Centro de Ciberseguridad Industrial

DENEXUS

Modeling of Catastrophic Cyber Events in Industrial Environments.

Impact on Portfolio Risk Accumulation

Romy Rodríguez-Ravines
rr@denexus.io | Sep 29, 2022

Turning Data into Knowledge

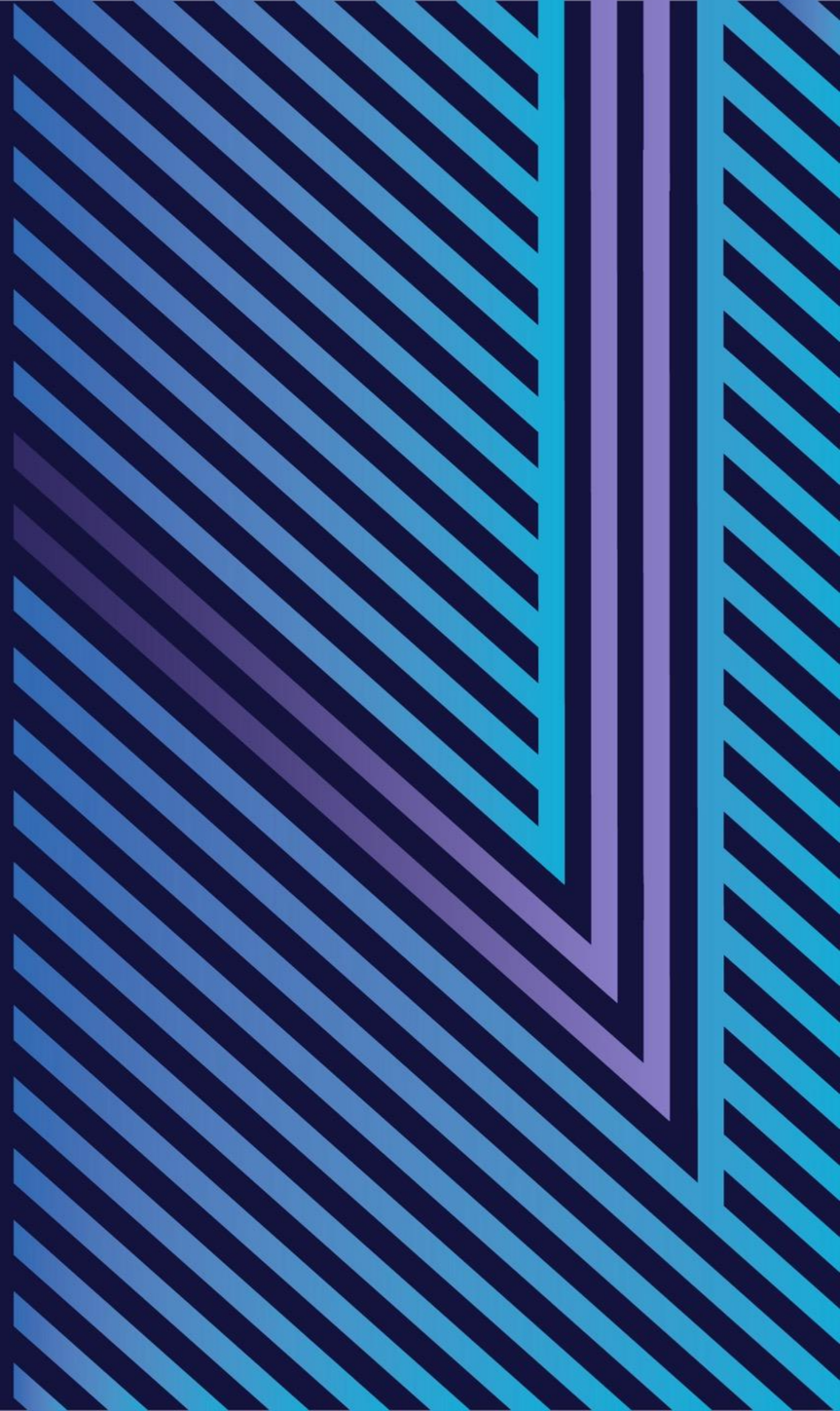
Overcoming Knowledge Siloes and Analyzing Complex Datasets

- Business Financials
- Risk Management
- Cyber Security
- Insurance
- ICS / OT

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

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

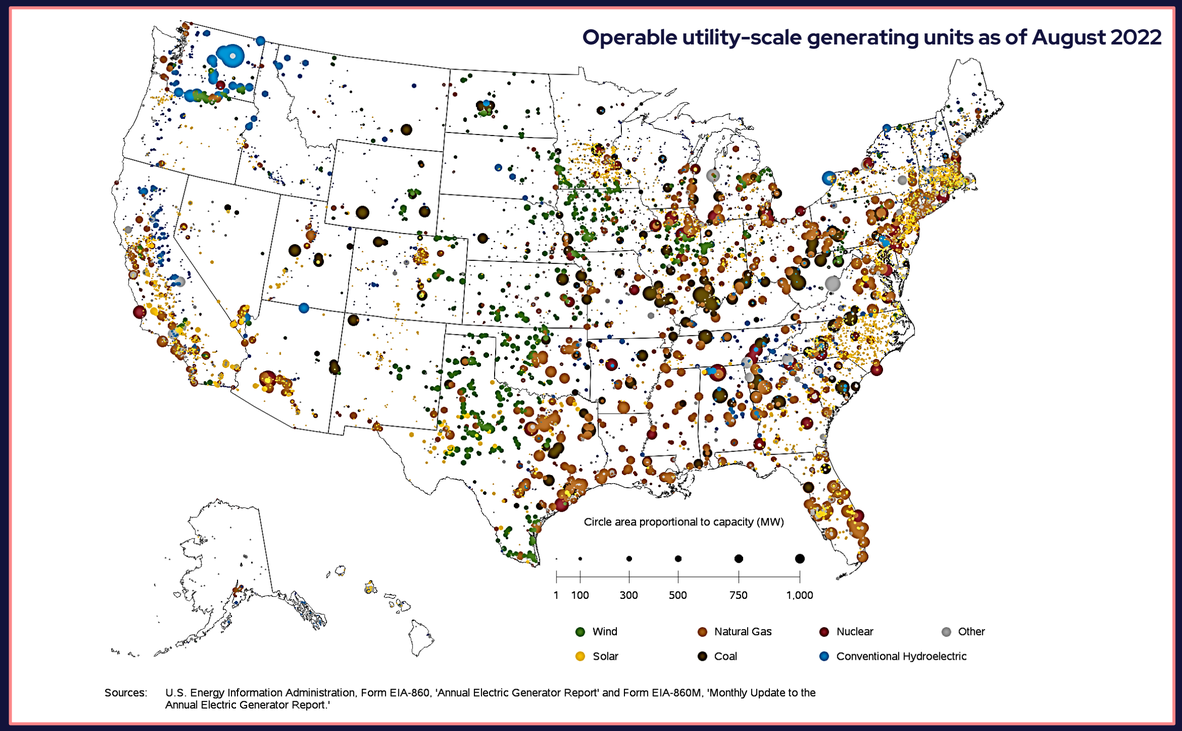
Catastrophes are infrequent events that cause severe loss, injury or property damage to a large population of exposures. While the term is most often associated with natural events (e.g. earthquakes, floods or hurricanes), it can also be used when there is concentrated or widespread damage from man-made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



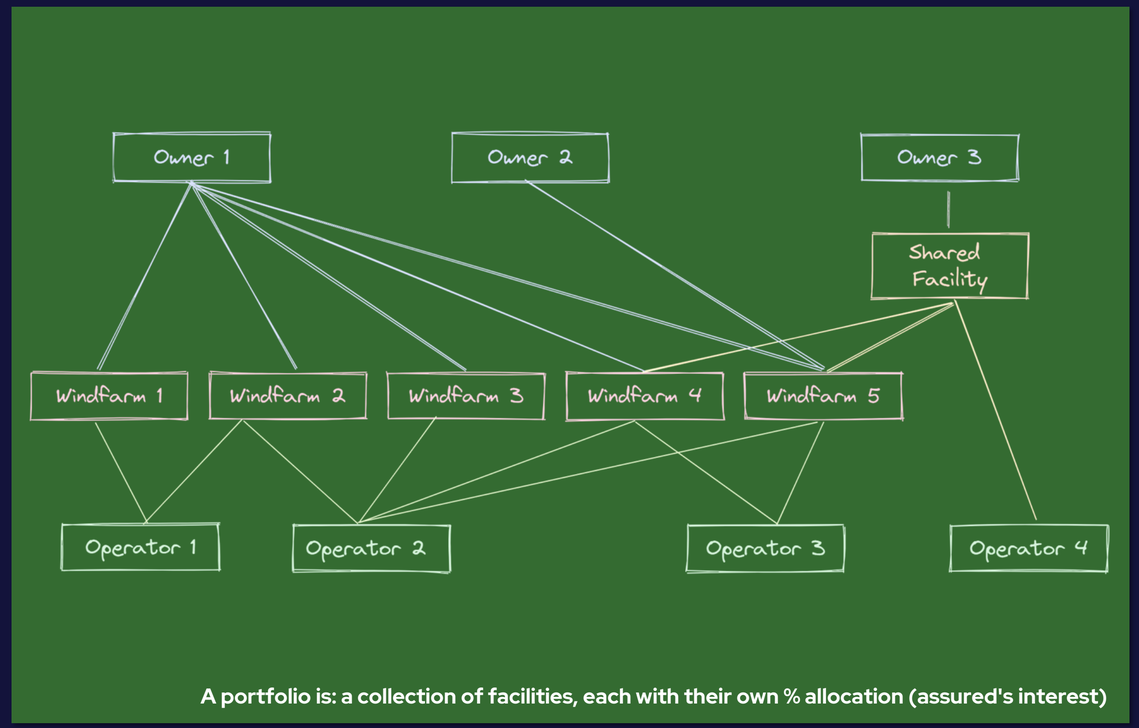
Sources: U.S. Energy Information Administration, Form EIA-860, 'Annual Electric Generator Report' and Form EIA-860M, 'Monthly Update to the Annual Electric Generator Report.'

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

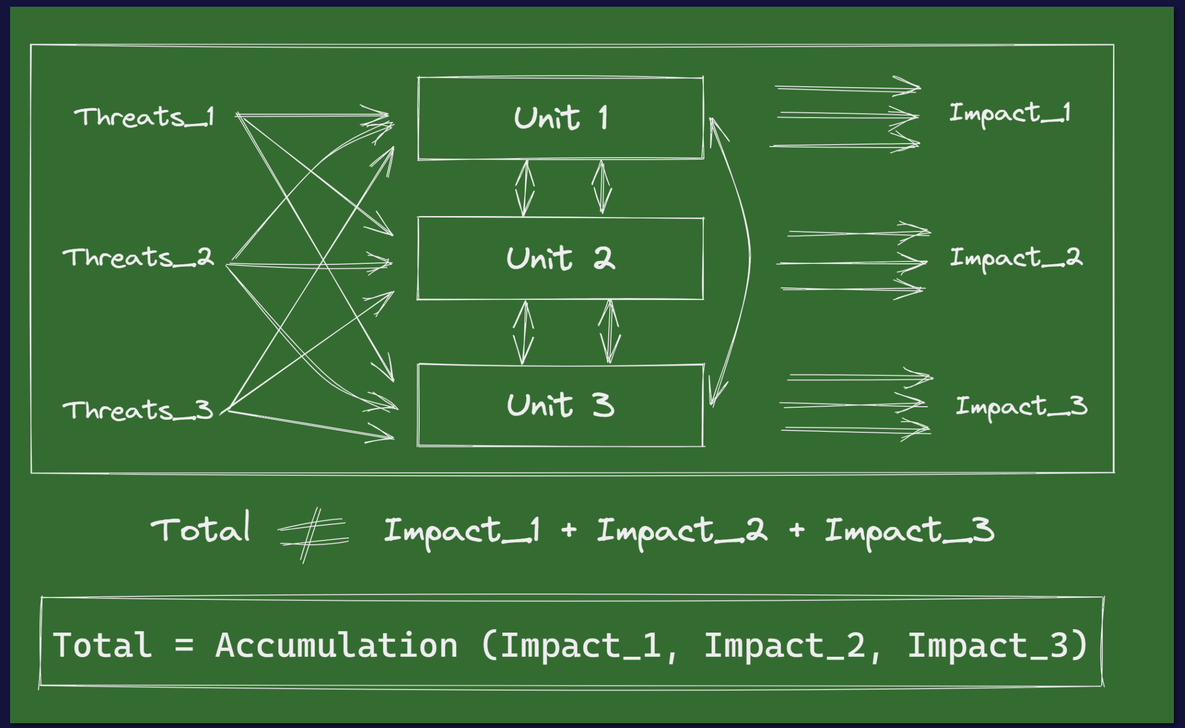
DENEXUS

Data is the foundation

Cyber CAT: Accumulation and Portfolio



A portfolio is: a collection of facilities, each with their own % allocation (assured's interest)



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.

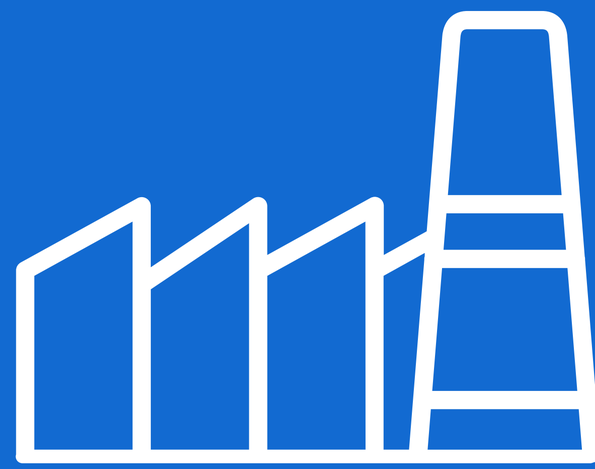
Why OT Data is Different?

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

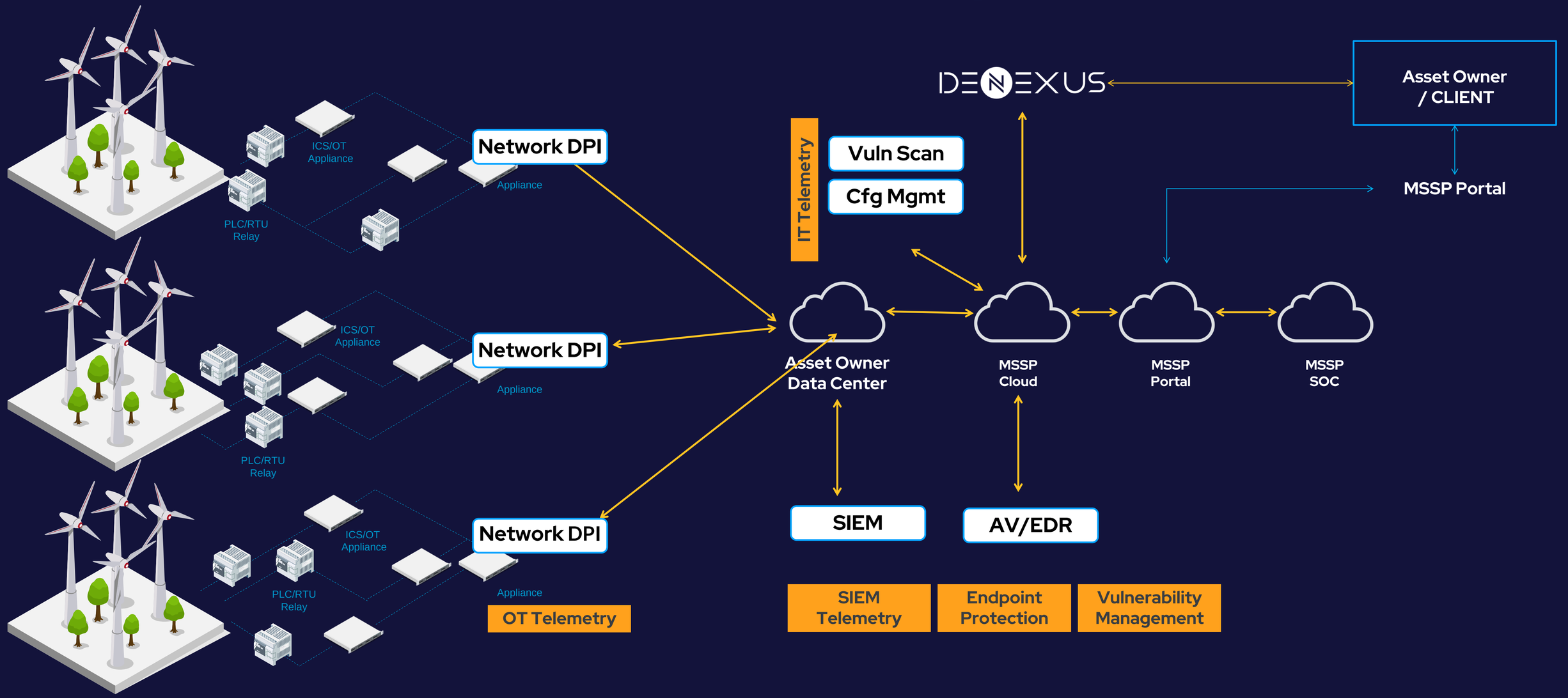
- Impact difference
- Industry – O&G vs. Electric Utility
- Sub Industry - Offshore Wind Turbines vs. Combined Cycle Plant
- Geographic, Public vs. Private, Small vs. Large Revenue



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.

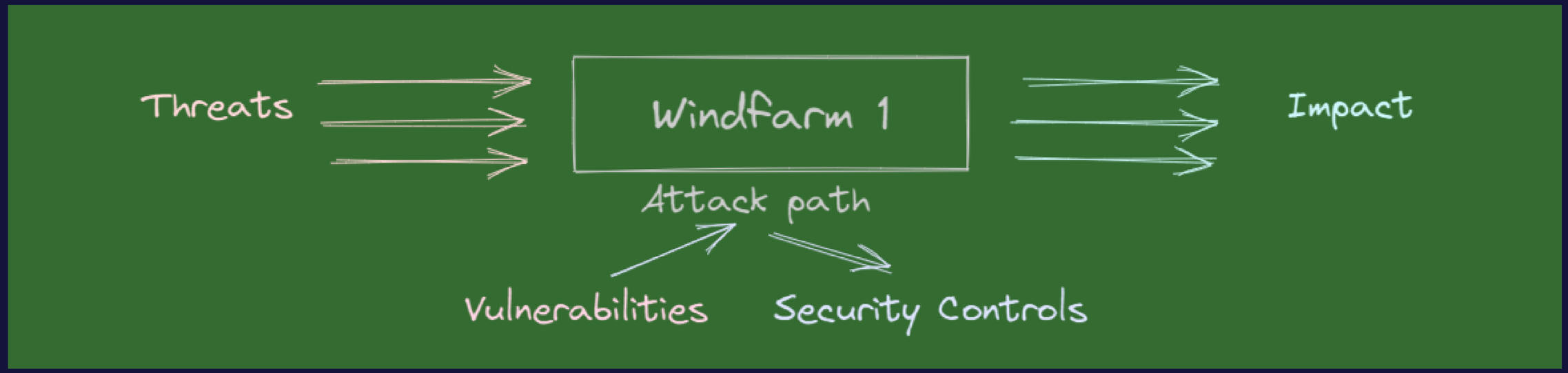
Firmographics

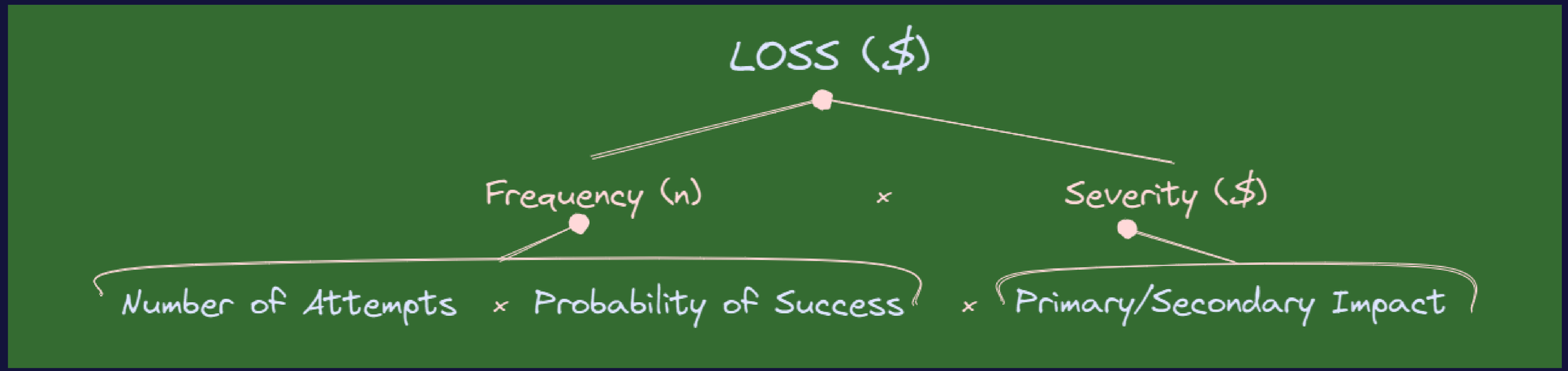
Organization -public- information: location, industry and sub-industry, revenue, size, age Attractiveness

DeNexus Knowledge Center

INDUSTRIAL CRQM | **FIT-FOR-PURPOSE**

Risk Quantification: putting data in context

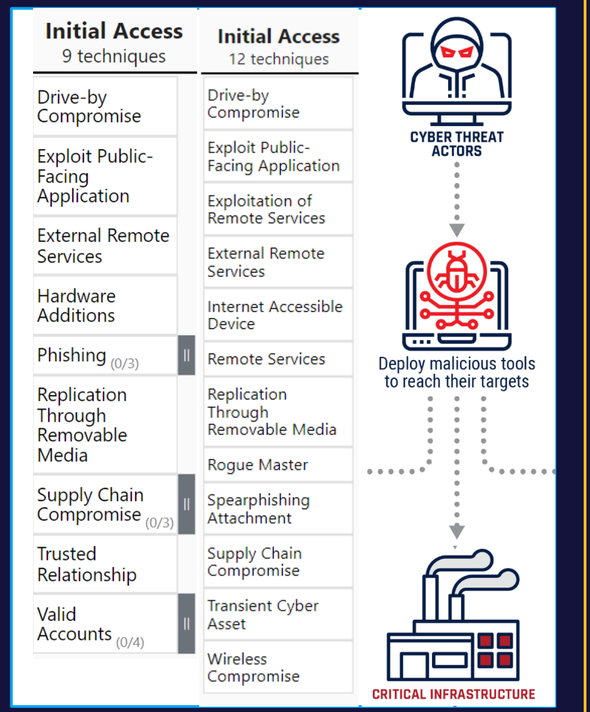




DeNexus Modeling System – Uniquely Approach

Number of Attempts

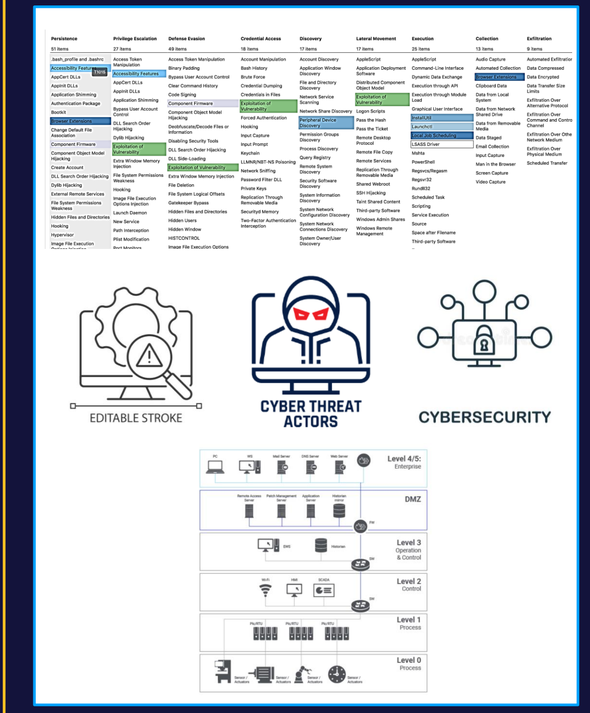
How many attempts in a year?



Powered by Outside-in Data

Attack Path Simulator

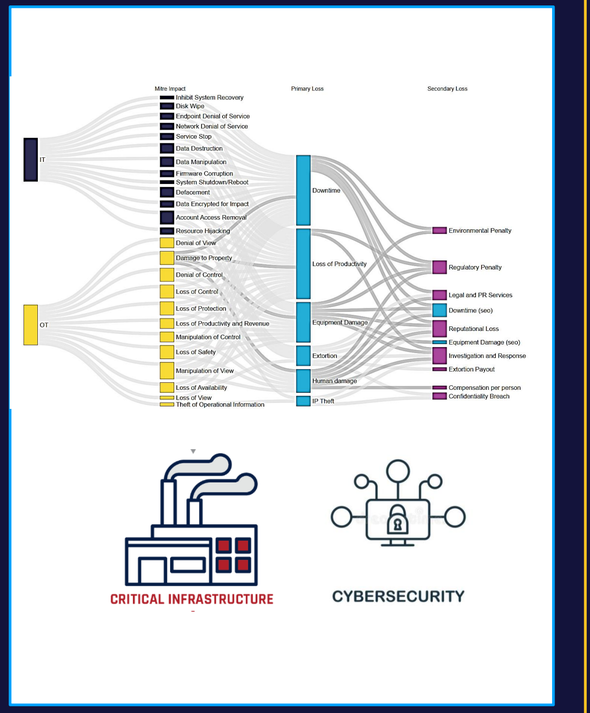
How can an incident propagate and cause a loss event?



Powered by Inside-Out & Outside-In Data

Loss / Severity /Impact

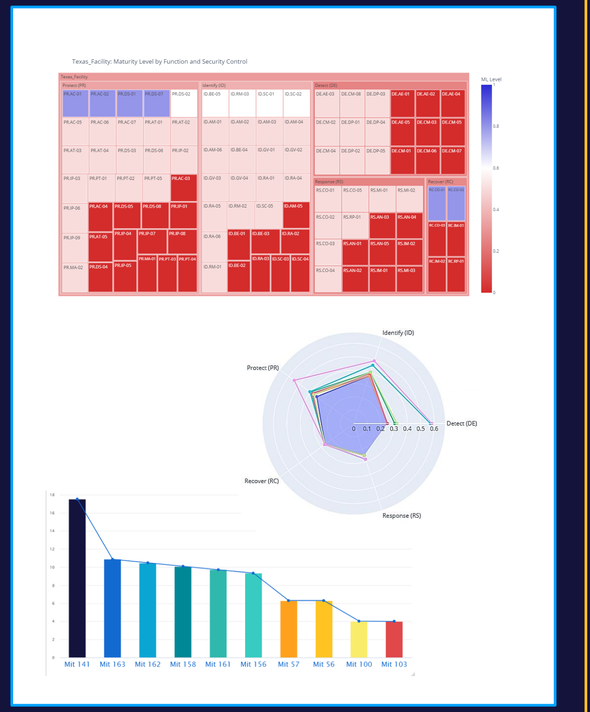
What is the financial impact ($)?



Powered by Business-Risk-Loss Data

Mitigation Recommendations

How to Mitigate? Unit Risk Level



Powered by Business-Risk-Loss Data

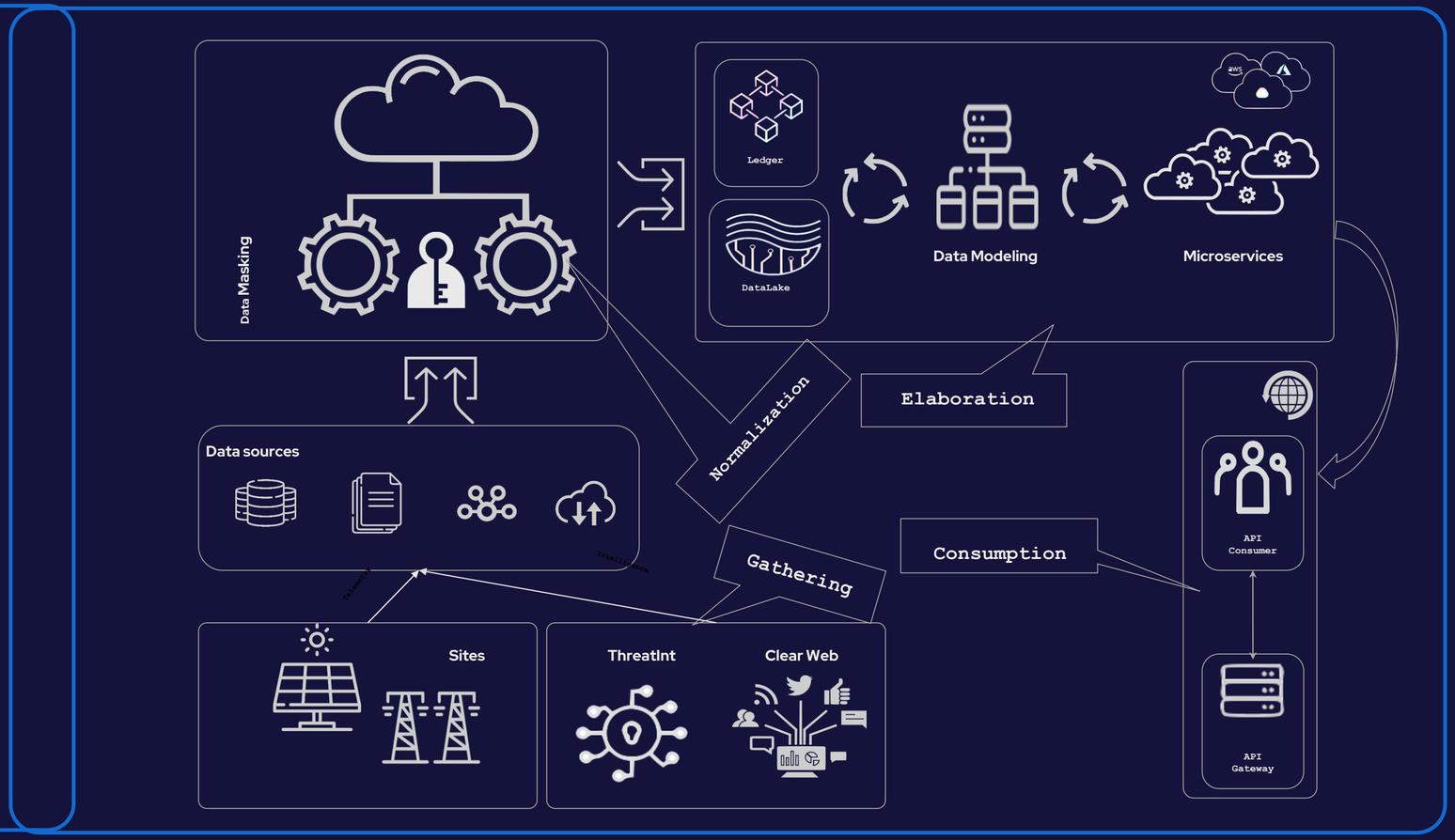
Trusted Ecosystem

Only one option to make it real

Data QUALITY

Data INTEGRITY

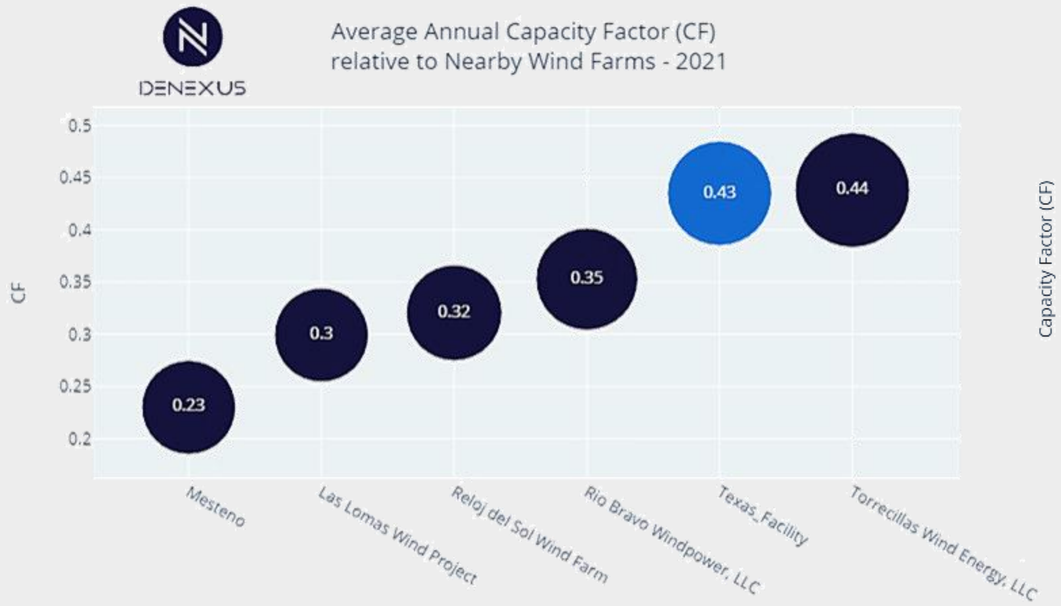
ACCOUNTABILITY

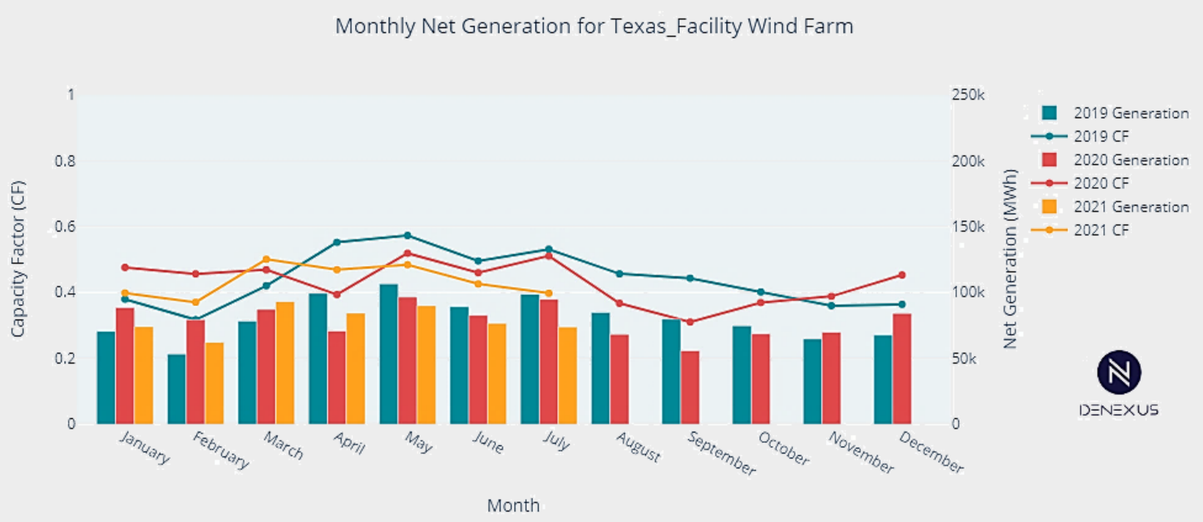


Unlocking the value

The site: Texas Facility

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





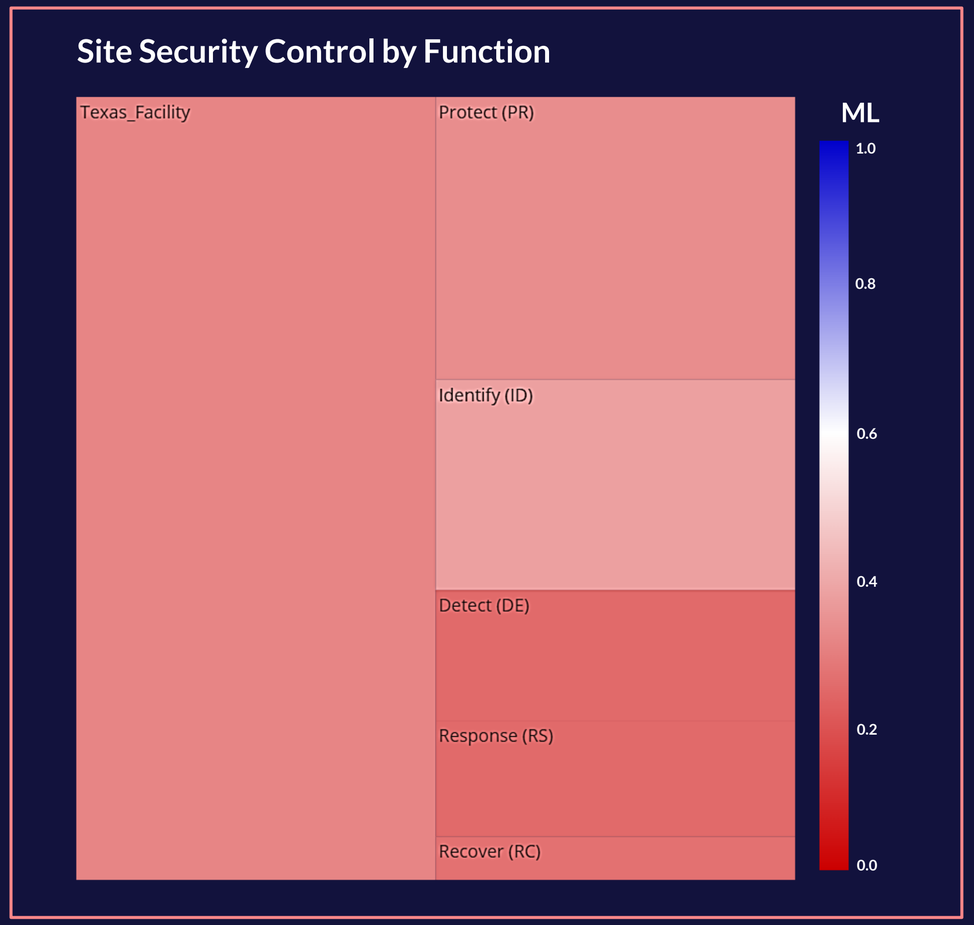
Country:	US
GPS:	32° 32' 25.152'' N
GPS:	99° 43' 8.112'' W
Operating since:	2010

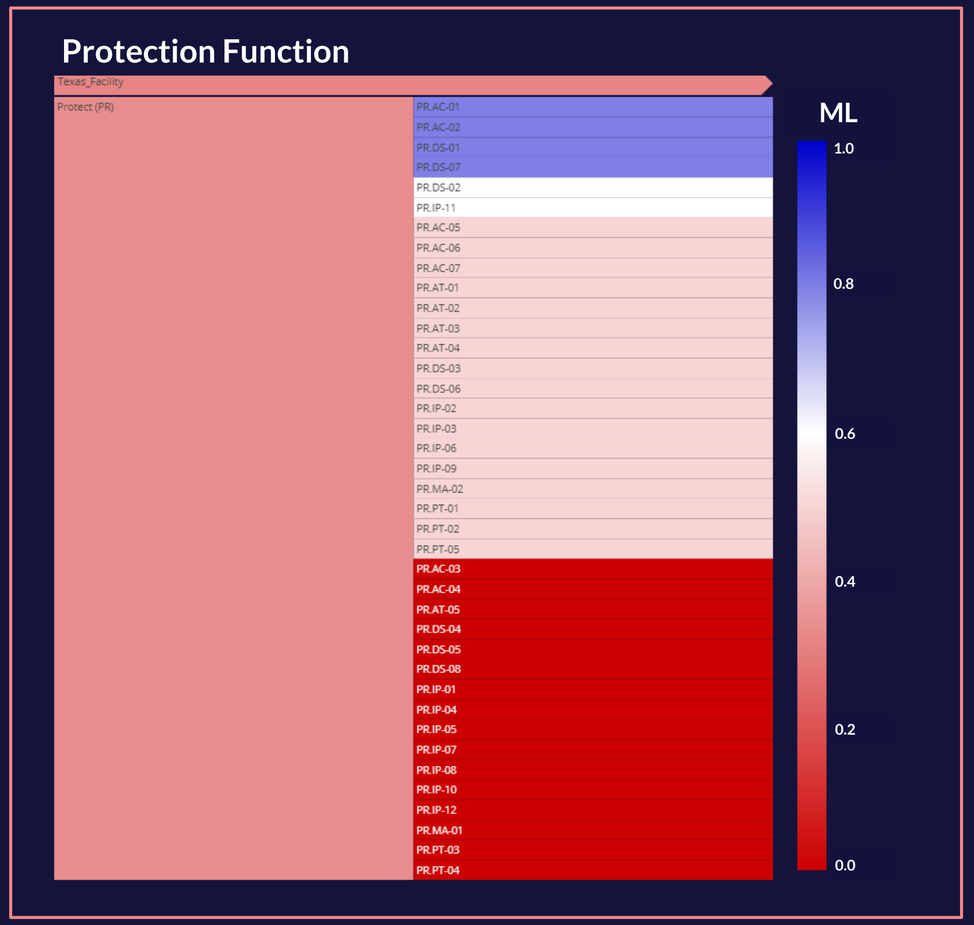
Owner:	Demo Wind Ventures
Operator:	Demo Operating Company
OEM:	VestasWind
Developer:	Demo Clean Power

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



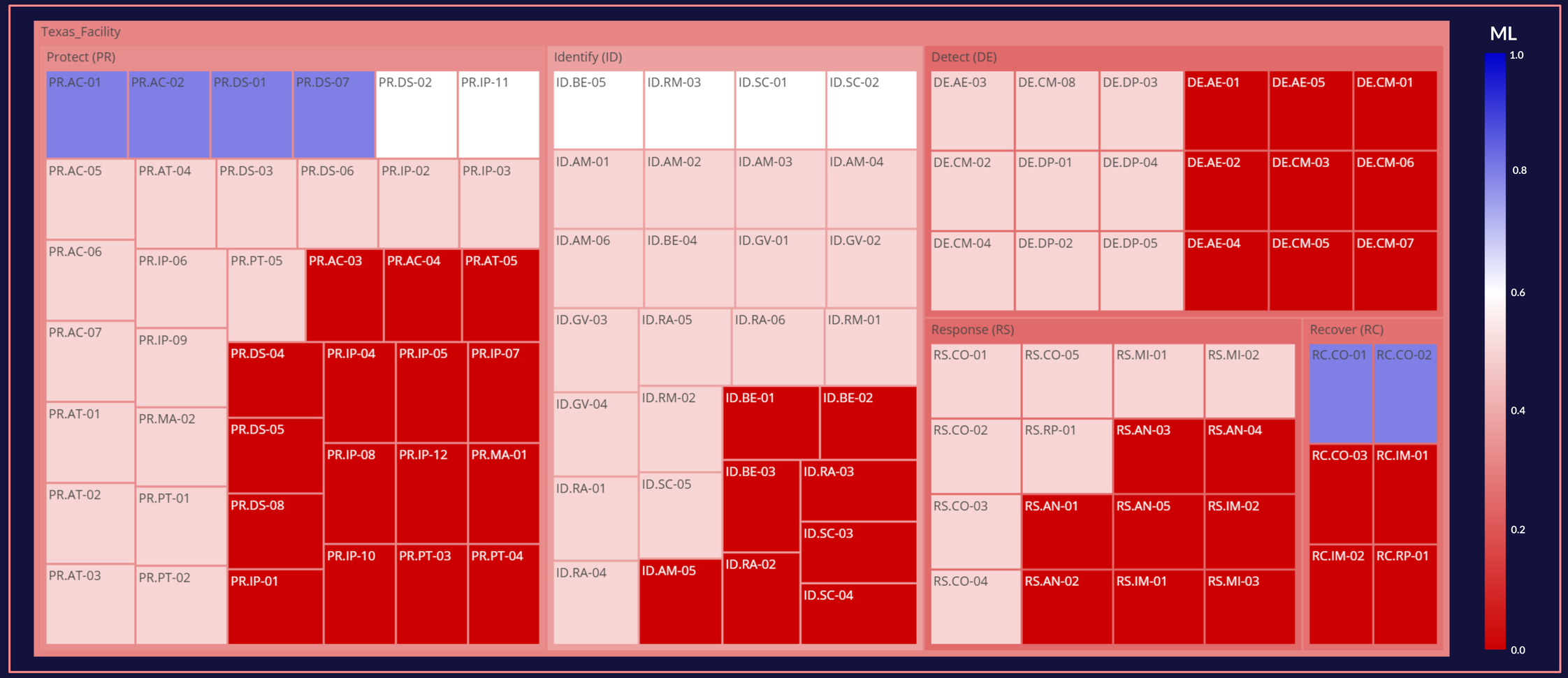


- Highest functional capability (strength) is *Identify*
- Lowest functional capability (weakness) is *Recover*

- 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*

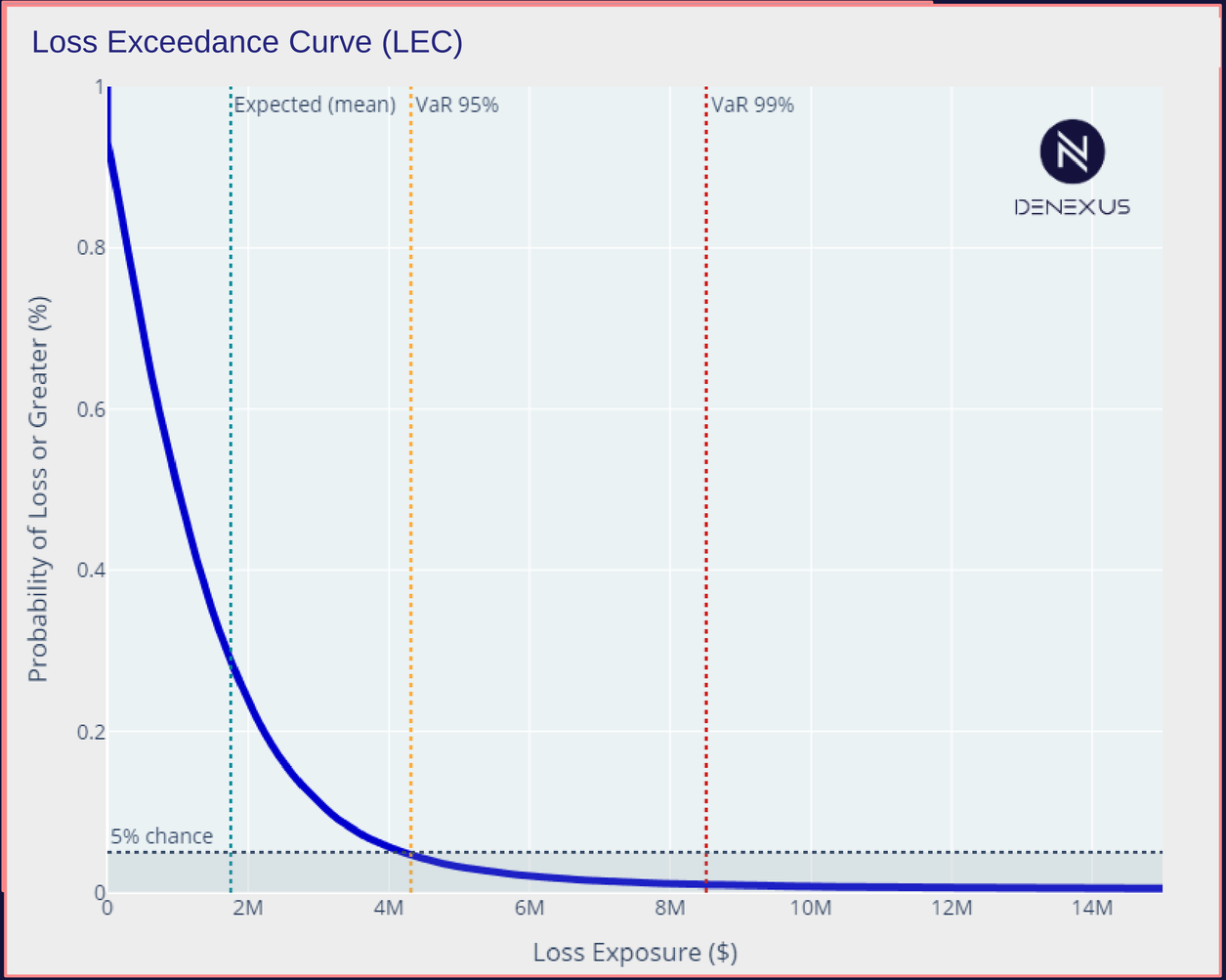
Capabilities Assessment – Cyber Security Framework

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



Site Cyber Risk Assessment

95% probability of Annual Cyber Loss of $4MM or greater



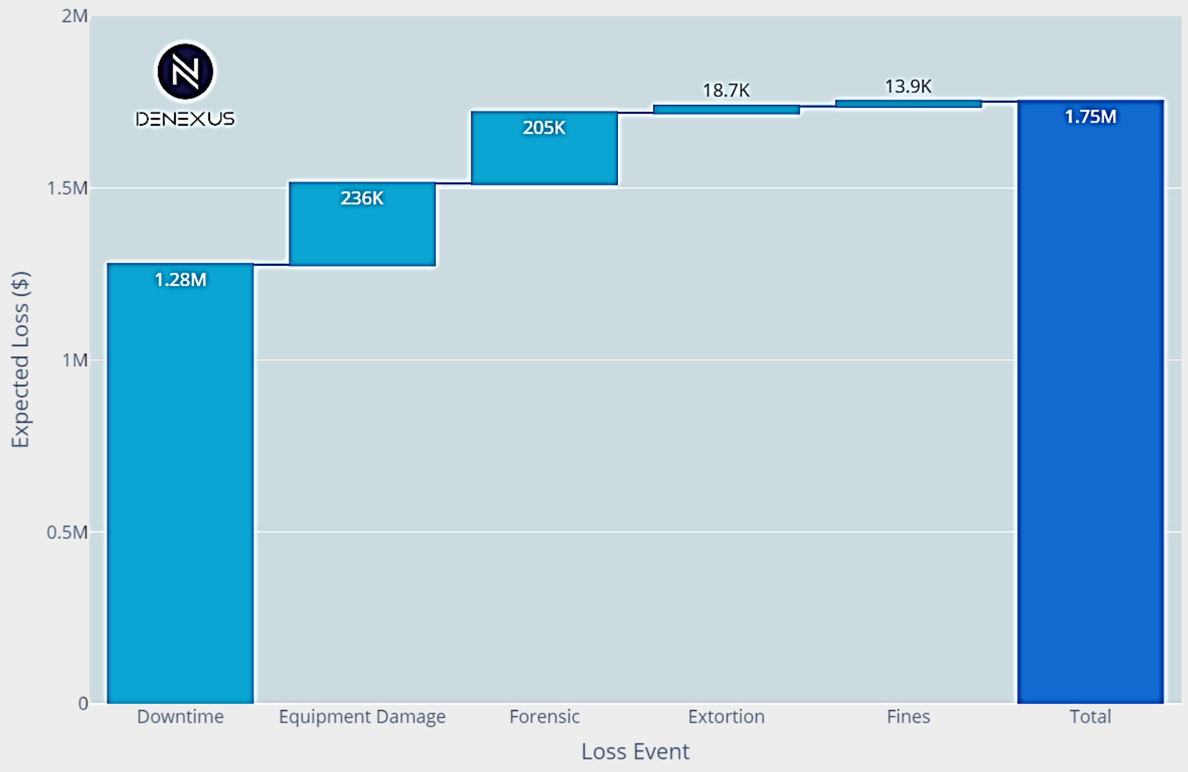
LEC visually display the probability that cyber loss will exceed some amount within a year

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

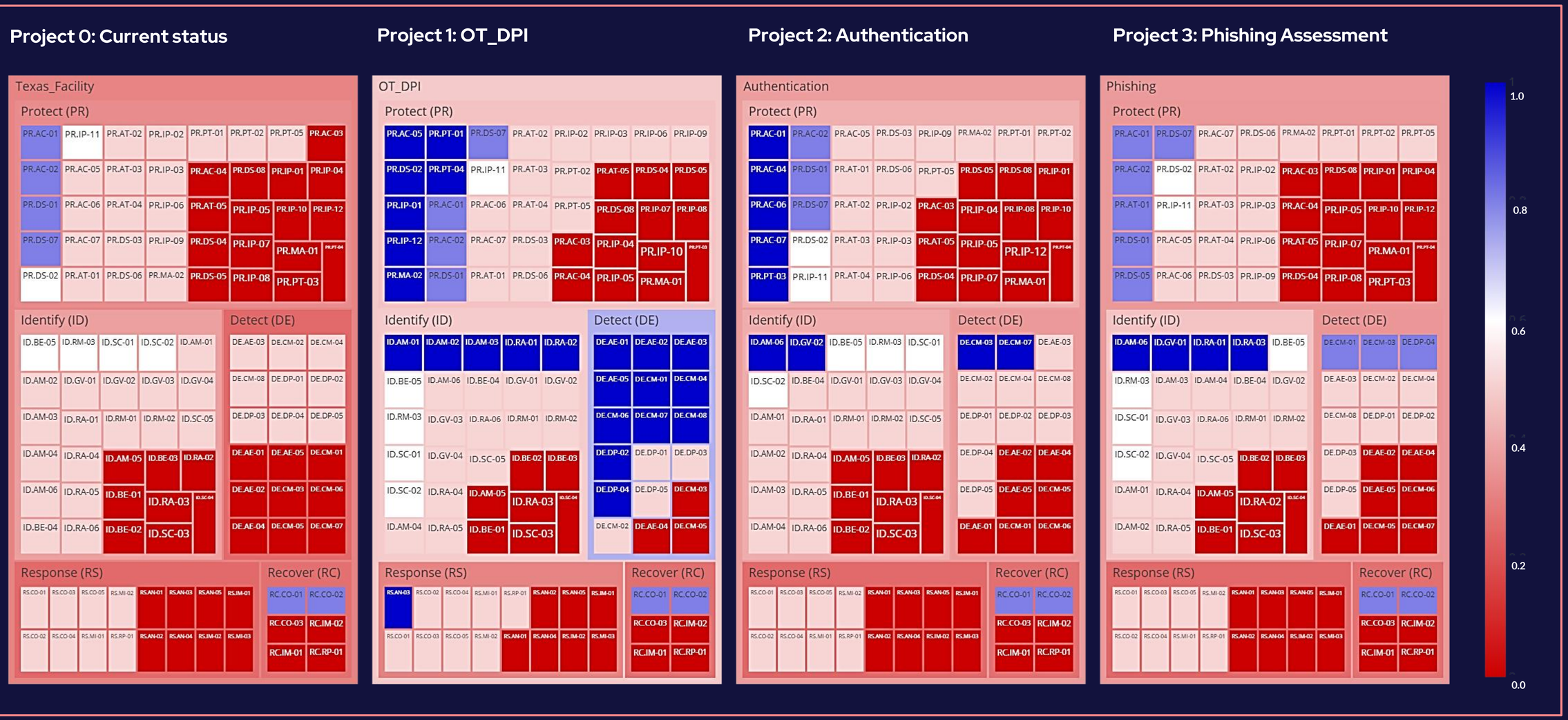
Breakdown of the Annual Expected Loss by Exposure Type



- 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?

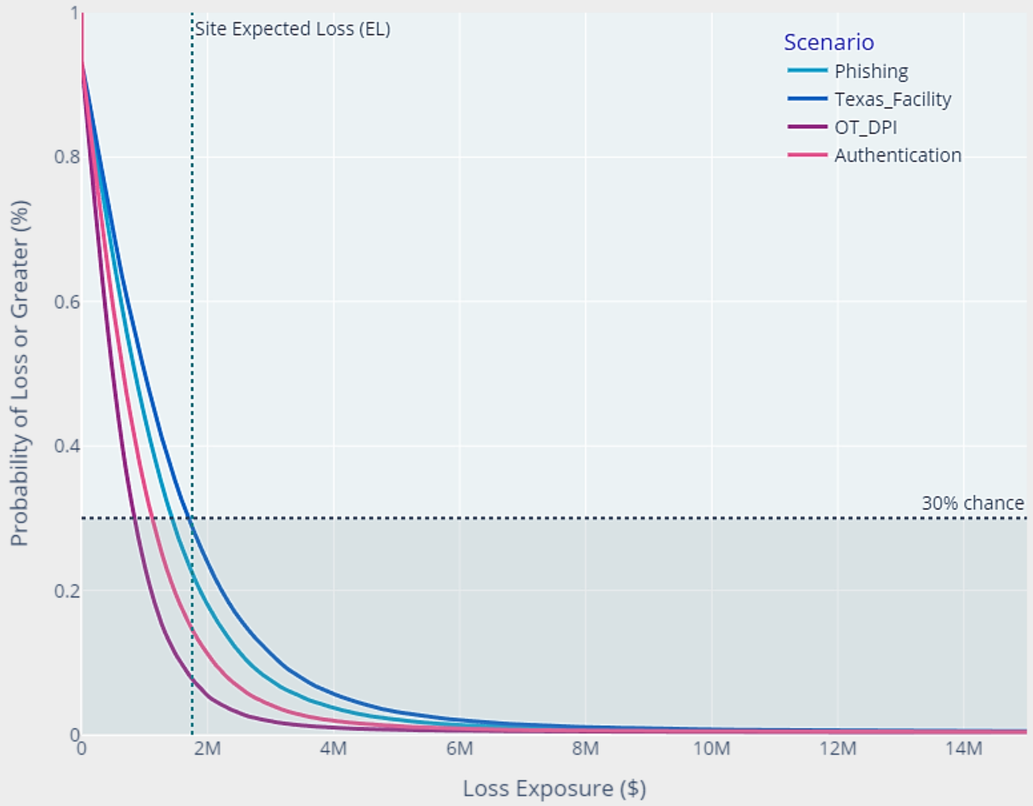
Customize the implementation scenario, or the contribution of any given sub control to that scenario definition.



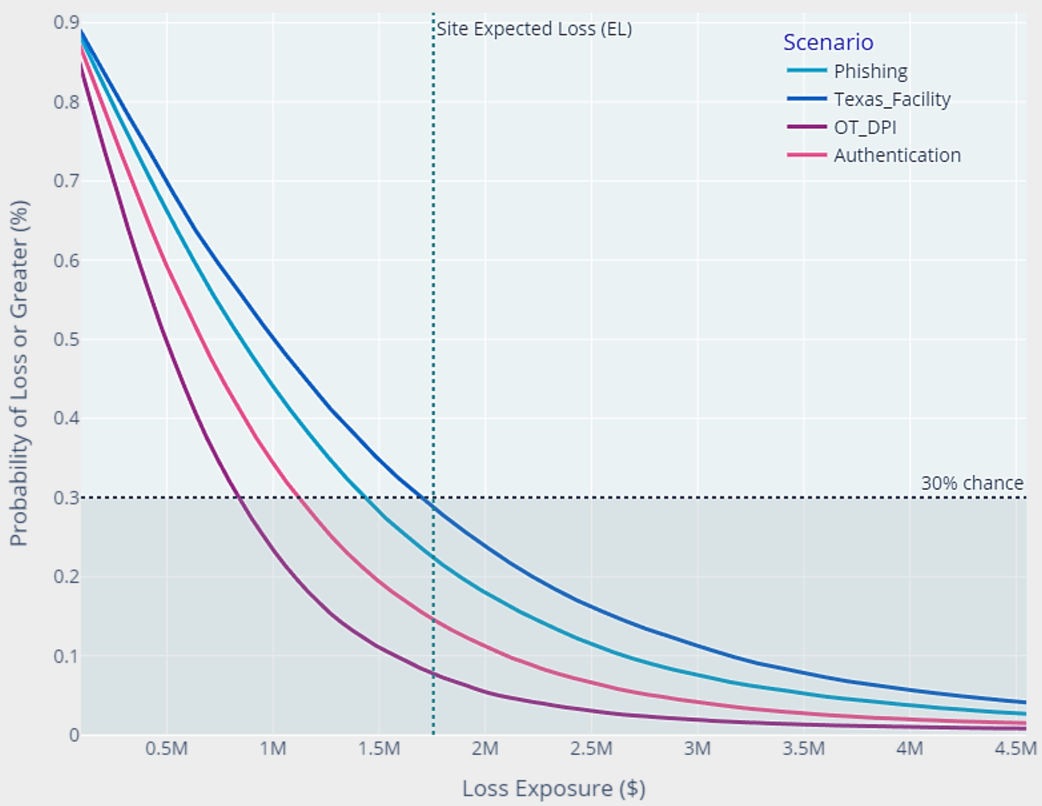
What scenario provides the most risk reduction

OT-DPI provides the biggest risk reduction

Loss Exceedance Curve by what-if scenario



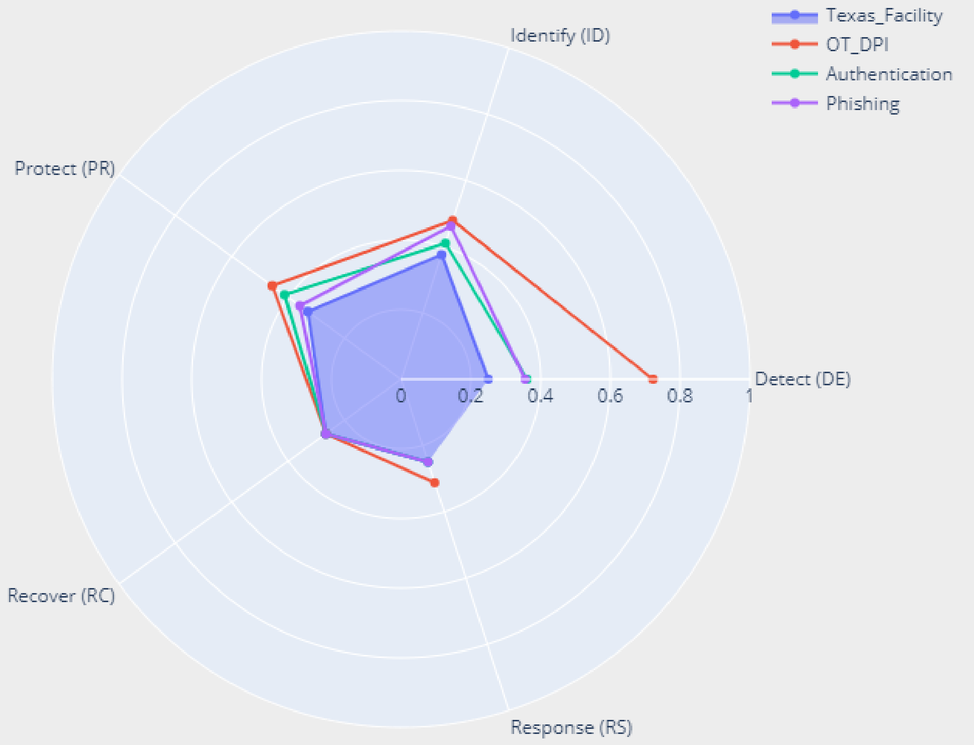
Risk Reduction – 30% chance



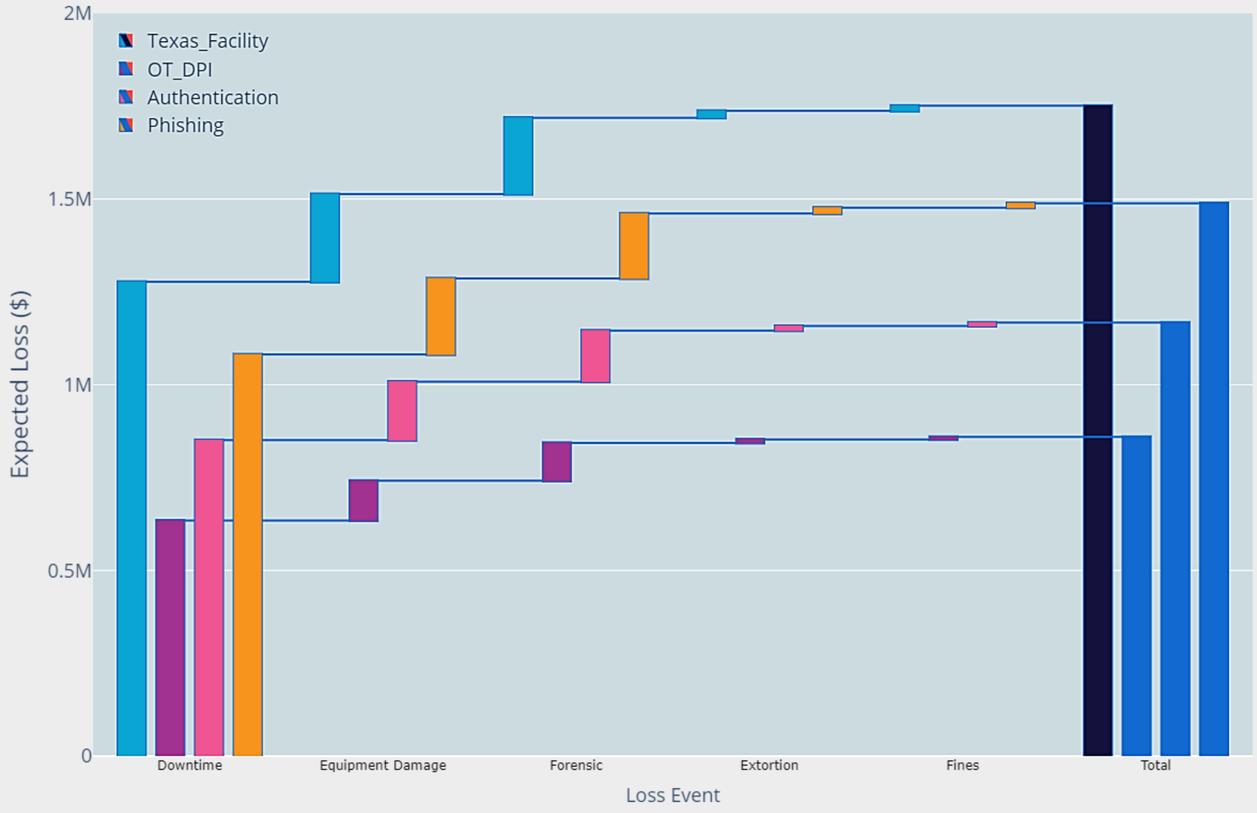
What scenario provides the most risk reduction?

Different initiatives | Different risk reduction

4 Security Control Portfolios



Expected Loss by Event Type: 4 Security Control Portfolios

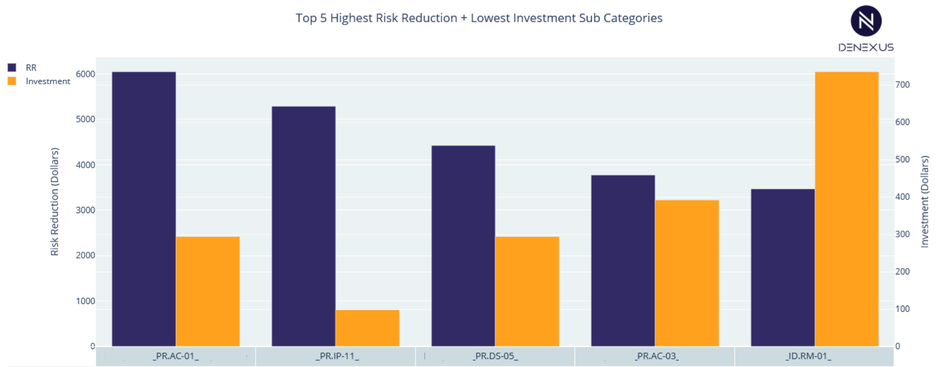


What mitigation provides the most risk reduction?

Recommendations based on ROI, NPV, Fastest

Top 5 Mitigation
Considering Highest Risk Reduction and Lowest Investment

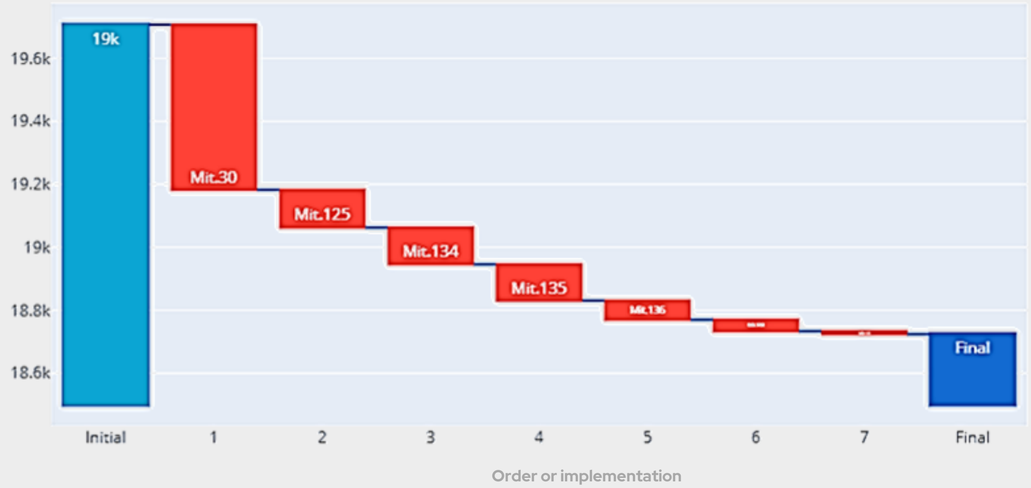
- Stand-alone mitigation analysis .
- Capex, Opex and time of implementation are inputs of the system



	_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

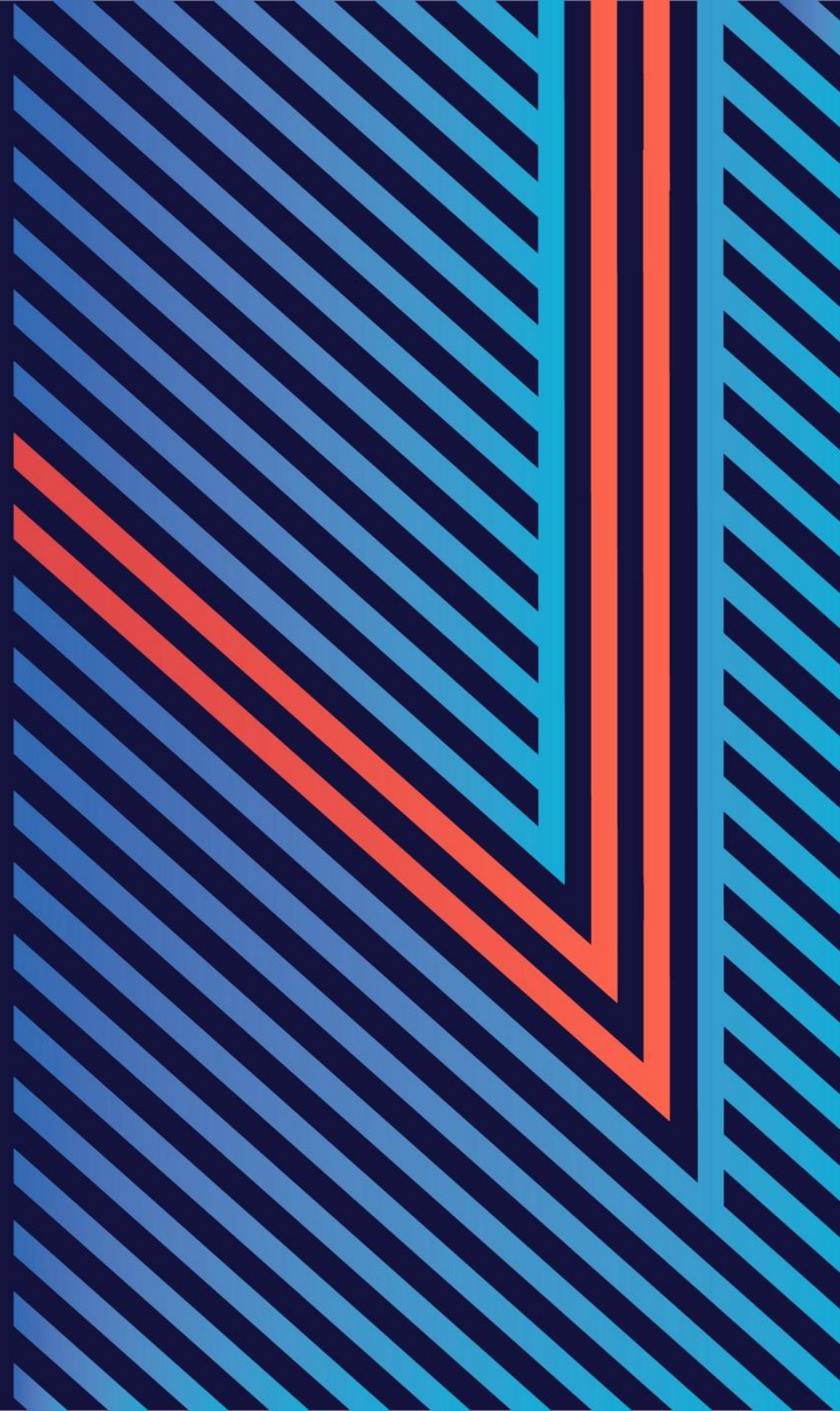
Top 7 Mitigation
Considering Highest Risk Reduction

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



DENEXUS

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

Thank You
Learn more @: DeNexus.io

Romy Rodriguez-Ravines
Risk Modeling

rr@denexus.io

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