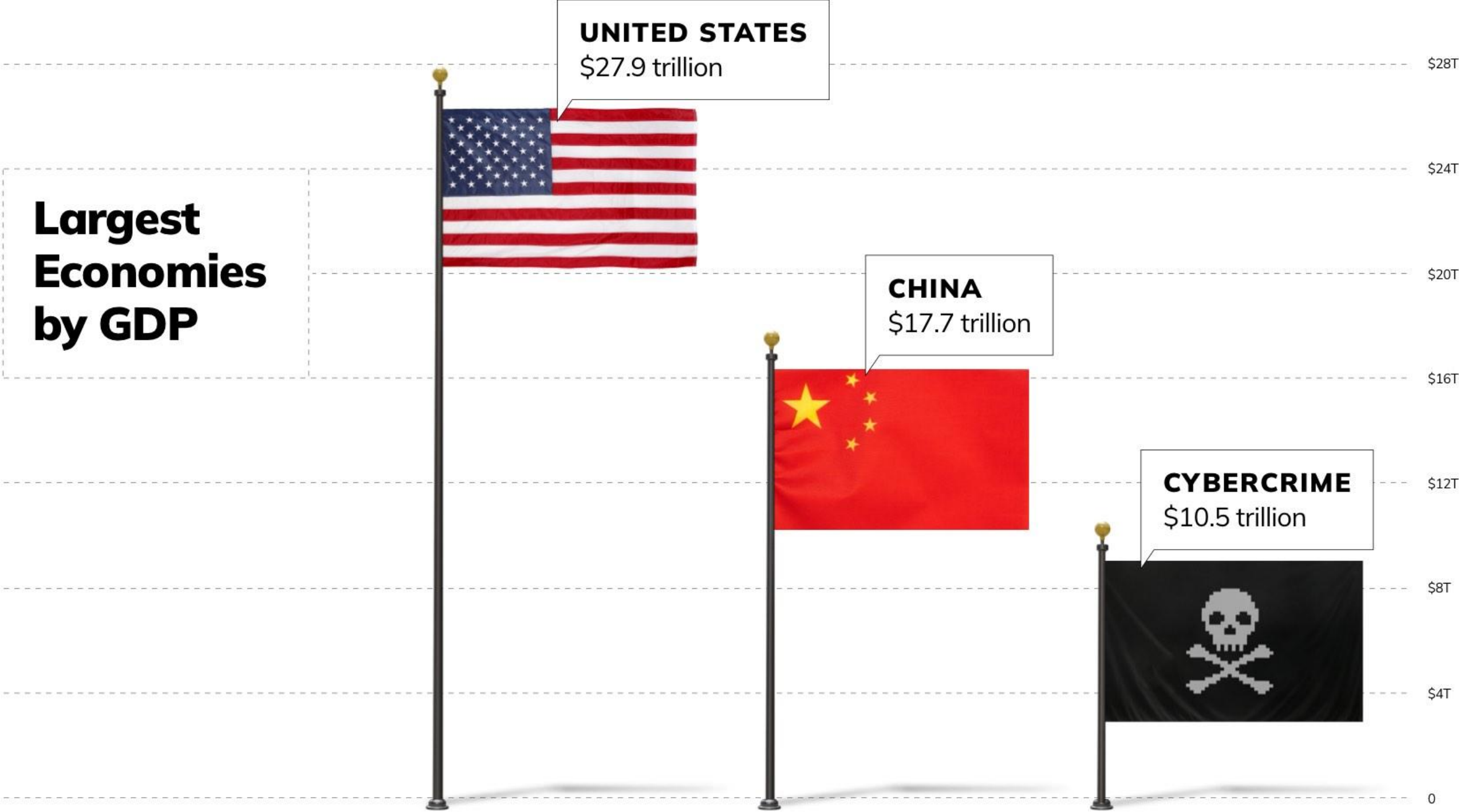
Product + MSSP

MSP SBOM Studio
MSP SBOM Consumer
MSP AIKIDO SEC
MSP TENABLE
MSP ESET
Secure DNS
Darkweb Monitoring
Ethical Phishing

Locations : Brussels – Ghent – Luxembourg

Always bright, better and beyond.

Largest Economies by GDP



Resultaten 2024

Dit zijn de belangrijkste inzichten uit de CS-barometer 2024.

•Maar liefst **1 op 2 van de Vlaamse ondernemingen (45,8%)** waren het voorbije jaar (2024) slachtoffer van een cyberaanval.

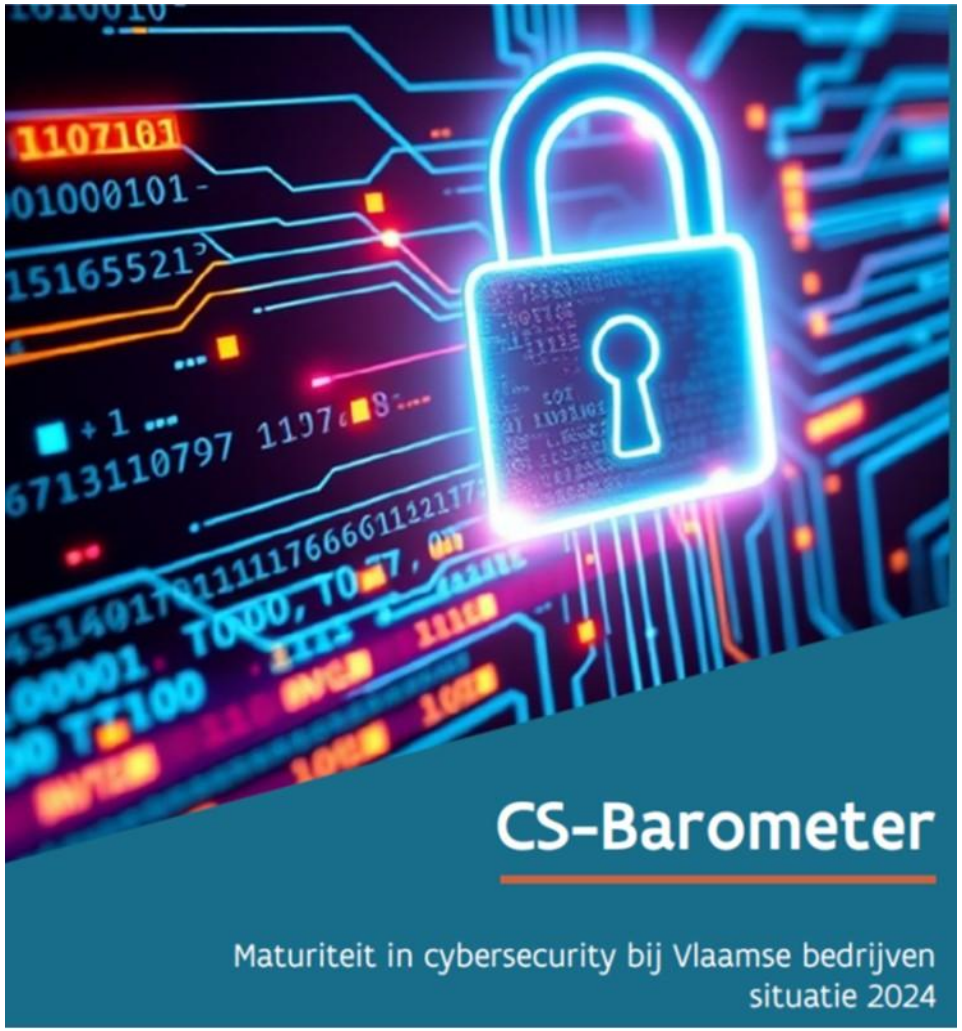
•Van alle cyberaanvallen zijn **1 op 10 ook effectief 'succesvol**', en berokkenden zo schade aan het bedrijf.

•Bijna de helft van de respondenten **(42,8%)** zegt dat onvoldoende opleiding en bewustmaking bij het personeel het grootste cyberrisico vormt.

•Hoewel een ruime **meerderheid van de bedrijven (71%)** denkt goed beschermd te zijn tegen cyberaanvallen, blijkt vooral bij kmo's dat procedures en maatregelen vaak ontoereikend zijn.

•Positief is wel dat steeds meer ondernemingen actie ondernemen en hun IT-budget voor de bestrijding van cyberaanvallen zien groeien. **(22% van totale IT-budget**). De helft van de bedrijven gaf evenveel uit aan CS als in 2023, de helft meer dan in 2023.

•We zien een toename in het nut of prioriteit toegekend aan een effectief CS-beleid, er wordt **meer druk uitgeoefend door klanten** om cyberveiligheid te garanderen (1 op 4), en er worden vaker **externe gespecialiseerde CS-dienstverleners** ingeschakeld (1 op 3).

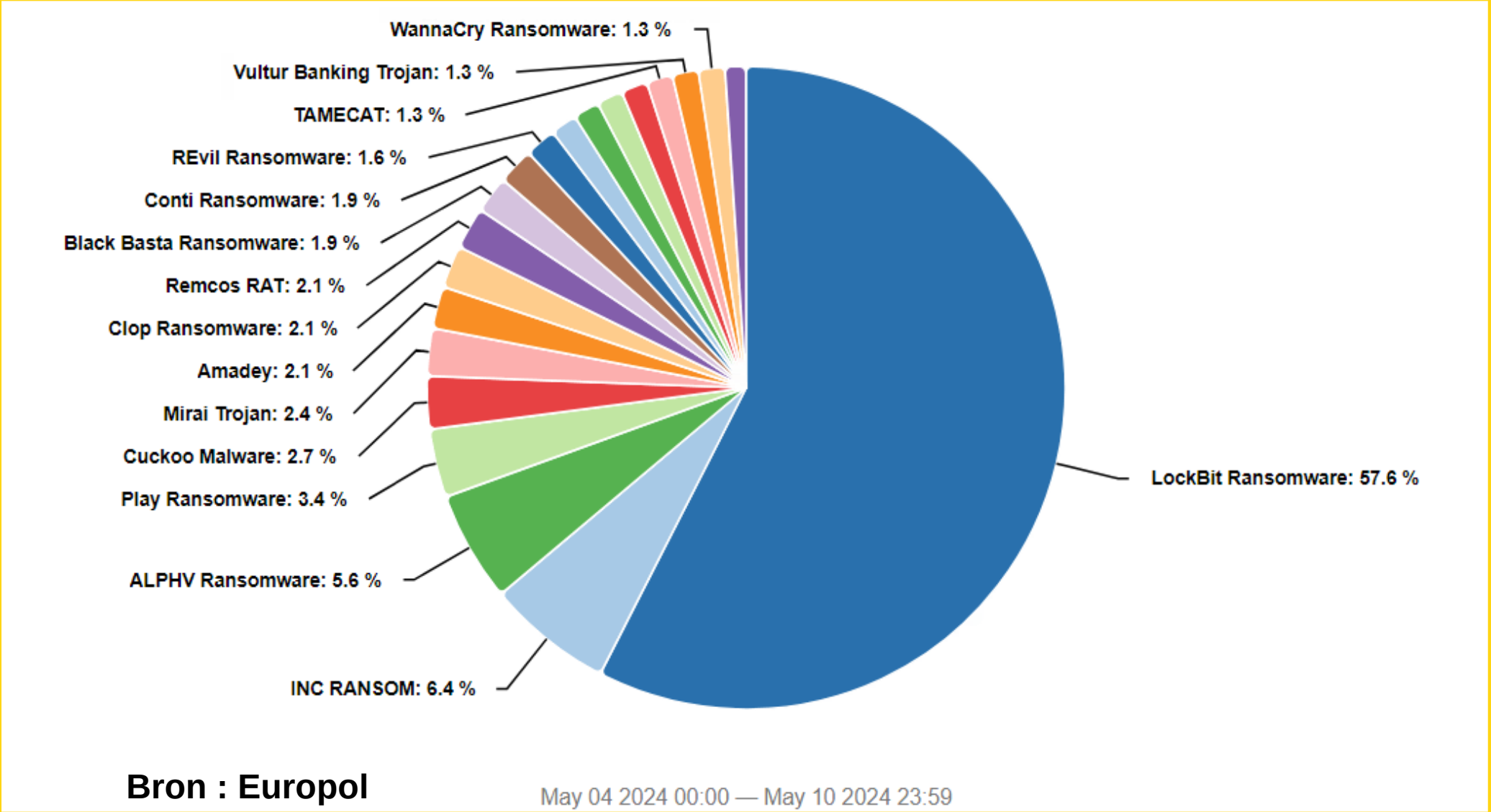


Oplossingen vanuit Europa

NIS2, DORA, CRA & AI ACT

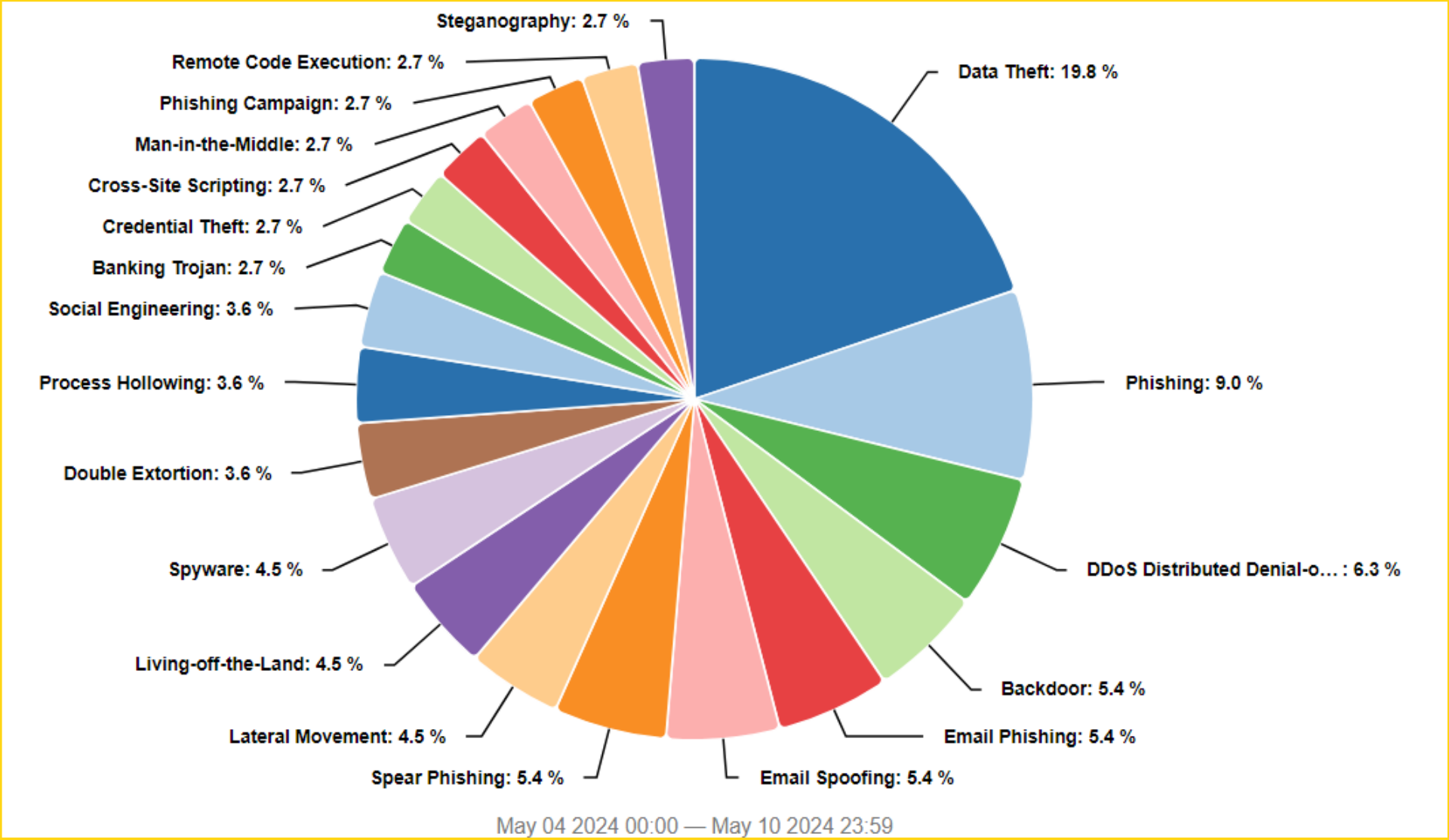
Data, AI & Cybersecurity de weg naar digitaal goud

Trending Malware Families Chart

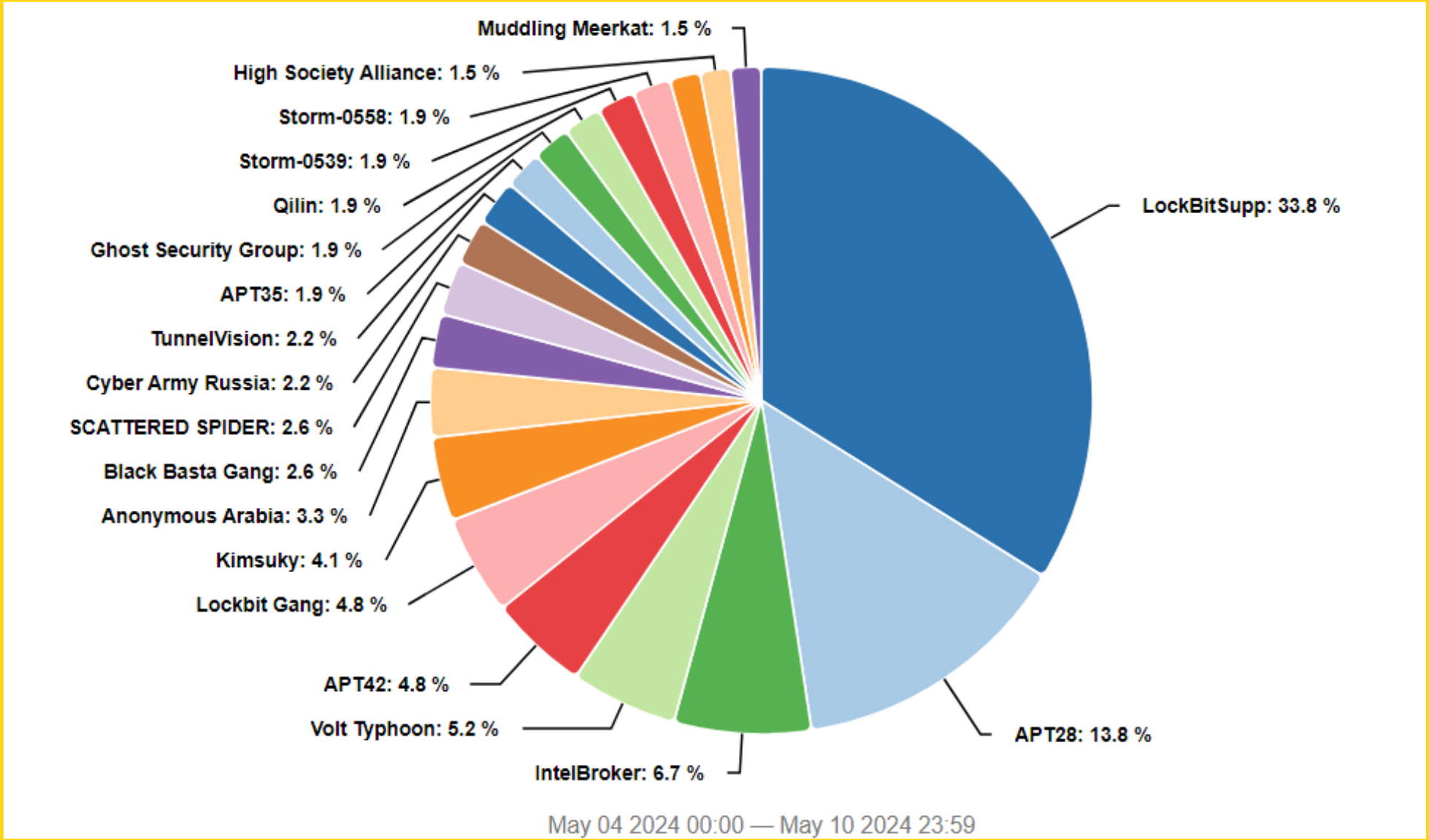


Bron : Europol

Attack Types by Mentions Graph



Trending Criminal Hacking Groups Chart



chrsm
Centre Hospitalier Régional
Sambre et Meuse

VDL
BUS & COACH

VERHELST
BOUWMATERIALEN

curando


SEA
invest


TVH


hogeschool
vives


OXFAM
Wereldwinkels


Belnet
dedicated connectivity

goed
thuiszorgwinkel
apotheek

beyers
TAKING COFFEE FURTHER

AML
MEDVET
AML
WEST
LABO
RIGO

fresh foodservice
DEKEYZER-OSSAER N.V.

MediaMarkt

Li Lait
- coffee & tea & more -

SPRIMOGLASS

LIMBURG.NET
DA'S PROPER GEDAAN

ESTD 1871
Duvel


DORA
Digital
Operational
Resilience
Act


NIS2


CYBER RESILIENCE ACT
WILL BE NEW INTERNATIONAL POINT
OF REFERENCE ON CYBERSECURITY

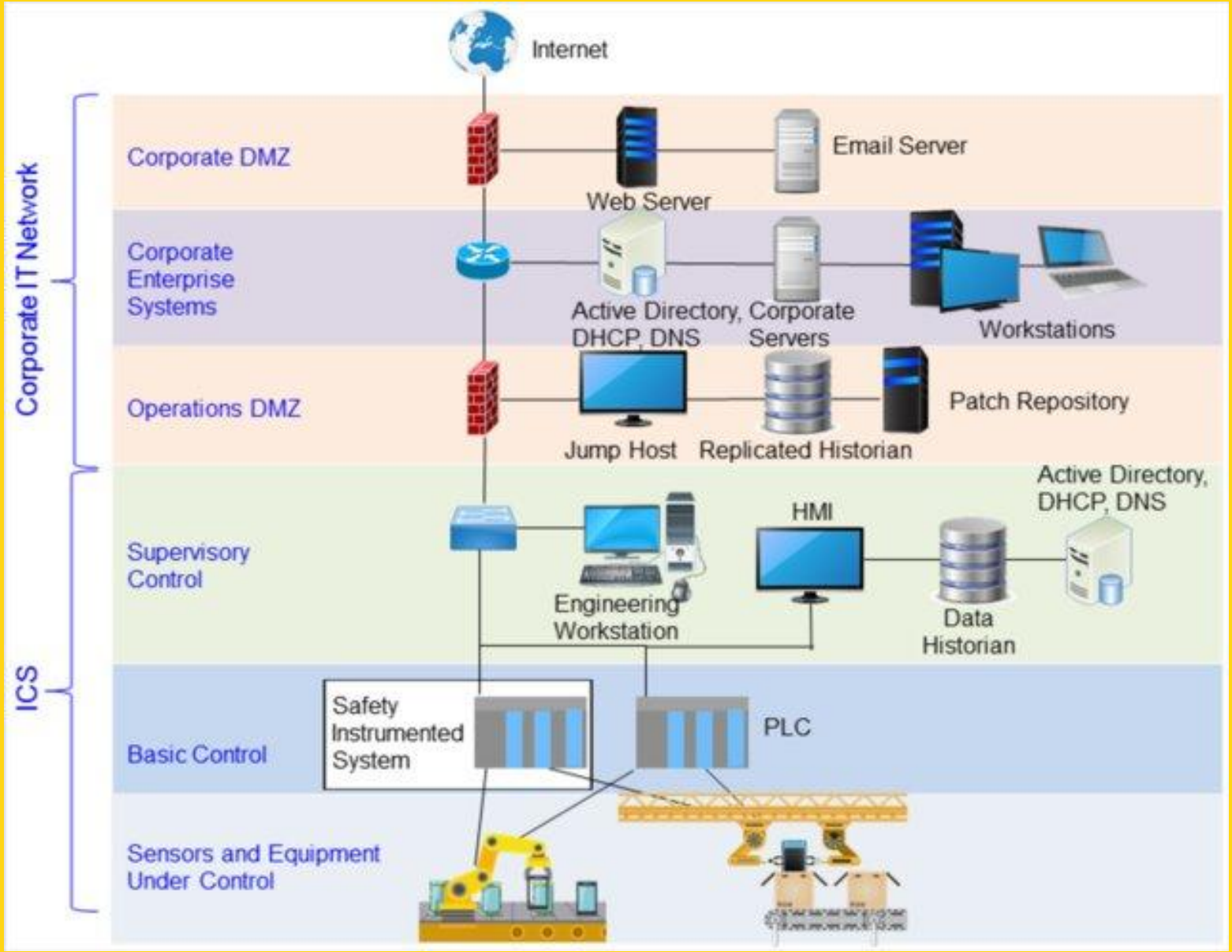

PCI
PCI DSS
COMPLI
EU AI ACT
IOT
ETSI EN 303 645
Software Secur
Standard
FDA


VULNERABILITY
MANAGEMENT


RISK


HOW TO PREVENT A
SUPPLY CHAIN ATTACK

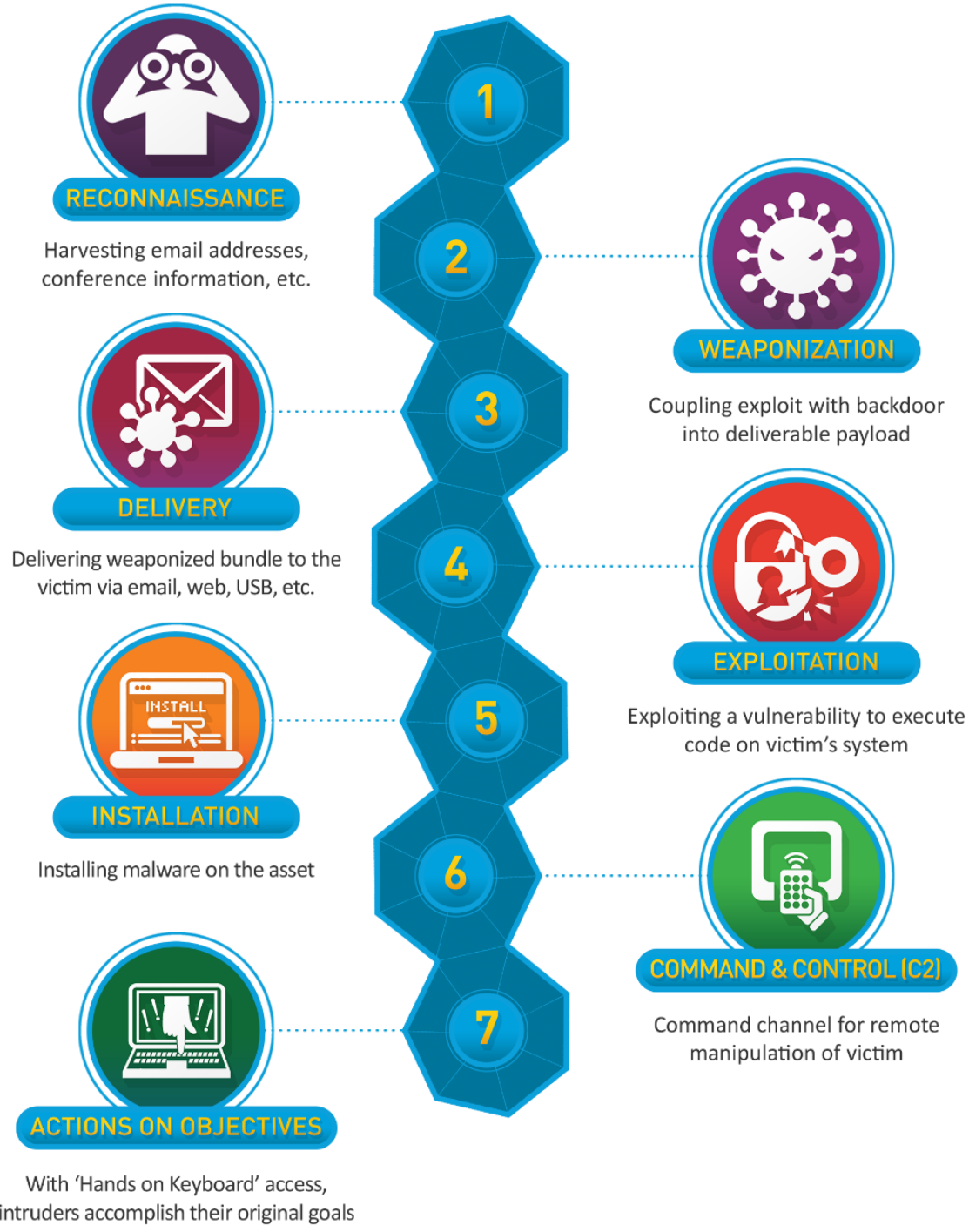

INCIDENT
RESPONSE
How To Respond Cyber Incident?



OT/ICS Security

Always bright, better and beyond.

Cyber Kill Chain



1	Reconnaissance	Collecting information about at target (network enumeration, email addresses, social media, etc.)
2	Weaponization	Adding exploit to malicious code (PDF document, remote template injection, etc.)
3	Delivery	Getting the malicious code to the victim (email, USB, compromised website, etc.)
4	Exploitation	Exploiting a targeted victim with a vulnerability (software, user, etc.)
5	Installation	Installing malicious code onto the system (droppers, backdoors, remote access tools, etc.)
6	Command & Control	Communicating with adversary from exploited system (collect taskings for campaign progression)
7	Actions on Objective	Achieve campaign objects (exfiltration of data, gain further access into the environment, extortion, etc.)

Kill Chain Stage	NIS2 Directive Compliance Measures	Approach to Enhance Learning
1. Reconnaissance	- Asset management- Threat intelligence sharing (Article 7)- Risk analysis (Article 21)	- Simulated OSINT games to spot data leaks- Red vs. Blue exercises to find hidden assets
2. Weaponization	- Vulnerability management (Article 21)- Secure software practices- Supply chain risk management	- Gamify code review or threat modeling- Simulate exploit development to spot weaknesses
3. Delivery	- Email & web filtering- Zero trust principles- Awareness training (Article 20)	- Phishing simulation platform with scoring- "Choose your attack vector" delivery games
4. Exploitation	- Patch management- Security-by-design (Article 21.2)- Real-time monitoring	- Capture-the-flag (CTF) challenges simulating exploit detection- Interactive vulnerability scanning labs
5. Installation	- Endpoint detection & response (EDR)- Antivirus & hardening- Least privilege enforcement	- Simulated malware sandbox analysis- Training: secure configuration competitions
6. Command & Control (C2)	- Network segmentation- Anomaly detection- Intrusion detection systems (IDS)	- Network traffic puzzle games- Red team drills to simulate and block C2 traffic
7. Actions on Objectives	- Incident response plans (Article 23)- Data protection (Article 21.1)- Forensic readiness	- Tabletop exercises- Real-time response simulations or ransomware scenario gamification

https://haveibeenpwned.com/?source=LINK

Home | Notify me | Domain search | Who's been pwned | Passwords | API | About | Donate

';--have i been pwned?

Check if your email address is in a data breach

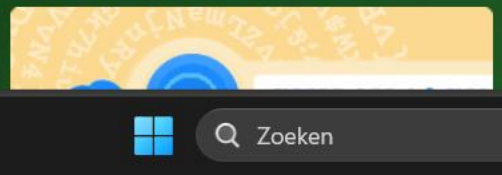
Kurt.Callewaert@capyx.be pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com



12°C Deels zonnig

Zoeken

NLD BEP

8:23 13/05/2025

BELGIË VOORLOPER EN TREKKER IN NIS2-TRANSPOSITIE
17 OKTOBER 2024

CENTRE FOR CYBERSECURITY BELGIUM

NIS 2 : FOR WHOM ? WHY ?

WHAT?

The directive n°2022/2555 ("NIS 2") is a revision of the directive n°2016/1148 ("NIS 1") (Network and Information Security). It is an EU legislation on the subject of cybersecurity.

WHICH OBLIGATIONS?

1. Register at the CCB (Safeonweb@work)
2. Take appropriate cybersecurity management measures.
3. Notify the CCB about significant cybersecurity incidents.
4. Carry out regular conformity assessments, verified by a conformity assessment body (essential entities).

WHY?

NIS 2 aims to establish a high and common level of cybersecurity in the EU by setting requirements regarding cybersecurity risk management measures and reporting obligations for organisations operating in different critical sectors.

FOR WHOM?

The (essential and important) entities who are established in Belgium and provide services in the sectors mentioned in annexes I and II.

Annex I: sectors of high criticality

DORA

- Energy
- Transport
- Financial market institutions
- Banking
- Health
- Drinking water
- Waster water
- Digital infrastructure
- ICT service management
- Public administration
- Space

Bijlage II: other critical sectors

- Postal and courier services
- Manufacture, production and distribution of chemicals
- Waste management
- Manufacturing
- Digital providers
- Research
- Production, processing and distribution of food

Key Measures & Compliance

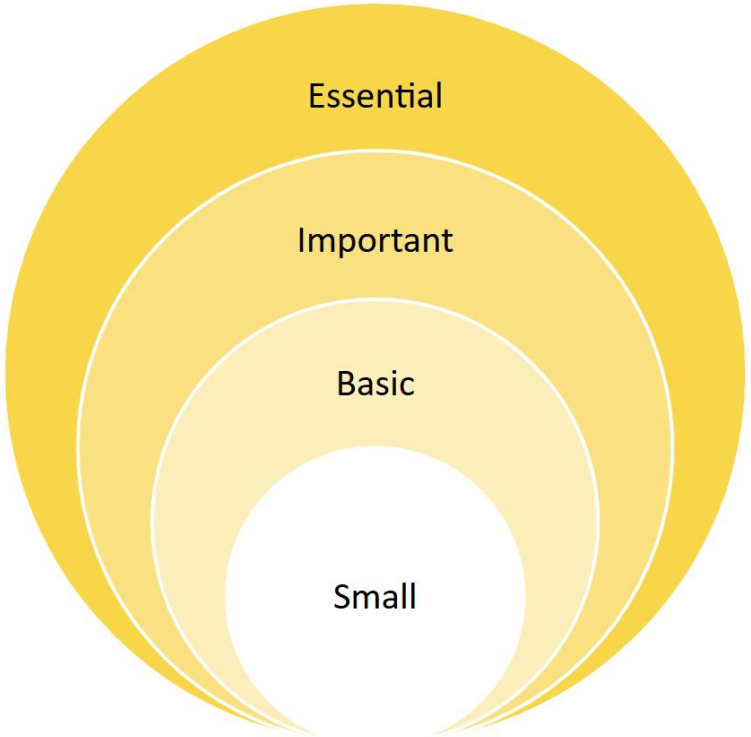
Actions for Operations

- **Risk Analysis**
  - To determine proportionality of measures to be taken
- **Minimum Security Requirements**
  - Incident handling (prevention, detection, response), Business continuity Plan
  - Encryption & Cryptography
  - Policies & Procedure (& testing them)
- **Supply Chain Security**
- **Training for Management**
- **Notify significant incidents, near misses, threats**
  - First notification: 24h
  - Interim report: 72h
  - Final report: 1 month
- **(Certification)**

All entities in scope need to do ALL of these

Cyber Fundamentals

CyFun

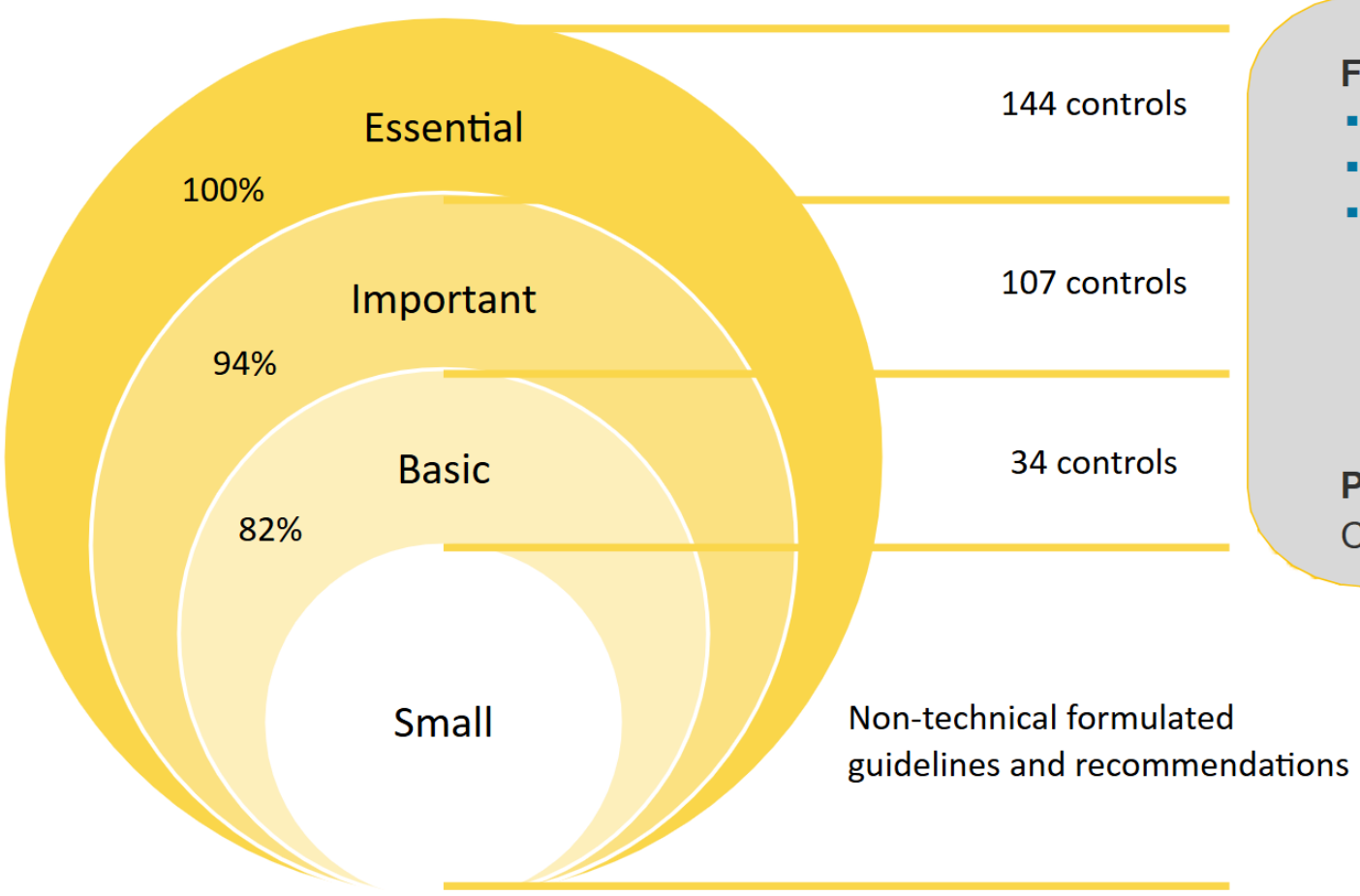


Levels

Based on

CERT.be
The Federal Cyber Emergency Team

capyx
Always bright, better and beyond.



Supports NIS 2 Compliance

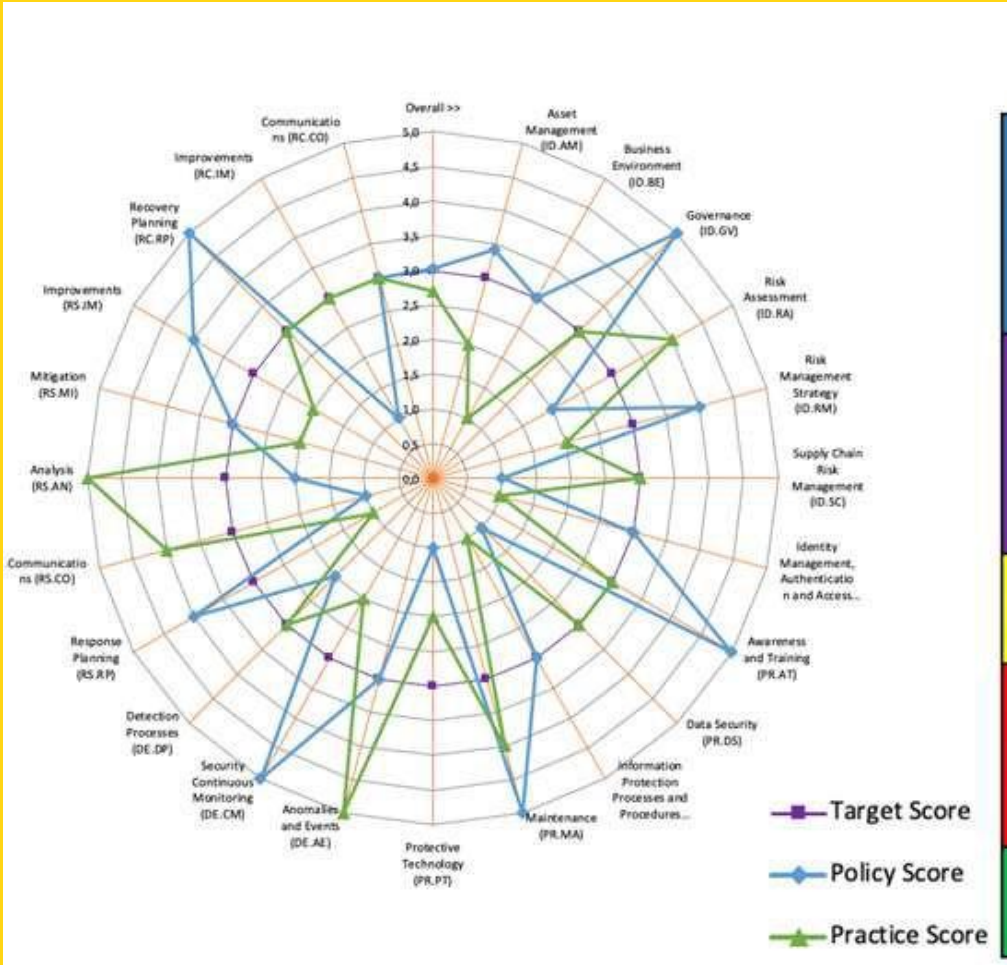
Framework:

- **Controls** (Requirements)
- **Guidance**
- **Normative references**:
  - *NIST CSF*
  - *ISO 27001/2*
  - *IEC 62443*
  - *CIS Controls*

Presumption of equivalence for ISO 27001
Certification or equivalent (Cfr NIS1)

capyx
Always bright, better and beyond.

Measurable and actionable



	CCB Cyberfundamentals Framework	Target Score	2023 Policy Score	2023 Practice Score
	Overall >>	3,00	3,02	2,70
IDENTIFY (ID)	Asset Management (ID.AM)	3,00	3,42	2,00
	Business Environment (ID.BE)	3,00	3,00	1,00
	Governance (ID.GV)	3,00	5,00	3,00
	Risk Assessment (ID.RA)	3,00	2,00	4,00
	Risk Management Strategy (ID.RM)	3,00	4,00	2,00
	Supply Chain Risk Management (ID.SC)	3,00	1,00	3,00
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)	3,00	3,00	1,00
	Awareness and Training (PR.AT)	3,00	5,00	3,00
	Data Security (PR.DS)	3,00	1,00	3,00
	Information Protection Processes and Procedures (PR.IP)	3,00	3,00	1,00
	Maintenance (PR.MA)	3,00	5,00	4,00
	Protective Technology (PR.PT)	3,00	1,00	2,00
DETECT (DE)	Anomalies and Events (DE.AE)	3,00	3,00	5,00
	Security Continuous Monitoring (DE.CM)	3,00	5,00	2,00
	Detection Processes (DE.DP)	3,00	2,00	3,00
RESPOND (RS)	Response Planning (RS.RP)	3,00	4,00	1,00
	Communications (RS.CO)	3,00	1,00	4,00
	Analysis (RS.AN)	3,00	2,00	5,00
	Mitigation (RS.MI)	3,00	3,00	2,00
	Improvements (RS.IM)	3,00	4,00	2,00
RECOVER (RC)	Recovery Planning (RC.RP)	3,00	5,00	3,00
	Improvements (RC.IM)	3,00	1,00	3,00
	Communications (RC.CO)	3,00	3,00	3,00

KEY MEASURES (KM) + Total Maturity Level

CyFun Framework Conformity Assessment Scheme

	BASIC	IMPORTANT	ESSENTIAL
Type of assessment	Verification	Verification	Certification
Assessment method	Verification of self-assessment	Verification of self-assessment	Certification audit
Assessment performed by	**Accredited** CAB	**Accredited** CAB	**Accredited** CAB
Accreditation standard	ISO/IEC 17029	ISO/IEC 17029	ISO/IEC 17021-1
Frequency	The verification statement reflects only the situation at the point in time it is issued. There is no repetitive cycle.		3yrs repetitive cycle Year 0: Complete Year 1&2: partial (surveillance)
Assurance evidence	Verified Claim	Verified Claim	Certificate

Key Measures	13*
	≥ 2,5/5 for each key measure
Total Maturity level	≥ 2,5/5 (see self-assessment tool – summary tab)

Key Measures	13 (Basic) + 8 (Important)*
	≥ 3/5 for each key measure
Total Maturity level	≥ 3/5 (see self-assessment tool – summary tab Important)

Key Measures	13 (Basic) + 8 (Important) + 8 (Essential)*
	≥ 3/5 for each key measure
Category Maturity	≥ 3/5 for each category
Total Maturity level	≥ 3,5/5 (see self-assessment tool – summary tab Important)

CYBER RESILIENCE ACT (CRA): NEW RULES WILL MAKE CONNECTED PRODUCTS MORE SECURE

On 20 November 2024, the Cyber Resilience Act (CRA) was published

“horizontal cybersecurity requirements for products with digital elements”.


2024
10 december
CRA treedt in werking
2026
10 september
Meldplicht actief misbruikte kwetsbaarheden
2026
10 december
Beschikbaarheid standaarden en notified bodies
2027
10 december
Producten met digitale elementen moeten voldoen aan de CRA
Voorbereiding
Bij de voorbereiding worden onder andere de geharmoniseerde standaarden ontwikkeld.
De meldplicht voor actief misbruikte kwetsbaarheden en incidenten gaat in.
Dit is de streefdatum, zodat producten alvast op conformiteit beoordeeld kunnen worden.
Alle eisen gaan in en alle producten met digitale elementen moeten voldoen aan de CRA.

Cyber Resilience Act – what do I need to do?

EU declaration of conformity
(Art. 28 / 32, Annex V / VI / VIII)

Goal: formally declare conformity
- public -

Internal assessment

Module A: internal control

Third-party assessment
(mandatory only for important / critical products)

Module H: quality assurance

Module B+C:
EU-type examination

EU cybersecurity certification scheme

Technical documentation
(Art. 31, Annex VII)

Goal: substantiate conformity
- not public -

Description, intended purpose

Cybersecurity risk assessment (Art. 13)

Vulnerability handling process
incl. SBOM, where applicable

Design information
Drawings, schemes, system architecture, interaction of system components, production and monitoring process

List of harmonised standards

Test reports (conformity assessment)

How support period was determined

Information & instructions to the user
(Art. 13, Annex II)

Goal: help user use product securely
- provided with product -

Intended purpose, essential functionalities

Security environment, security properties

Foreseeable circumstances / misuse that may lead to cybersecurity risk

Necessary measures for secure use:
(de-)commissioning, operations, changes affecting security, installation of security updates

Essential requirements (Annex I, to be detailed in harmonised standards)

During design

principles / incident prevention
- Integrity & confidentiality of data
- Availability of essential functions
- Access control, authentication
- Limitation of attack surface
- Minimisation of data use / secure removal

resilience / incident readiness
- Impact reduction in case of incident
- Minimise negative effect of incident on other services
- Logging
- SBOM

During operations

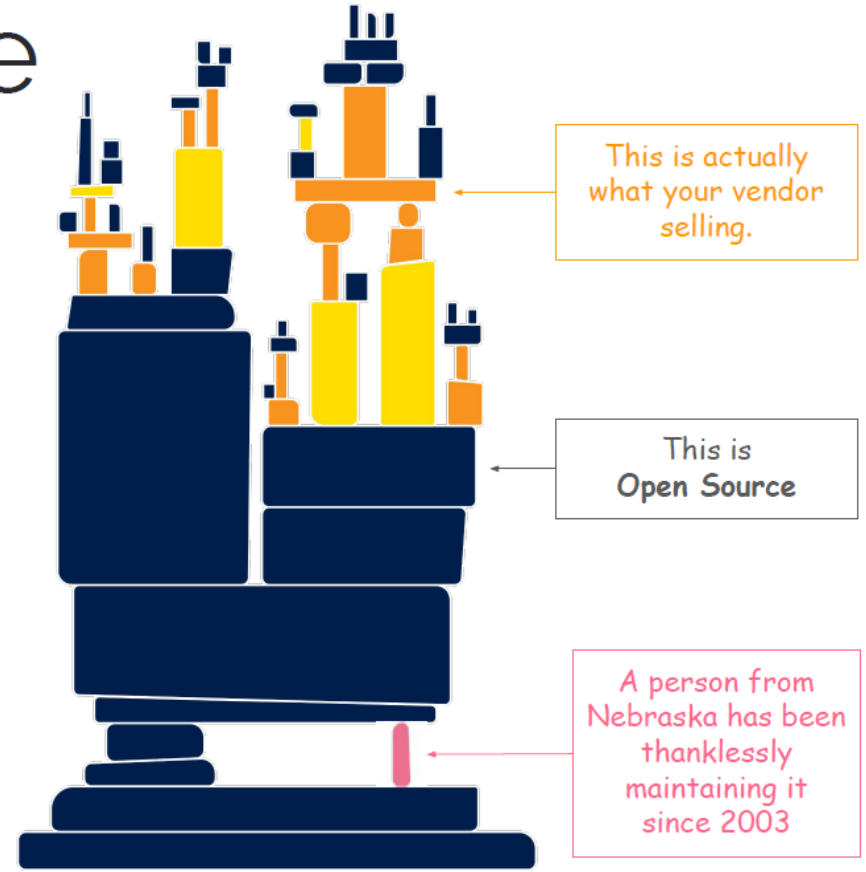
vulnerability and incident handling
- Publicly disclose fixed vulnerabilities (coordinated disclosure)
- Security updates: fast, free, automated, through secure distribution channel
- Regular tests and reviews

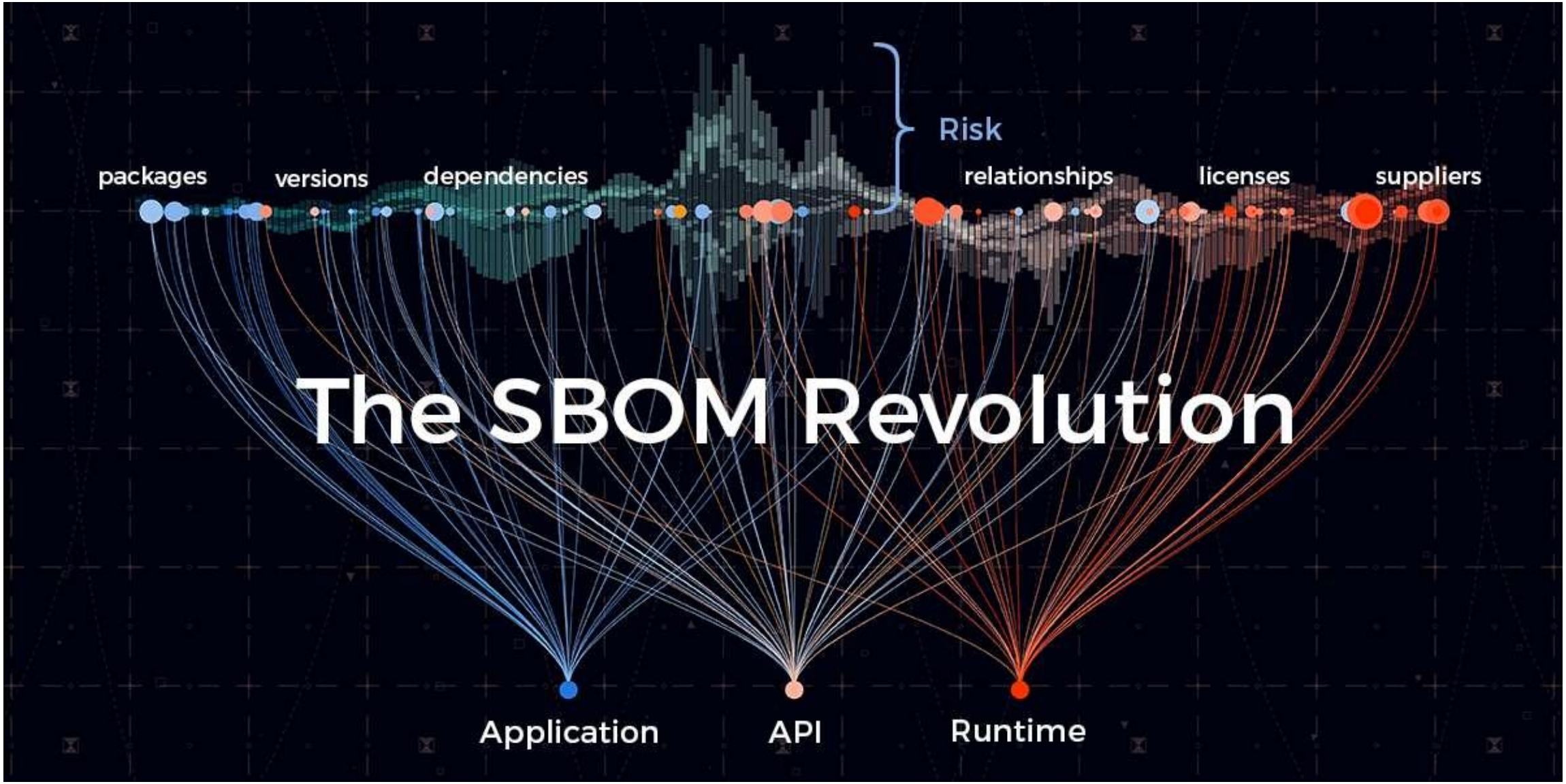
70% Open Source

What is in your software assets? What risks they carry?

- Critical Vulnerabilities
- IP License infringements
- End of life or support components
- Malicious supply chain attacks
- Counterfeit hardware components
- Abandoned open source software

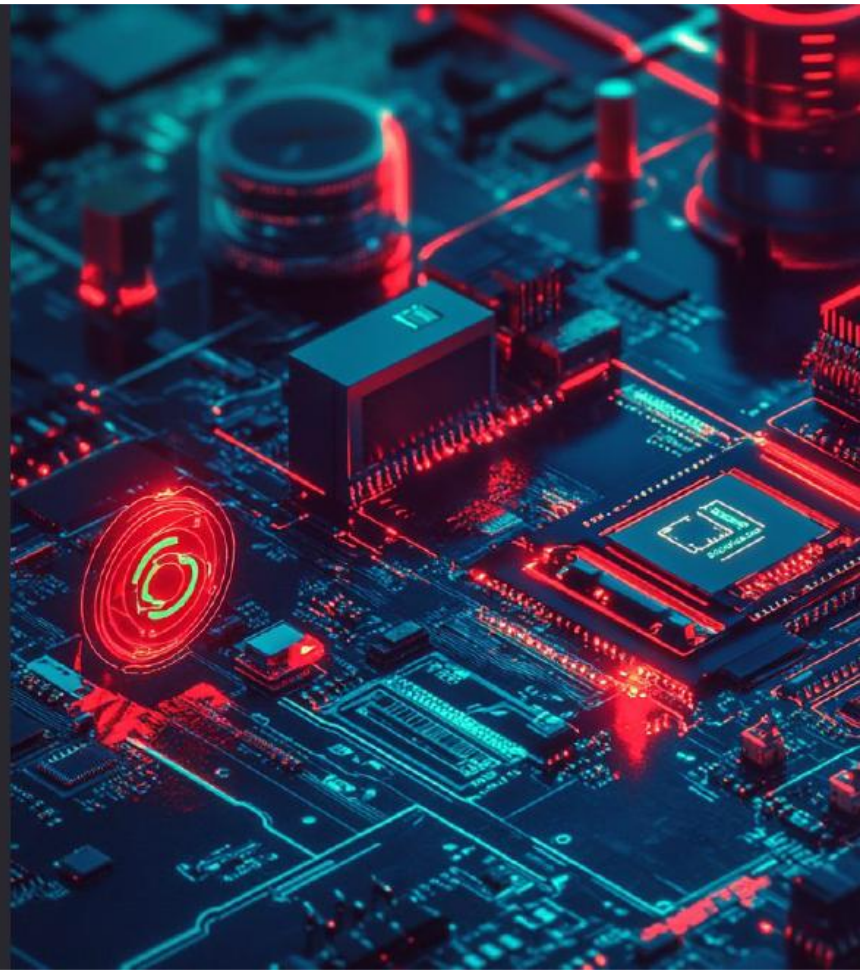
CyBeats




Risk
packages
versions
dependencies
relationships
licenses
suppliers
The SBOM Revolution
Application
API
Runtime

SBOM Contains

- **SBOM** - Software Bill of Materials
  A comprehensive list of all software components, libraries, and their dependencies.
- **HBOM** - Hardware Bill of Materials
  A detailed inventory listing all physical components and hardware.
- **AIBOM** - AI Bill of Materials
  A breakdown of the AI models, datasets, and algorithms.
- **CBOM** - Cryptography Bill of Materials
  A detailed inventory of all cryptographic components, including algorithms, keys, and certificates.



SBOM Lifecycle

CyBeats

When **evaluating** a new software solution, an SBOM provides transparency into the software's components, enabling better assessment of security vulnerabilities, license compliance, and overall risk management.

Evaluation

When **procuring** new software, contracts are evolving to require SBOMs, offering critical visibility into the software's components for improved security, compliance, and proactive risk management.

Procurement

SBOMs are essential for **Third-Party Risk Management** and ongoing risk monitoring enabling organizations to identify vulnerabilities, manage licensing risks, and continuously monitor for security threats throughout the software lifecycle.

TPRM

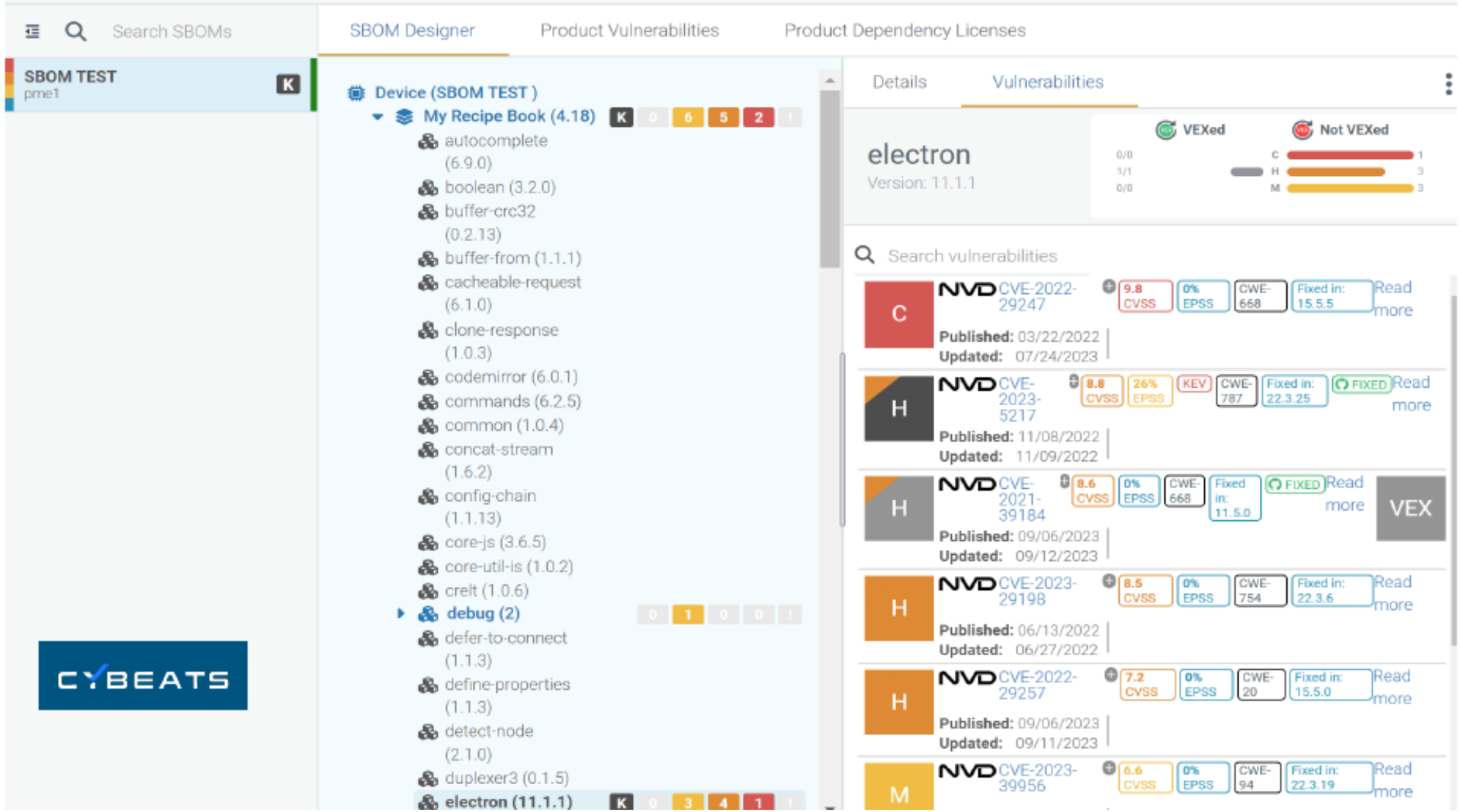
SBOMs enhance **asset inventory** by offering a detailed record of software components, enabling better tracking, management, and linking these assets to their network presence.

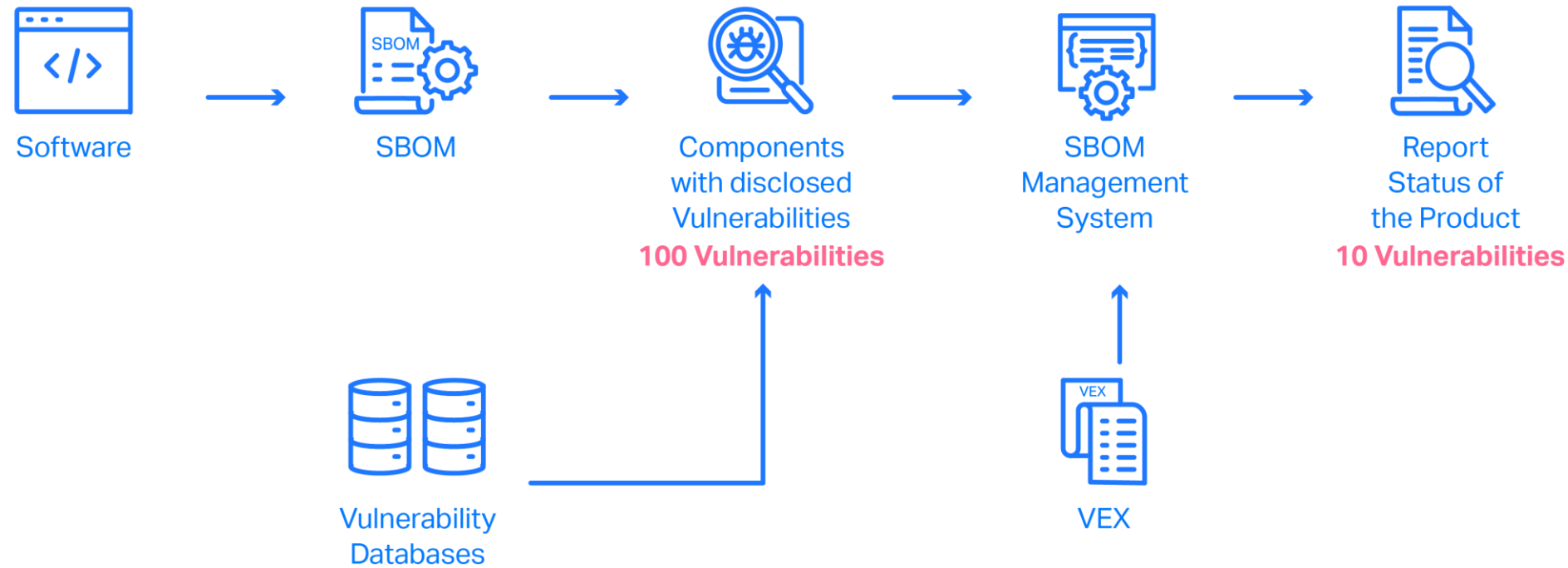
Asset Inventory & Operations

SBOMs help in **incident response** by providing a detailed map of software components, allowing teams to quickly identify vulnerabilities. This proactive approach ensures that risks are addressed before they can be exploited.

Incident Response

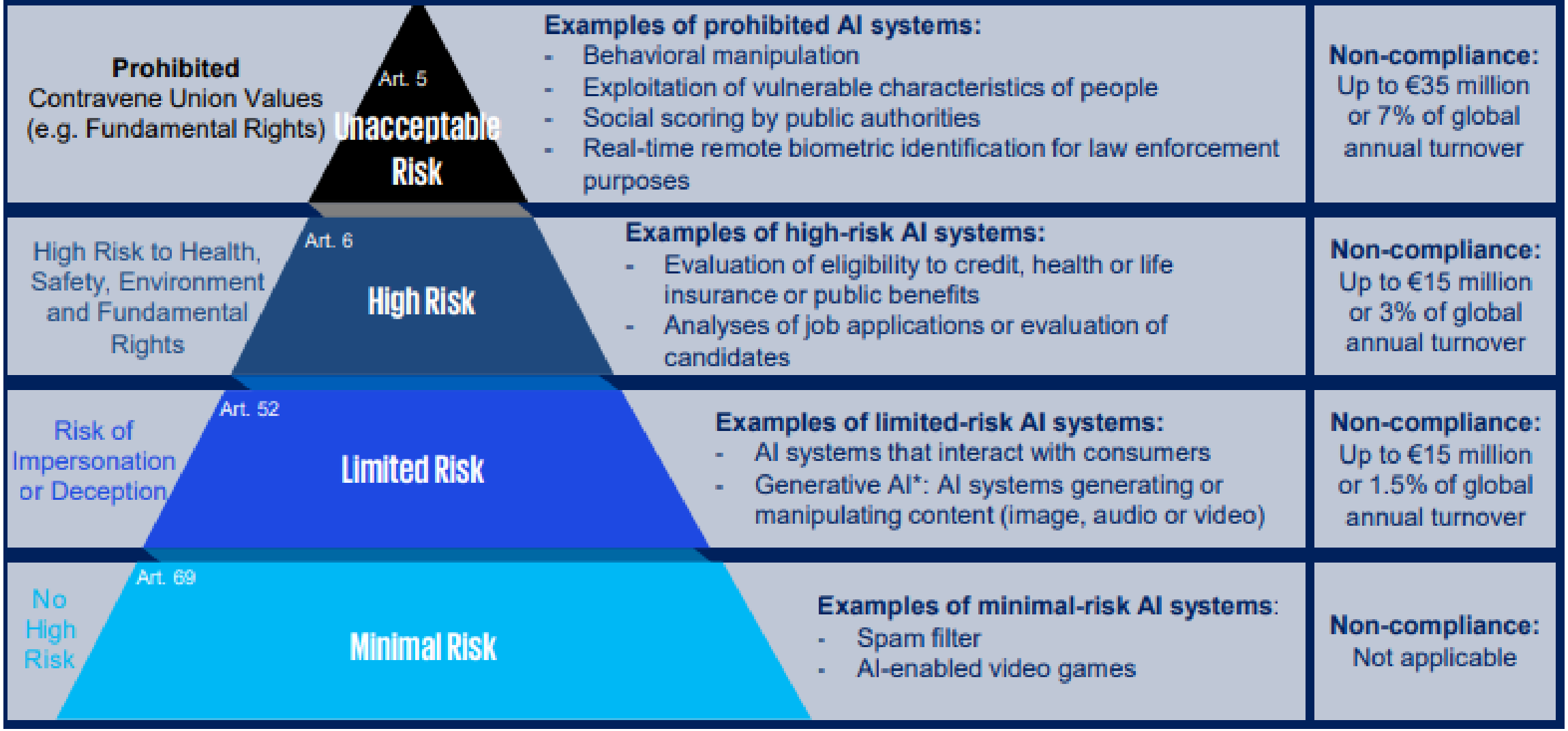
SBOM Studio - High-Level Architecture


Search SBOMs
SBOM Designer
Product Vulnerabilities
Product Dependency Licenses
SBOM TEST
pme1
K
Device (SBOM TEST)
My Recipe Book (4.18)
K 0 6 5 2
autocomplete (6.9.0)
boolean (3.2.0)
buffer-crc32 (0.2.13)
buffer-from (1.1.1)
cacheable-request (6.1.0)
clone-response (1.0.3)
codemirror (6.0.1)
commands (6.2.5)
common (1.0.4)
concat-stream (1.6.2)
config-chain (1.1.13)
core-js (3.6.5)
core-util-is (1.0.2)
crelt (1.0.6)
debug (2)
0 1 0 0
defer-to-connect (1.1.3)
define-properties (1.1.3)
detect-node (2.1.0)
duplexer3 (0.1.5)
electron (11.1.1)
K 0 3 4 1
Details
Vulnerabilities
electron
Version: 11.1.1
VEXed
Not VEXed
0/0
1/1
0/0
C 1
H 3
M 3
Search vulnerabilities
C
NVD CVE-2022-29247
9.8 CVSS
0% EPSS
CWE-668
Fixed in: 15.5.5
Read more
Published: 03/22/2022
Updated: 07/24/2023
H
NVD CVE-2023-5217
8.8 CVSS
26% EPSS
KEV
CWE-787
Fixed in: 22.3.25
FIXED
Read more
Published: 11/08/2022
Updated: 11/09/2022
H
NVD CVE-2021-39184
8.6 CVSS
0% EPSS
CWE-668
Fixed in: 11.5.0
FIXED
Read more
VEX
Published: 09/06/2023
Updated: 09/12/2023
H
NVD CVE-2023-29198
8.5 CVSS
0% EPSS
CWE-754
Fixed in: 22.3.6
Read more
Published: 06/13/2022
Updated: 06/27/2022
H
NVD CVE-2022-29257
7.2 CVSS
0% EPSS
CWE-20
Fixed in: 15.5.0
Read more
Published: 09/06/2023
Updated: 09/11/2023
M
NVD CVE-2023-39956
6.6 CVSS
0% EPSS
CWE-94
Fixed in: 22.3.19
Read more
CYBEATS


Software
SBOM
SBOM
Components
with disclosed
Vulnerabilities
100 Vulnerabilities
SBOM
Management
System
Report
Status of
the Product
10 Vulnerabilities
Vulnerability
Databases
VEX
VEX

Op 12 juli werd de AI Act gepubliceerd in het Europees Publicatieblad , dus 1 augustus 2026 klaar zijn met de voorbereiding

The AI Act takes a risk-based approach



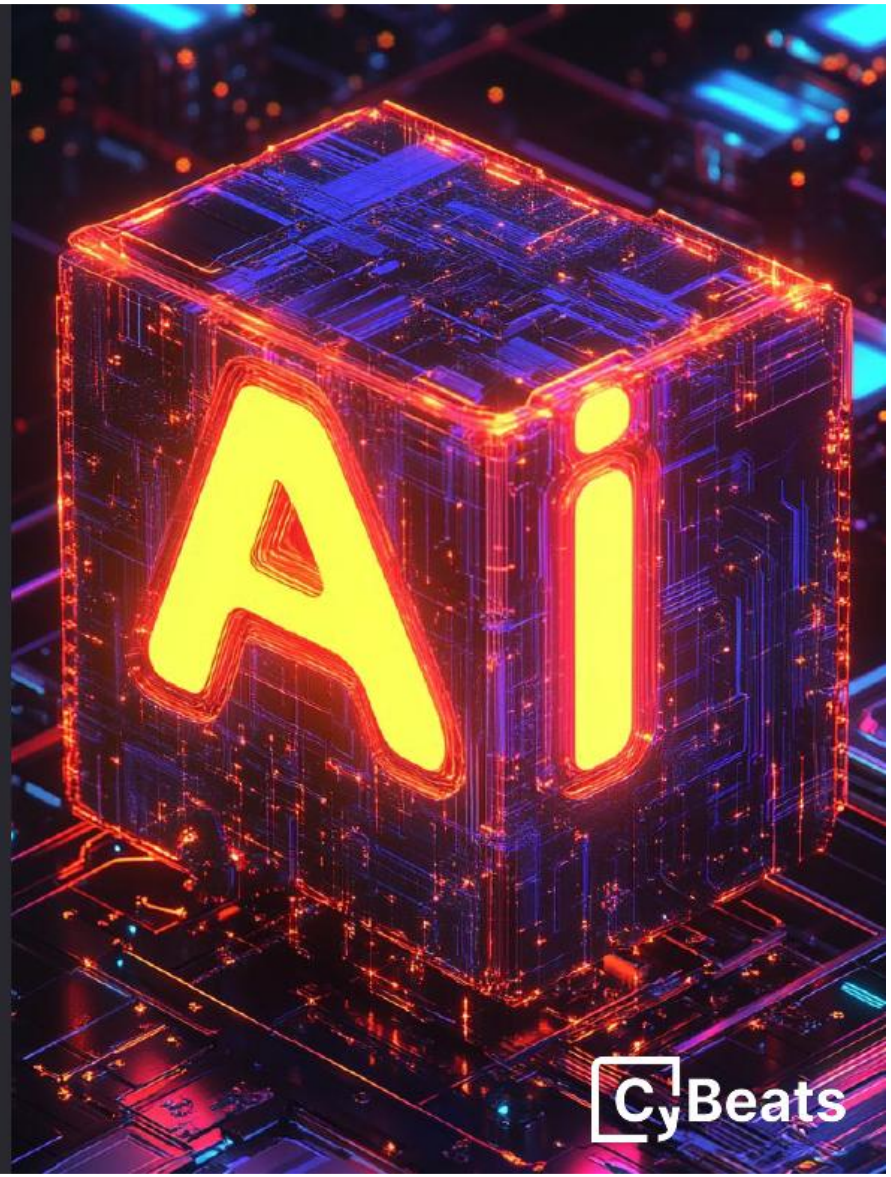
AIBOM

- **Models** - Model Card
  Provides detailed information about AI models, including their architecture, datasets used for training, and performance metrics

- **Data Sets** - Models are trained using Data Sets
  In an AIBOM, datasets used to train AI models can be vulnerable to poisoning, where malicious data compromises the model's reliability.

- **Governance** - AI Bill of Materials
  Governance in AIBOM ensures the proper oversight, tracking, and management of AI components and datasets, promoting transparency, compliance, and accountability throughout the AI lifecycle.

- **Considerations** - Ethical, Environmental, Fairness



Next: AIBOM Interoperability

Model Card

Inventory and transparency

Integration into MLSecOps

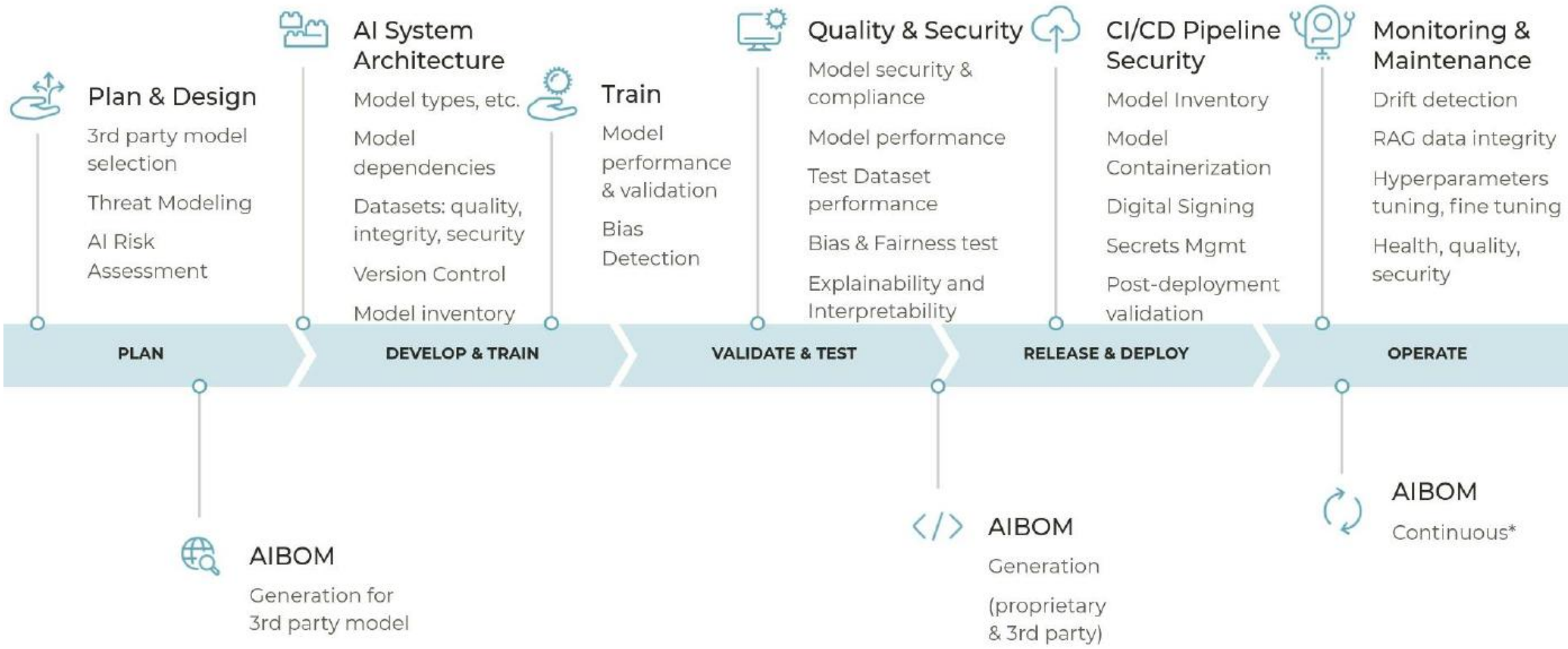
AIBOM generation and consumption

3rd Party Model Assessment

Licensing, ethics, regulatory, security

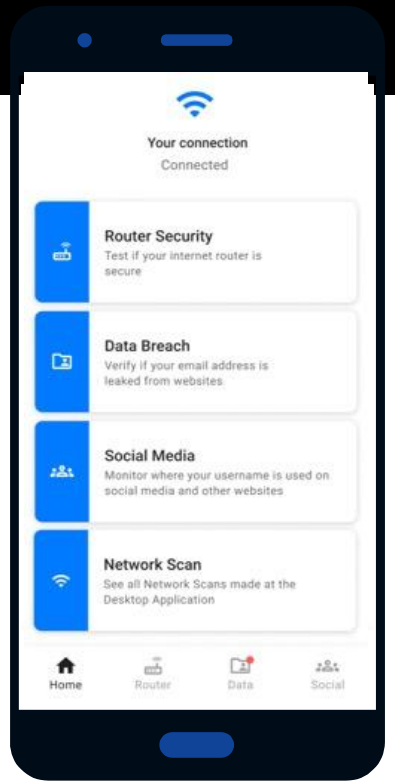
Proprietary Model Assessment

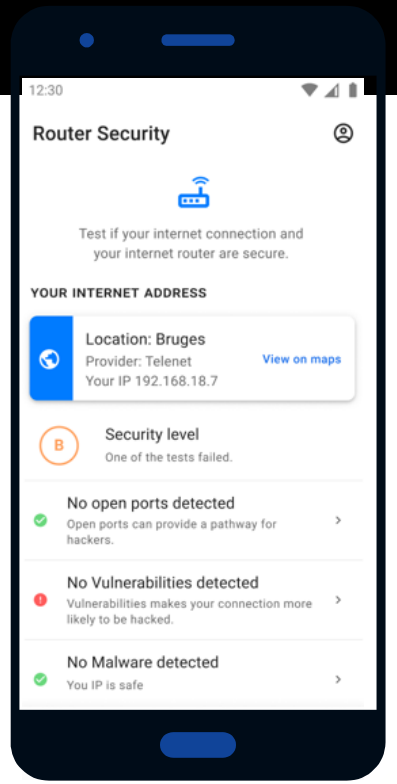
Ethics, regulatory, security, 3rd party model dependencies

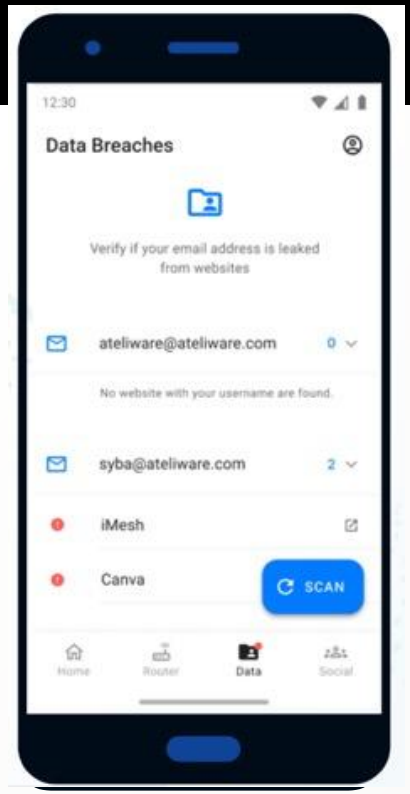


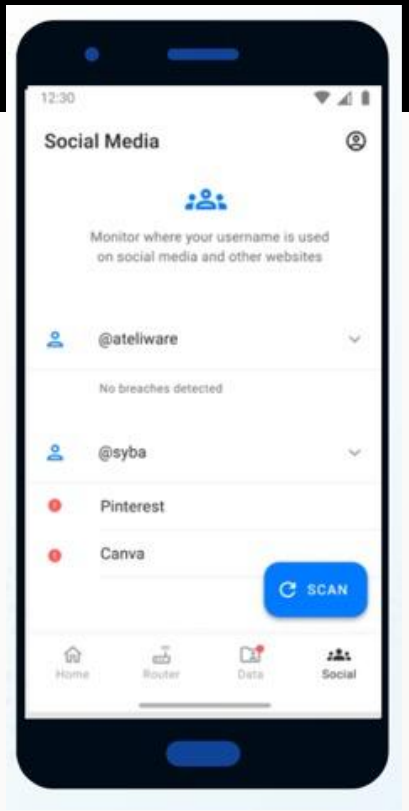
AIBOM Integration into MLSecOps

Syba | Being secure online









Q&A

capyx

Always
bright, better
and beyond.

Kurt Callewaert
Business Line Director Cybersecurity
CS Researcher of the year 2023
Meetdistrict Gent
Phone: +32 473340465
Email: Kurt.Callewaert@capyx.be
Website: www.capyx.be