Modeling of Catastrophic Cyber Events in Industrial Environments.

Impact on Portfolio Risk Accumulation

Romy Rodríguez-Ravines
rr@denexus.io | Mar 10, 2023

Romy Rodriguez-Ravines

Going beyond data | Statistics + Machine Learning

Advanced Analytics Expert.

reravines@gmail.com
https://ravinesromy.org/
https://www.linkedin.com/in/ravinesromy/
@RavinesRomy

Education

2003–2006 **Doctor of Philosophy, Statistics**
UFRJ. Rio de Janeiro, Brazil

2001–2003 **Master's Degree, Statistics**
UFRJ. Rio de Janeiro, Brazil

1994–1997 **Master's Degree, Systems Engineering**
UNI. Lima, Peru

1989–1994 **Bachelor's Degree, Statistics**
UNALM. Lima, Peru

Work Experience

Spain

DeNexus
03/2021 – Now (FT)

Head of Research and Modeling Strategies

Cyber Risk quantification, Loss Exposure, Accumulation, Cyber Catastrophe

Avanade
09/2019 – 06/2020 (FT)

Group Manager of Advanced Analytics

Knowledge Mining, Documents Classification, ML Industrialisation (MLOPs), CDP | Azure ML Services, Cognitive Services (AI), Databricks, D365 Customer Insights | Insurance, Energy, Industry innovation.

Innova-tsn
10/2017 – 08/2019 (FT)

Senior Manager of Advanced Analytics

Voice of Customer, NPS, CEX, EEX, Sales, Demand, Audience in TV, Customer Churn, Document & Text Analytic, Diagnosing and monitoring predictive models, Recommendation Systems | Topic Modelling, Sentiment Analysis, Demand Forecasting, Classification algorithms, ML, Statistics | Airline Transportation, Banking, Media, Pharma, Training.

Bayes Forecast
02/2008 – 09/2017 (FT)

Chief Knowledge Officer

Marketing Mix Models, Behavioural Segmentation, Demand for new products, Cost-predictive models, Customer churn, Propensity to complain, Risk of default, Credit card fraud, Debt collection, Cross-selling activities | Time Series, Dynamic Models, Hierarchical Models, Bayesian Inference | Banking, FMCG, Media, Retail, Teleco, Technology, Transport, Security.

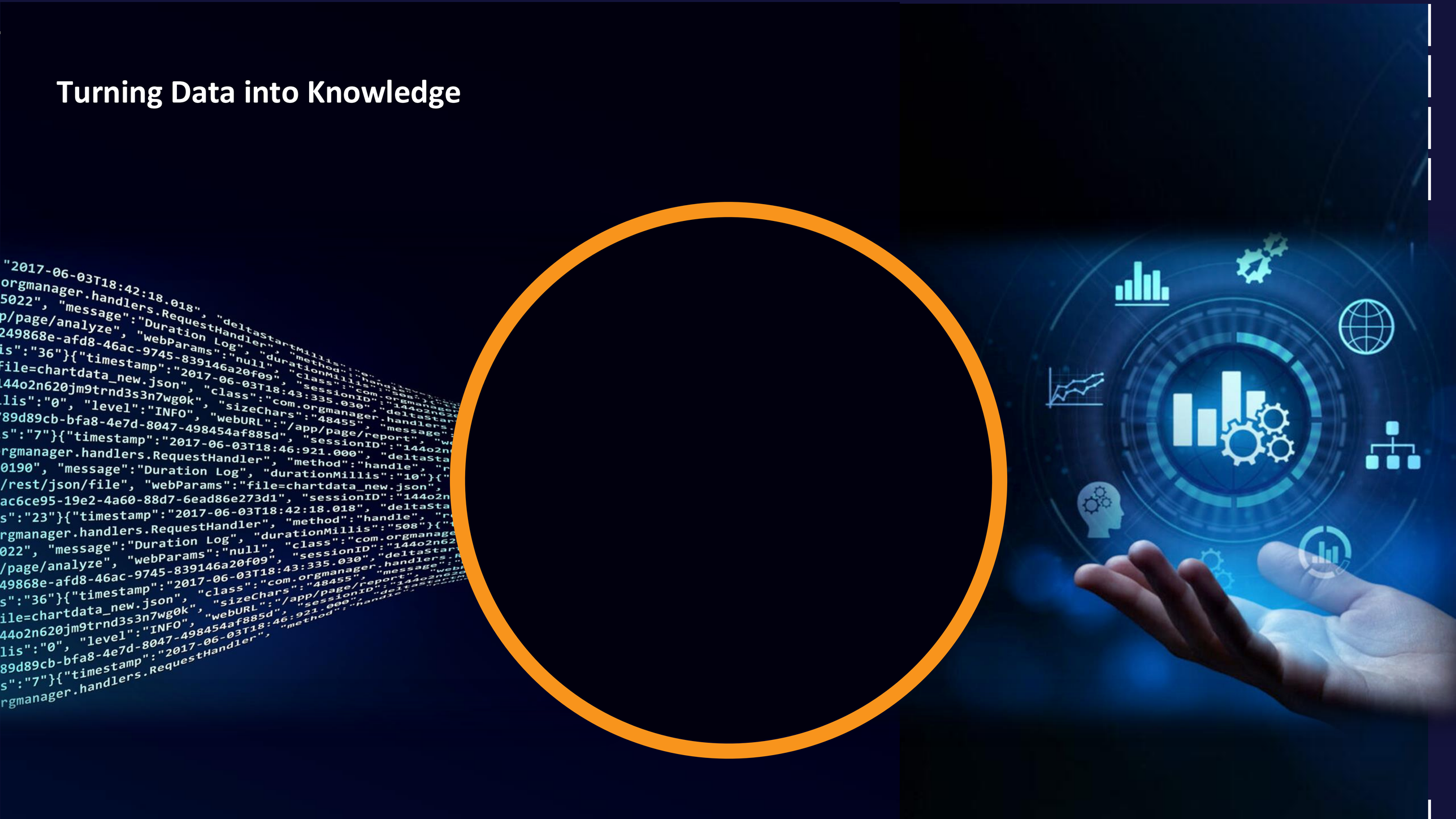
Universities & Business Schools
06/2014 – Now (PT)

Guest Lecturer

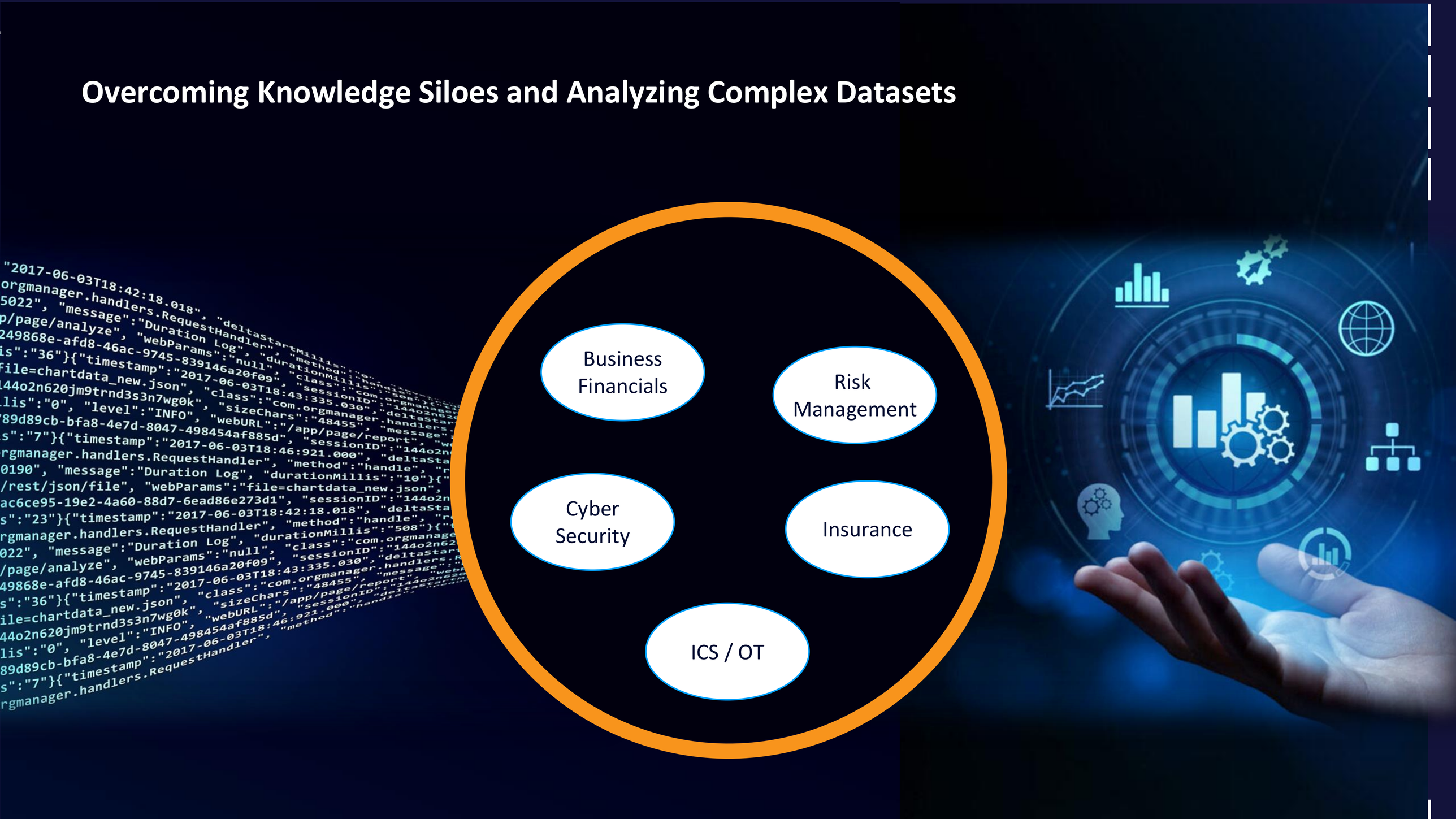
</> Nebrija University. BD in Economics and International Business (EN)
</> Carlos III University (UC3M). Master in Statistics for Data Science (EN)
</> Rey Juan Carlos University (URJC). Master in Data Science
</> CIFF Business School. Master in Big Data and Business Analytics
</> EAE Business School. Master in BI and Technology Innovation

Data Science, Predictive Analytics, Dynamic Bayesian Models, Econometrics, Statistics.

Turning Data into Knowledge



Overcoming Knowledge Siloes and Analyzing Complex Datasets



The only evidence-based data and self-adaptive cyber risk quantification model for industrial environments.

We Are DeNexus

Build the global standard of industrial cyber risk quantification for agencies, shareholders, investors, boards and risk transfer market

Jose M. Seara, CEO

2019	$9m	+30
Funded	Pre-A	Employees

"With DeRISK, we understand our cybersecurity posture and can prioritize risk reduction and mitigation actions based on actionable financial data"

Ken Young

COO at Apex Clean Energy

"We are impressed with the DeNexus team and their approach to assessing and prioritizing cyber risk"

John Franzino

CEO at GridSEC

BlackRock

EDF

APEX CLEAN ENERGY

Naturgy

GridSME SUBJECT MATTER EXPERTS

CYPRESS CREEK RENEWABLES

idemitsu

IDEMITSU RENEWABLES

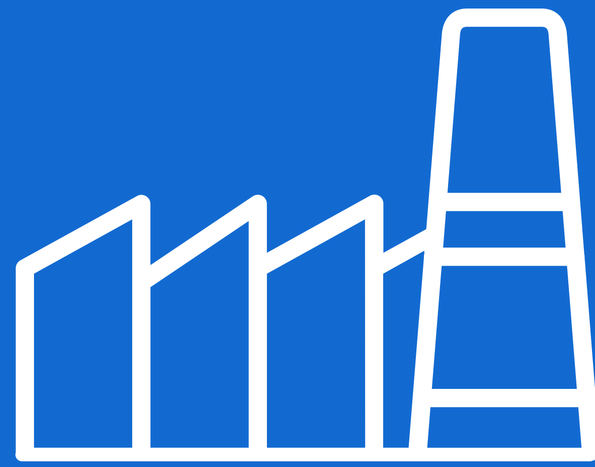
Why OT Data is Different?

ModBus, BacNet, OPC

- 20 years install base
- Large capital

- Fleets of Asset are Aggregates can now be seen with OT-DPI
- Knowing the segmentation strategies allows for risk quantification

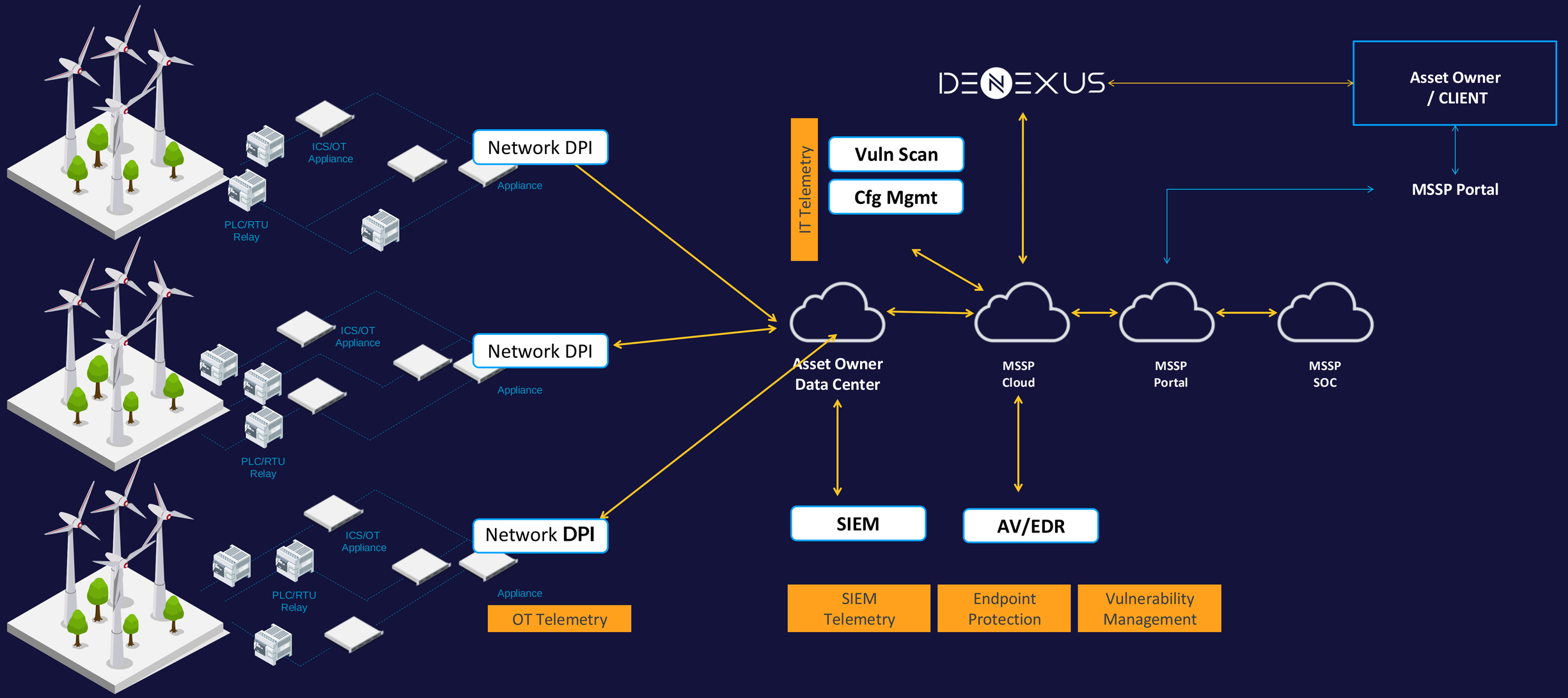
- Impact difference
- Industry – O&G vs. Electric Utility
- Sub Industry - Offshore Wind Turbines vs. Combined Cycle Plant
- Geographic, Public vs. Private, Small vs. Large Revenue



PORTFOLIO ACCUMULATION | BOTTOM-UP | FIT-FOR-PURPOSE

One Client in US >60 Sites

Inside-Out and Outside-in Risk Visibility, RT Quantification, 24x7 Management



Built for Purpose: OT Inside Out Data

2nd Generation Risk Modeling Requires Continuous OT Data from Inside Process Networks

Inside Data

Sensors inside the OT network collect information about the existing assets, software/firmware, configuration, control systems in place.

Outside Data

Threat intelligence and contextual information from public and private and proprietary data sources.

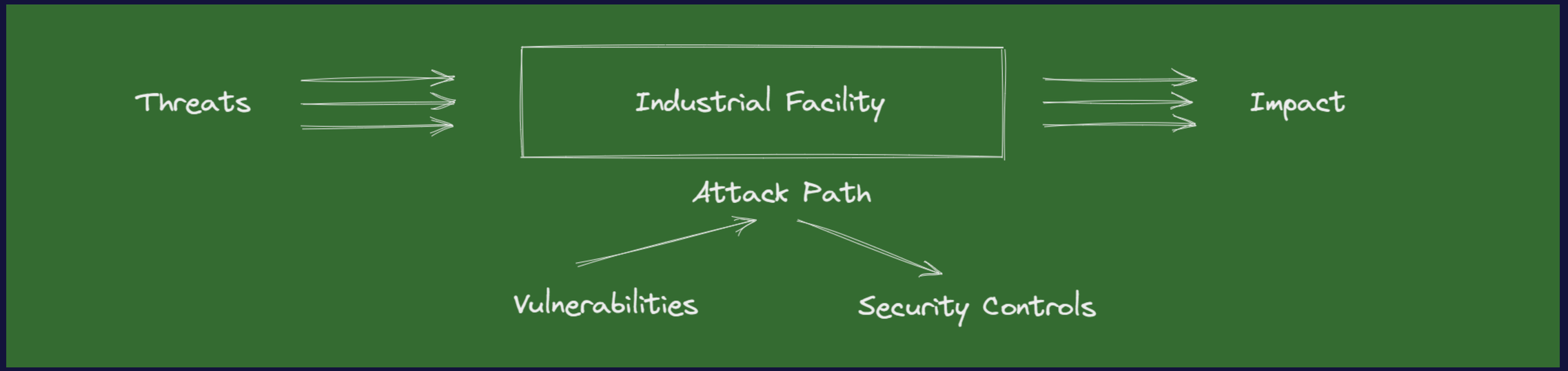
Firmographics

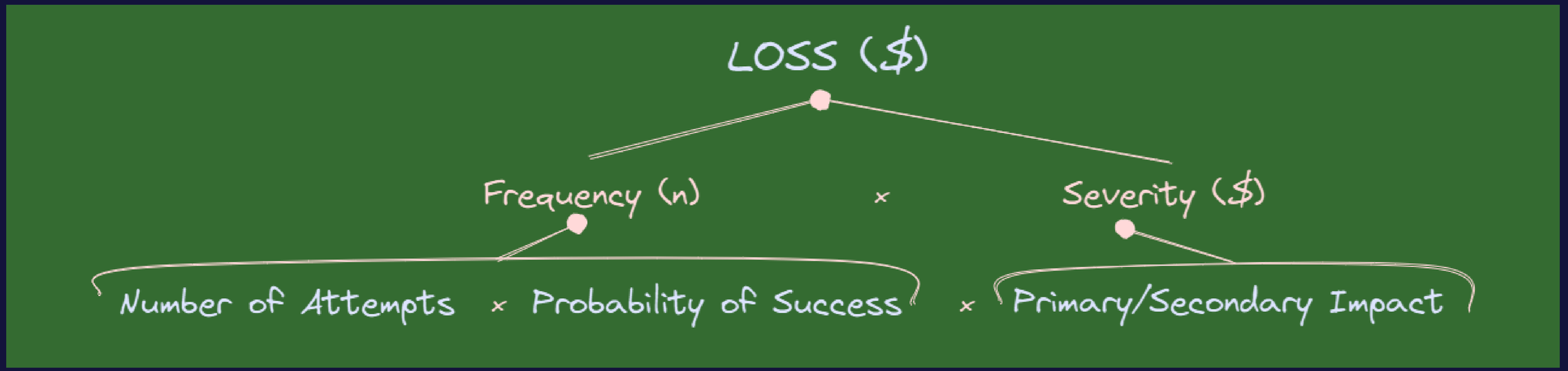
Organization -public- information: location, industry and sub-industry, revenue, size, age
Attractiveness

DeNexus Knowledge Center

INDUSTRIAL CRQM | FIT-FOR-PURPOSE

Risk Quantification: putting data in context

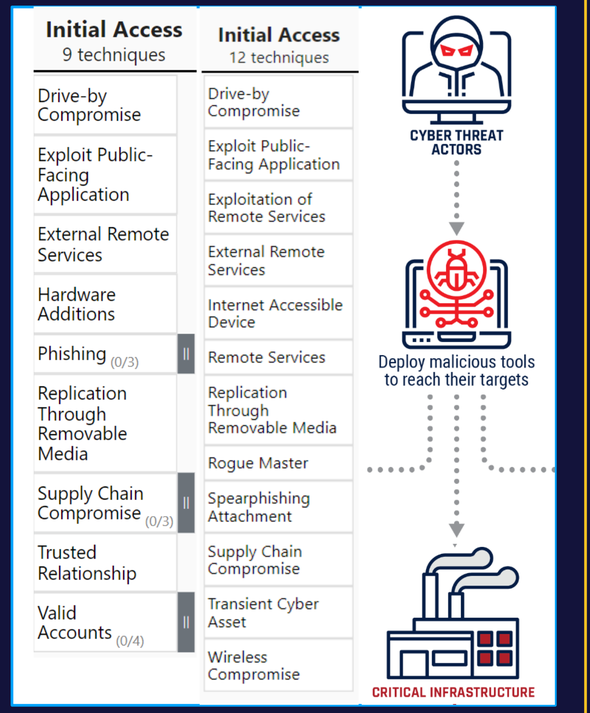




DeNexus Modeling System – Unique Approach

Number of Attempts
- NoA -

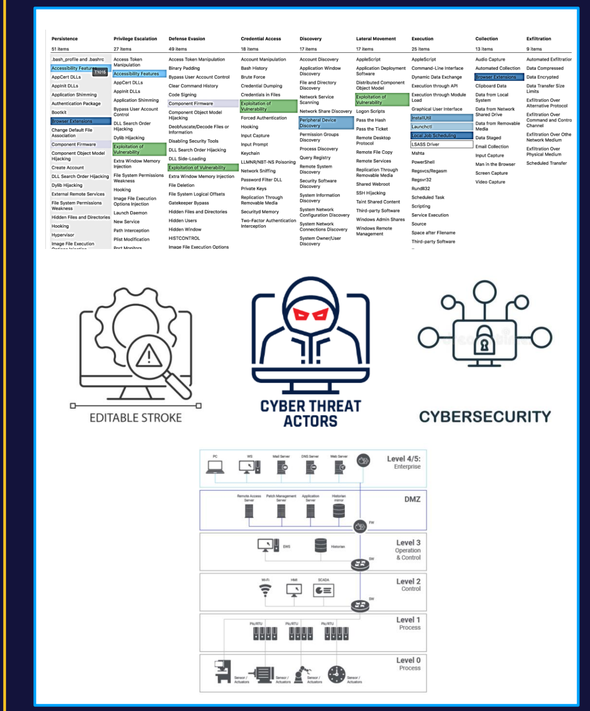
How many attempts in a year?



Powered by
Outside-in Data

Attack Path Algorithm
- APA -

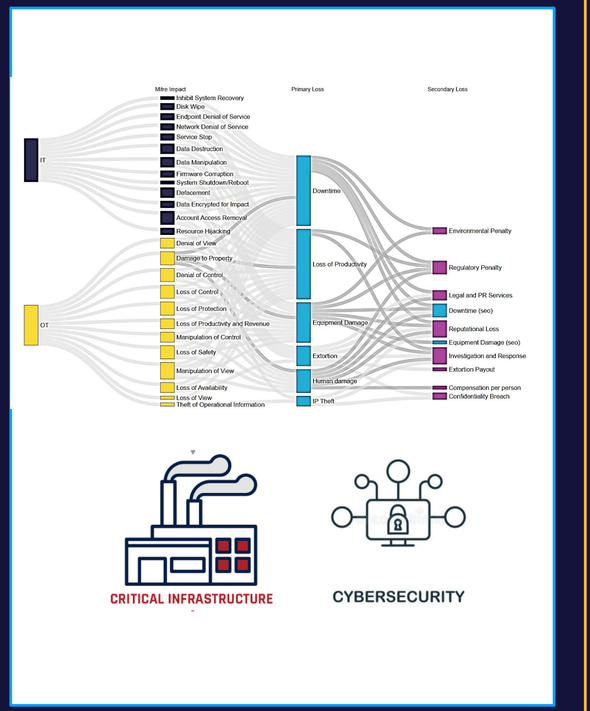
How an incident can propagate and cause a loss event?



Powered by
Inside-Out & Outside-In Data

Loss Event Impact
- LEI -

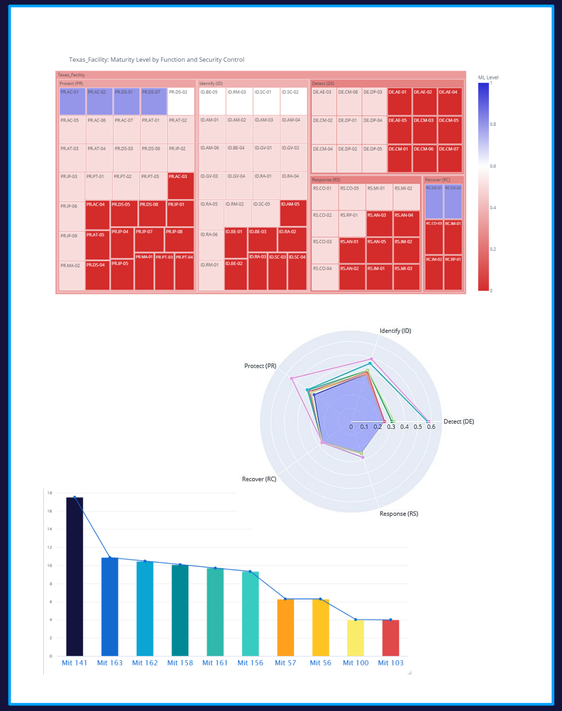
What is the financial impact **($)**?



Powered by
Business-Risk-Loss Data

Mitigation Recommendations
- MRS -

How to Mitigate?
Control-based, Project-based



Powered by
Business-Risk-Loss Data

DENEXUS

Data feedback-loop
DeRISK-> DKC

DeNexus Knowledge Center

Updated as of Feb. '23

Outside-in Data

OPEN THREAT EXCHANGE · Mediatoolkit · CROWDSTRIKE · MISP Threat Sharing · APEC capec.mitre.org · CVE Common Vulnerabilities and Exposures · Blueliv. · censys · SHODAN · MITRE ATT&CK · CWE Community · NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION · IEC · ISO 27001 · NIST CSF · DEFEND · FIRST

Inside-out Data

FORESCOUT · NOZOMI NETWORKS · CLAROTY · INDUSTRIAL DEFENDER · CROWDSTRIKE · tenable · nessus Professional

Firmographics and Financial Data

Verisk · eia · RocketReach · RANSOMWHERE

Cyber Incidents Data

U.S. DEPARTMENT OF ENERGY · Temple University College of Liberal Arts — Cybersecurity in Application, Research and Education Lab — Critical Infrastructure Ransomware Attacks (CIRA) · ICS STRIVE · NIST National Institute of Standards and Technology · SCIDMARK SYSTEMS AND CYBER IMPACT DATABASE MARKUP · Kon Briefing · CSIS CENTER FOR STRATEGIC & INTERNATIONAL STUDIES · vz-risk / veris · SecuraBV / OTCAD · HACKMAGEDDON · CLOUDIAN · PRC Privacy Rights Clearinghouse · TI Safe · RISI

Metadata

FBI CYBER DIVISION · CHUBB · NetDiligence · enisa European Network and Information Security Agency · SECTRIO A DIVISION OF SUBEX · DRAGOS · WATERFALL Stronger Than Firewalls · statista · verizon · Ponemon INSTITUTE · FORTINET

- Region, Industry vertical, Ownership, #employees, Supply Chain
- Attractiveness, Attack Surface
- Threat Actors
- Cybersecurity Controls
- Cyber incidents Tactics, Techniques
- Vulnerabilities
- Benchmark of Incidents (Incident database, Clients Assessments, Synthetic Profiles)
- Impacts & Losses
- Mitigations Controls & Projects Capex, Opex, Implementation time

DERISK

NoA
Number of Attempts

SCOTT
Security Controls for OT

APA
Attack Path Algorithm
Unit, Portfolio

LEI
Loss Event Impact
Unit, Portfolio

MRS
Cyber Risk Mitigation Recommendations

Cyber Risk Quantification & Management

- Executive Dashboard
- Portfolio Builder
- Risk Assessment
- Risk Analysis
- Indicators . Control, Risk, Performance
- Compliance Overview
- Mitigation Recommendations
- What If Scenarios
- Reports

DeRISK – Validation and Calibration

Benchmark of incidents – Continuous effort – Dedicated team

Statistical Quality

The loss distribution is obtained with a sequential sampling problem:

- Convergency of numerical methods
- Variability of quantiles
- Robustness of the results
- Tail stability

Sensitivity Analysis

- Hundreds of inputs used
- Contribution per input
- Robustness to changes in the input's definition
- Comparison of distributions

Suite of tests

Business Quality

Benchmark of cases to analyze and validate, make sense, each piece of the system with SMEs

V5 Benchmark

Synthetic Profiles	Clients Assessments	Incident-based
7	3	4

- Quantified $ losses within realistic range
- Results realistic to ICS/OT systems and industries

Unlocking the value in data

Costly Unanswered Questions

Single-Risk Assessment

Mitigation Strategies

Project builder What-if?

Portfolio-Risk Accumulation

How do we price and assess cyber risk premiums?

Takeaways

DeRISK – 2nd Generation Cyber Risk Modeling

Inside-Out data contextualized with underlying Industrial Process & Business data

The Challenge

- We need CRQM
- NAT CAT models not for CYBER CAT
- Reliable models
- 1st generation failed

The Answer

- **Data is the foundation**
  - Inside-Out & Outside-In evidence-based data
- **Data in context**
  - Underlying Industrial Process & Business data
- **Data-driven decisions**
  - Continuous risk evaluation in financial terms
  - Efficient ROI-based risk mitigation
  - Determination of risk to be transferred
- **Bottom-up accumulation**
- **Trusted Ecosystem**
  - Encrypted Data
  - Safe Insights

DeNexus Knowledge Center

Trusted Ecosystem

What is Cyber Risk?

Just another enterprise level risk…

INDUSTRIAL CYBER RISK

IN·DUS·TRI·AL CY·BER RISK / IN'DƏSTRĒƏL 'SĪBƏR RISK/

THE POTENTIAL LOSS OF LIFE, INJURY, DAMAGED ASSETS, FINANCIAL LOSS, AND OTHER HARM FROM THE FAILURE OR MIS-OPERATION OF DIGITAL TECHNOLOGIES AND COMMUNICATION NETWORKS USED FOR OPERATIONAL CAPABILITIES.

When will the next phishing email arrive?

Will you suffer a data breach?

When will a cyberattack on my organization happen?

Two Stakeholders. One Challenge

Cybersecurity stakeholders are vulnerable, insurance firms are exposed and blind

The Industrial Enterprise

75%
of CEO's could be personally liable by 2024

500%
Growth in Ransomware in 2020 targeting ICS/OT

$20 Billion
In estimated costs due to Ransomware in 2020

1.Gartner - Predicts 2020: Security and Risk Management Programs
2.FORTINET - 2020 State of Operational Technology and Cybersecurity Report
3.Purplesec.- 2021 Ransomware Statistics, Data, & Trends

The (re)insurers

58%
of US organizations do not have Cyber Risk coverage

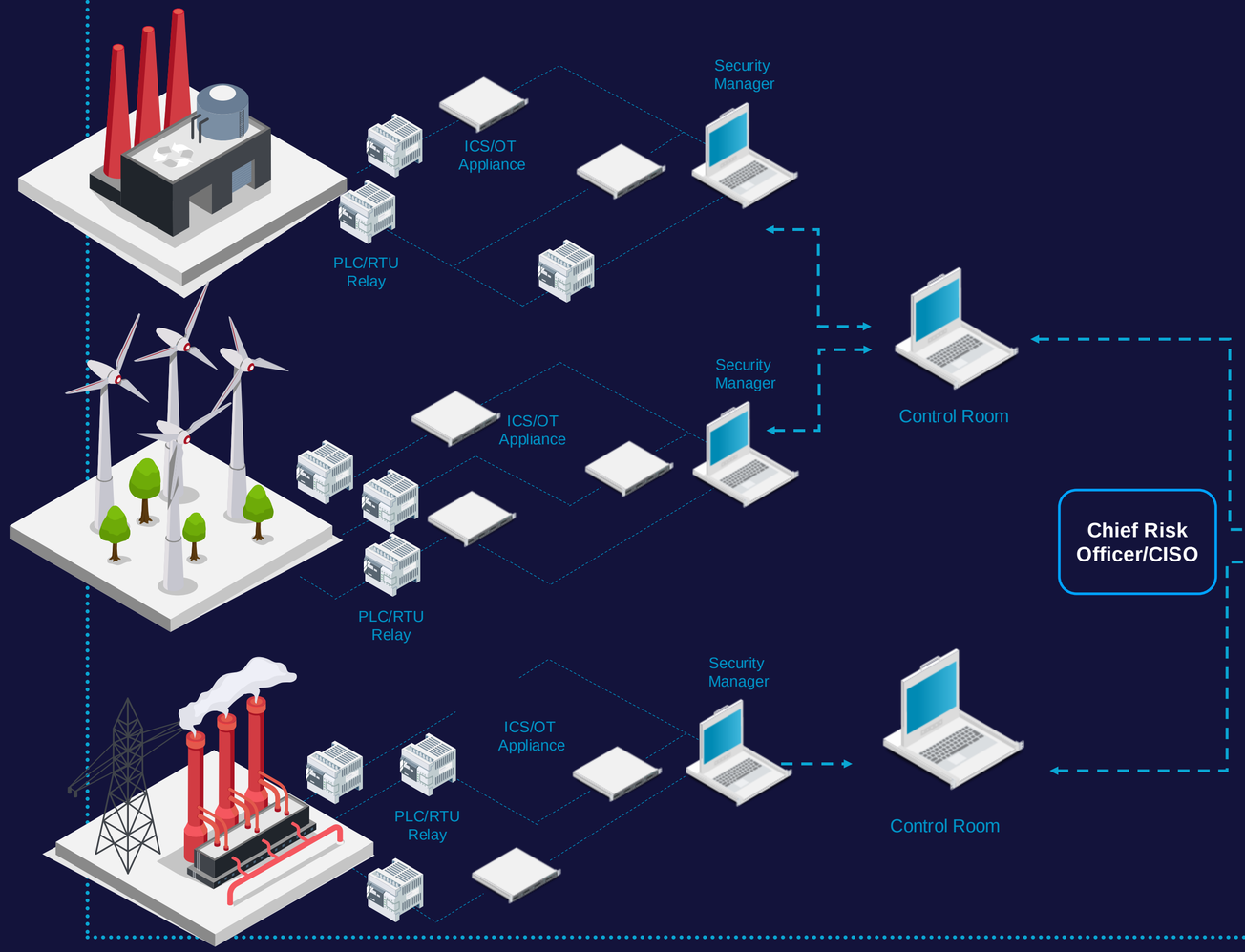
66.9%
Average Loss Ratio in 2020

96%
Pricing increase year/over/year in Q3 2021
40% increase compared to Q2 2021

1.Insurance Insider February 11, 2021
2.NAIC-s 2020 Cyber Insurance Report
3.Marsh Cyber Insurance Market Overview: Q4 2021

Quantify, Manage, and **Solve Cyber Risk**

Unanswered Questions



Chief Risk Officer/CISO

Industrial Enterprise

What is our risk-reduction ROI on cybersecurity investments? (tools + talent + training)

Are we spending our security team's time and resources optimally?

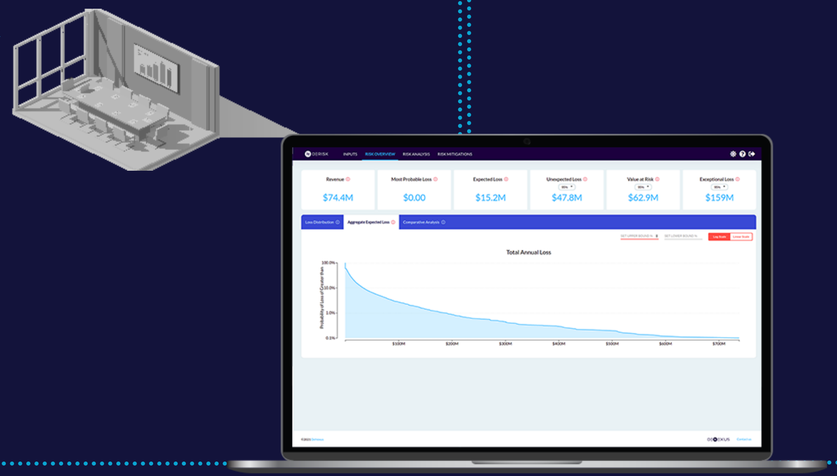
Are we overspending on duplicate defenses where your risk just doesn't justify the price?

Insurance / (Re)insurance

Are we doing a proper risk selection?

Are we allocating the right amount of capital to cover future claims/losses?

Are our accumulation assessments and catastrophic scenario analysis, correct?



What is the Point?

Qualitative information is not sufficient for efficient Risk Management

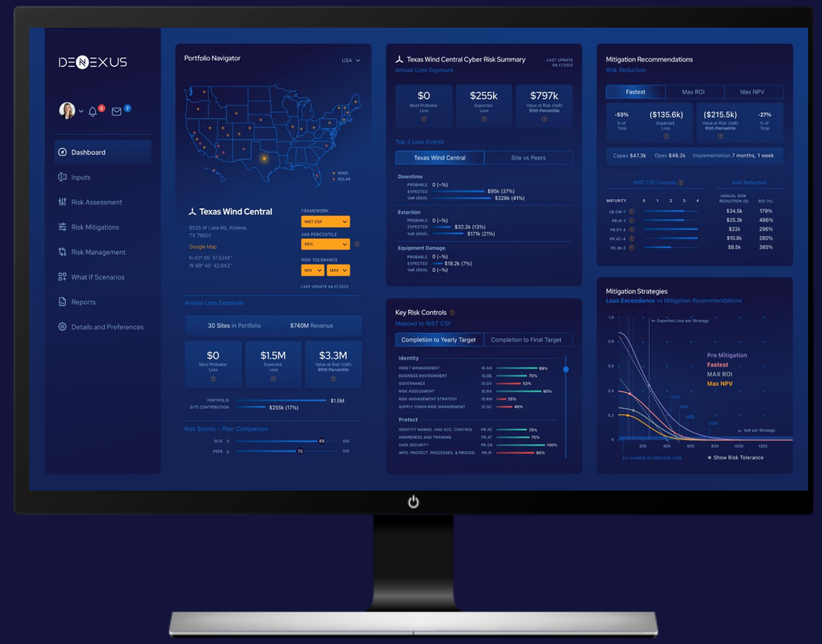
- Poorly understood – Insufficient empirical data
- Highly dynamic – Fluid risk drivers
- Impacted by both internal and external factors
- Impacted by human behavior, intentional or not
- **That could result on systemic risk insurable? … or even systematic risk uninsurable ? under certain circumstances**

Quantifying Cyber Risk and Uncertainty with Rigorous Analytics Methodologies

There is no full risk picture without data and science

The Solution - 2nd Generation Cyber Risk Modeling

DeRISK Platform



OT focused, Inside-Out & Outside-In
Cyber Risk Quantification SaaS platform

Evidence-based, Real-time, Data-driven, Self-adaptive, Automatic

Value Cyber Risk

ROI-based Security

Manage Risk Exposure

Transfer Risk

Build Risk Transfer Capacity

Modeling of Catastrophic Cyber Events in Industrial Environments. Impact on Portfolio Risk Accumulation

Why Do We Need Cyber Catastrophe Models?

[Nat] CAT: definition

American Academy of Actuaries

Catastrophes are infrequent events that cause severe loss, injury or property damage to a large population of exposures. While the term is most often associated with natural events (e.g. earthquakes, floods or hurricanes), it can also be used when there is concentrated or widespread damage from man-made disasters (e.g. fires, explosion, pollution, terrorism or nuclear fallout)

Path of hurricane Andrew, Aug 1992, colours represent wind speeds

65 people were killed
Damage total exceeded $26 billion
Insurance claims totalled $15.5 billion

Before Andrew, people thought the worst case scenario was about $7 billion (Karen Clarke)

Andrew was responsible for the failure of at least 16 insurers between 1992 and 1993 (Insurance Information Institute)

[Nat] CAT: challenges

American Academy of Actuaries

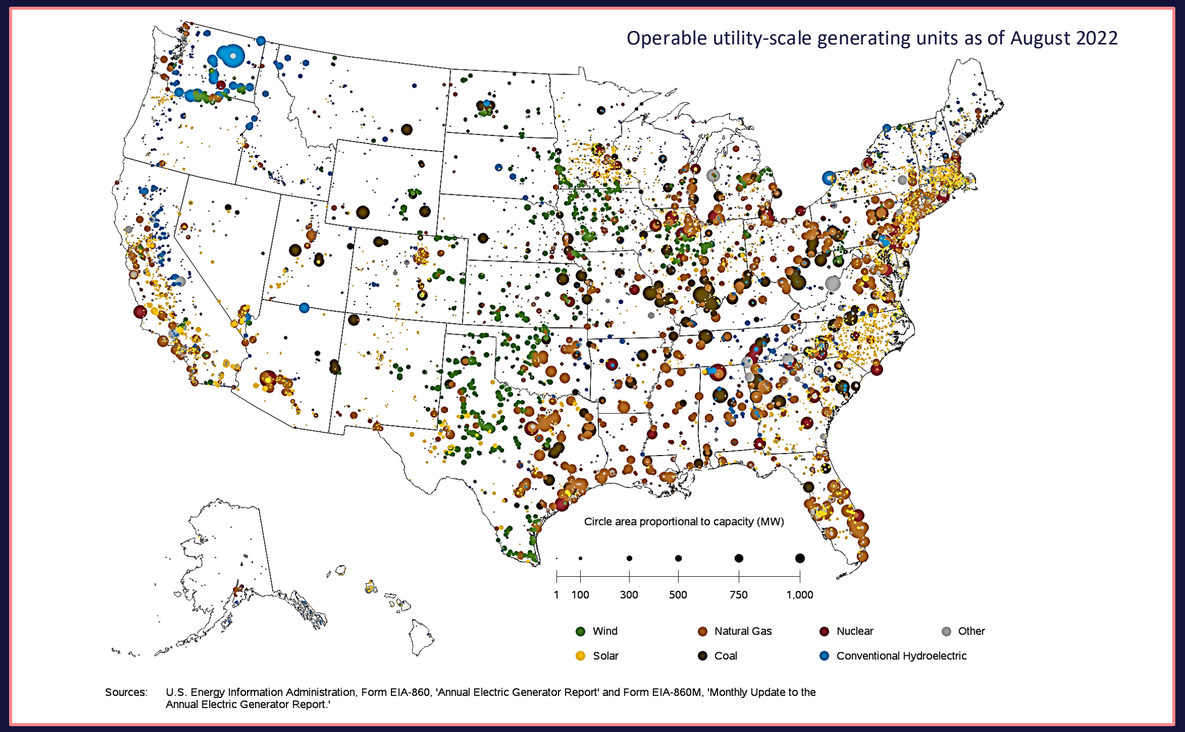
Catastrophes are infrequent events that cause severe loss, injury or property damage to a large population of exposures. While the term is most often associated with natural events (e.g. earthquakes, floods or hurricanes), it can also be used when there is concentrated or widespread damage from man-made disasters (e.g. fires, explosion, pollution, terrorism or nuclear fallout)

Path of hurricane Andrew, Aug 1992, colours represent wind speeds

LOW FREQUENCY EVENTS | SCARCE HISTORICAL DATA | [SPATIAL] CORRELATION | RELIABLE MODELS

Cyber CAT: even more challenging

Path of hurricane Andrew, Aug 1992, colours represent wind speeds

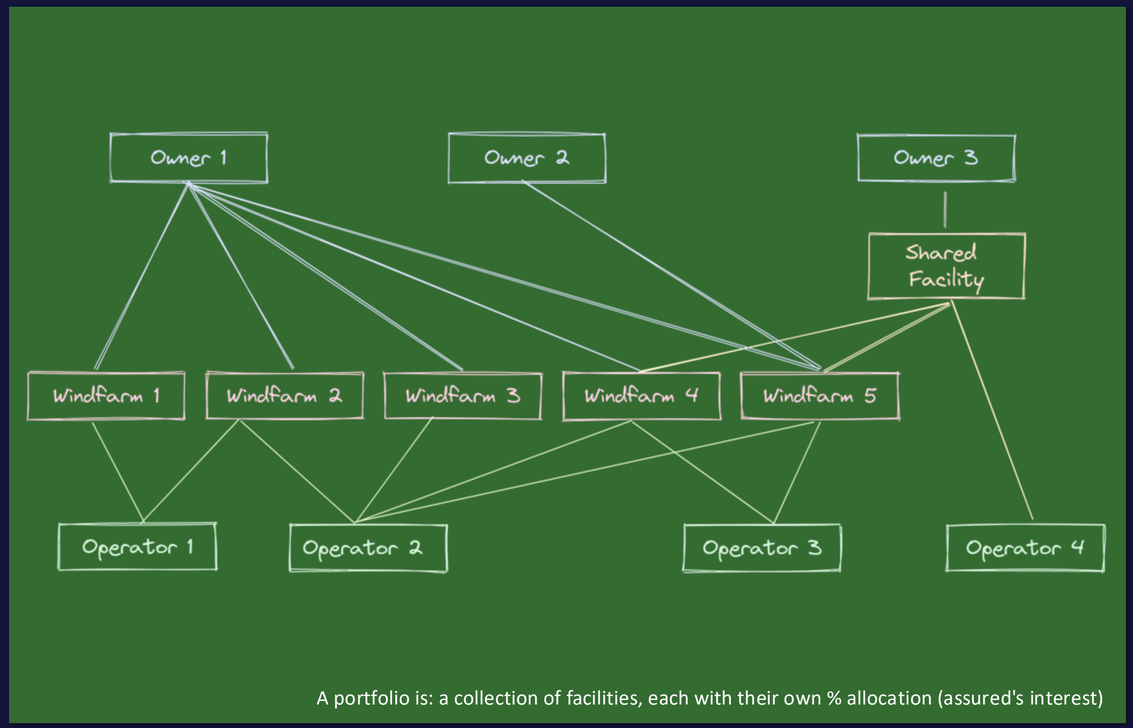


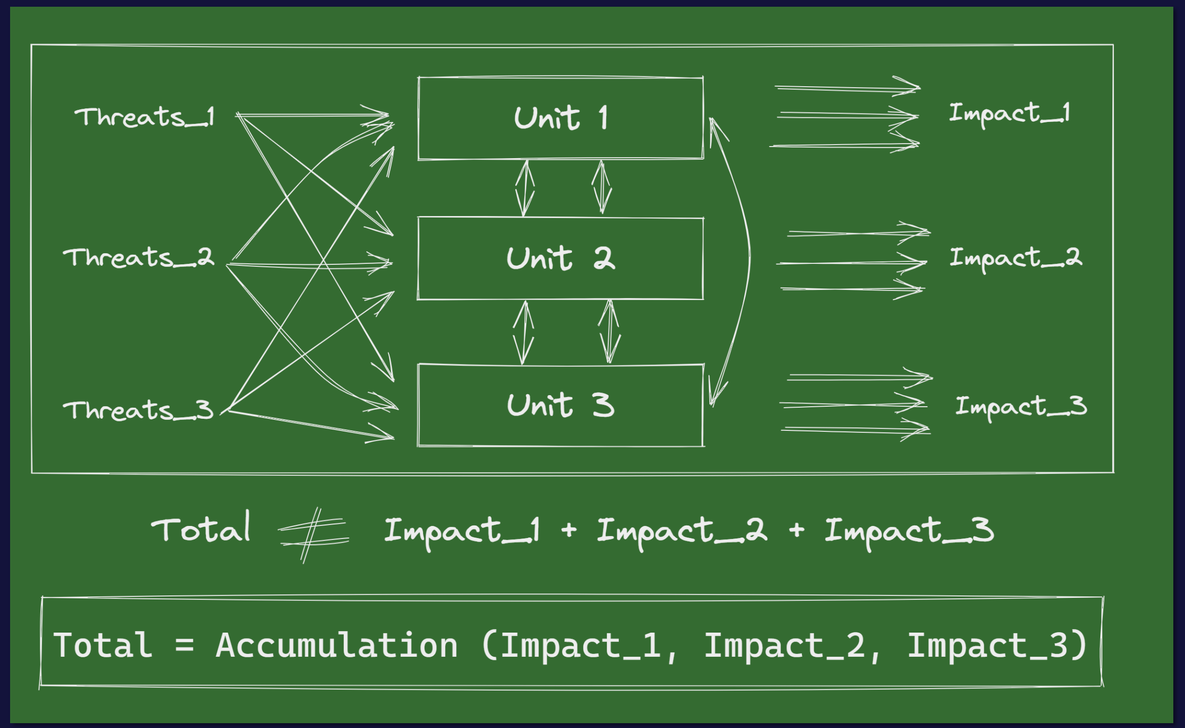
Sources: U.S. Energy Information Administration, Form EIA-860, 'Annual Electric Generator Report' and Form EIA-860M, 'Monthly Update to the Annual Electric Generator Report.'

EVENT SET	SOURCES OF CORRELATION	MANY MANIFESTATIONS OF LOSS	1st GENERATION FAILED

Data is the foundation

Cyber CAT: Accumulation and Portfolio





A large loss happens in isolation, either by accident or as the result of a sophisticated attack
An accumulation happens because all the affected facilities shared a common trait.
Such a common trait underpinned the event leading to the loss, and in hindsight was a source of correlation within the portfolio.

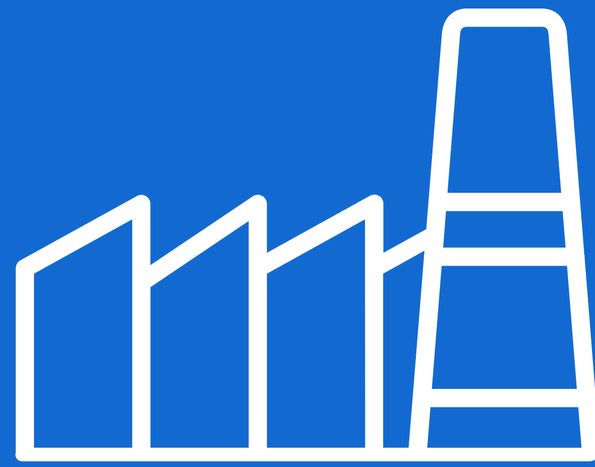
Why OT Data is Different?

ModBus, BacNet, OPC

- 20 years install base
- Large capital

- Fleets of Asset are Aggregates can now be seen with OT-DPI
- Knowing the segmentation strategies allows for risk quantification

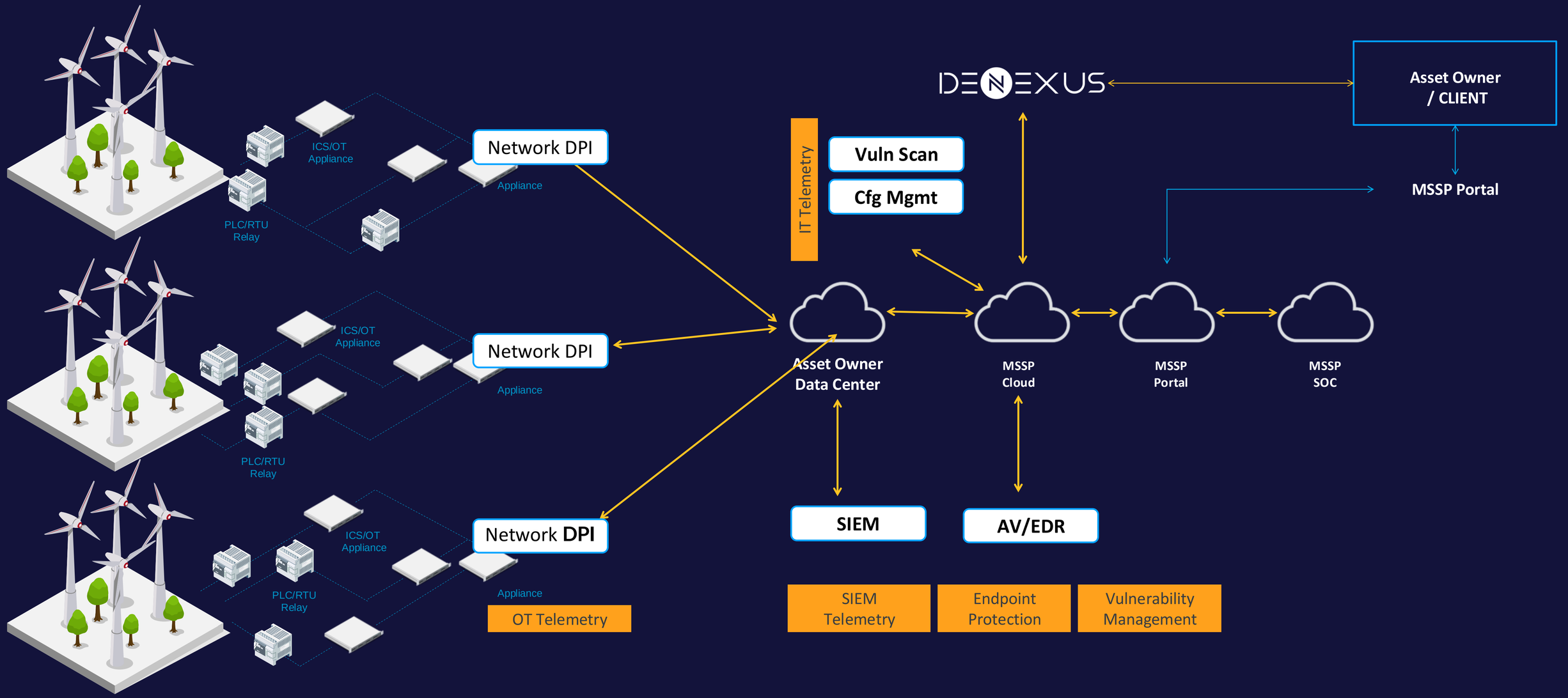
- Impact difference
- Industry – O&G vs. Electric Utility
- Sub Industry - Offshore Wind Turbines vs. Combined Cycle Plant
- Geographic, Public vs. Private, Small vs. Large Revenue



PORTFOLIO ACCUMULATION | BOTTOM-UP | FIT-FOR-PURPOSE

One Client in US >60 Sites

Inside-Out and Outside-in Risk Visibility, RT Quantification, 24x7 Management



Built for Purpose: OT Inside Out Data

2nd Generation Risk Modeling Requires Continuous OT Data from Inside Process Networks

Inside Data

Sensors inside the OT network collect information about the existing assets, software/firmware, configuration, control systems in place.

Outside Data

Threat intelligence and contextual information from public and private and proprietary data sources.

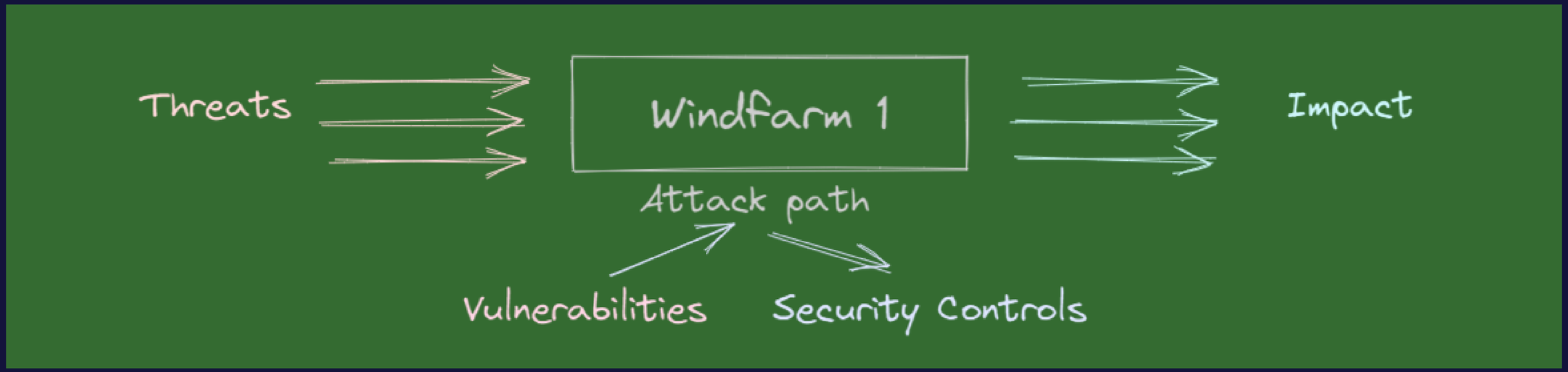
Firmographics

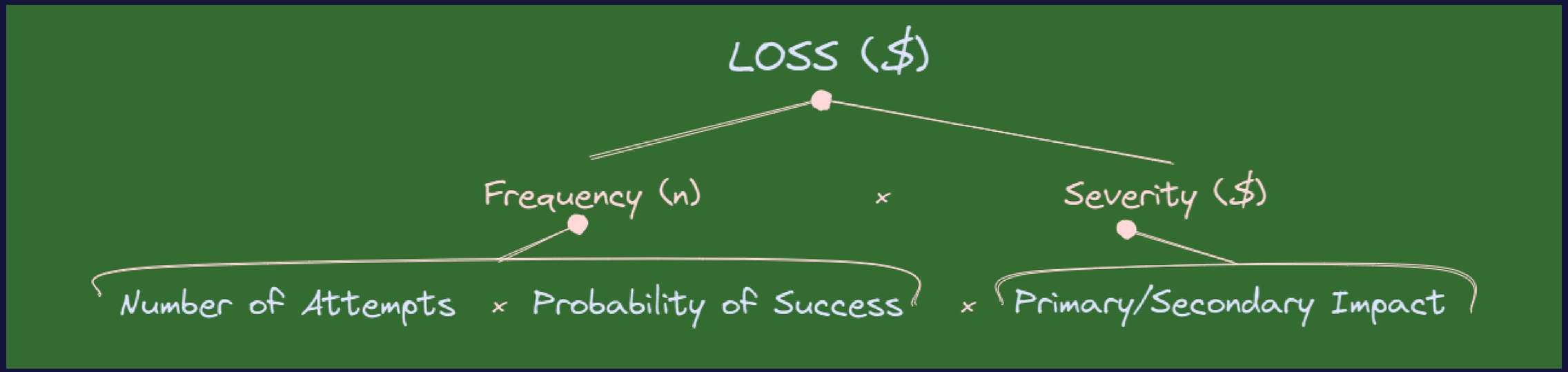
Organization -public- information: location, industry and sub-industry, revenue, size, age
Attractiveness

DeNexus Knowledge Center

INDUSTRIAL CRQM | FIT-FOR-PURPOSE

Risk Quantification: putting data in context

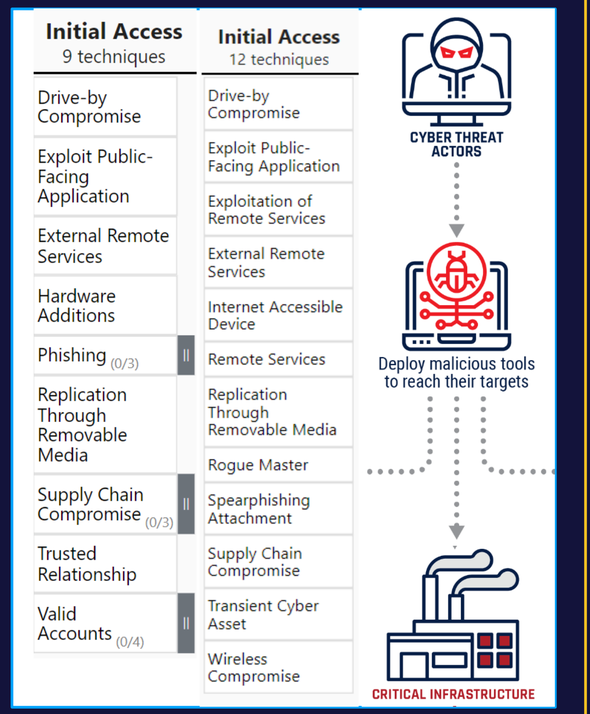




DeNexus Modeling System – Uniquely Approach

Number of Attempts

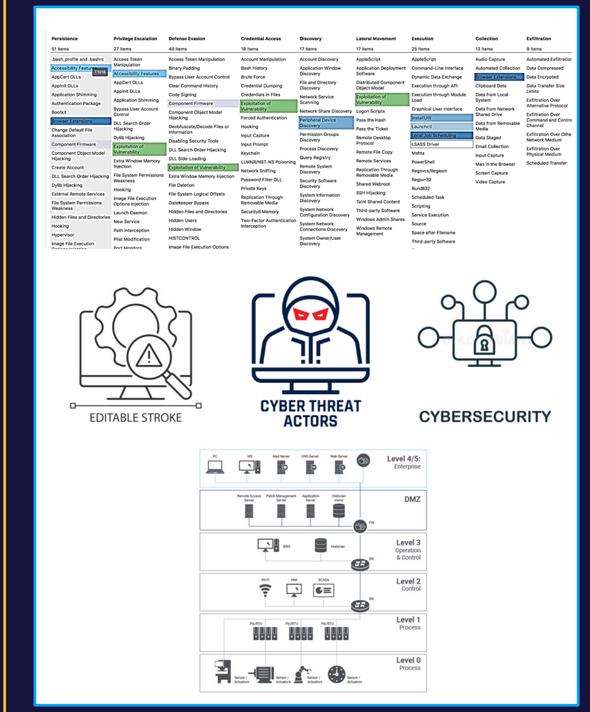
How many attempts in a year?



Powered by Outside-in Data

Attack Path Simulator

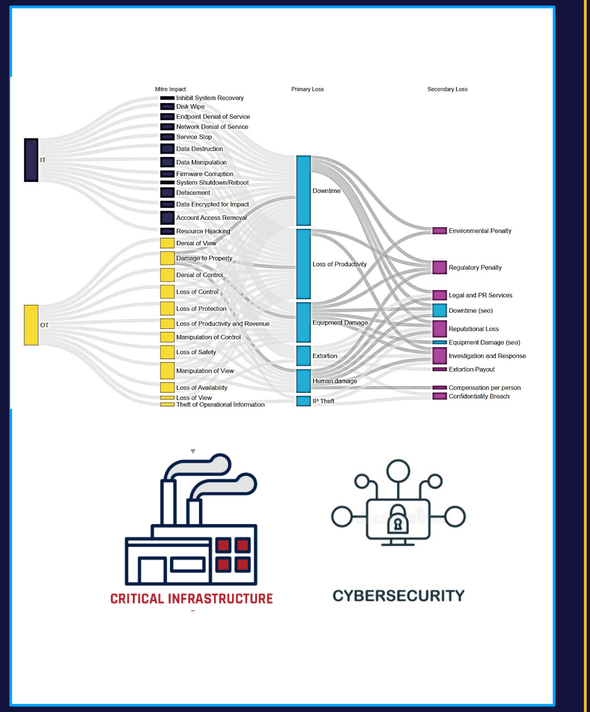
How can an incident propagate and cause a loss event?



Powered by Inside-Out & Outside-In Data

Loss / Severity /Impact

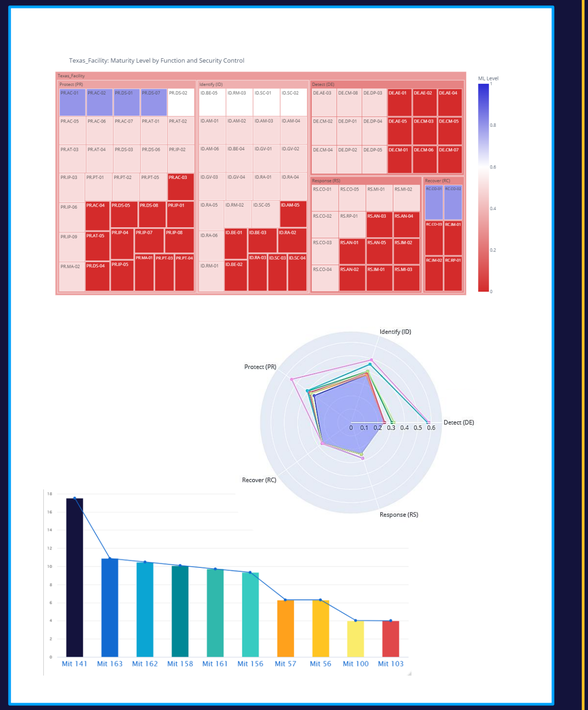
What is the financial impact **($)**?



Powered by Business-Risk-Loss Data

Mitigation Recommendations

How to Mitigate? Unit Risk Level



Powered by Business-Risk-Loss Data

DENEXUS

Data feedback-loop
DeRISK-> DKC

DeNexus Knowledge Center

Updated as of Feb. '23

Outside-in Data

OPEN THREAT EXCHANGE · Mediatoolkit · CROWDSTRIKE · MISP Threat Sharing · APEC capec.mitre.org · Common Vulnerabilities and Exposures · Blueliv. · censys · SHODAN · MITRE ATT&CK · CWE Community · NERC North American Electric Reliability Corporation · IEC · ISO 27001 · NIST CSF · DEFEND · FIRST

Inside-out Data

FORESCOUT · NOZOMI NETWORKS · CLAROTY · INDUSTRIAL DEFENDER · CROWDSTRIKE · tenable · nessus Professional

Firmographics and Financial Data

Verisk · eia · RocketReach · RANSOMWHERE

Cyber Incidents Data

U.S. DEPARTMENT OF ENERGY · Temple University College of Liberal Arts · Cybersecurity in Application, Research and Education Lab · Critical Infrastructure Ransomware Attacks (CIRA) · ICS STRIVE · SCIDMARK SYSTEMS AND CYBER IMPACT DATABASE MARKUP · NIST National Institute of Standards and Technology · Kon Briefing · CSIS CENTER FOR STRATEGIC & INTERNATIONAL STUDIES · vz-risk / veris · HACKMAGEDDON · SecuraBV / OTCAD · PRC Privacy Rights Clearinghouse · TI Safe · CLOUDIAN · RISI

Metadata

FBI · CHUBB · NetDiligence · enisa European Network and Information Security Agency · SECTRIO A DIVISION OF SUBEX · DRAGOS · WATERFALL Stronger Than Firewalls · statista · verizon · Ponemon INSTITUTE · FORTINET

Region, Industry vertical, Ownership, #employees, Supply Chain

Attractiveness, Attack Surface

Threat Actors

Cybersecurity Controls

Cyber incidents Tactics, Techniques

Vulnerabilities

Benchmark of Incidents (Incident database, Clients Assessments, Synthetic Profiles)

Impacts & Losses

Mitigations Controls & Projects Capex, Opex, Implementation time

DERISK

NoA
Number of Attempts

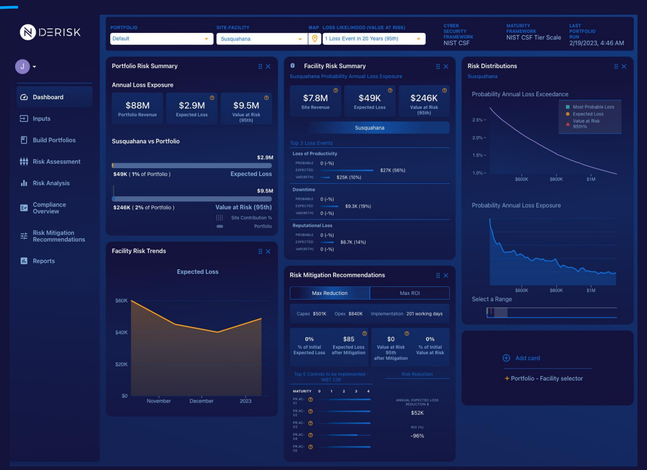
SCOTT
Security Controls for OT

APA
Attack Path Algorithm
Unit, Portfolio

LEI
Loss Event Impact
Unit, Portfolio

MRS
Cyber Risk Mitigation Recommendations

Cyber Risk Quantification & Management



- Executive Dashboard
- Portfolio Builder
- Risk Assessment
- Risk Analysis
- Indicators . Control, Risk, Performance
- Compliance Overview
- Mitigation Recommendations
- What If Scenarios
- Reports

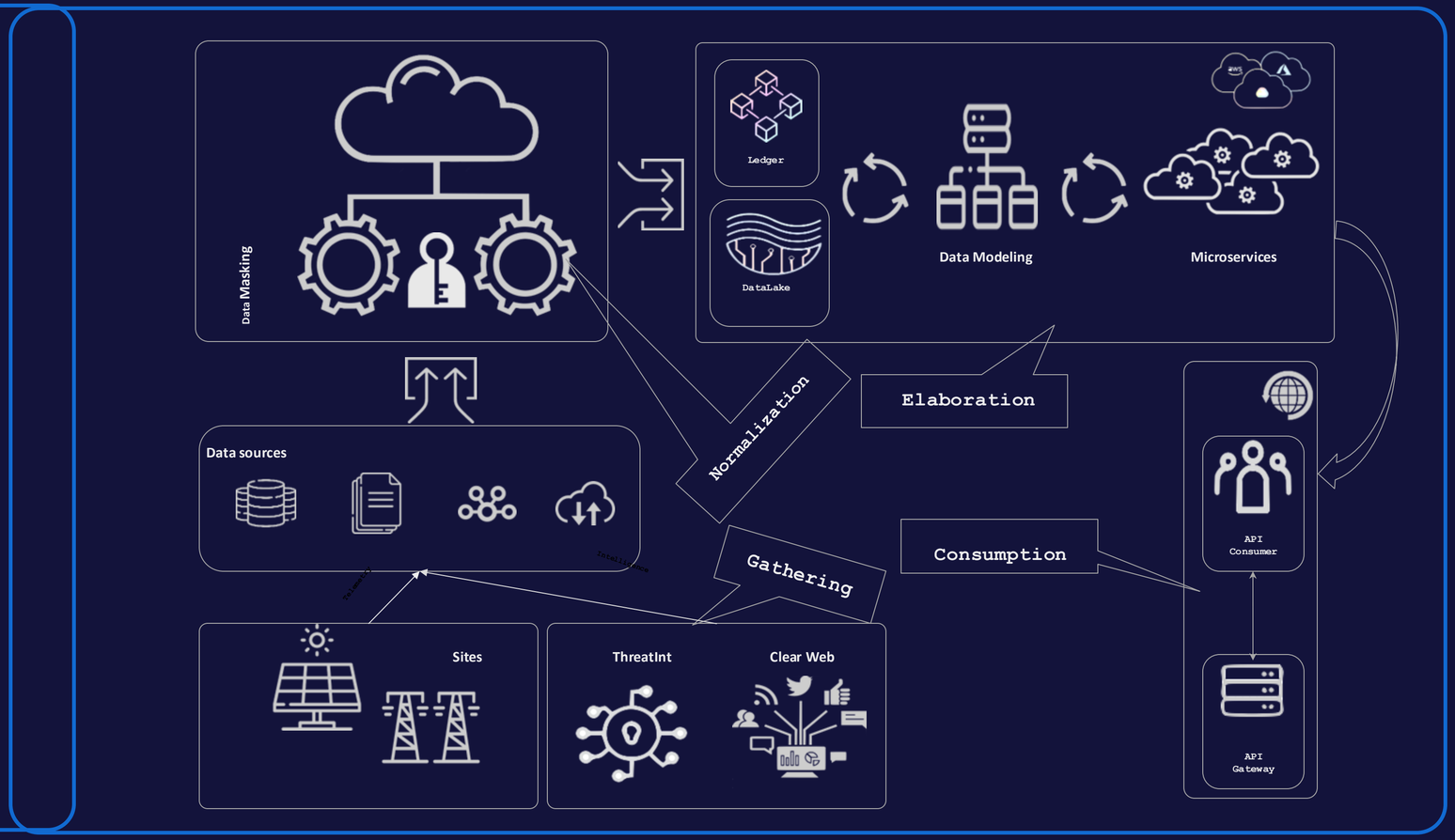
Trusted Ecosystem

Only one option to make it real

Data QUALITY

Data INTEGRITY

ACCOUNTABILITY



NoA: Number of Attempts

How many attempts in a year?

Organization and context

Firmographics

- Region
- Vertical
- Revenue / Growth
- Employee count
- Ownership
- Stock market

Contextual

- Supply Chain
- Unconventional Signals
- Attractiveness

Threat Intel & Monitoring

- Own leaked credentials
- Supply chain leaked credentials
- DNS subdomains found
- Attack surface (total external exposure footprint)

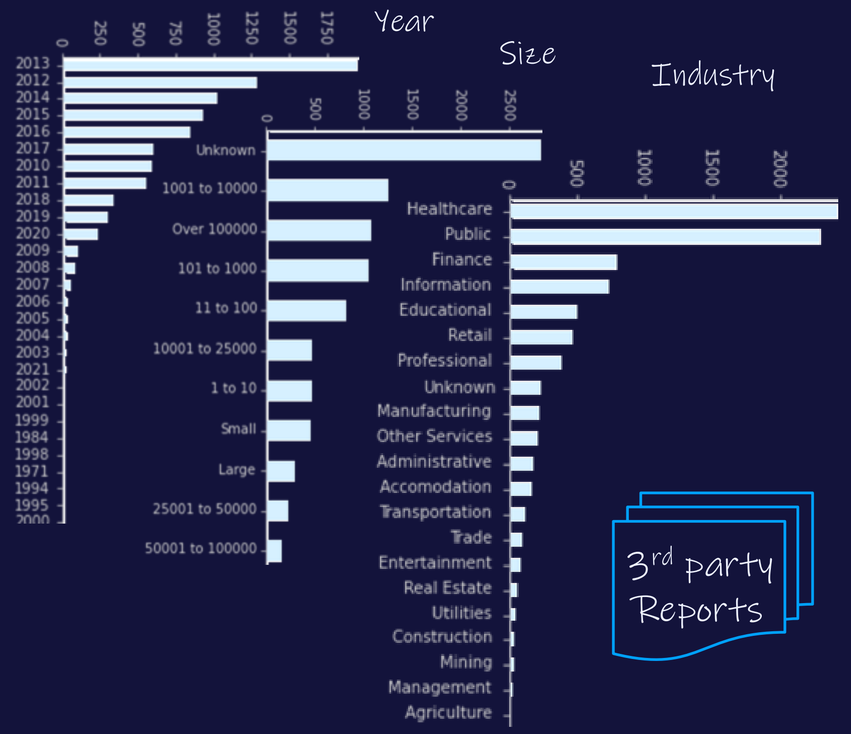
Cyber Threats

Initial Access Vector

Cyber Threat Landscape

- Threat actors (Activity, Capacity, Targets, etc.)
- External vulnerabilities

Metadata on Cyber Incidents

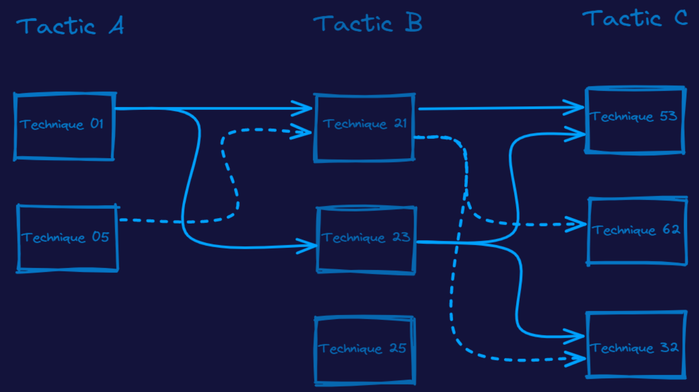


3rd party Reports

APA: Attack Path Algorithm

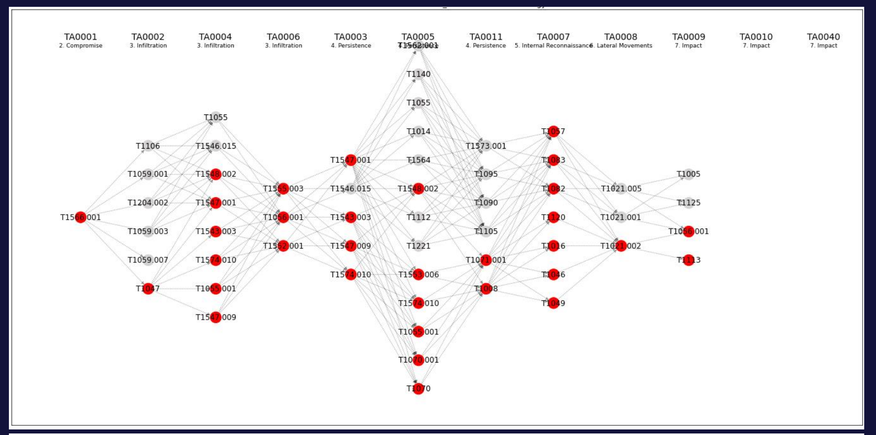
How can an incident propagate and cause a loss event?

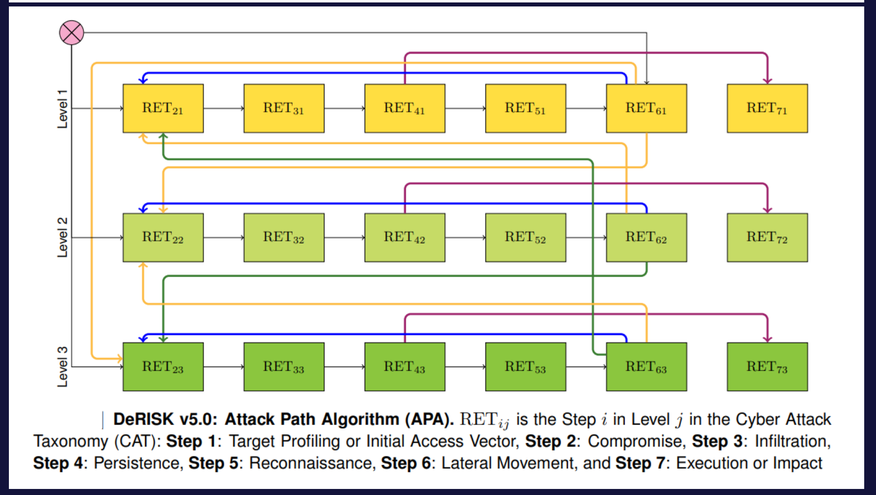
What and How?



Players

Probability of Success



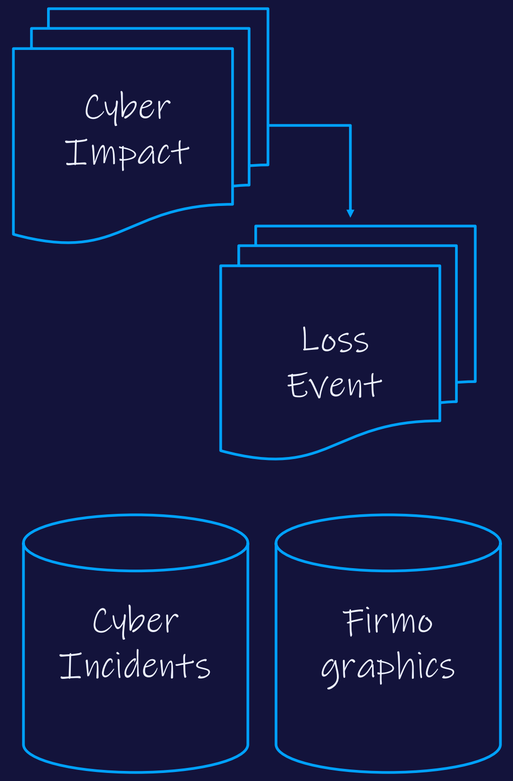


DeRISK v5.0: Attack Path Algorithm (APA). RET_{ij} is the Step i in Level j in the Cyber Attack Taxonomy (CAT): **Step 1**: Target Profiling or Initial Access Vector, **Step 2**: Compromise, **Step 3**: Infiltration, **Step 4**: Persistence, **Step 5**: Reconnaissance, **Step 6**: Lateral Movement, and **Step 7**: Execution or Impact

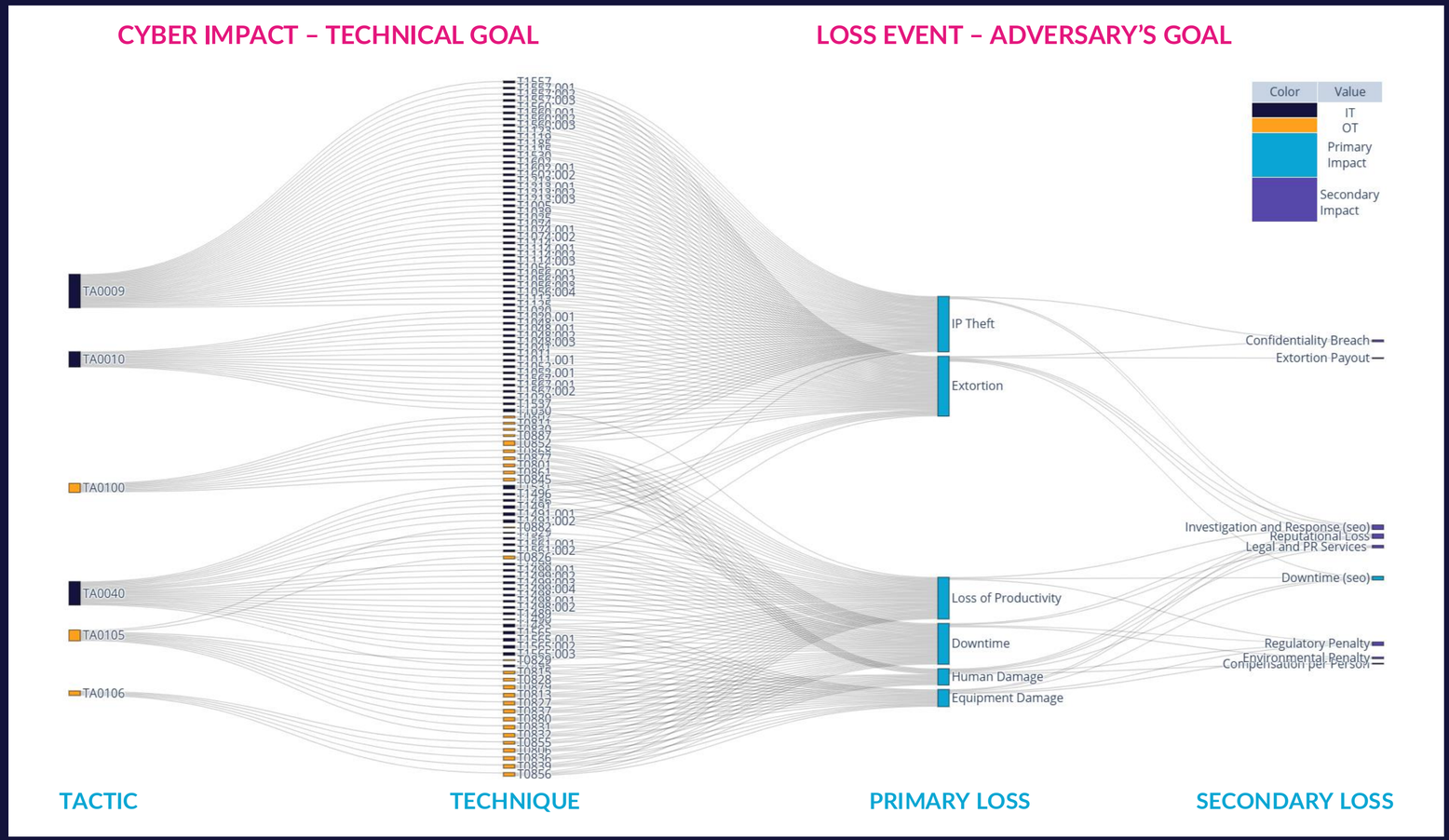
LEI: Loss Event Impact

What is the financial impact ($)?

What, How and How much?

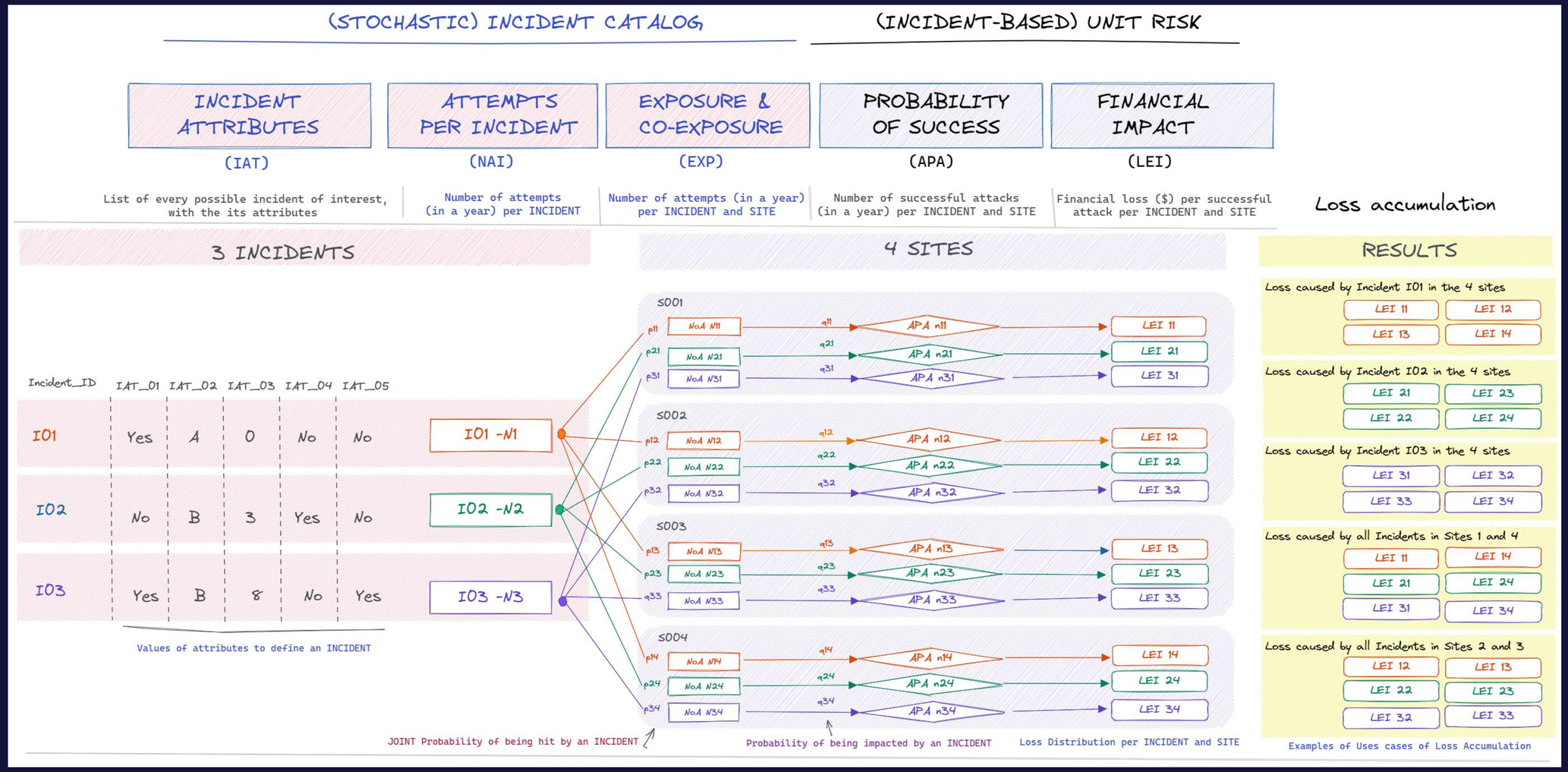


Impact propagation



Cyber CAT: Accumulation and Portfolio

Dependency Structure – Vine Copulas



DeRISK – Validation and Calibration

Benchmark of incidents – Continuous effort – Dedicated team

Statistical Quality

The loss distribution is obtained with a sequential sampling problem:

- Convergency of numerical methods
- Variability of quantiles
- Robustness of the results
- Tail stability

Sensitivity Analysis

- Hundreds of inputs used
- Contribution per input
- Robustness to changes in the input's definition
- Comparison of distributions

Suite of tests

Business Quality

Benchmark of cases to analyze and validate, make sense, each piece of the system with SMEs

V5 Benchmark

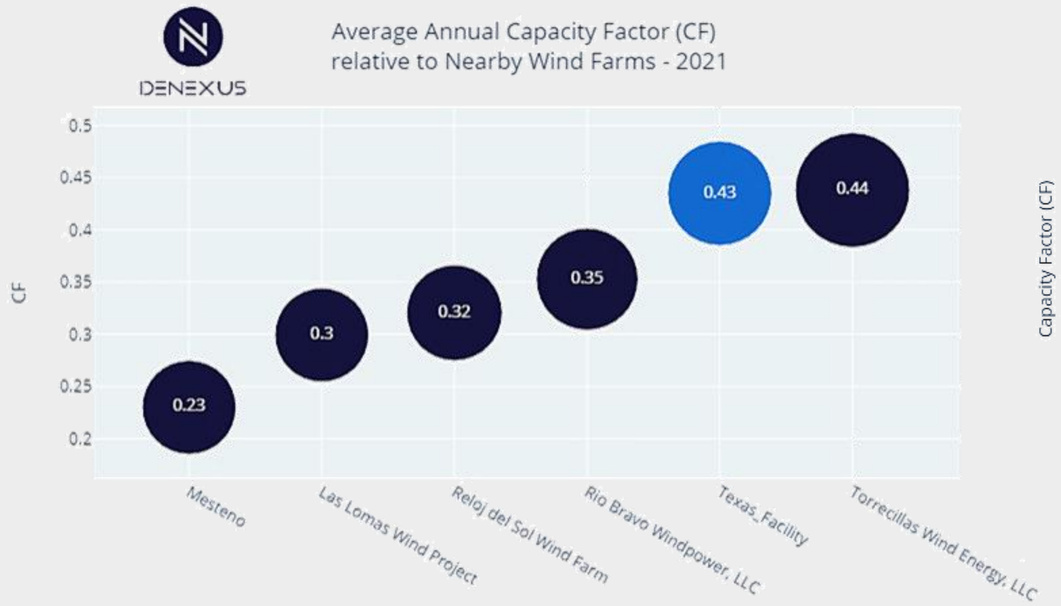
Synthetic Profiles	Clients Assessments	Incident-based
7	3	4

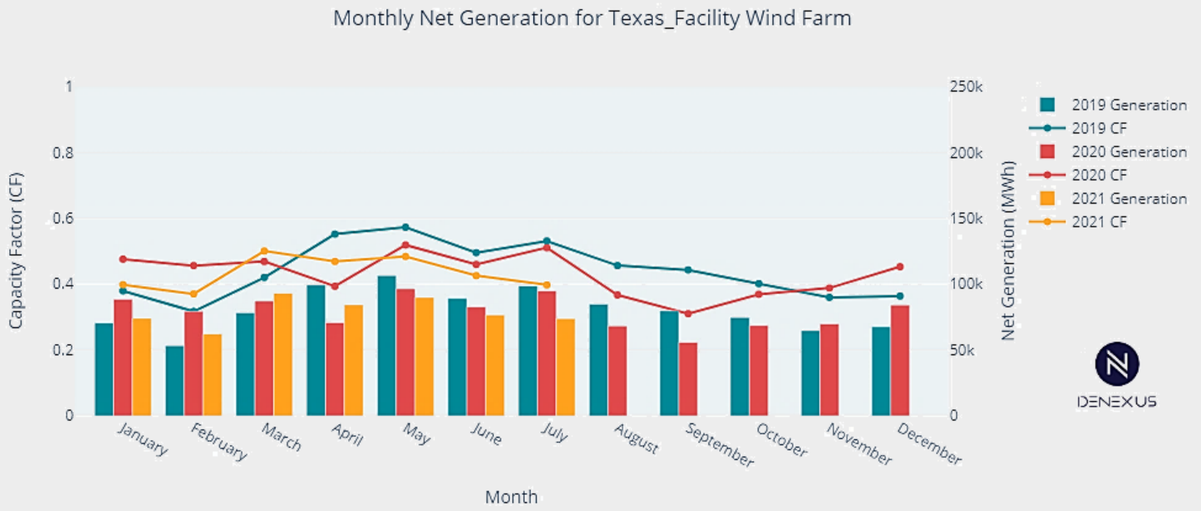
- Quantified $ losses within realistic range
- Results realistic to ICS/OT systems and industries

Unlocking the value

The site: Texas Facility

Facility performs more efficiently than most of its regional peers. Similar annual net generation in the last 3 years.





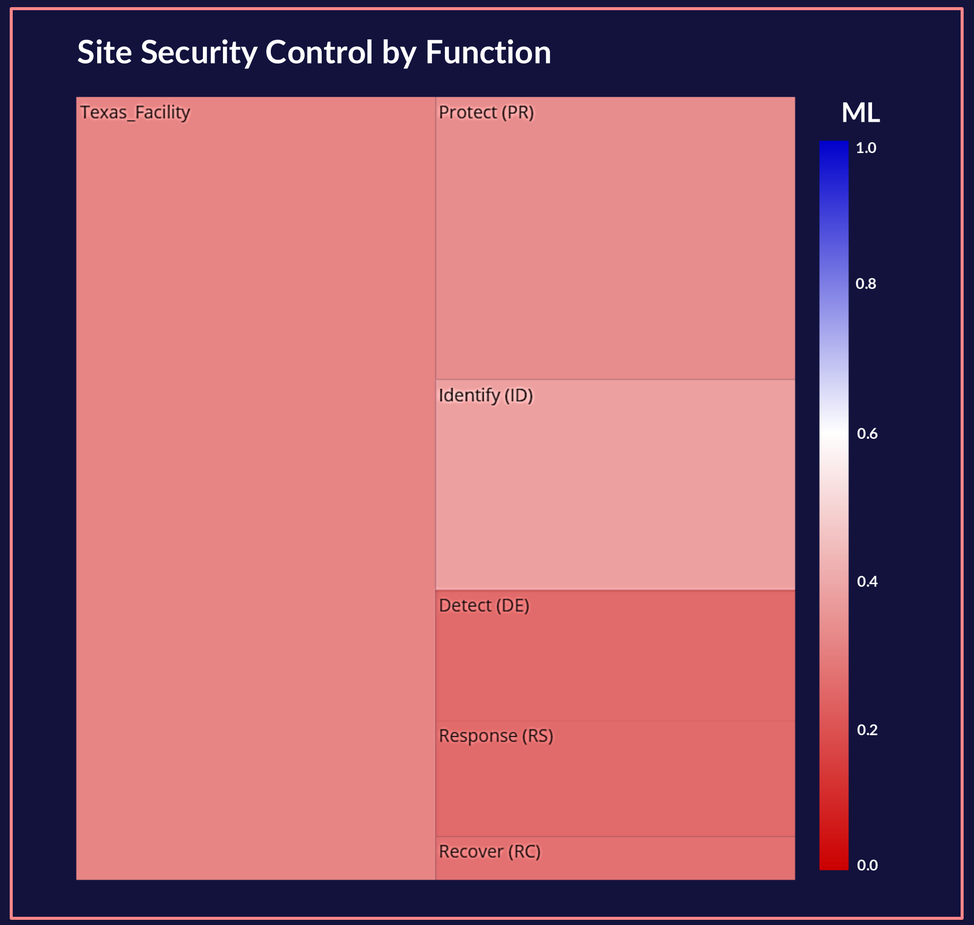
Country:	US
GPS:	32° 32' 25.152" N
GPS:	99° 43' 8.112" W
Operating since:	2010

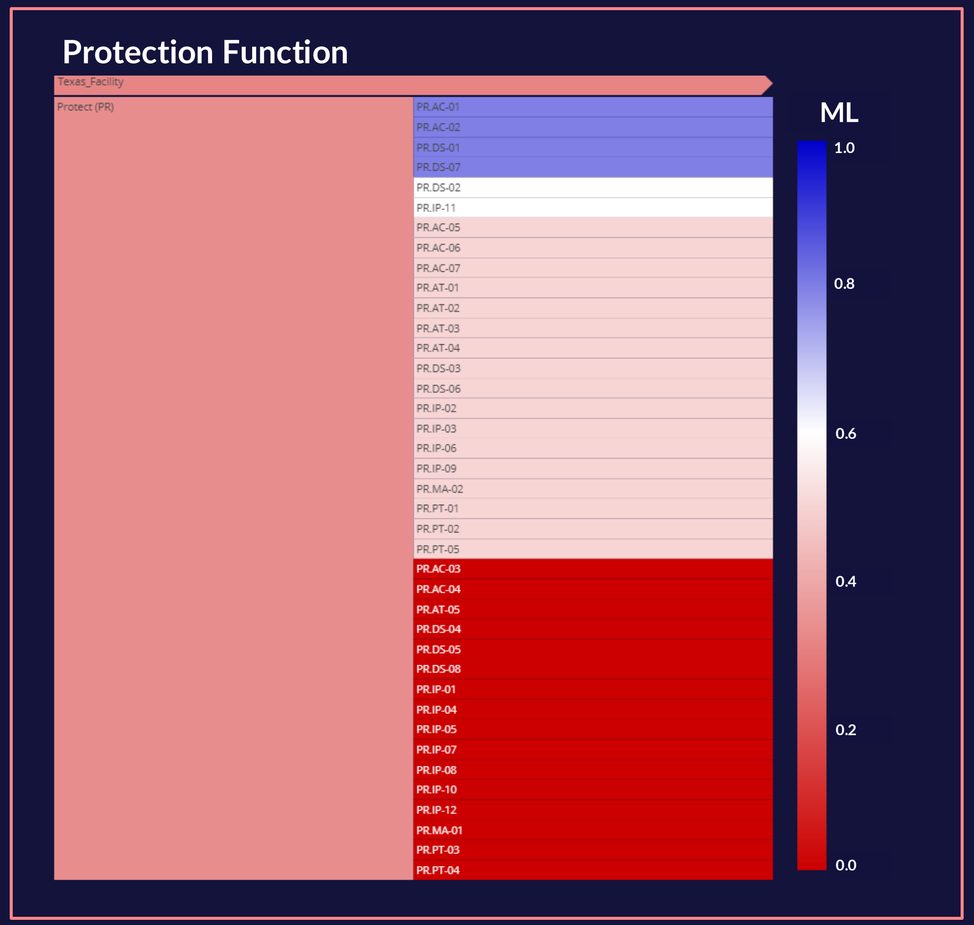
Owner:	Demo Wind Ventures
Operator:	Demo Operating Company
OEM:	VestasWind
Developer:	Demo Clean Power

Number of Turbines:	125 Vestas V100/2000
Turbine Capacity (MW):	2.0
Farm Capacity (MW):	250
Fuel Type:	Wind

Capabilities Assessment - Cyber Security Framework

Strength: Identify | Weakness: Recover





- Highest functional capability (strength) is *Identify*
- Lowest functional capability (weakness) is *Recover*

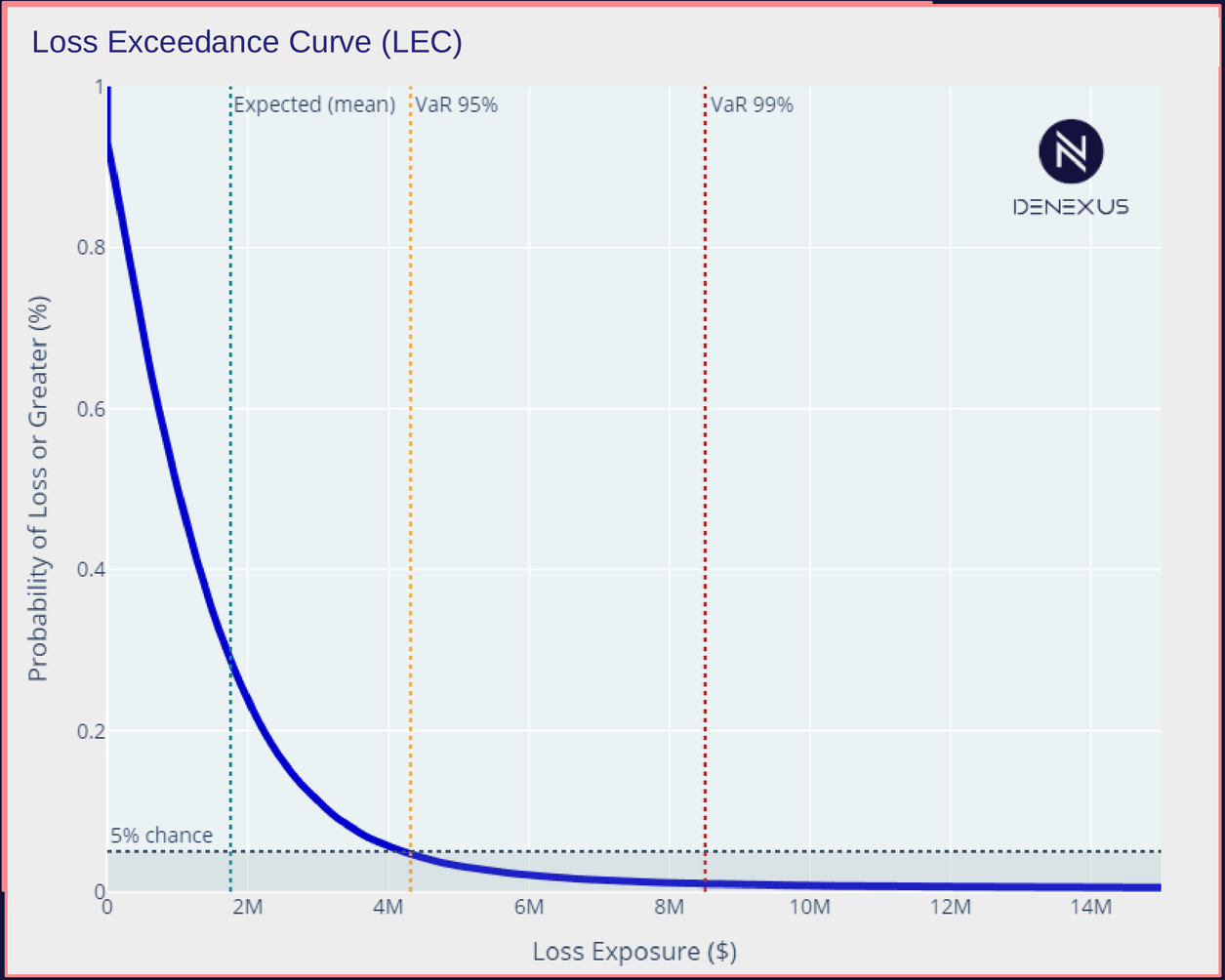
- 4 out of 36 Security Control with Protection Function are above 0.8
- 14 out of 36 Security Control with Protection Function are *Not initiated*

Capabilities Assessment - Cyber Security Framework

Protect Function contains the most advanced capabilities. Many security controls not initiated

Site Cyber Risk Assessment

5% probability of Annual Cyber Loss of $4MM or greater



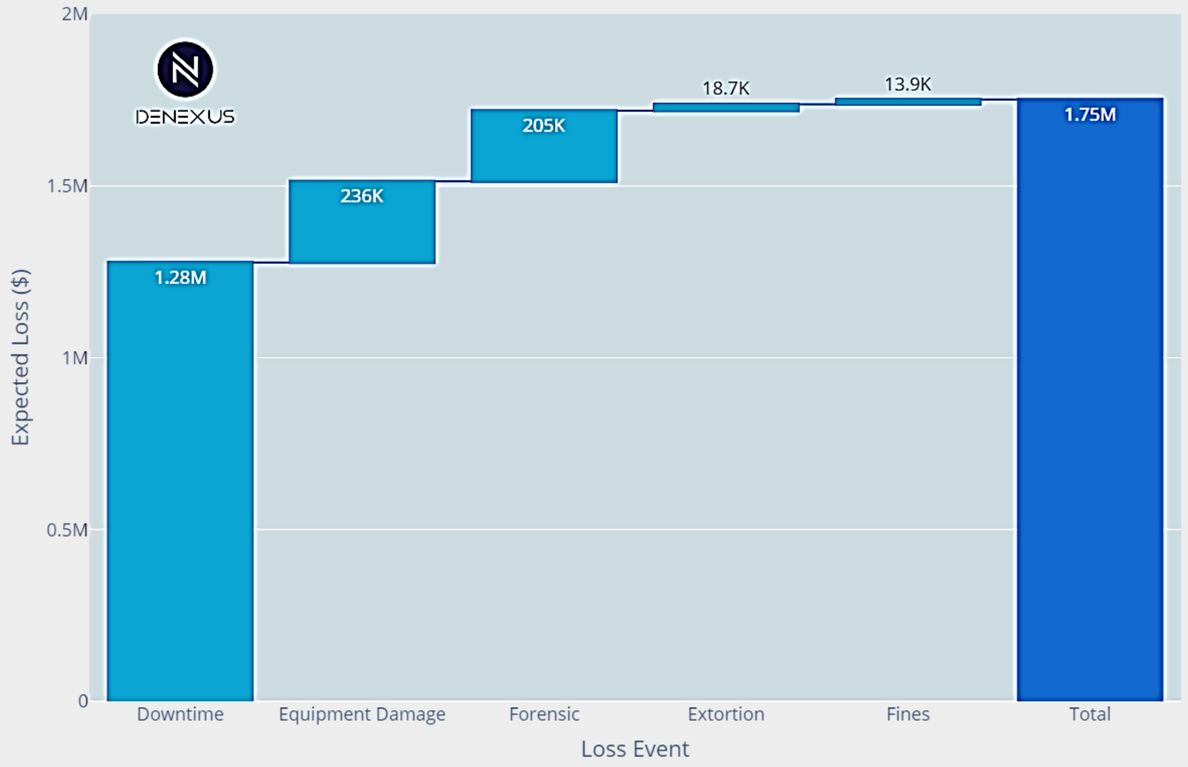
LEC visually display the probability that cyber loss will exceed some amount within a year

Metric	Value	Description
Revenue	$35.9M	DeNexus sourced starting number for site. Update for specificity.
Expected Loss	$2.0MM	In statistical terms, the expected loss is the mean loss that we would expect over a given period of time (year). The expected loss is an average used for provisioning.
Unexpected Loss	$1.20MM	Unexpected losses are loss percentiles in excess of the expected loss
Value-at-Risk (95%)	$4.00MM	VaR is a measure of risk that tries to answer the following question: "How bad can things get?"" In statistical terms, the VaR is the loss value for which the probability of observing a larger loss, given the available information, is equal to 1-p
Exceptional Loss	$8.3MM	Unexpected loss does not include exceptional losses beyond the loss percentile defined by a confidence level. Exceptional losses are in excess of the sum of expected loss plus the unexpected loss, which is equal to the loss percentile L(a).

Where is the cyber risk?

Annual Expected Loss ($) by Exposure Type

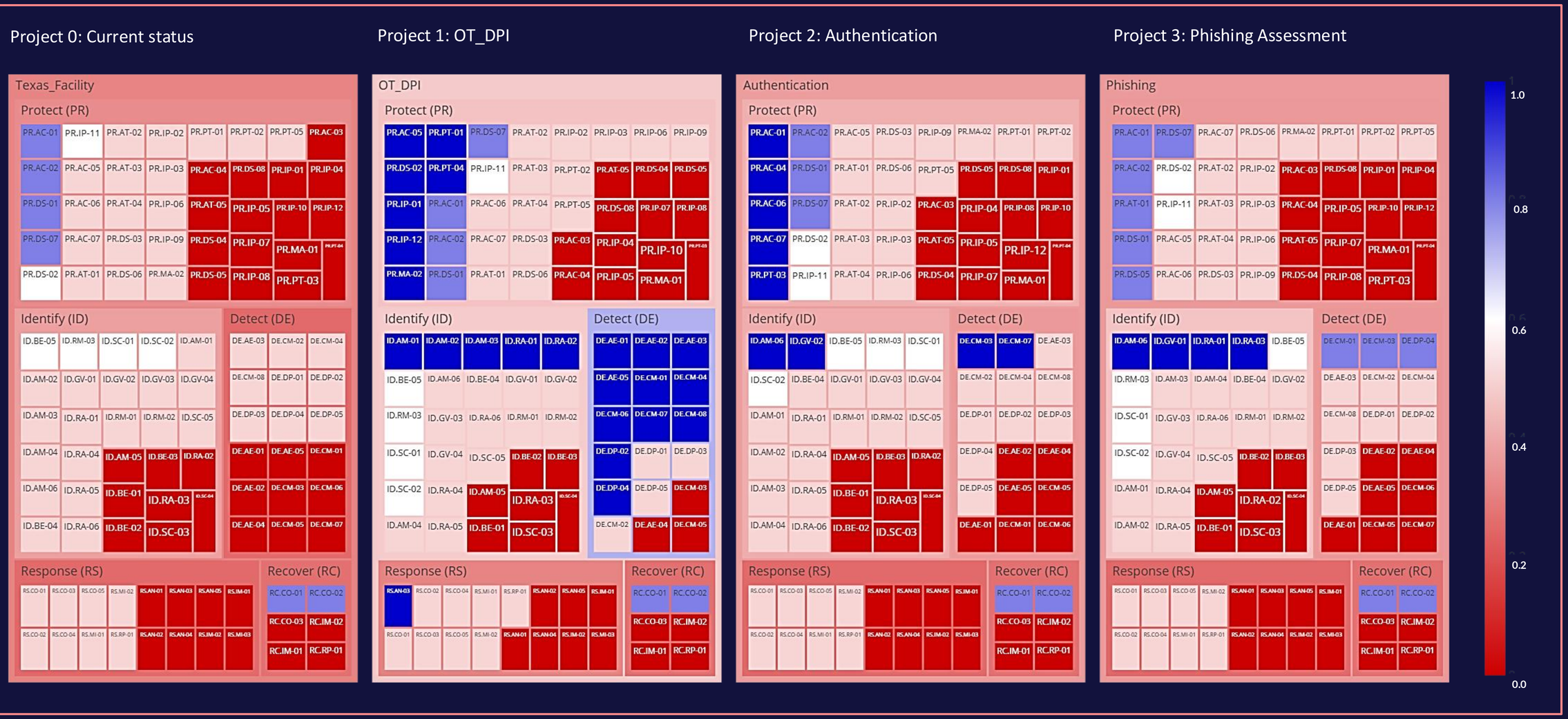
Breakdown of the Annual Expected Loss by Exposure Type



- Coverage: Liability Insurance vs. Property Insurance.
- If one were assessing an insurance policy, notice 73% of cyber risk is in Downtime whereas Equipment Damage represents only 13% of site risk

What-if?

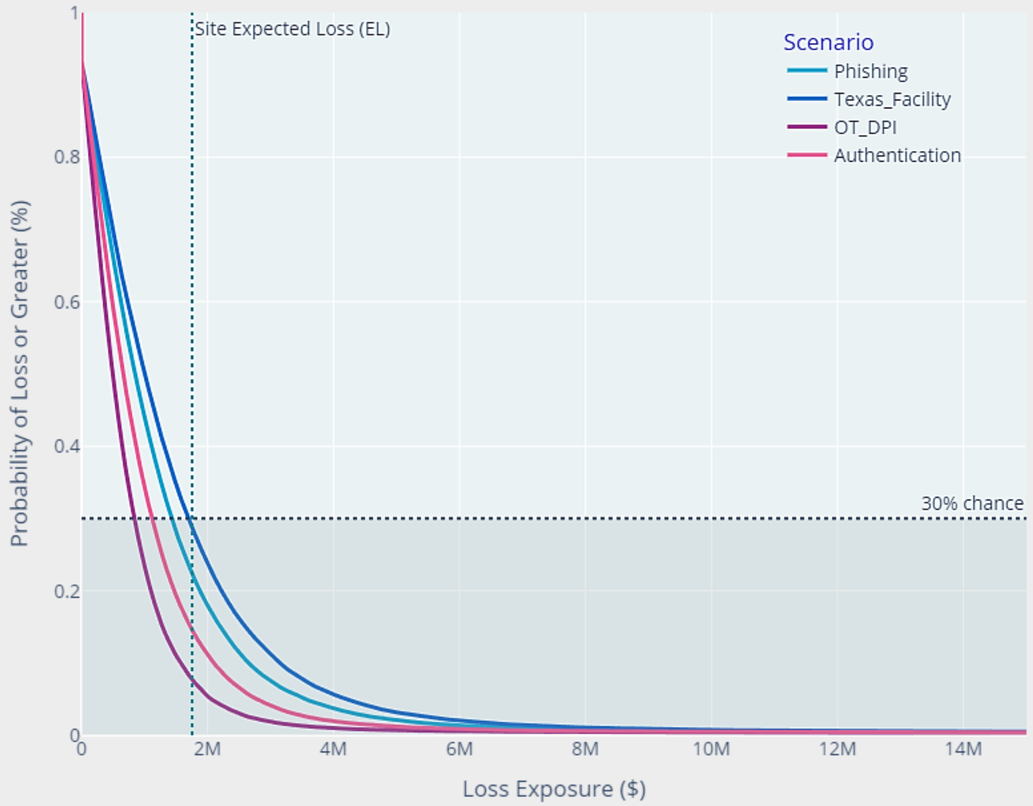
Customize the implementation scenario, or the contribution of any given sub control to that scenario definition.



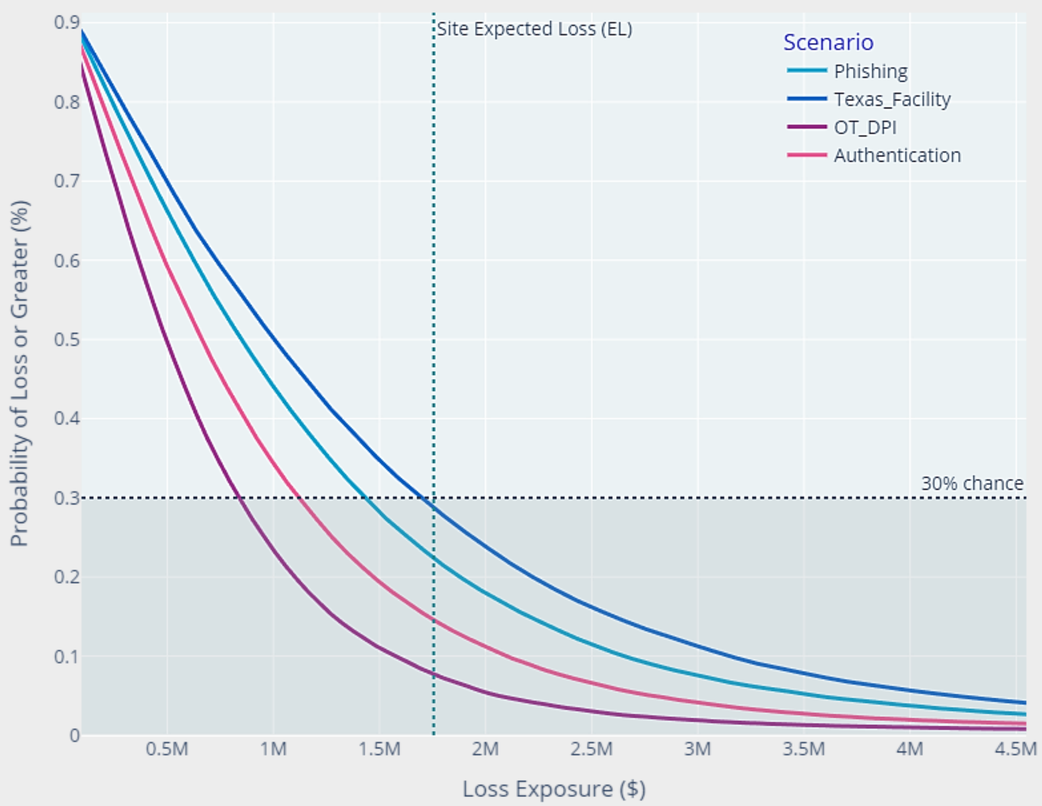
What scenario provides the most risk reduction

OT-DPI provides the biggest risk reduction

Loss Exceedance Curve by what-if scenario



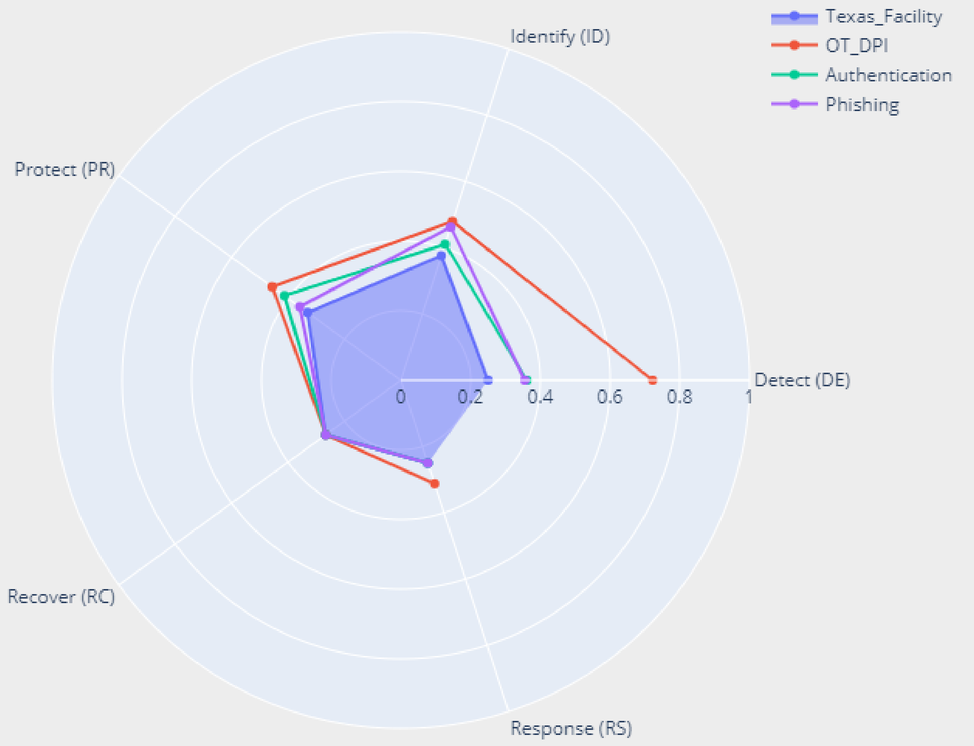
Risk Reduction – 30% chance



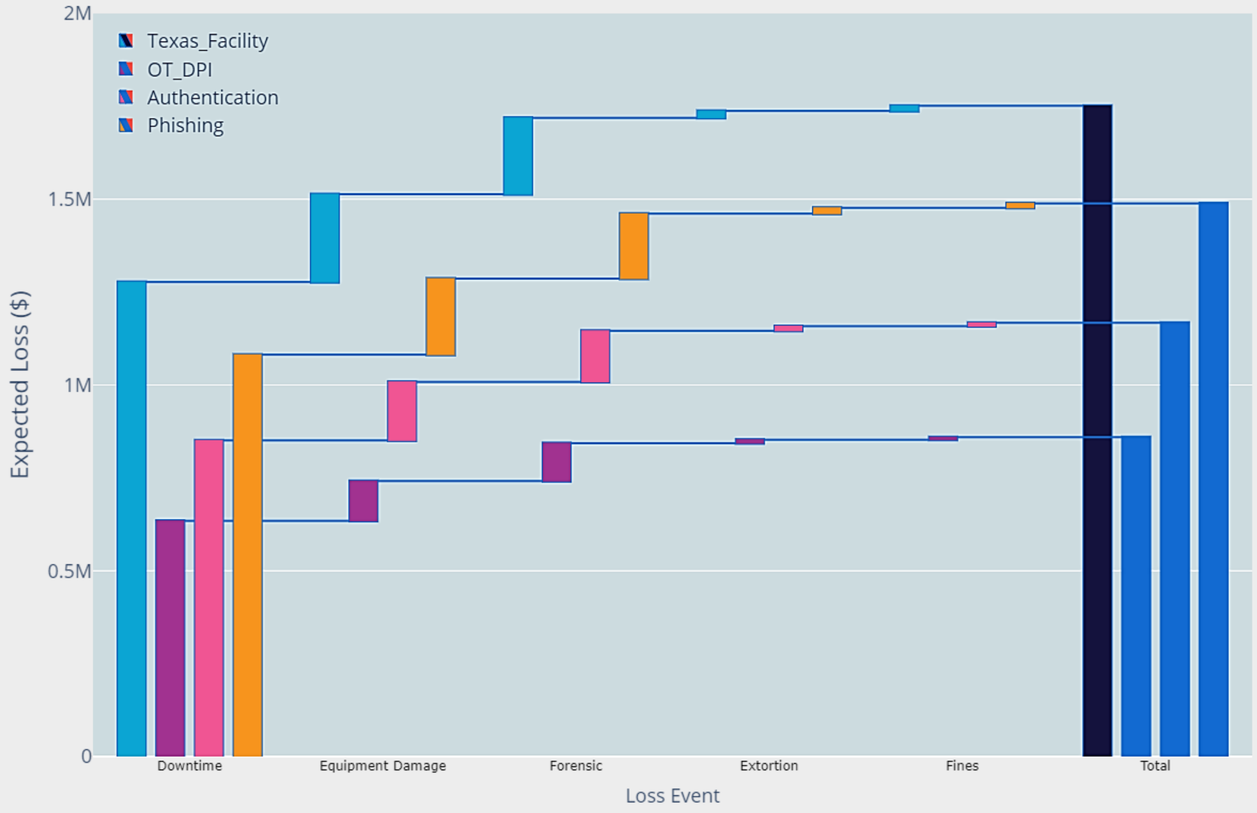
What scenario provides the most risk reduction?

Different initiatives | Different risk reduction

4 Security Control Portfolios



Expected Loss by Event Type: 4 Security Control Portfolios



What mitigation provides the most risk reduction?

Recommendations based on ROI, NPV, Fastest

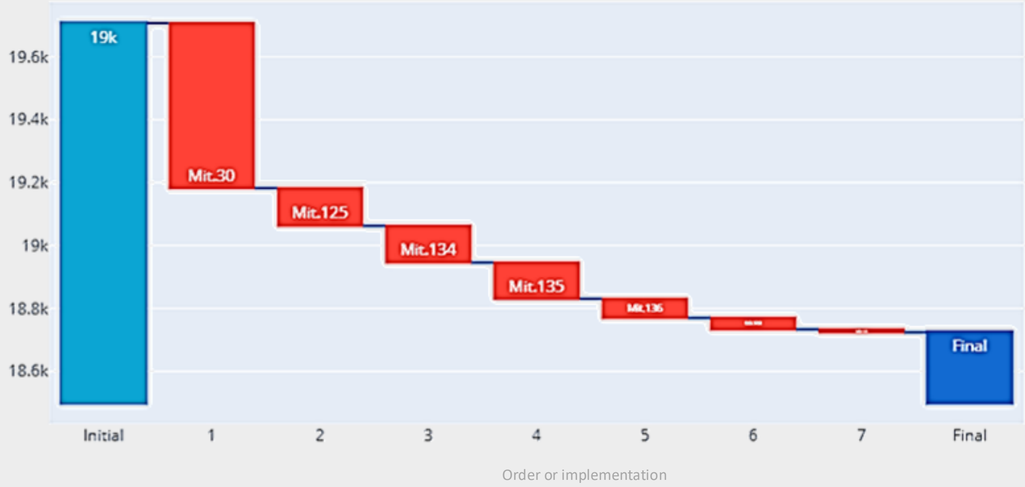
Top 5 Mitigation
Considering Highest Risk Reduction and Lowest Investment

- Stand-alone mitigation analysis .
- Capex, Opex and time of implementation are inputs of the system

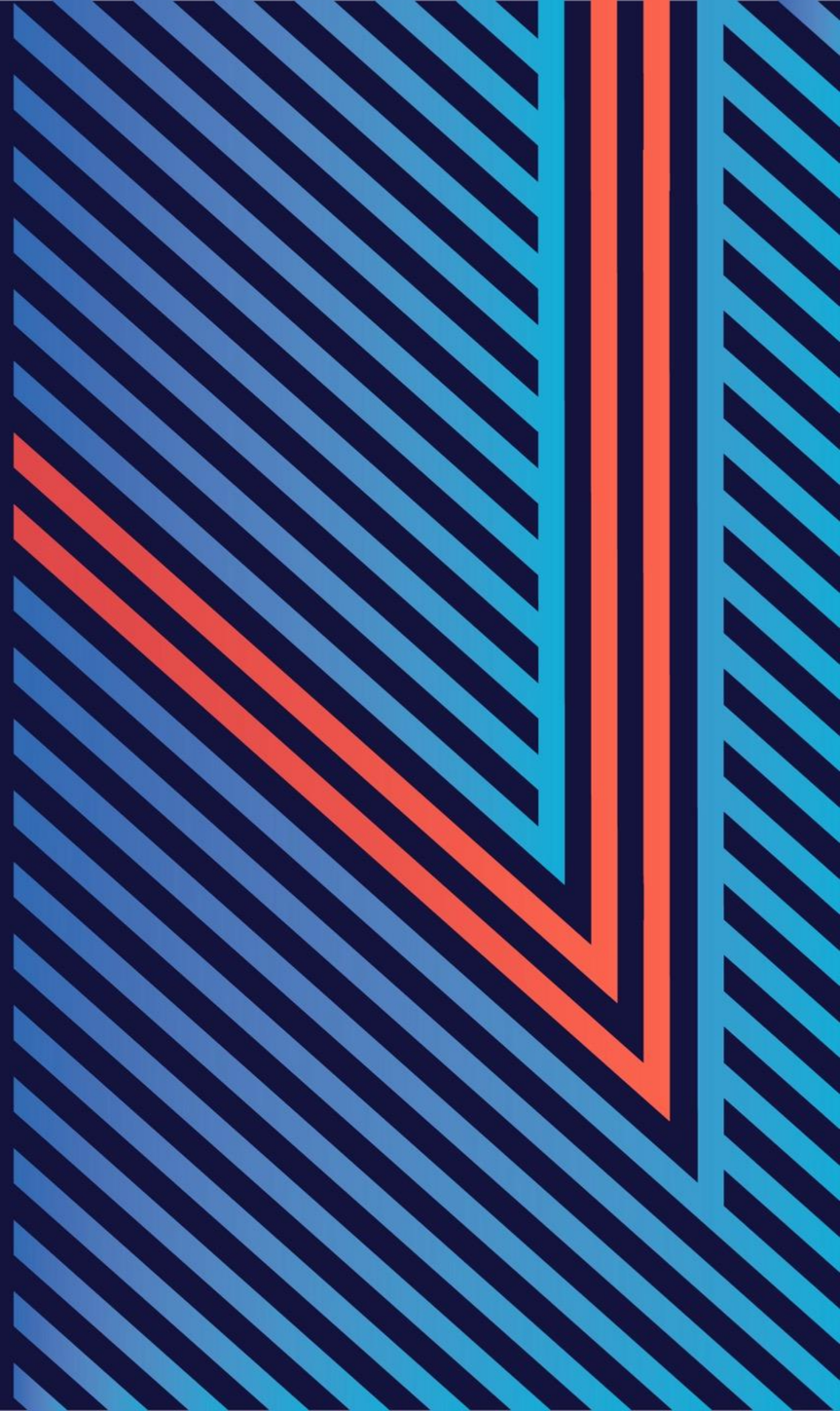
	_PR.AC-01_	_PR.IP-11_	_PR.DS-05_	_PR.AC-03_	_ID.RM-01_
Security Control	PR.AC-01	PR.IP-11	PR.DS-05	PR.AC-03	ID.RM-01
Current ML	Risk-Informed	Repeatable	Risk-Informed	Risk-Informed	Partial
Recommended ML	Repeatable	Adaptable	Repeatable	Adaptable	Risk-Informed
Risk Reduction ($)	6046	5287	4423	3772	3465
Investment ($)	294	98	294	392	735
Man Hours	2	1	2	3	6
Description	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	Cybersecurity is included in human resouRecoveres practices (e.g., deprovisioning, personnel screening)	Protections against data leaks are implemented	Remote access is managed	Risk management processes are established, managed, and agreed to by organizational stakeholders

Top 7 Mitigation
Considering Highest Risk Reduction

- Optimal mitigation Portfolio .
- Capex, Opex and time of implementation and Dependency between mitigations are inputs of the system



With DeRISK …



Unlocking the value in data

Costly Unanswered Questions for Industrial Underwriters

Single-Risk Assessment

Mitigation Strategies

Project advance What-if?

Portfolio-Risk Accumulation

How do we price and assess cyber risk premiums?

Takeaways

DeRISK – 2nd Generation Cyber Risk Modeling

Inside-Out data contextualized with underlying Industrial Process & Business data

The Challenge

- We need CRQM
- NAT CAT models not for CYBER CAT
- Reliable models
- 1st generation failed

The Answer

- **Data is the foundation**
  - Inside-Out & Outside-In evidence-based data
- **Data in context**
  - Underlying Industrial Process & Business data
- **Data-driven decisions**
  - Continuous risk evaluation in financial terms
  - Efficient ROI-based risk mitigation
  - Determination of risk to be transferred
- **Bottom-up accumulation**
- **Trusted Ecosystem**
  - Encrypted Data
  - Safe Insights

DeNexus Knowledge Center

Trusted Ecosystem

Takeaways

DeRISK – 2nd Generation Cyber Risk Modeling

Inside-Out data contextualized with underlying Industrial Process & Business data

The Challenge

- We need CRQM
- NAT CAT models not for CYBER CAT
- Reliable models
- 1st generation failed

The Answer

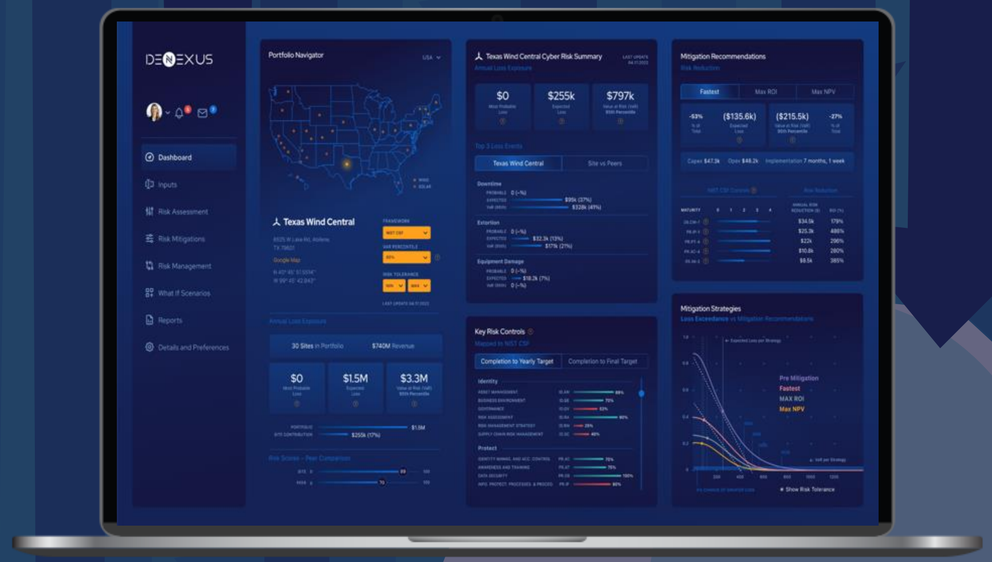
- **Data is the foundation**
  - Inside-Out & Outside-In evidence-based data
- **Data in context**
  - Underlying Industrial Process & Business data
- **Data-driven decisions**
  - Continuous risk evaluation in financial terms
  - Efficient ROI-based risk mitigation
  - Determination of risk to be transferred
- **Bottom-up accumulation**
- **Trusted Ecosystem**
  - Encrypted Data
  - Safe Insights

DeNexus Knowledge Center

Trusted Ecosystem

Thank You

Learn more @: DeNexus.io



Romy Rodriguez-Ravines

Head of Research and Modeling Strategies

rr@denexus.io