



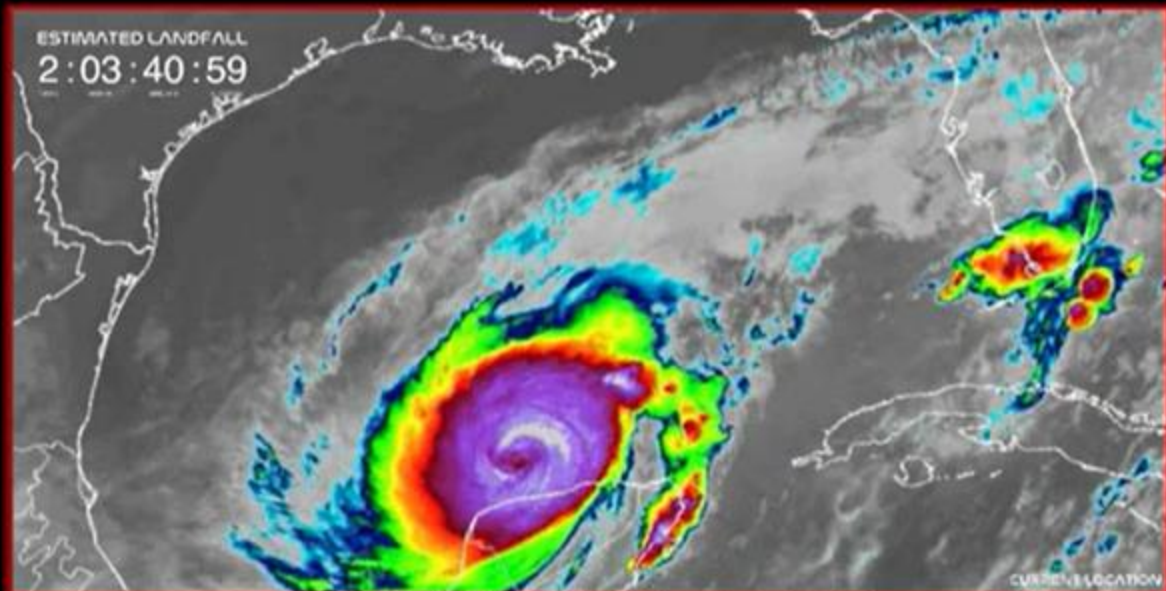
DE **N** EXUS™

**End-to-end Cyber Risk Management**  
*Energy & Industrial Sectors*

NEXT FORECAST IN : : 07 : 19 : 00

# HURRICANE MILTON

CATEGORY 1 2 3 4 5



Hurricane Milton Rapid Intensification Continues; Evacuations Underway  
Hurricane Hunter Aircraft Confirms Milton Pressure At 898.6mb & Dropping (only 3rd time in recorded history)  
Sustained Winds Of 180mph (289 km/h) Gusting To 220mph (354km/h) & Increasing



I275 EB from ST. PETERSBURG



I275 EB in TAMPA



I75 NB from SUN CITY



I75 & HWY27 Junction NB



I-75 NB AT MM 328.4

LOOKING: NW



I4 NB from Lakeland



I75 NB from TAMPA



I4NB from LAKE MONROE



I95 NB from DAYTONA



I-95 SB AT MM 265.1

LOOKING: N



**FOX4**

# TROPICAL STORM HELENE

ADVISORY	LOCATION	WIND	MOVEMENT	PRESSURE
10:00 AM	35.1°N 83.8°W	45 MPH	N at 32 MPH	975 MB



**BILLION-DOLLAR DISASTER HURRICANE HELENE**

**ACCUWEATHER PRELIMINARY  
ESTIMATE**

**\$225-250 Billion**

**IN TOTAL DAMAGE & ECONOMIC LOSSES  
FROM HURRICANE HELENE FROM  
DEVASTATING STORM SURGE, DAMAGING  
WINDS & HISTORIC FLOODING**



# CYBERTHREAT LIVE MAP EN

MAP STATISTICS DATA SOURCES BUZZ WIDGET

### SPAIN


# 12 MOST-ATTACKED COUNTRY

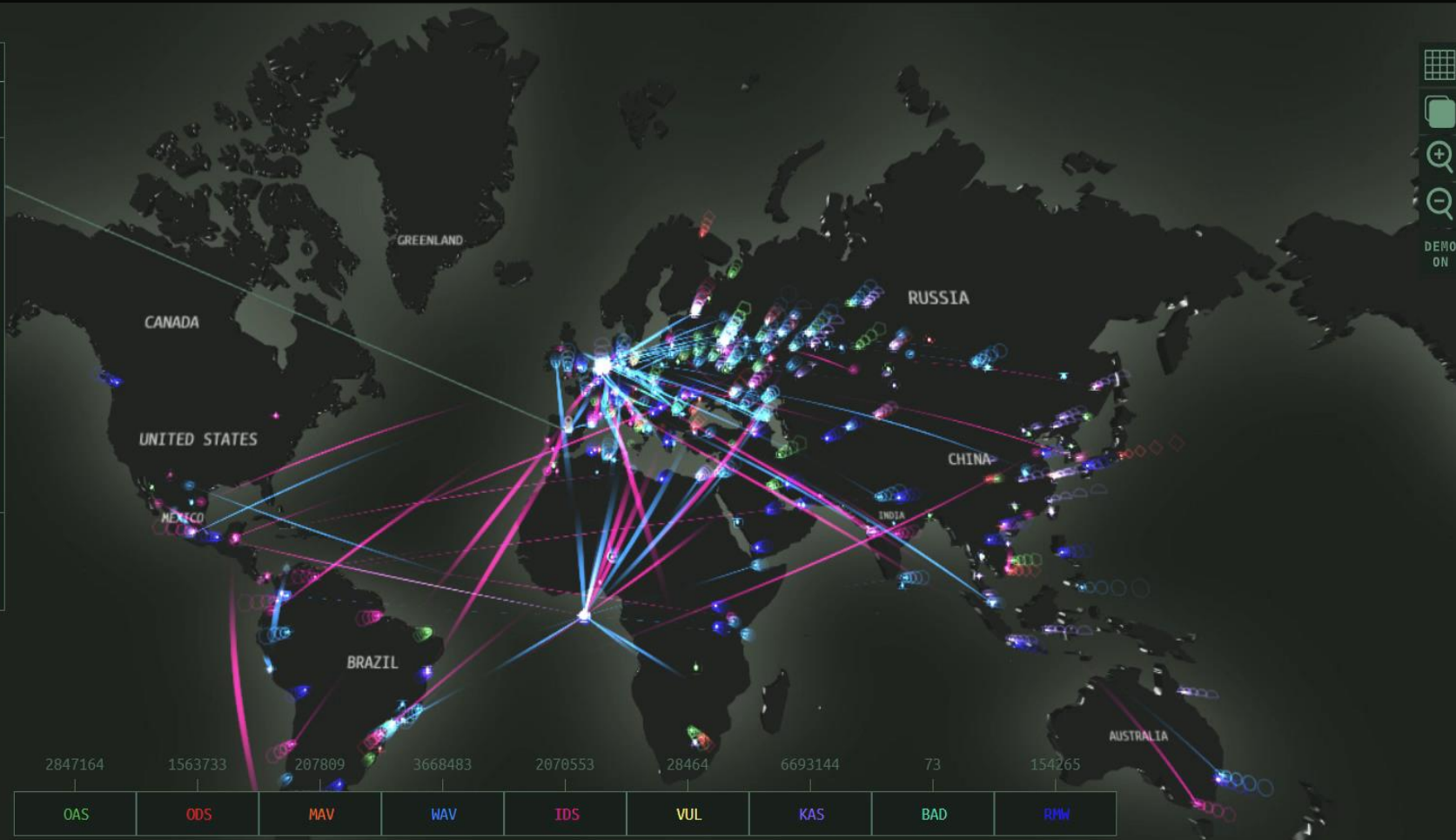
OAS	25469
ODS	22105
MAV	5936
WAV	80327
IDS	84420
VUL	909
KAS	9620
BAD	0
RHW	277

Detections discovered since 00:00 GMT

[More details](#)

Share data



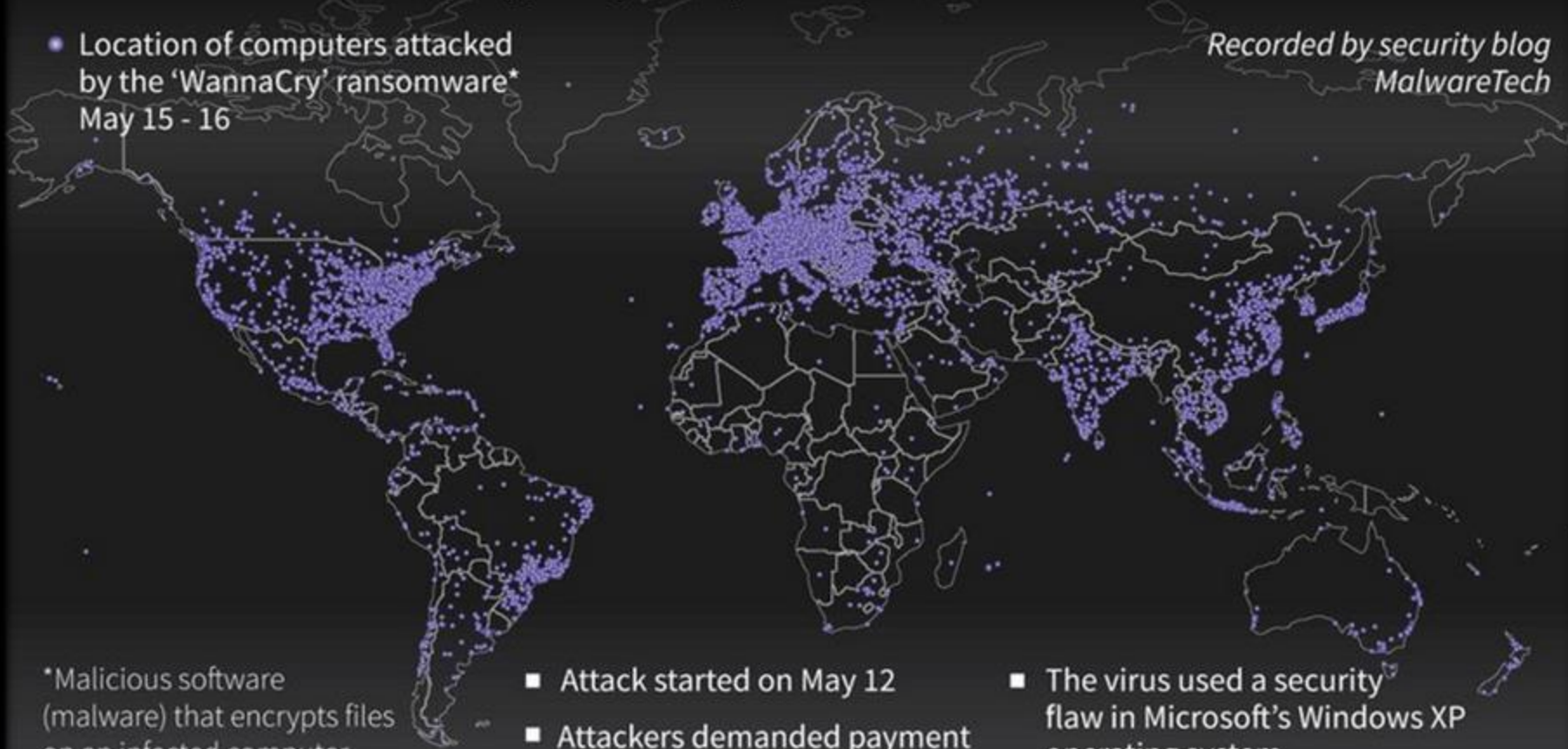
  
  
  
  
DEMO ON

# 'Wannacry' ransomware attack

Worldwide attack in mid May crippled up to 300,000 computers in 150 countries

- Location of computers attacked by the 'WannaCry' ransomware\*  
May 15 - 16

Recorded by security blog  
MalwareTech



\*Malicious software (malware) that encrypts files on an infected computer and demands payment to unlock them

- Attack started on May 12
- Attackers demanded payment of \$300 in virtual currency Bitcoin
- The virus used a security flaw in Microsoft's Windows XP operating system
- Hackers exploited NSA\*\* software leaked earlier this year

Sources : [Intel.malwaretech.com](http://Intel.malwaretech.com)/[US Homeland Security](http://USHomelandSecurity.com)/[Europol](http://Europol.com)/[National Security Agency](http://NationalSecurityAgency.com)

© AFP

CISOs and CFOs need quantitative insights to  
justify and prioritize cybersecurity investments

**\$215 Billion**<sup>[1]</sup>

annual spend on Cybersecurity

**\$20 Billion**<sup>[2]</sup>

Annual spend on Cyber Insurance

Sources: [1] Gartner Group for 2024, [2] Munich Re estimates of cyber insurance market for 2025

**"You can't manage what you don't  
MEASURE."**

— Peter F. Drucker





DE **N** EXUS™

**End-to-end Cyber Risk Management**  
*Energy & Industrial Sectors*

# DeRISK™

## Cyber Risk Quantification & Management Platform

DeRISK™ is the only evidence-based, **data-driven** platform that translates **OT cyber risk** exposures and vulnerabilities into business metrics such as the **financial impact of potential cyber events**.



# It's Cyber Risk in



# Values





# What is Financial Quantification of Cyber Risk?

Gartner, “A method of expressing [cyber] risk exposure from interconnected digital environments to the organization in business terms [...] using a combination of

- Business logic
- Mathematical models
- Loss event history
- Current risk assessment

To produce defensible exposure  
value ranges of a chosen period



The screenshot shows the Gartner website's glossary page for Cyber-Risk Quantification. The page header includes the Gartner logo and navigation links for Information Technology, Insights, Expert Guidance, Tools, and Connect with Peers. The breadcrumb trail reads: Gartner Glossary > Information Technology Glossary > C > Cyber-Risk Quantification. The main heading is "Cyber-Risk Quantification" in a large, bold, dark blue font. Below the heading is a paragraph of text: "Cyber-risk quantification is a method for expressing risk exposure from interconnected digital environments to the organization in business terms. Risk exposure can be expressed in currency, market share, customer and beneficiary engagement and disruption in products or services over a chosen period. Defensible exposure value ranges are determined using a combination of business logic, mathematical models, loss event history and current risk assessment."

**It's Cyber Risk in \$\$\$ Values.**

What is the **PROBABILITY** that a loss (\$\$\$) of a certain size or greater will occur in a year?



# Annual loss curve and exposure distribution



"There is a % (probability) of observing an annual loss higher than \$ (dollar amount)."

Source: DeRISK Demo (denexus.io)

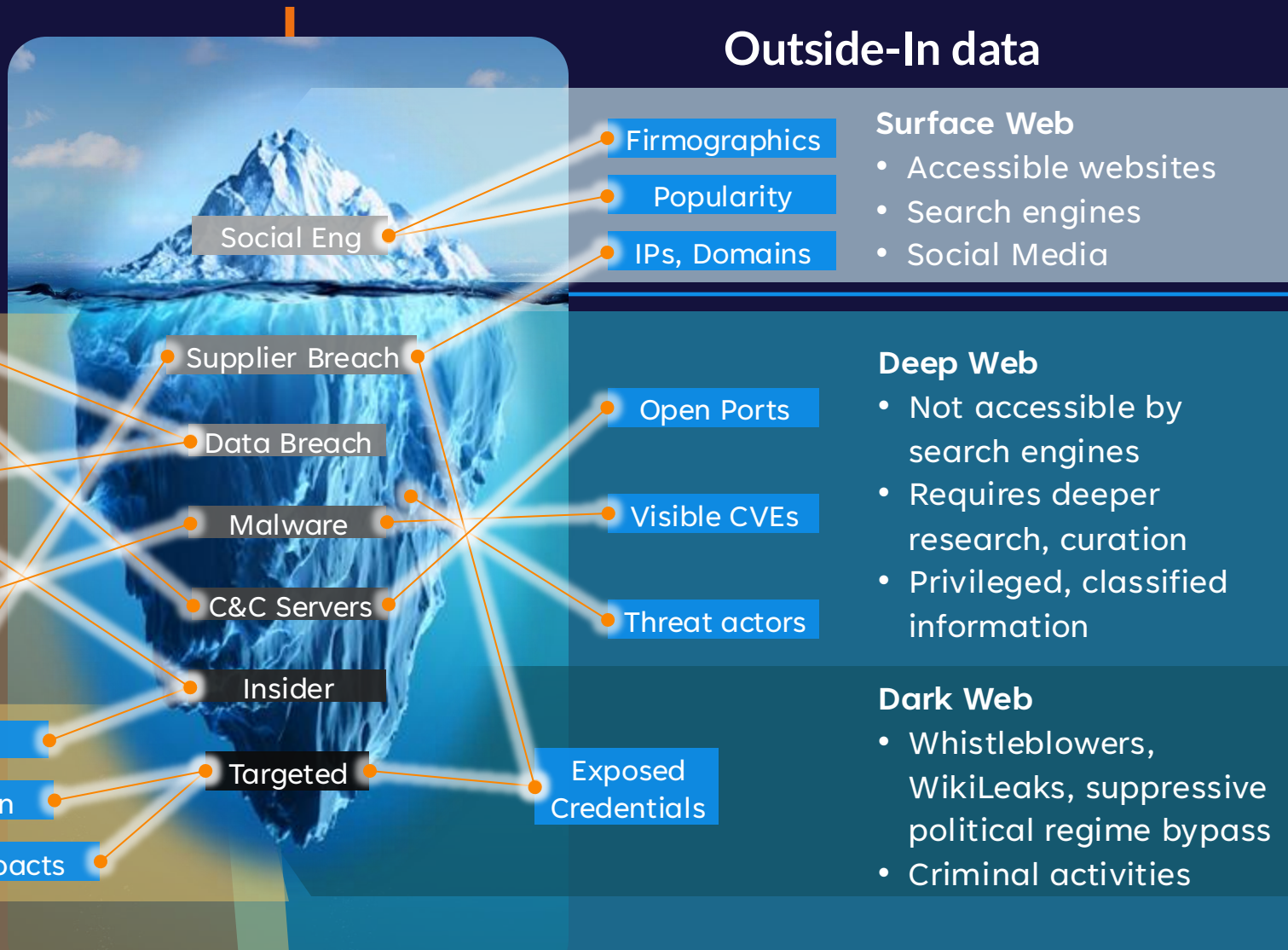


# Analyzing Complex Datasets

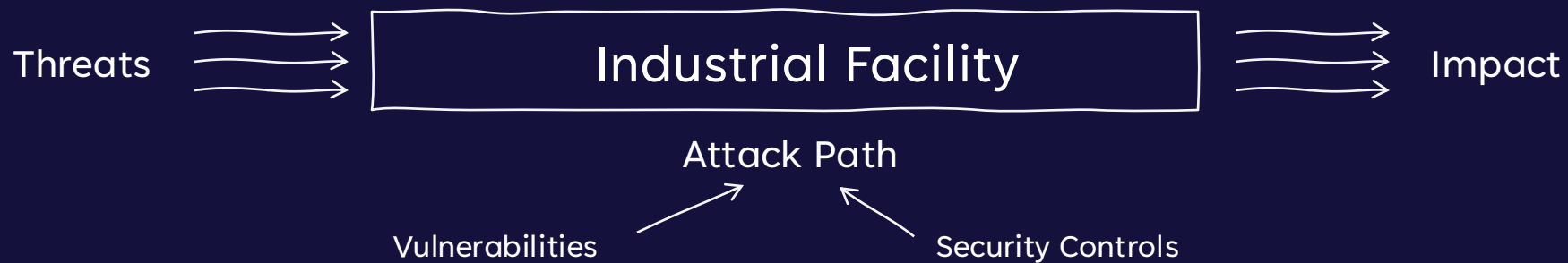
## Inside-Out data



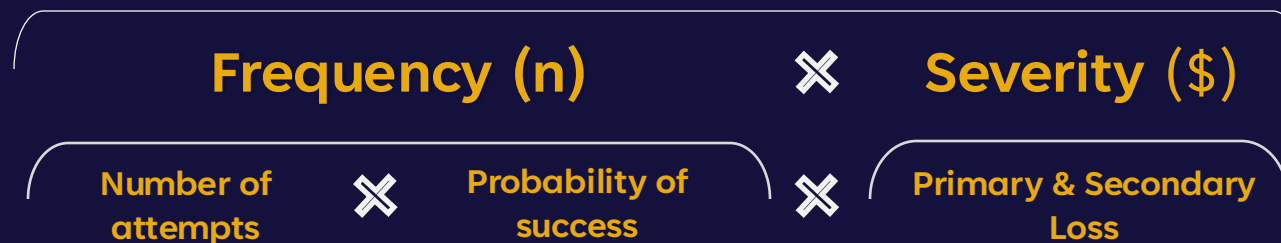
## Outside-In data



# DeRISK™ | Business Logic



## Annual Cyber Loss (\$)



Leveraging standards and frameworks

MITRE ATT&CK Enterprise & ICS, proprietary version of FAIR Taxonomy

Supporting NIST CSF, ISO 27001, and proprietary DNX CSF

# DeRISK™ | Data Analytics & Risk Modeling

## INPUT

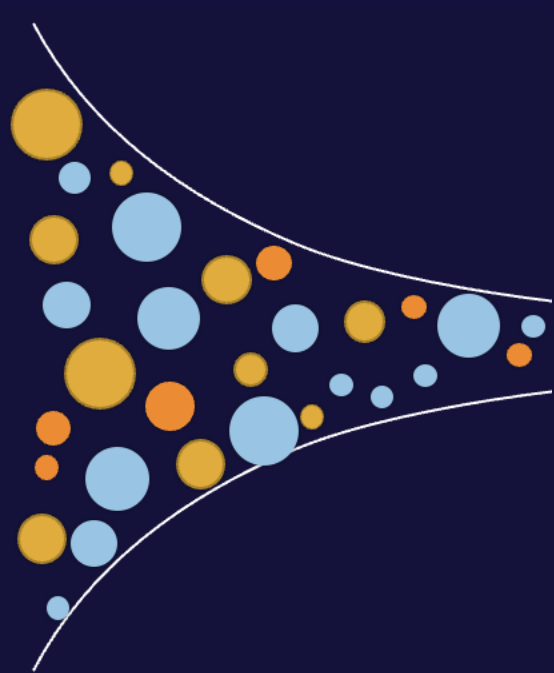
Raw data

## DeRISK AI engine

## OUTPUT

Business Analysis

Online Application

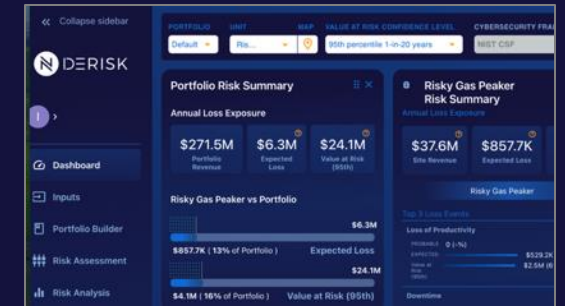
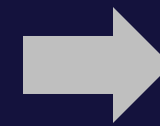


Number of Attack Attempts

Attack Path Simulator

Loss Event Simulator

Risk Mitigation System



Executive reports

Loss Event	Annual Expected Loss (\$)	Loss (in Days of Revenue)	Event Contribution (%)
Loss of Confidentiality	\$3,815,210	5.1	62.0%
Initial Access Vector (IAV)	Annual Expected Loss (\$)	Loss (in Days of Revenue)	Event Contribution (%)
Exploitation Of Remote Services	\$1,834,123	2.5	30.7%
Remote Services	\$1,716,350	2.3	28.8%
External Remote Services	\$724,885	1.0	12.1%
Phishing	\$477,483	0.6	8.0%
Drive-By Compromise	\$463,390	0.6	7.8%



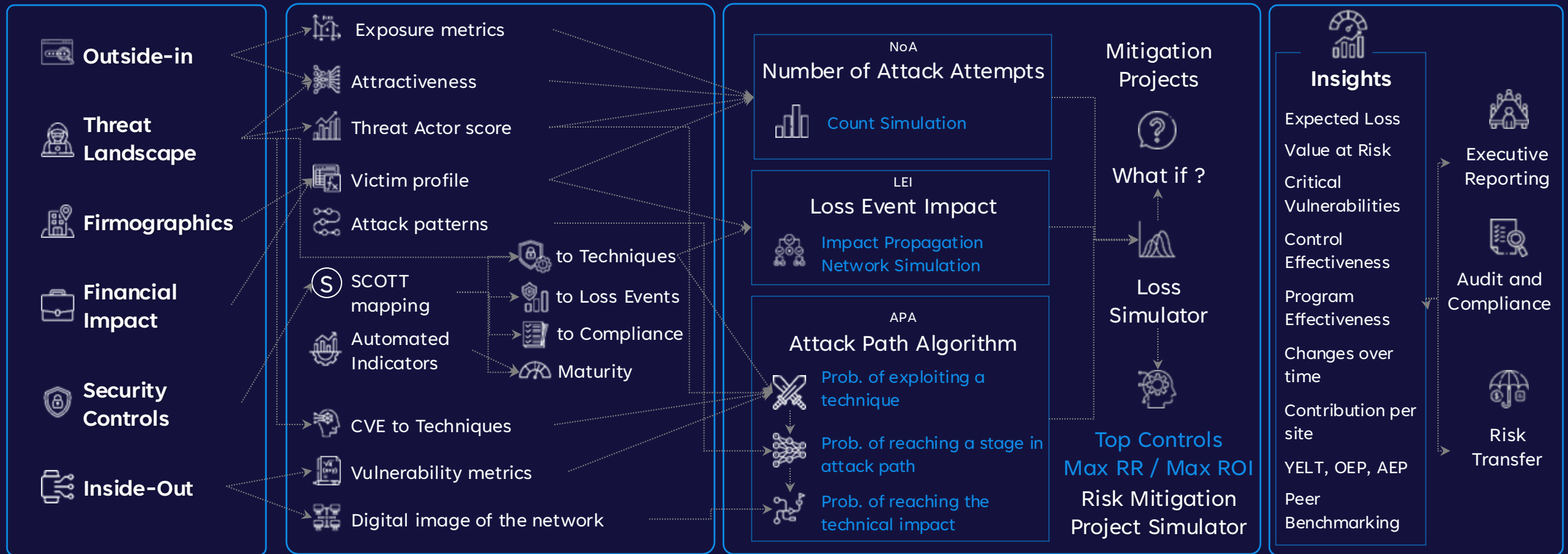
# DeRISK™ | Data Science Life Cycle

## Data Collection

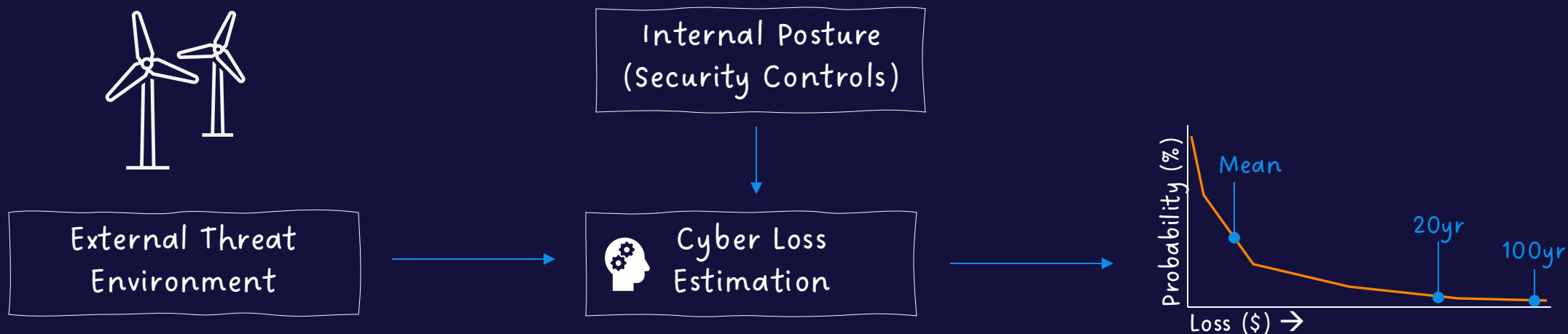
## Measurements

## Modeling

## Reporting



# Case Study: Energy - Wind Renewables

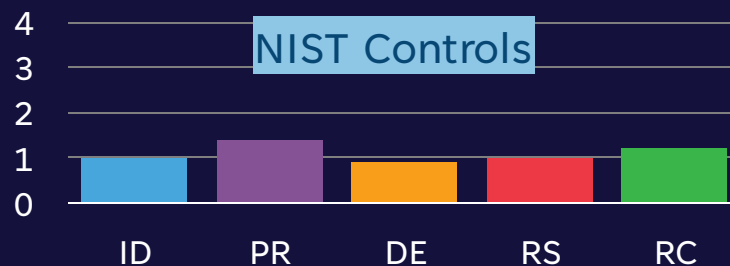


## Background

- Low frequency of incidents in this subindustry
- Low attractiveness

## Security Controls

- Maturity: Basic
- Significant vulnerabilities



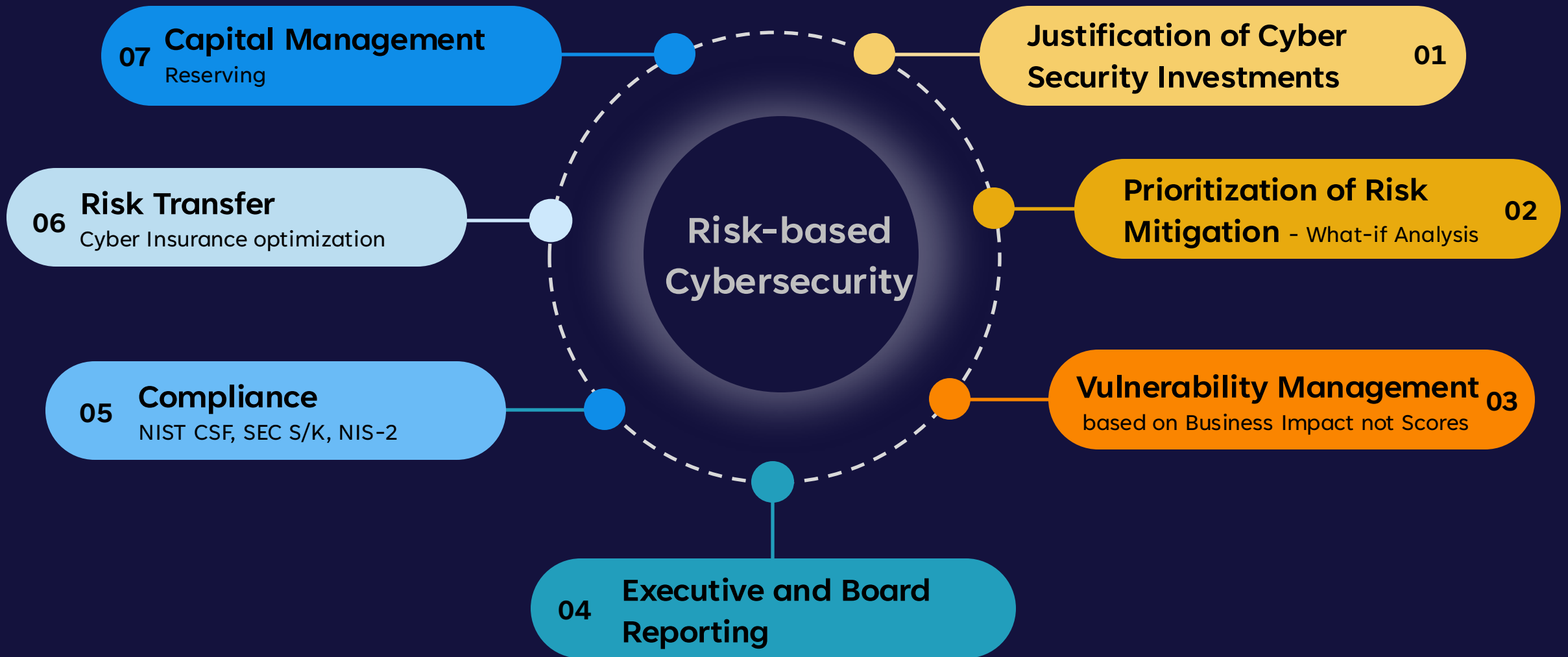
## Estimated Loss

- Mean: 5.7% of Revenue
- 20yr: 21% of Revenue
- 100yr: 140%

## Best Mitigation Projects

- 1) Backup & recovery plan
- 2) Hardening / better controls

# Use Cases







# Cybersecurity Incident Compendium

# Cybersecurity Incident Compendium

An enriched knowledge base on industrial incidents with a cyber risk focus

DeNEXUS

## DKC Industrial Incidents

This dashboard shows information about industrial cyber incidents retrieved from several public databases about OT cyber incidents.

Elaboration: DKC Benchmark Team. Last update: Feb 28, 2024

denexus-uswest2 rr@denexus.io

---

### Section 1

#### Explore Cyber Incidents across all Data Sources

Select one or more DATA SOURCES  
NOTE: The same incident can be found in multiple data sources

EUROREPOC X ICSSTRIVE X KONBRIEFING X TISAFE X CISSM X

Select one INDUSTRIAL VERTICAL  
NOTE: Same incident can target more than one vertical

Contains

Pick a TIME period  
Select one year period

2023-01 → 2024-02

#### Data Sources

OT Cyber Incidents

- ICSStrive
- TISafe

General Cyber Incidents

- Jam Cyber
- Kon Briefing
- CISSM
- EuRepec

---

#### Cyber Incidents by YEAR and DATA SOURCE

Total number of cyber incidents in each source

Year	Source	Count
2024	EUROREPOC	114
	KONBRIEFING	136
	TISAFE	20
	CISSM	1,714
	EUROREPOC	666
2023	CISSM	1,714
	EUROREPOC	666
	ICSSTRIVE	278
	KONBRIEFING	1,852
	TISAFE	84

#### Cyber Incidents by MONTH and DATA SOURCE

Number of incidents in the selected data source per year. NOTE: 19\*\* indicates and "Before 2000", 18\*\* indicates unknown). Remember that data sources have different scopes and update frequencies.

#### Last UPDATE

Last date of data extraction from the original sites

source_database	Totals
CISSM	2024-01-15
EUROREPOC	2024-02-28
ICSSTRIVE	2024-01-29
KONBRIEFING	2024-02-19
TISAFE	2024-02-19
<b>Totals</b>	<b>10120</b>

---

#### Cyber Incidents Details

Use keywords to filter the list of cyber incidents

# Cybersecurity Incident Compendium

Why?

## Cyber Incidents Databases

Websites on the open Internet are the main sources of cyber incident data.

All of them publicly available sources, free of charge, without any restrictions or required credentials.

European Repository of Cyber Incidents

HACKMAGEDDON  
Information Security Timelines and Statistics

SEC | EDGAR

ICS STRIVE  
INDUSTRIAL CONTROL SYSTEM  
COVERING SECURITY, THREATS, REGULATIONS, INCIDENTS, VULNERABILITIES WITH EXPERTS

Ti Safe Incident Hub  
Industrial Cybersecurity Incidents Database

UNIVERSITY OF MARYLAND  
18 56  
CISSM CYBER ATTACKS DATABASE

**Kon Briefing**

*and more*

Lack of consistency

Partial view

Unstructured data

# Cybersecurity Incident Compendium

## What?

UPDATED STRUCTURED DATA on disclosed cyber incidents

Enriched **KNOWLEDGE BASE** on attack and victims

Leveraging **DATA ANALYTICS** Tools + **ML** + **AI**

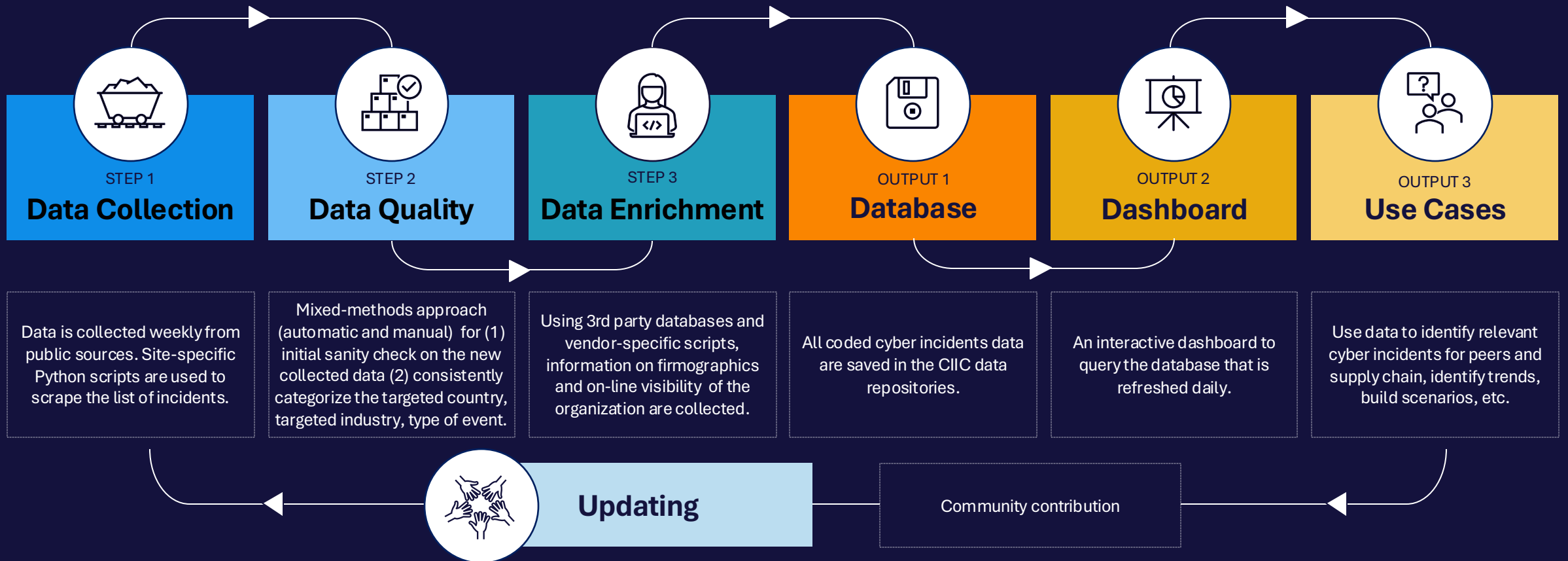
**DYNAMIC REPOSITORY** for data analysis and knowledge sharing





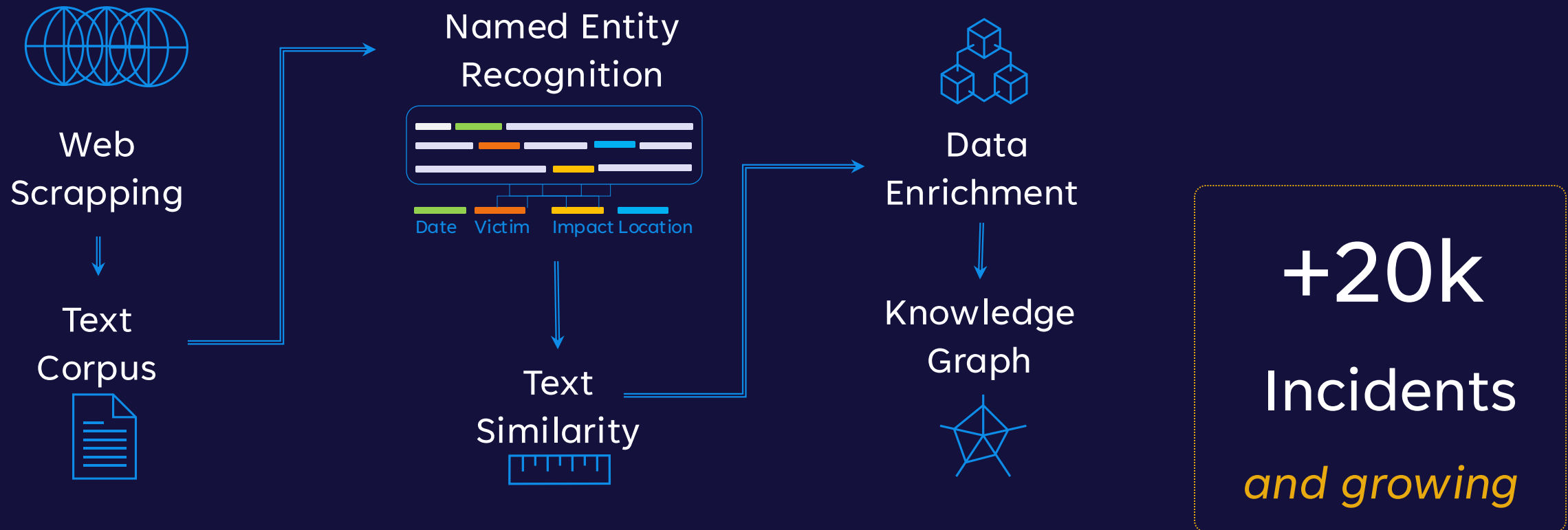
# CIC Data Science Life Cycle

## How?



# CIC & ML/AI

## Analytics in Disclosed Cyber Attacks



NER to Descriptions and News

# CIC & ML/AI

## Attractiveness to cyber attacks



Hidden patterns / Attractiveness



Victim

No Victim

93% Train  
92% Test

The more significant the attractiveness, the greater the risk of cyber incidents

# Cybersecurity Incident Compendium

#UAXMakers

How do cyber threats **EVOLVE** by region, sector and type?

**EXPECTED ATTACKS** next month/year by region, sector?

What makes a company more **ATTRACTIVE** to attackers?

Who is exploited, what are the **IMPACTS**? How many **CLAIMS**?

*and more*





DE  NEXUS™

[denexus.io](https://denexus.io)

THANK YOU