



Leveraging Data AI for Cyber Risk Management

How Data Science is Changing the Game

The Challenge

CISOs and CFOs lack insights to justify and make informed decisions about cybersecurity investments and cyber risk priorities

\$215 Billion^[1]

annually spent on Cybersecurity

\$20 Billion^[2]

annually spent on Cyber Insurance

With no financial analysis of cyber risk priorities or best approach
Industrial environments (OT) have even less information

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

— Peter F. Drucker

Cyber Risk Management

Risk-based Cybersecurity & data-driven Risk Management based on business impact





**Full-stack Cyber Risk Management
for Industrial Enterprises &
Physical Critical Infrastructures**

5-D Rule for Cyber Risk Management

Dynamic

Distributed

Defensible

Data-driven

Decision-enabling

Cyber-Physical Systems & Industry Verticals

RENEWABLE ENERGY



THERMAL ENERGY



TRANSMISSION



MANUFACTURING



DATA CENTERS



TRANSPORTATION



Information Security (Infosec) Fundamentals

IT Security

Protecting data & systems

- 1) Confidentiality
- 2) Integrity
- 3) Availability



ICS/OT Security: IT + PHYSICAL

Protecting digital systems that control physical assets



- 1) Safety
 - 2) Observability (inputs: sensors)
 - 3) Controllability (outputs: actuators)
 - 4) Availability
 - 5) Integrity
 - 6) Confidentiality
- } Priorities are reversed

What is financial quantification of cyber risk?

Estimating financial loss of a cyber-attack affecting ICS/OT

What is Quantification of Cyber Risk?

“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”

A screenshot of the Gartner website showing the 'Cyber-Risk Quantification' page. The page header includes the Gartner logo and navigation links: Information Technology, Insights, Expert Guidance, Tools, and Connect with Peers. Below the header is a breadcrumb trail: 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.'

Not Qualitative BUT Quantitative Analysis. It's Cyber Risk in \$\$\$ Values

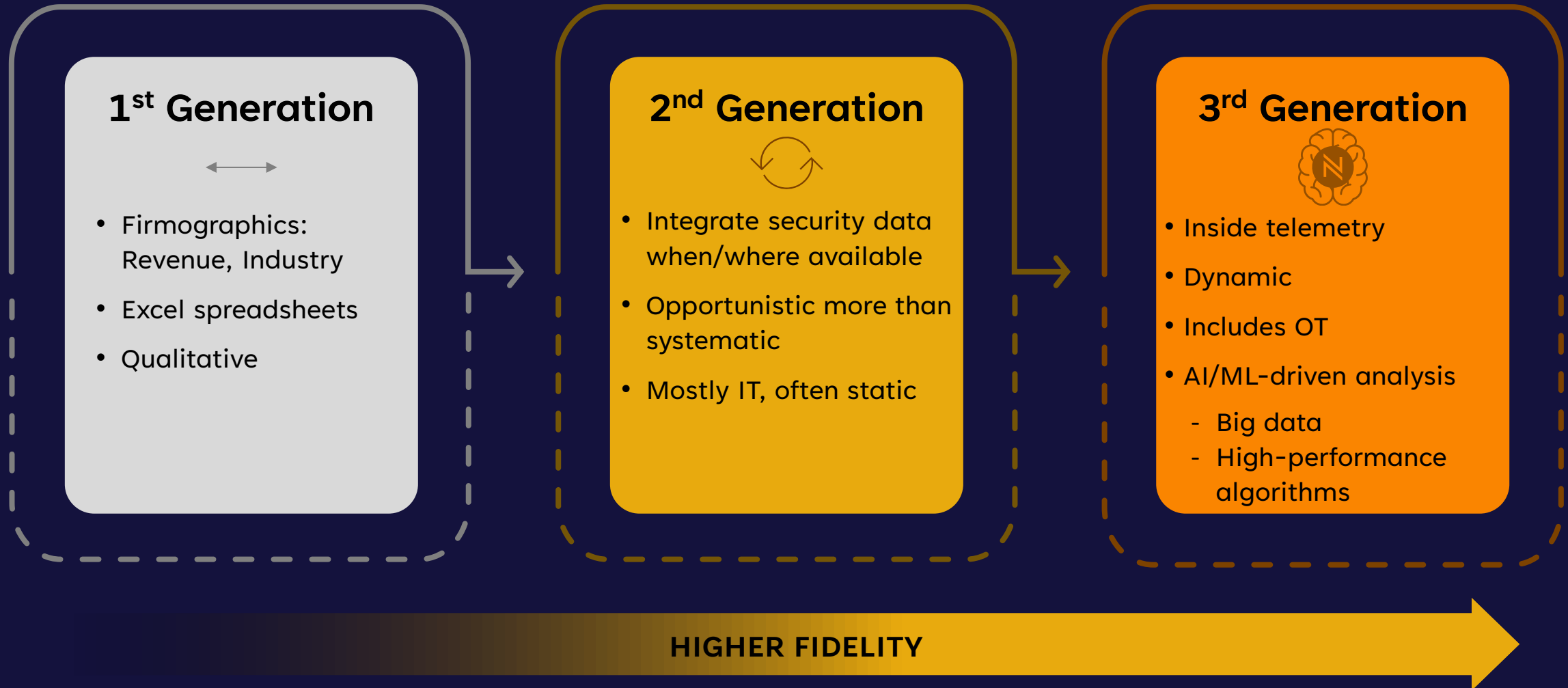
It's Cyber Risk in



Values

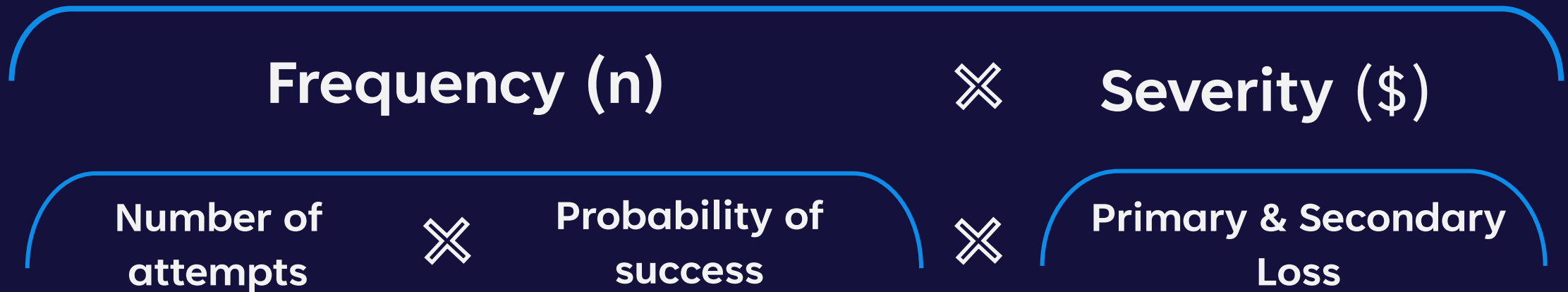


Quantitative Approach to Cyber Risk



Quantitative Approach to Cyber Risk

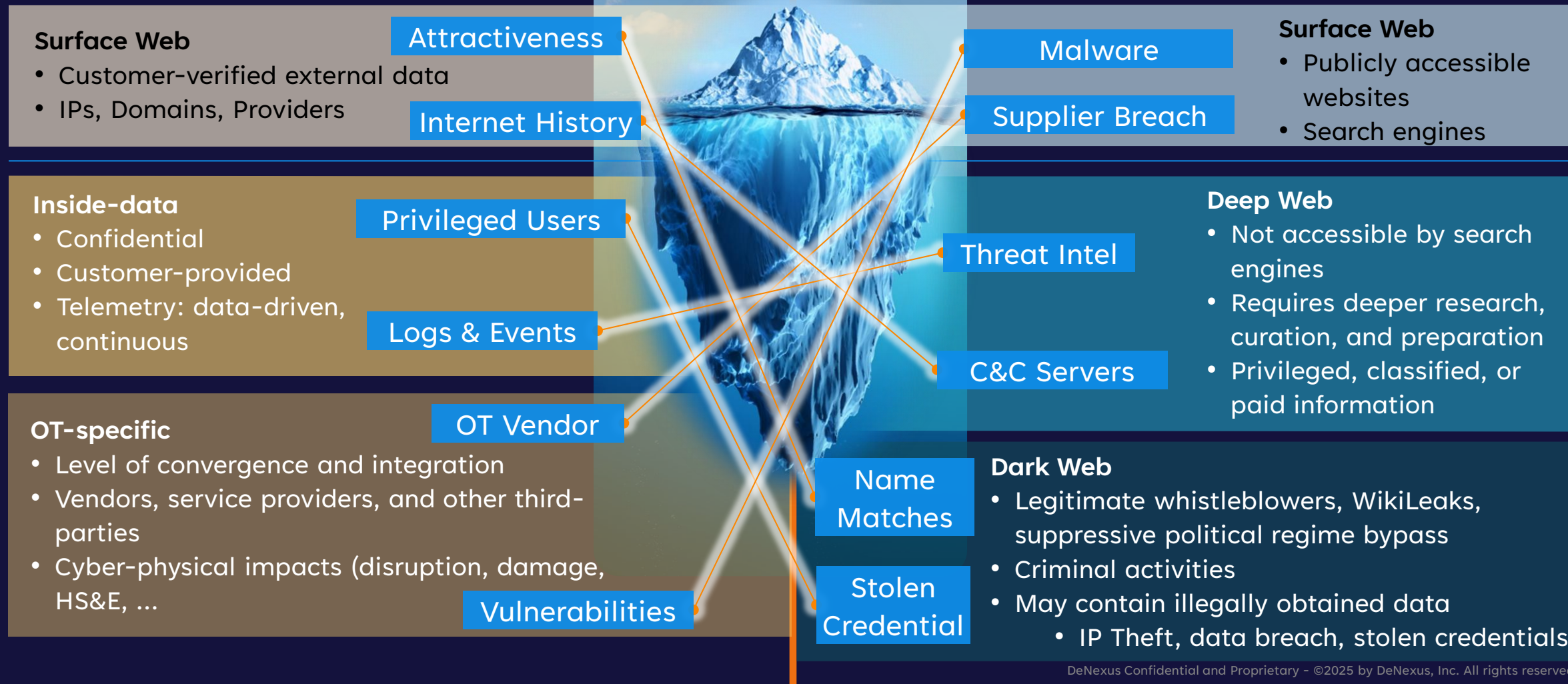
Cyber Loss (\$) from Operational Technology



Probability of Success is driven by how the OT is Network is Built and Protected

Leverage Data for cyber risk management

Inside-data | Outside-data



Data from Internal OT Telemetry

Remote Access

Patch Installed

Firewall Rules

Network Topology

Cyber Asset Inventory

USB Inserted

Communications
Matrix / Links
(Who talks to who?)

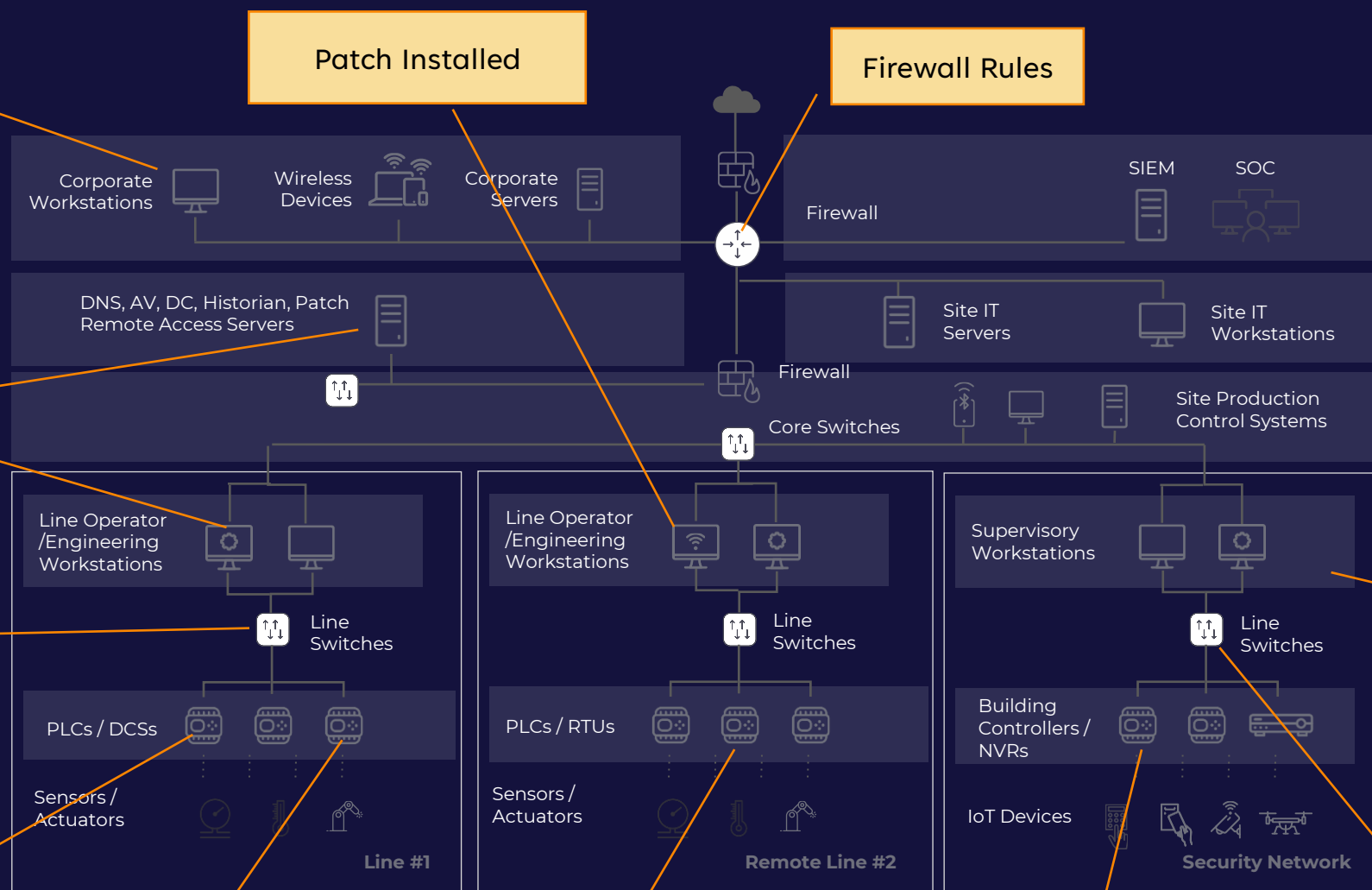
Network Anomaly

Make, Model, Version

Vulnerabilities, CVEs

Communication
Baseline

End of Life



Level 5
Enterprise IT Networks
and Data Centers

Level 4
Site IT Networks

Level 3 and Level 3.5
Site Operations Control
and ICS-Demilitarized
Zone (DMZ)

Level 2
Area Supervisory
Control

Level 1
Control Network

Level 0
Field Network

Subnets

DKC - Data Available

Outside-in Data



Inside-out Data



Firmographics and Financial Data



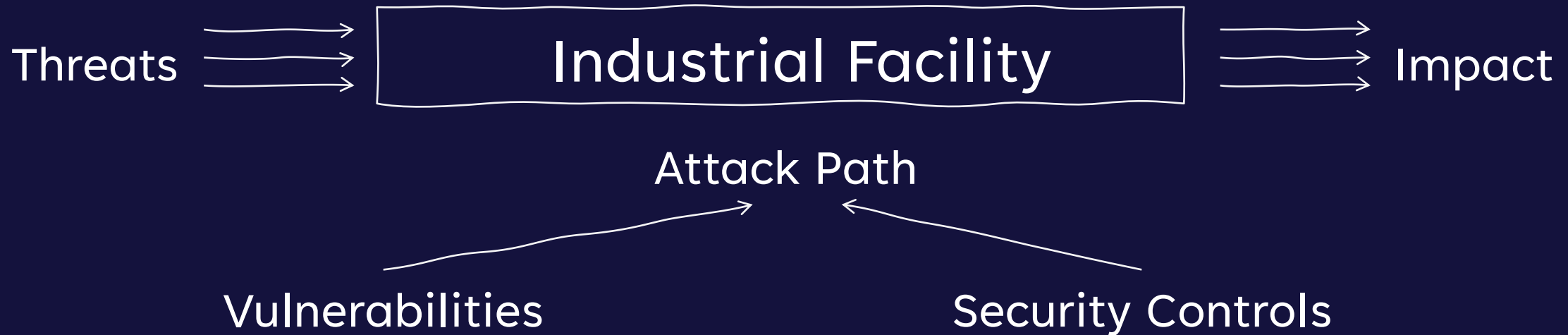
Cyber Incidents Data



Metadata



Modeling the OT Network and Attacks



Frequency (n)

Number of
attempts



Probability of
success

Severity (\$)

Primary & Secondary
Loss

Leverage Data for cyber risk management

Modeling the OT Network and Attacks

Real Environment

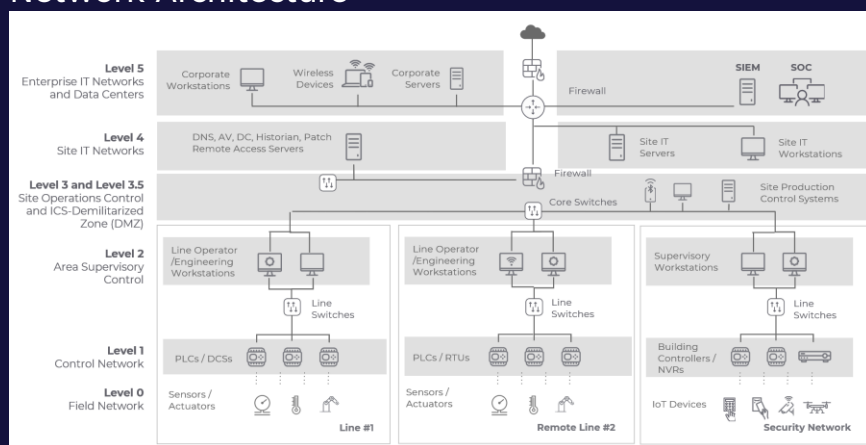
Cyber Threat Landscape



Vulnerabilities & Technical Debt

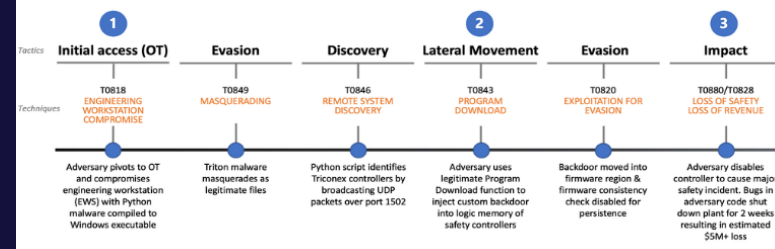
	Critical	High	Medium	Low	Exploitable
1999 - 2004	1	9	61	3	42
2005 - 2009	9	15	34	34	20
2010 - 2014	67	234	272	6	175
2015 - 2019	96	225	234	3	160

Network Architecture

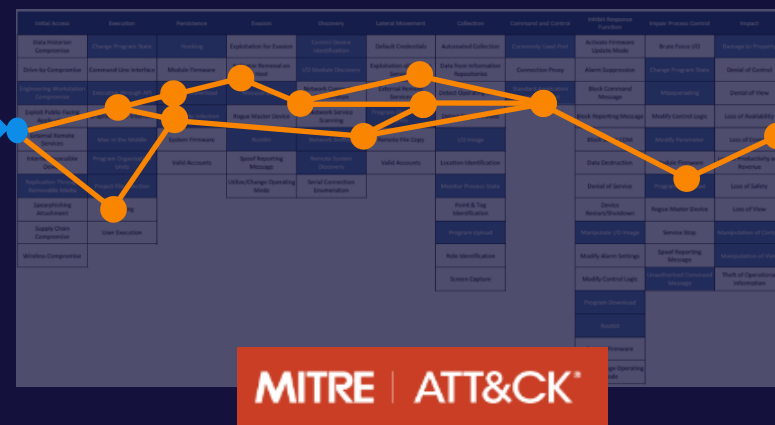


Digital Twin - for Simulation

Mapping the TRITON kill-chain to MITRE ATT&CK for ICS

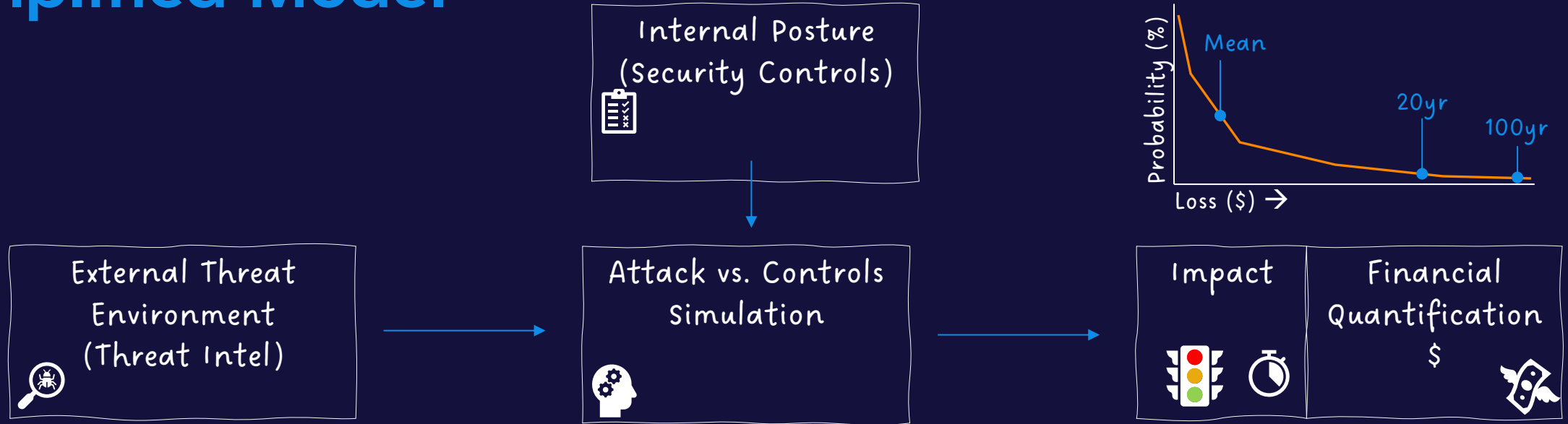


Initial Access



Cyber Impact

Simplified Model



Cyber Threat Intelligence

- Actors, Malware, TTPs, CVEs, EPSS, Skill
- Victimology
- Cyber Incident history

How many attacks?

Attack Simulation

- Evaluate effectiveness of
 - cyber safeguards & vulnerabilities, versus
 - threat landscape

Can incident propagate to loss event?

Financial Quantification

- Transform incidents into financial losses
 - Probability & Impact
- Continuously assess risk

What is the financial impact?

Cyber Risk Modeling

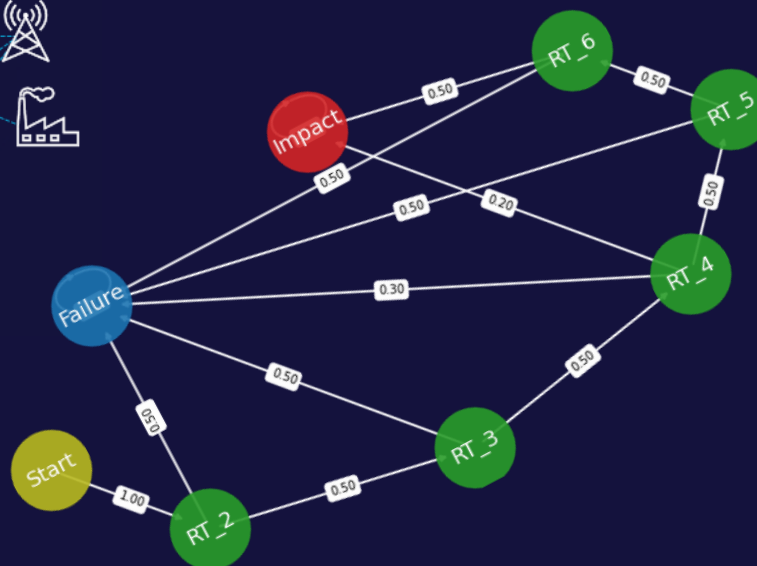
How many attacks?



Count processes with
Bayesian Inference

Powered by
Outside-in Data

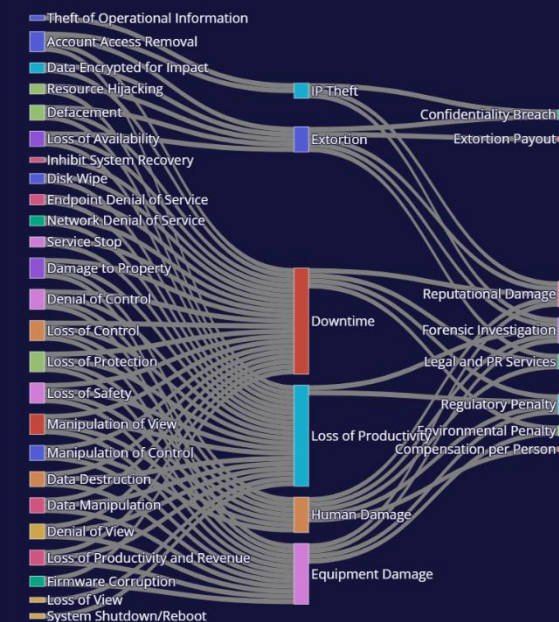
Can incident propagate
to loss event?



Absorbing Markov Chain Models
Branched Random walks

Powered by
Inside-Out & Outside-In Data

What is the financial
impact?



Graph analytics
Stochastic optimization with simulated
annealing

Powered by
Business-Risk-Loss Data

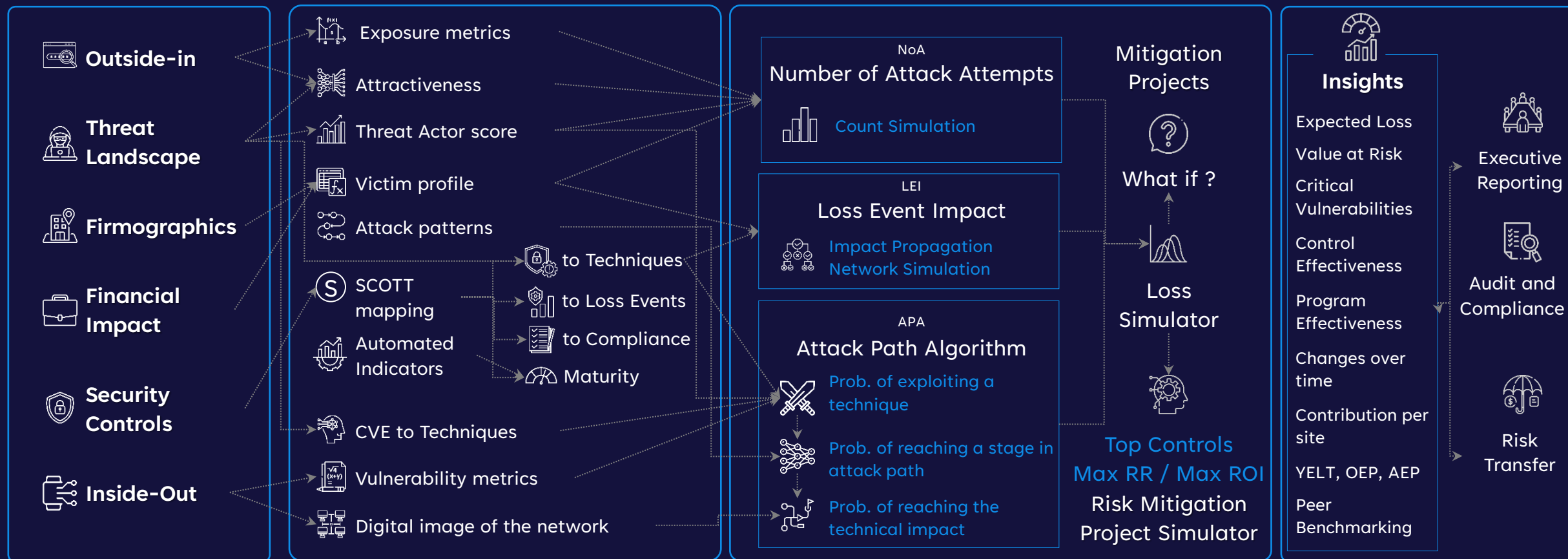
Data Science Life Cycle

Data Collection

Measurements

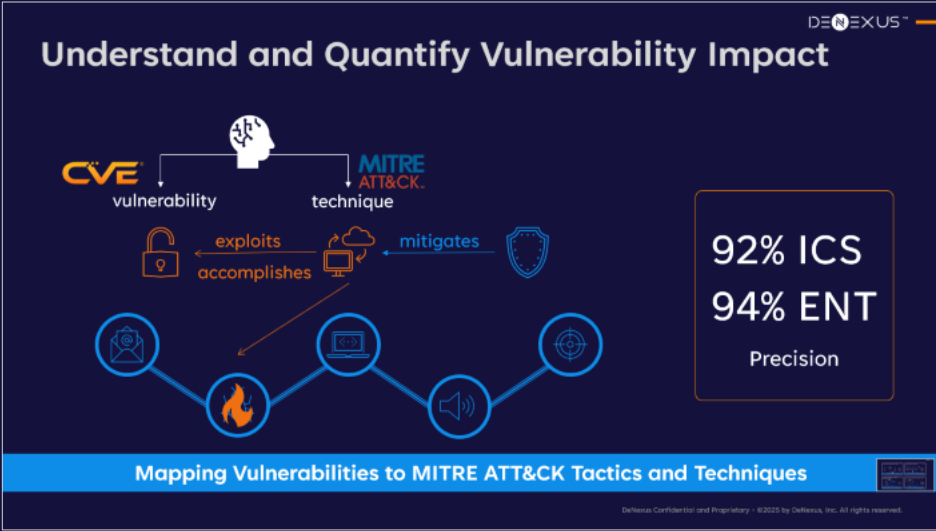
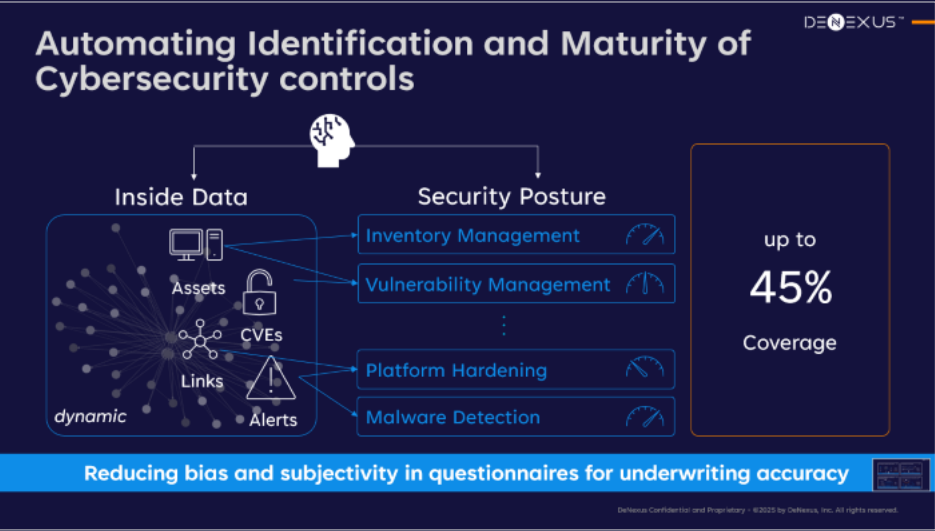
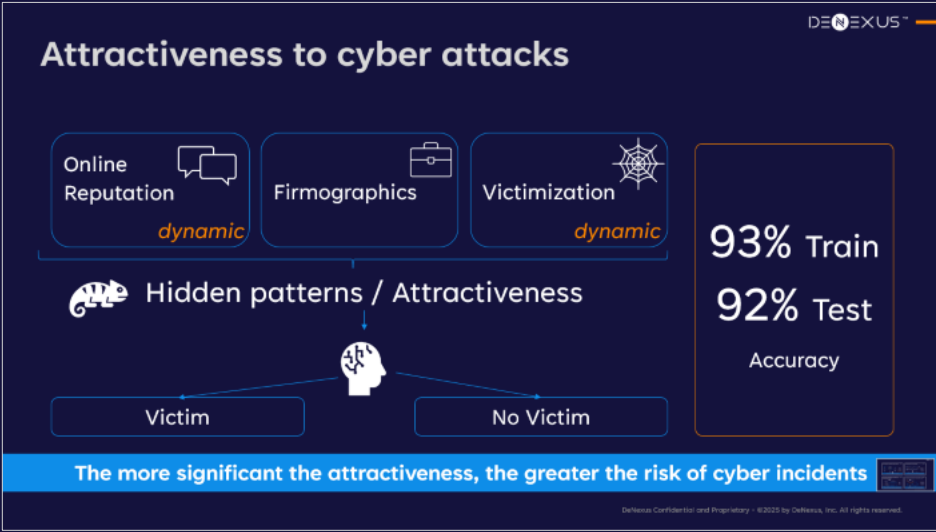
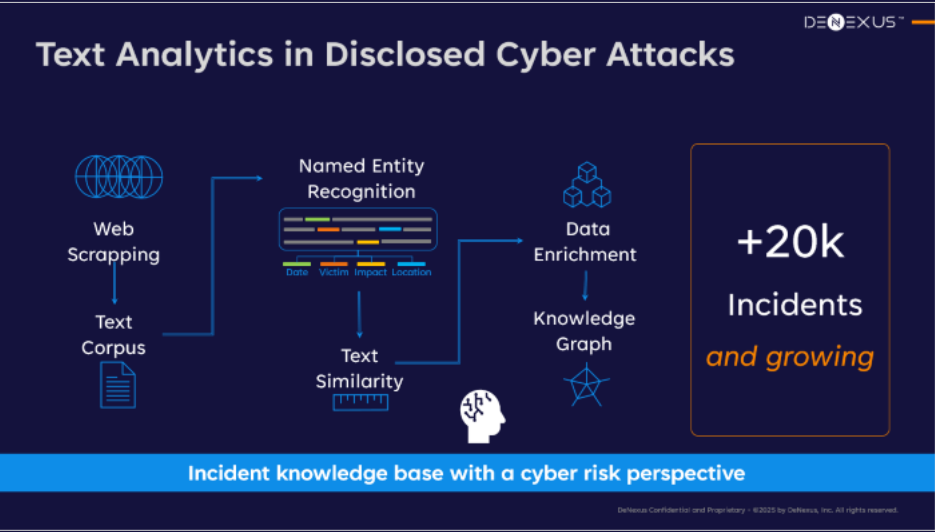
Modeling

Reporting

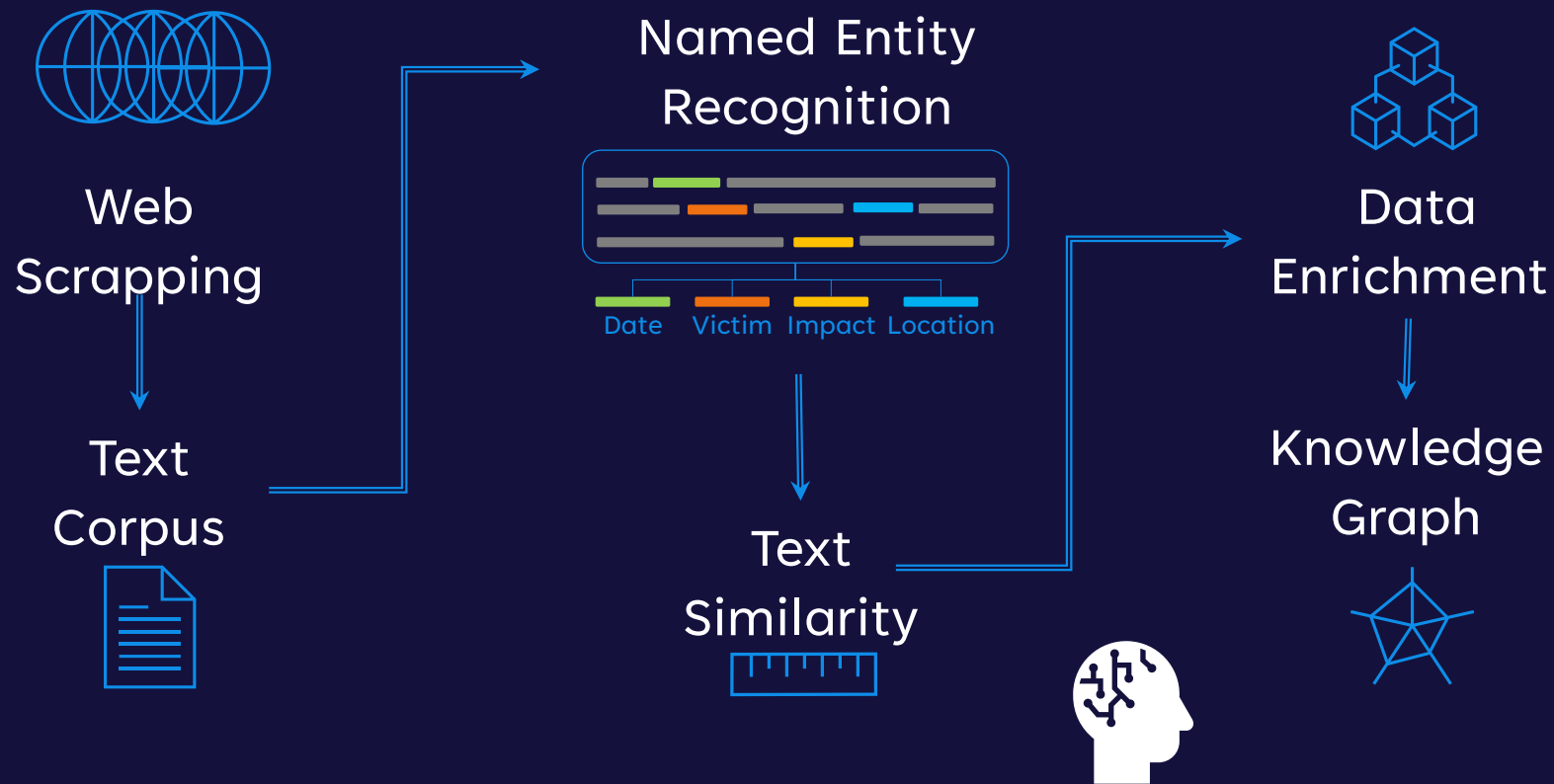


Leveraging data for 3rd Gen CRQM

Estimating financial loss of a cyber-attack affecting ICS/OT



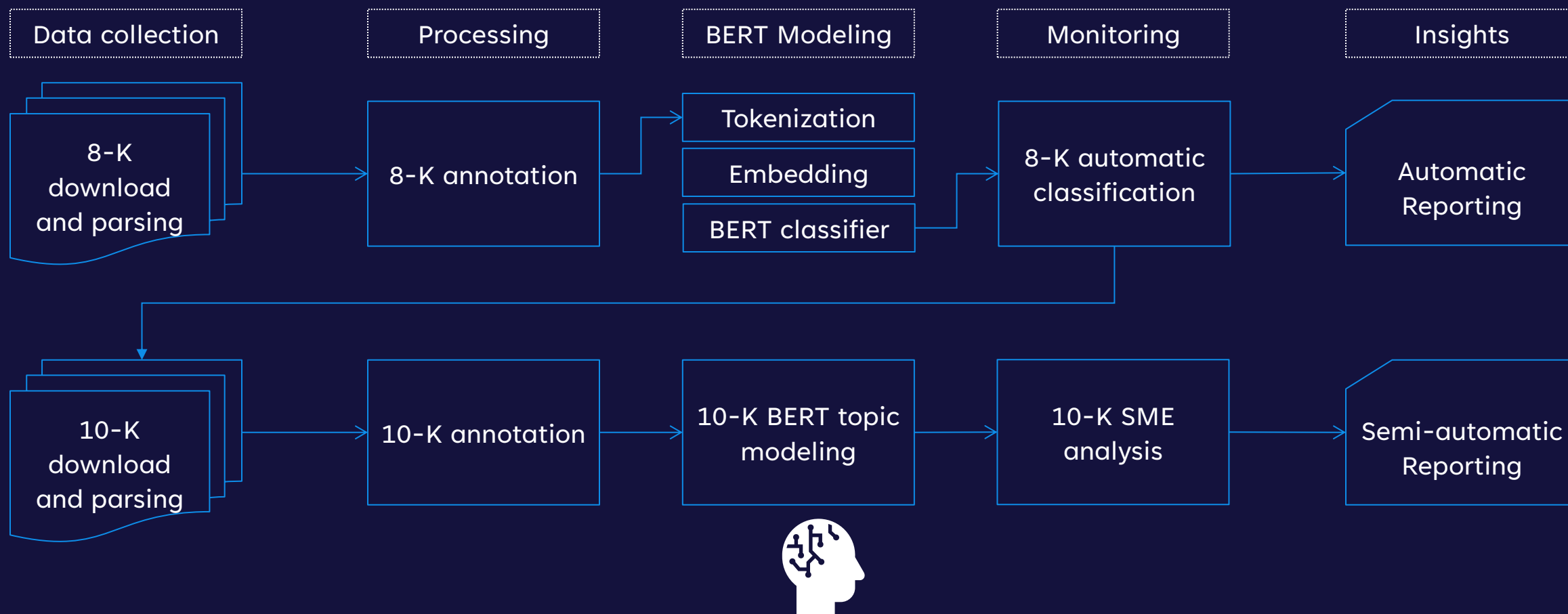
Text Analytics in Disclosed Cyber Attacks



+20k
Incidents
and growing

Incident knowledge base with a cyber risk perspective

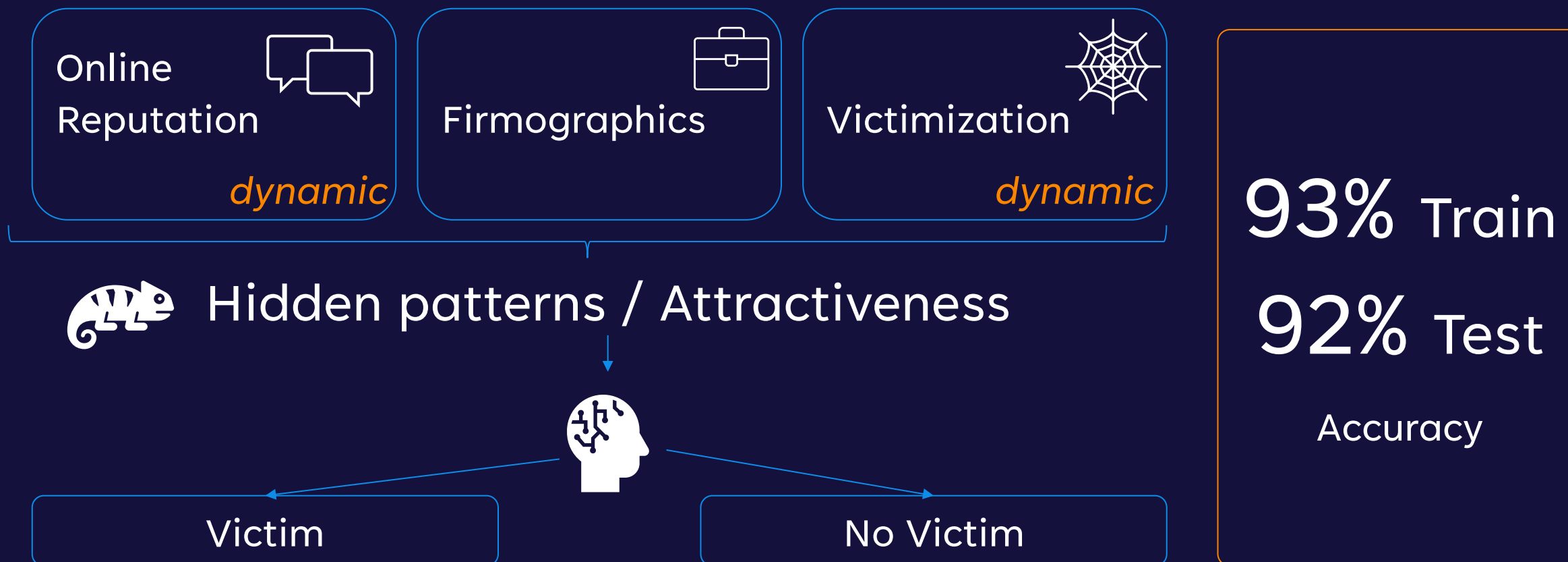
Intelligent Monitorization of SEC 8-K



CRQ provides immediate guidance to decide what to disclose

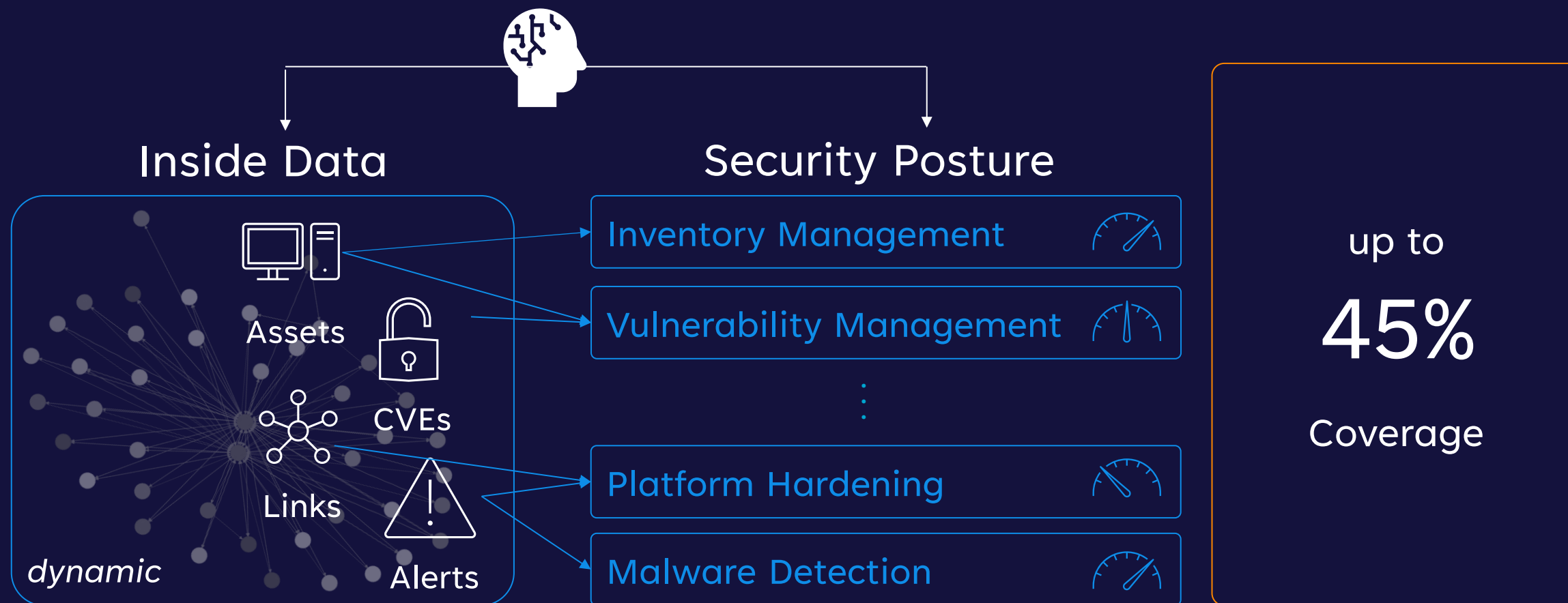


Attractiveness to cyber attacks



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

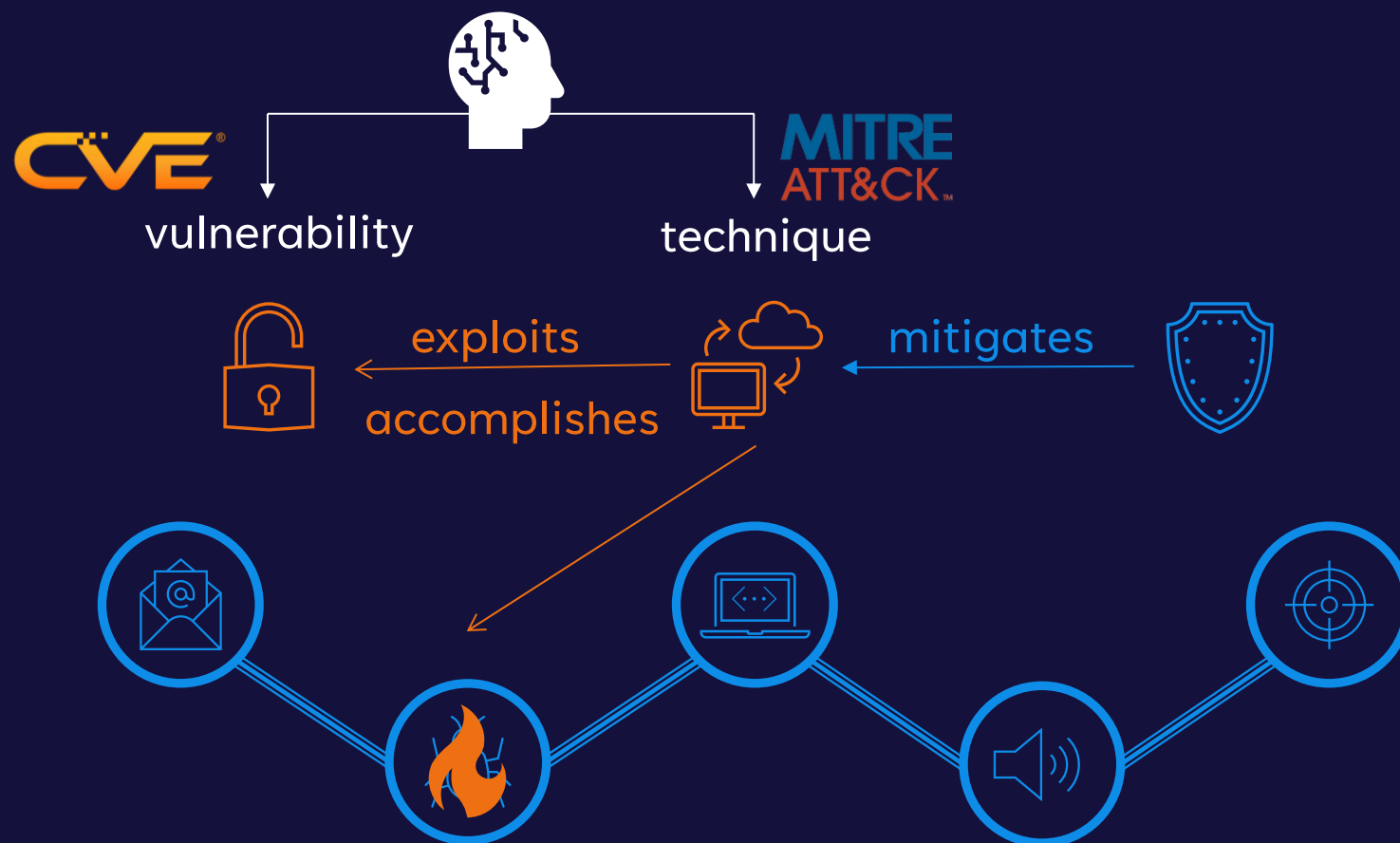
Automating Identification and Maturity of Cybersecurity controls



Reducing bias and subjectivity in questionnaires for underwriting accuracy



Understand and Quantify Vulnerability Impact



92% ICS
94% ENT
Precision

Mapping Vulnerabilities to MITRE ATT&CK Tactics and Techniques





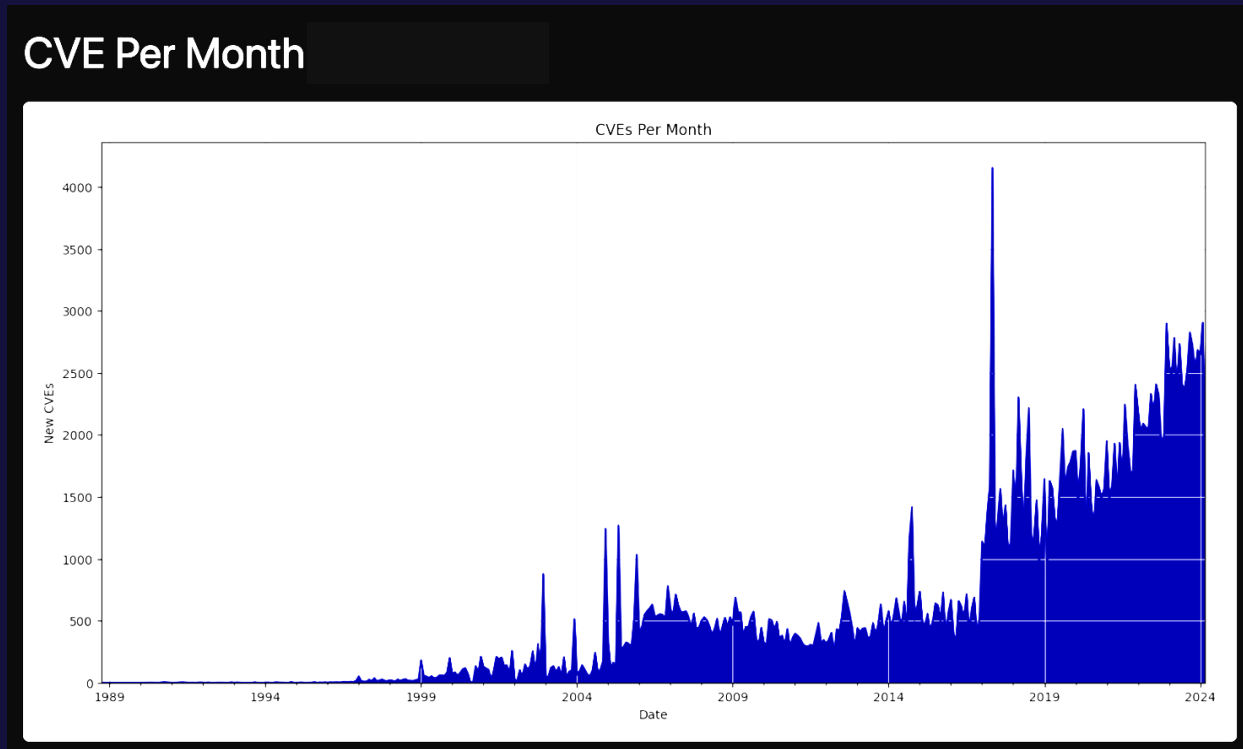
With AI, Cyber Risk Mitigation does not have to be a Guessing Game

Translating Vulnerabilities (CVEs) into Dollars at Risk
True Risk-Based Vulnerability Management



Thousands of Vulnerabilities in the wild and in OT networks

Growing exponentially



Scoring Mechanisms translated into Heatmaps not telling the entire story

What to remediate first to reduce dollars at risk?

CVSS (severity)

EPSS (likelihood/probability of exploitation in the wild)

KEV (known exploited)

Distribution of all vulnerabilities by CVSS Scores

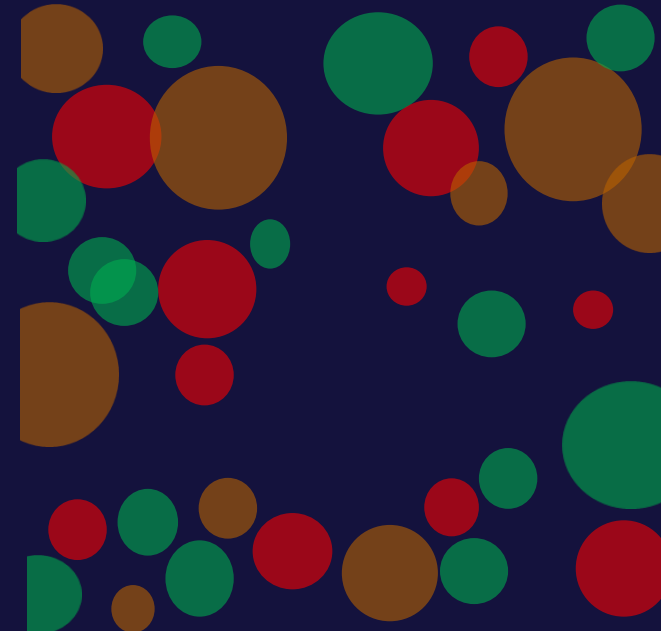
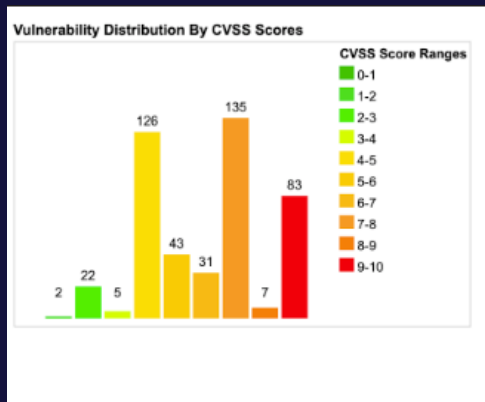
CVSS Score	Number Of Vulnerabilities	Percentage
0-1		0.00
1-2	2	0.40
2-3	22	4.80
3-4	5	1.10
4-5	126	27.80
5-6	43	9.50
6-7	31	6.80
7-8	135	29.70
8-9	7	1.50
9-10	83	18.30
Total	454	

Weighted Average CVSS Score: **7**

Today's Vulnerability Environment

Limited to No Context Roles of Devices & Cybersecurity Controls Business

- How much does red 9 cost over orange 7?
- If I fix 2 oranges does that equal one red?
- How are we sure 3-4 green is not that bad?



Take Control with Value at Risk Simulation

Using DeRISK™

- Portfolio, Facility or Zone Level analysis
- Context for the business
 - TOP 10 vulnerabilities -> \$5M Value at Risk
 - Address these 10 Vulnerabilities to reduce exposure by 40%
 - Let your insurer know that you have addressed \$20M in exposure this year prior to renewal

Top 10 Vulnerabilities Contributing to Loss

IDs and External Data								Annual Loss		VaR 95th	
Vulnerability ID	Vendor	Role	Network	Device Count	CVSS	EPSS	Mean Age (days)	\$	% Contribution	\$	% Contribution
CVE-2008-2976	30805, Cisco	windows_pdc	Corporate	78	5.6	0.742	666	\$977,646	91%	\$44,358	57%
CVE-1999-0362	VMware, Inc.	other	DMZ	29	9.8	0.922	913	\$977,637	100%	\$250,280	96%
CVE-2013-1793	Schneider (ION8650)	rtu	DMZ	1	2.0	0.955	321	\$963,249	94%	\$273,911	87%
CVE-2009-4921	VMware, Inc.	other	DMZ	4	3.4	0.005	527	\$844,153	64%	\$92,582	18%
CVE-2013-1793	Osisoft (PI)	historian	DMZ	44	4.7	0.752	505	\$707,426	12%	\$128,825	96%
CVE-2009-1678	Private	other	IoT	24	9.1	0.015	552	\$689,998	41%	\$360,593	40%
CVE-2012-6612	LiteON	Engineering Station	Corporate	65	5.6	0.047	578	\$605,731	75%	\$335,886	51%
CVE-2008-4843	Rockwell	plc	Corporate	97	3.3	0.568	319	\$527,281	31%	\$465,284	6%
CVE-2014-3156	30805, Cisco	unknown	IoT	28	7.8	0.407	817	\$446,117	21%	\$188,477	66%
CVE-2014-9560	, Cisco	ghost	Corporate	32	0.4	0.543	164	\$395,564	65%	\$115,231	33%



Practical, Data-Driven and Business-Oriented Solution to Prioritize CVEs

What could an attacker achieve by exploiting a vulnerability?

Common Vulnerabilities
and Exposures (CVEs)

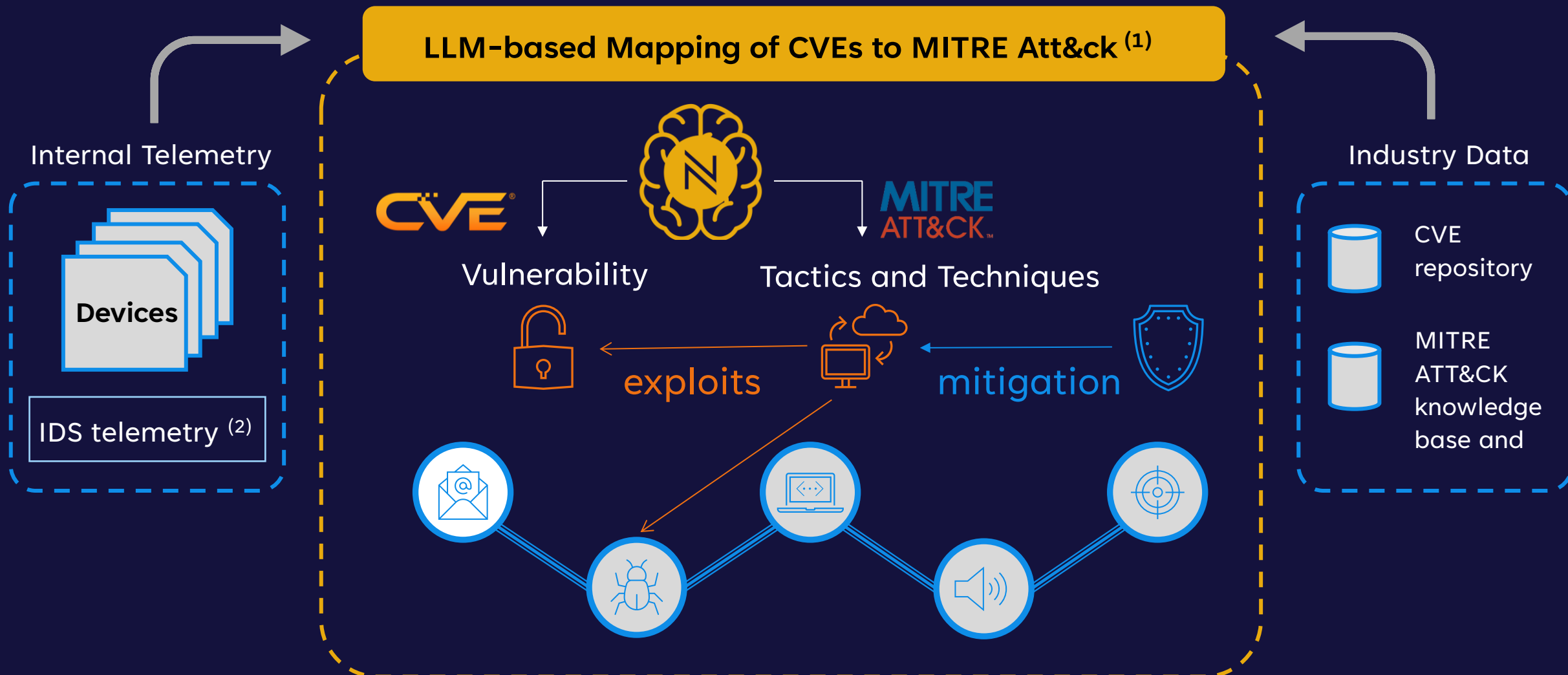


MITRE ATT&CK Tactics,
Techniques, and
Procedures (TTPs)

Total 271,773 published CVEs from 1988 to 2024-11-29
75% of CVEs are between 2015 and 2024



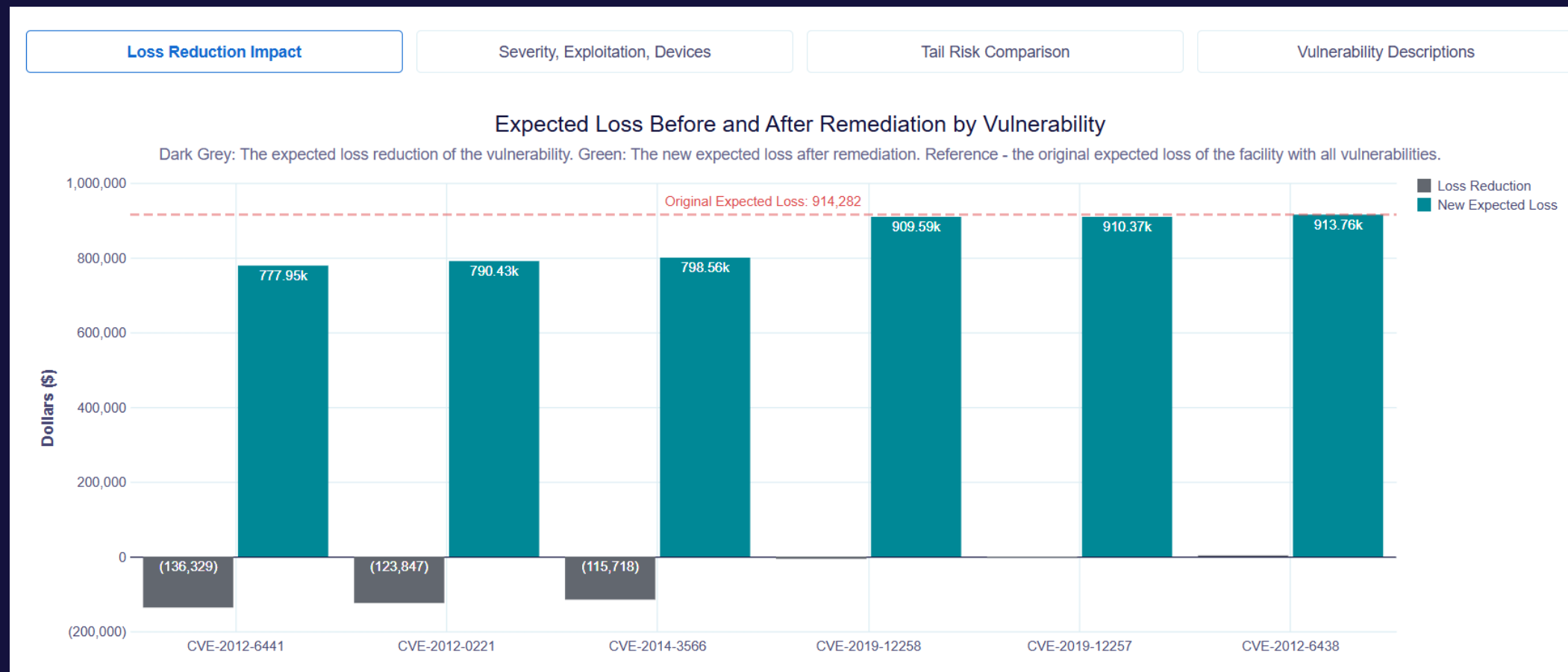
Gen-AI to automate Mapping to MITRE Att&ck



(1) Patents Pending. Mapping to MITRE Att&ck for Enterprise and for ICS

(2) DeNexus' Technology Partners

Expected Loss After Remediation



Vulnerabilities Mapped to Value at Risk

Vulnerabilities & Devices

Annual Expected Loss
(EL, Mean)
\$914,282

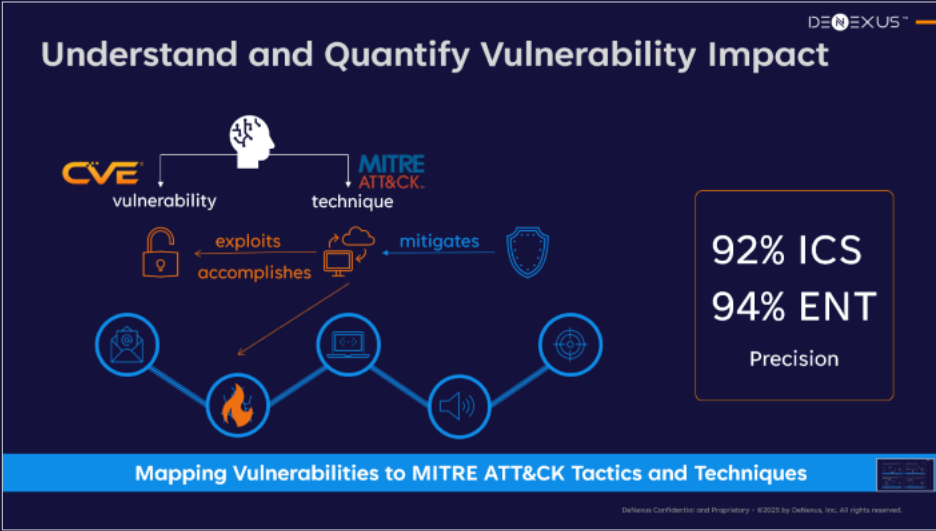
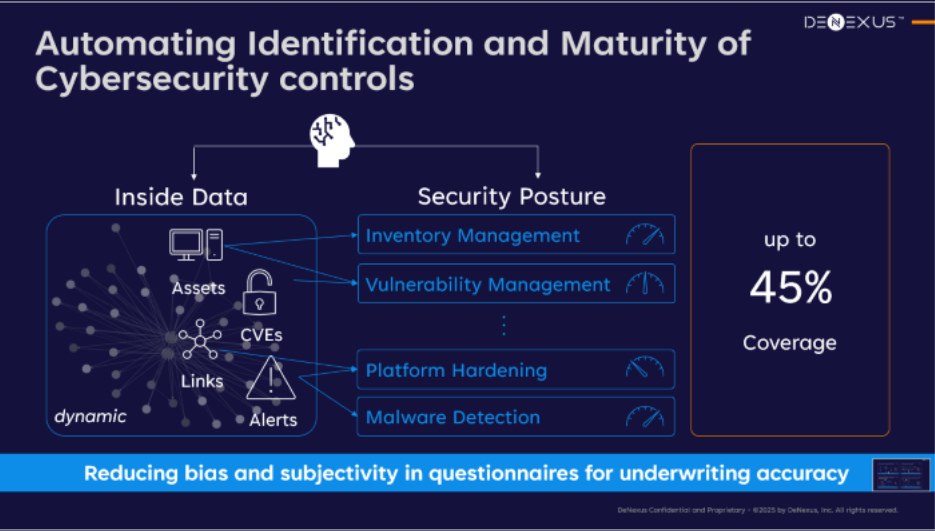
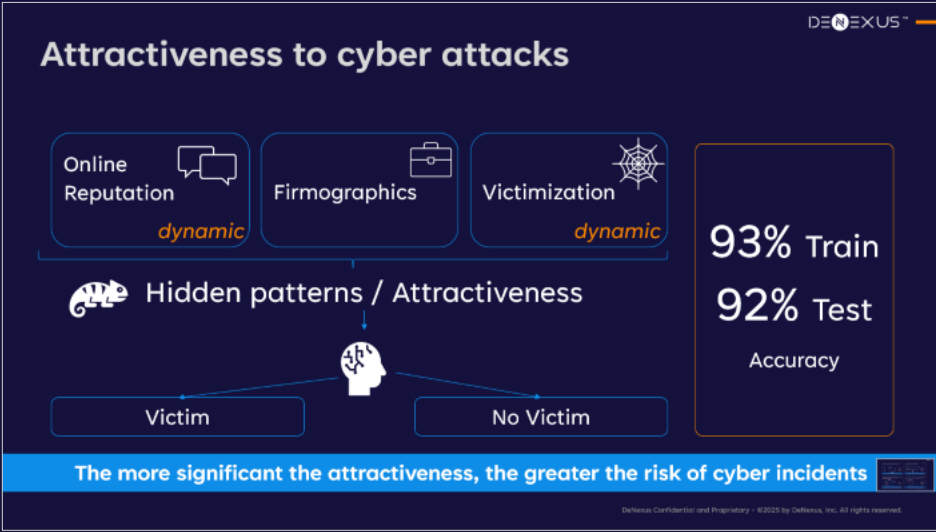
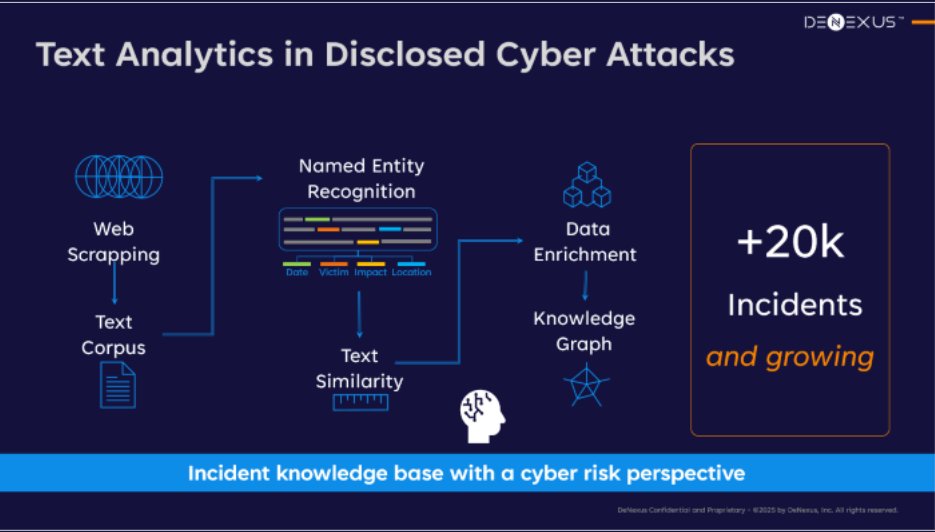
Rare Scenario
1 in 20 years
(VaR 95th Percentile)
\$4,955,816

Extreme Scenario
1 in 100 years
(VaR 99th Percentile)
\$19,879,869

Loss Reduction

The estimated decrease in overall risk when a specific vulnerability is completely eliminated **across all devices** in the system.

Vulnerability ID	Device Vendor	Device Role	Device Networks	Device Count	CVSS	EPSS	EL \$	EL %	VaR 95 \$	VaR 95 %	VaR 99 \$	VaR 99 %
CVE-2012-6441	Rockwell	PLC	...	1	4.0	0.86	(136,329)	-14.9%	(1,110,176)	-22.4	(1,910,963)	-9.6
CVE-2012-0221	Unknown	Master, Slave	...	2	4.0	0.77	(123,847)	-13.5%	(1,004,790)	-20.3	(1,759,633)	-8.9
CVE-2014-3566	Hirschmann (RS20), Hirschmann (Railswitch)	Network Switch	...	149	3.4	0.97	(115,718)	-12.7%	(963,124)	-19.4	(1,552,198)	-7.8
CVE-2019-12258	Hirschmann (Railswitch)	Network Switch	...	19	7.5	0.09	(4,691)	-0.5%	(30,127)	-0.6	(108,274)	-0.5
CVE-2019-12257	Hirschmann (Railswitch)	Network Switch	...	19	9.8	0.92	(3,908)	-0.4%	(29,759)	-0.6	(14,431)	-0.1
CVE-2012-6438	Rockwell	PLC	...	1	6.2	0.93	(524)	-0.1%	(31,422)	-0.6	0	0.0



Computing Systems 3rd Generation

- Privacy preserving
 - Stateless computation of sensitive data
 - Enforced de-identification and full encryption
 - Verifiable transparency
- AI and high-performance
 - Cutting edge GPU and advance networking, to enable complex simulations
 - Realtime analytics and large-scale AI model training

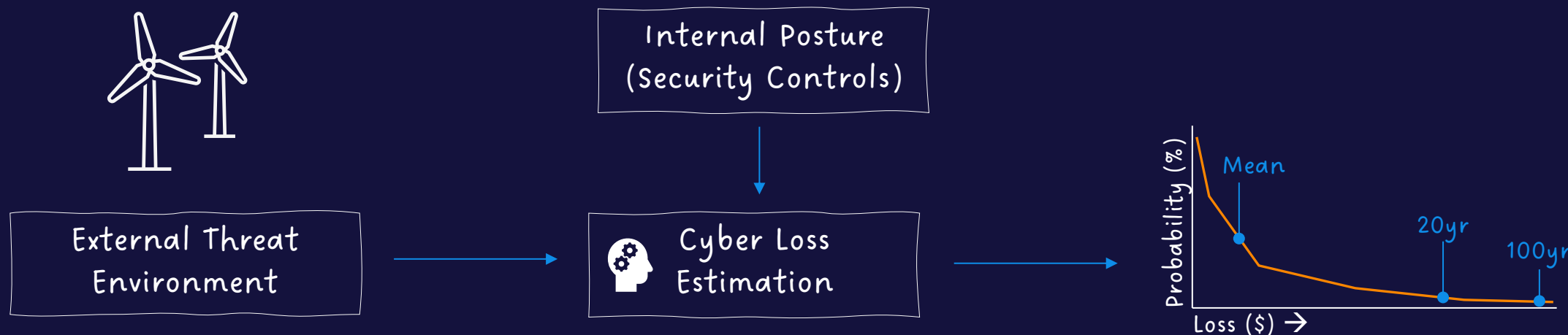
50 Million simulations run weekly on every clients' unit risk

Joined NVIDIA Inception program to keep optimizing models, and computing needs

Financial quantification of cyber risk

Estimating financial loss of a cyber-attack affecting ICS/OT

Case Study 1: Wind Renewables

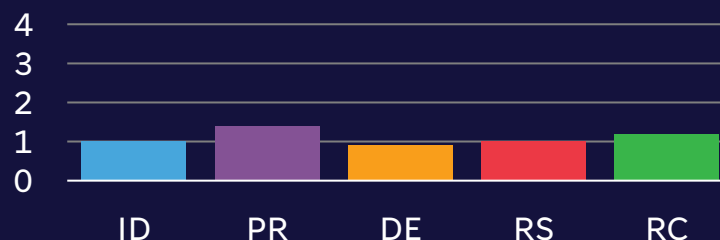


Background

- Low annual revenues
- Low frequency of loss events in this subindustry
- Low awareness of company (low attractiveness)
- Low activity in dark web

Security Controls

- Maturity: Basic
- Significant vulnerabilities
 - CVSS and EPSS



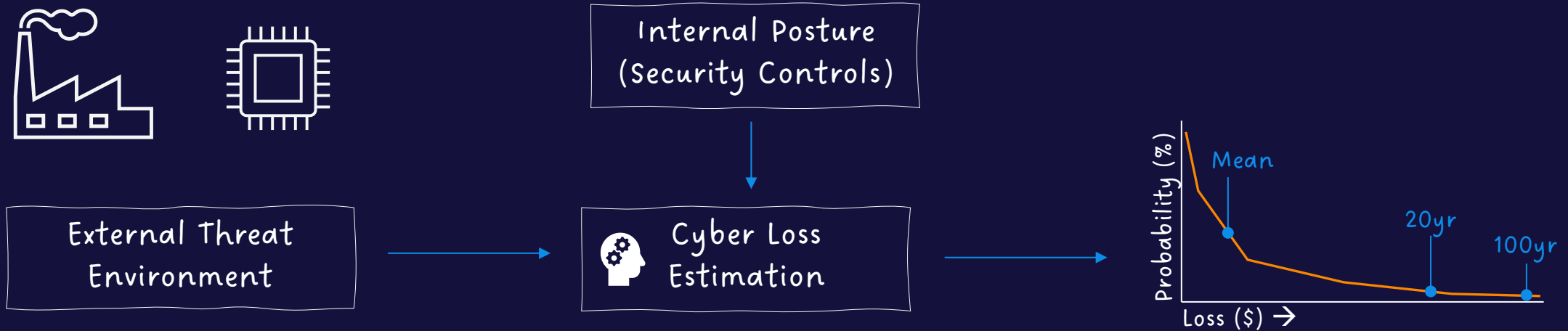
Estimated Loss

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

Best Mitigations

- 1) DRP/BCP
- 2) Technical improvements & hardening

Case Study 2: Electronics Manufacturing

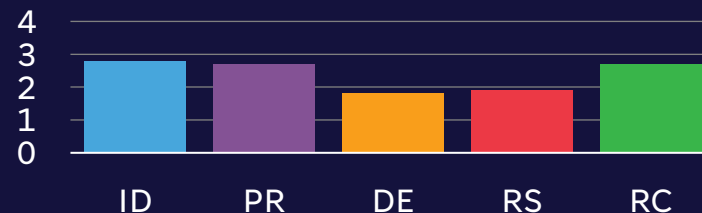


Background

- Very high frequency of loss events in this vertical
- High awareness of company (high attractiveness)
- Moderate activity in dark web

Security Controls

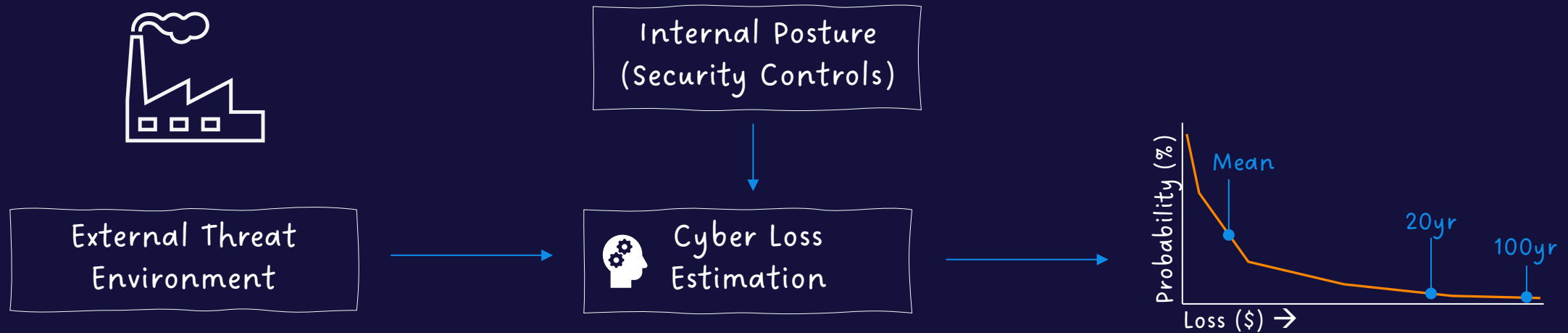
- High maturity in IT
- Medium maturity in OT: Risk-based



Estimated Loss

- Mean: 0.45% of Revenue
- 20yr: 0.46% of Revenue
- 100yr: 13% of Revenue

Case Study 3: Critical Manufacturing

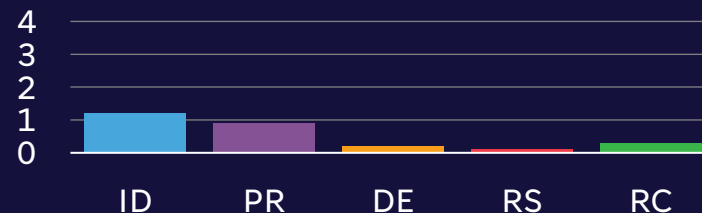


Background

- Very high frequency of loss events in this vertical
- Low awareness of company (low attractiveness)
- Low activity in dark web

Security Controls

- High maturity in IT
- Low maturity in OT
 - Virtually no detection & response



Estimated Loss

- Mean: 3% of Revenue
- 20yr: 19% of Revenue
- 100yr: 31% of Revenue

Best ROI Projects

- 1) DRP/BCP
- 2) Monitoring

Output Samples: Expected Losses

by Facility

Facility Name	Industry	Sub-Industry	Country	Production Capacity	Annual Revenue (\$)	Expected Loss (\$)	Loss Contribution (%)	Revenue Contribution (%)
Mature Solar Gen	Electricity	Solar	US	300	\$56,325,680	\$36,845	0.6%	20.7%

by Type of Loss

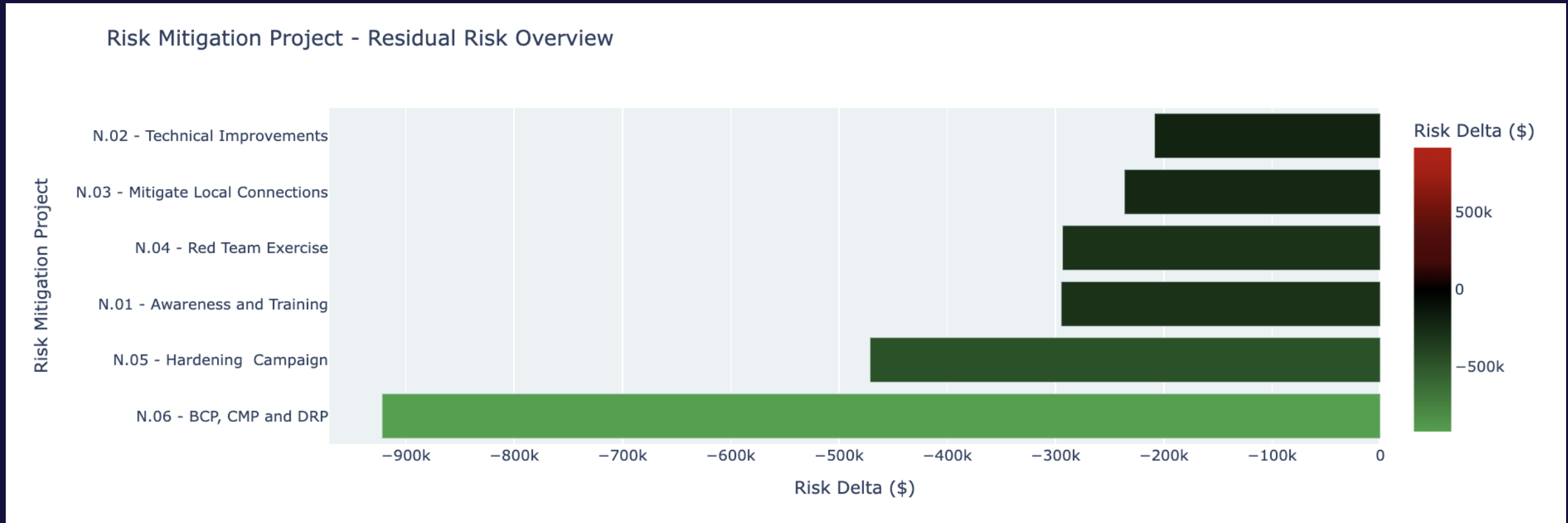
Facility Name	Industry	Sub-Industry	Loss Event	Annual Expected Loss (\$)	Loss (in Days of Revenue)	Event Contribution (%)	Event Revenue Loss Contribution (%)
Compliant Wind Gen	Electricity	Wind	Loss Of Productivity	\$3,815,210	5.1	63.9%	1.4%
Risky Wind Gen	Electricity	Wind	Downtime	\$1,406,060	1.9	23.6%	0.5%
Risky Gas Peaker	Electricity	CombinedCycle	Extortion	\$296,295			
Average Wind Gen	Electricity	Wind	Equipment Damage	\$189,211			
			Forensic Investigation	\$164,765			

by Attack Vector

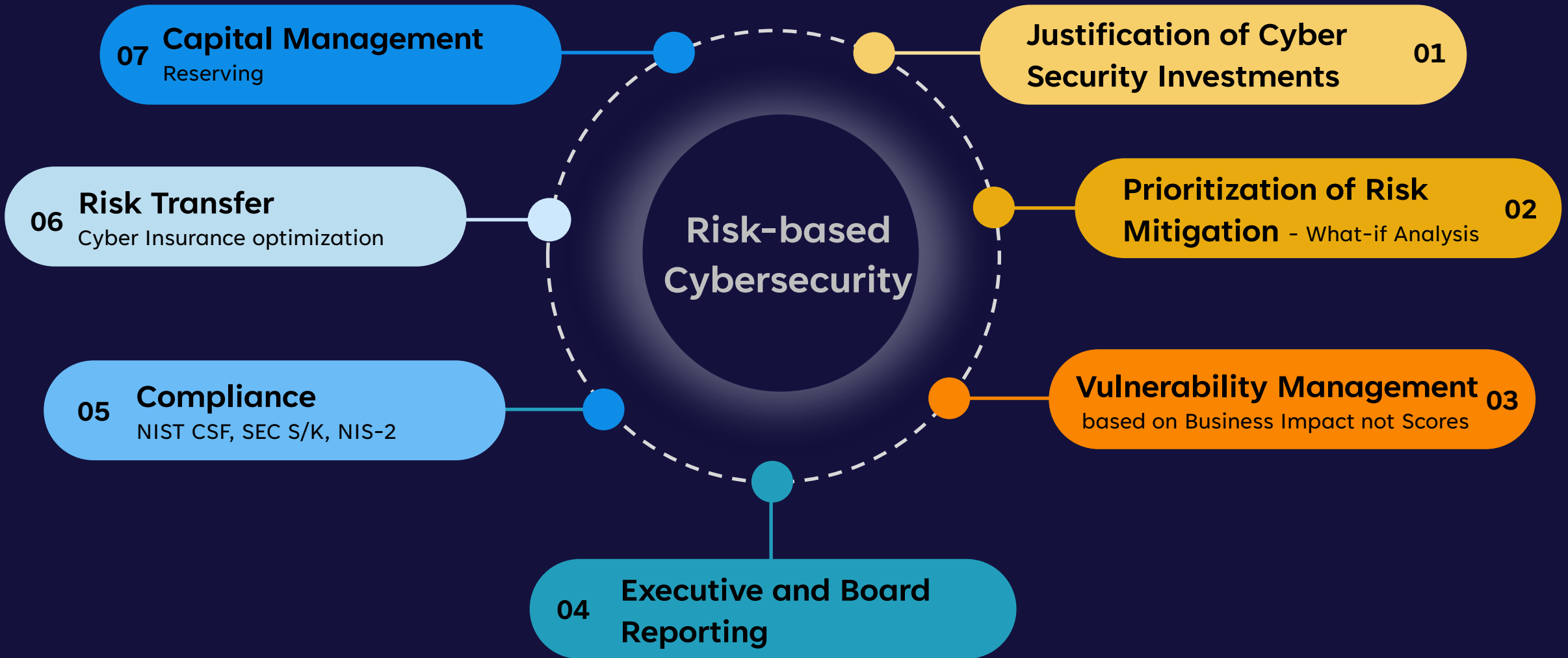
Initial Access Vector (IAV)	Annual Expected Loss (\$)	Loss (in Days of Revenue)	Event Contribution (%)	Event Revenue Loss Contribution (%)
Exploitation Of Remote Services	\$1,834,123	2.5	30.7%	0.7%
Remote Services	\$1,716,350	2.3	28.8%	0.6%
External Remote Services	\$724,885	1.0	12.1%	0.3%
Phishing	\$477,483	0.6	8.0%	0.2%
Drive-By Compromise	\$463,390	0.6	7.8%	0.2%

Case Study: Risk Mitigation Projects

Analysis of Alternatives – Comparing Reduction of Risk



Cyber Risk Management



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)



AI Use Case 3rd Generation

Large Language Model Querying



“Give me the vulnerabilities with \$1M loss potential at customer A’s US facilities”



“Give the best 5 controls with \$1M CAPEX budget, \$100k yearly expenses, and <6 months deployment. Show risk reduction, return on investments, and peers' comparison. Show the residual Value at Risk, and capital needs considering my insurance program”

E2E encrypted access to Cyber Insights made easy

Cyber Risk Management

Risk-based Cybersecurity & data-driven Risk Management based on business impact



DE NEXUS™

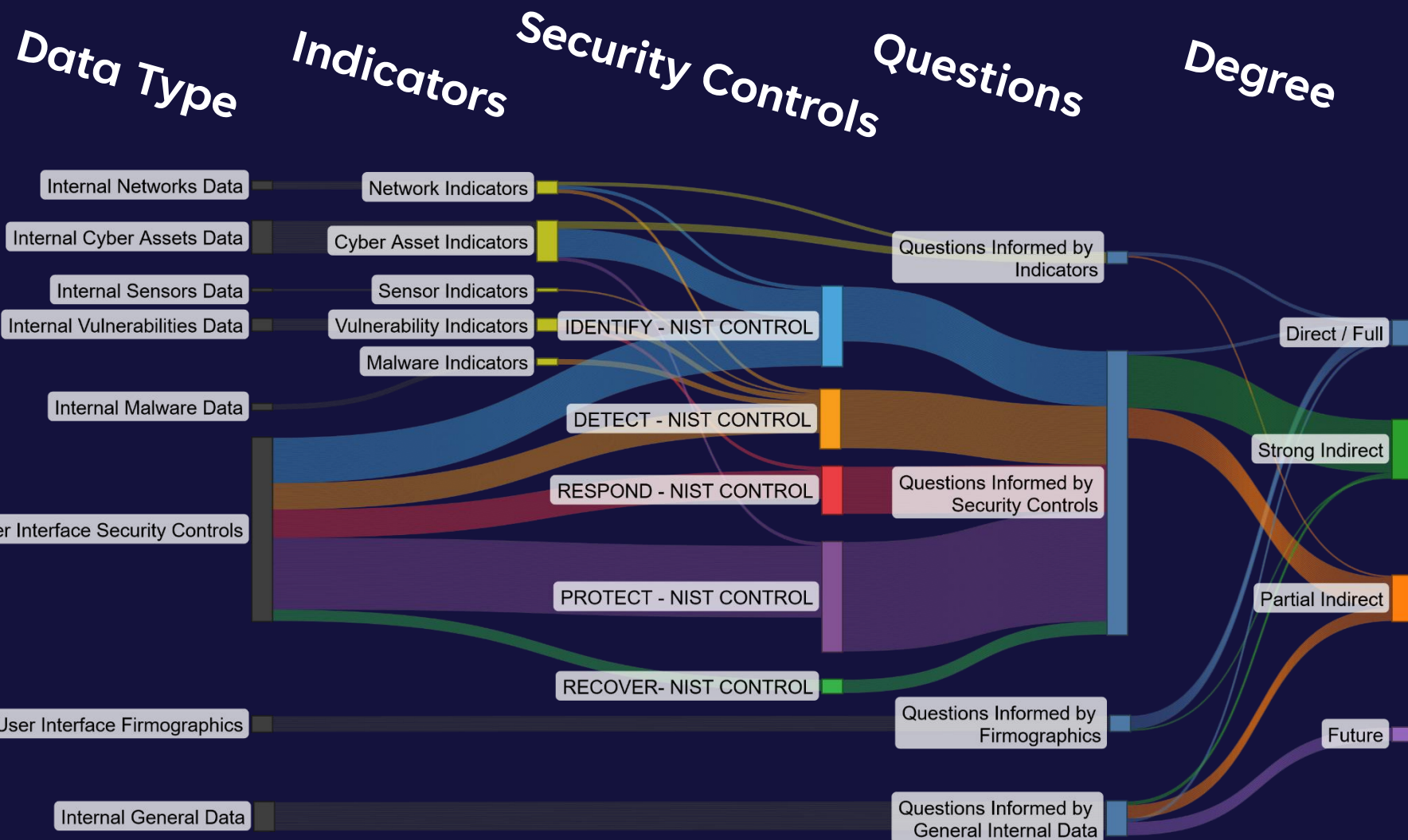
denexus.io

THANK YOU

© DeNexus, Inc. Confidential and Proprietary

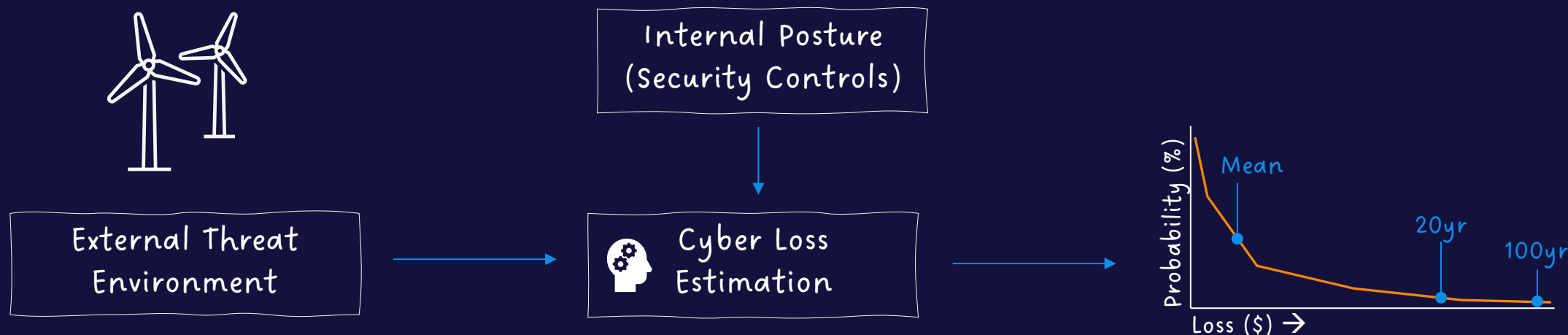


Cyber Telemetry Mapped to Cyber Insurance



up to
75%
Coverage

Case Study: Energy - Wind Renewables

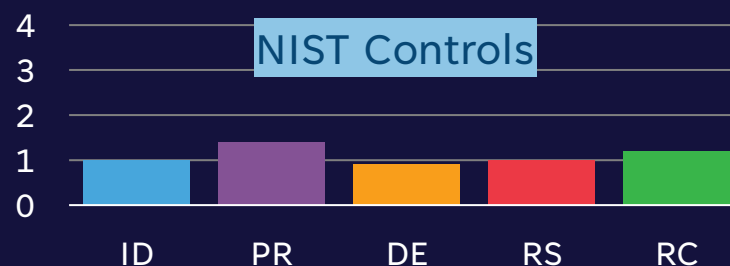


Background

- 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