

Modeling of Catastrophic Cyber **Events in Industrial Environments.**

Impact on Portfolio Risk Accumulation



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

Confidential & Proprietary. Copyright © by DeNexus, Inc.



Turning Data into Knowledge

"2017-06-03T18:42:18. orgmanager.handlers.RequestHandlesta 5022", "message":"Duration Log", "delta p/page/analyze", "webparams":"null", "duration 249868e-afd8-46ac-9745-839146a20f09; "class":"delta is":"36"}{"timestamp":"2017-06-03T18:335.0030; "delta ile=chartdata_new.json", "class":"comorgmanages: 4402n620jm9trnd3s3n7wg0k", "sizechars":"48455; "message:"delta ueu "lovel":"INFO", "webURL":"/app/page/reports" uu lis":"0", "level":"INFO", "webURL":"/app/page/report", "wessage": 89d89cb-bfa8-4e7d-8047-498454af885d", "sessionID":"144o2nd" s":"7"}{"timestamp":"2017-06-03T18:46:921.000", "deltasta rgmanager.handlers.RequestHandler", "method":"handle", "r 0190", "message":"Duration Log", "durationMillis":"10"}{" /rest/json/file", "webParams":"file=chartdata_new.json", ac6ce95-19e2-4a60-88d7-6ead86e273d1", "sessionID":"144o2n s":"23"}{"timestamp":"2017-06-03T18:42:18.018", "deltaSta rgmanager.handlers.RequestHandler", "method":"handle", "re // Manufer, "right for the state of the 022", "message":"Duration Log", "durationMillis":"508"}{"1



Overcoming Knowledge Siloes and Analyzing Complex Datasets

lis":"0", "level":"INFO", "webURL":"48455", "message": 89d89cb-bfa8-4e7d-8047-498454af885d", "sessionID":"144o2nd" s":"7"}{"timestamp":"2017-06-03T18:46:921.000", "deltasta rgmanager.handlers.RequestHandler", "method":"handle", "r 0190", "message":"Duration Log", "durationMillis":"10"}{" /rest/json/file", "webParams":"file=chartdata_new.json", ac6ce95-19e2-4a60-88d7-6ead86e273d1", "sessionID":"144o2n s":"23"}{"timestamp":"2017-06-03T18:42:18.018", "deltaSta rgmanager.handlers.RequestHandler", "method":"handle", 022", "message":"Duration Log", "durationMillis":"508"}{"1 WebParams":"null", "class":"com.orgmanage 49868e-afd8-46ac-9745-839146a20f09", "sessionID":"14402n62 s":"36"}{"timestamp":"2017-06-03T18:43:335.030","delta ile=chartdata_new.json", "class":"com.orgmanage..mess.ase.weit 4402n620jm9trnd3s3n7wg0k", "sizechars::"/app/pagesion:neita.ase.weit 1is":"0", "level":"INFO", %ebURL":"/app/pagesion:neita.ase.weit 89d89cb-bfa8-4e7d-8047-498454af888sd", 921-96-96 89d89cb-bfa8-4e7d-8047-498454af88sd", meeting s":"7"}{"timestamp":"2017-06-03T18:43:335.030", "timestamp":"2017-06-03T18:43:335.030", "sizechars: "sizechars::"/app/pagesion:neita.ase.weita.a /page/analyze", "webParams":"null", "class":"com.orgmanage

Business Financials

Cyber Security



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



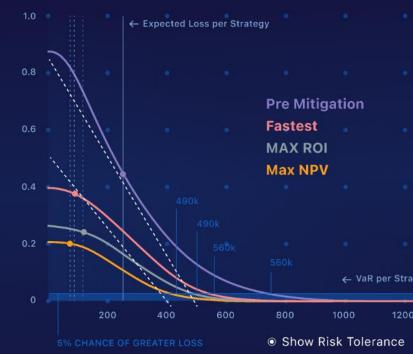
Mitigation Recommendations

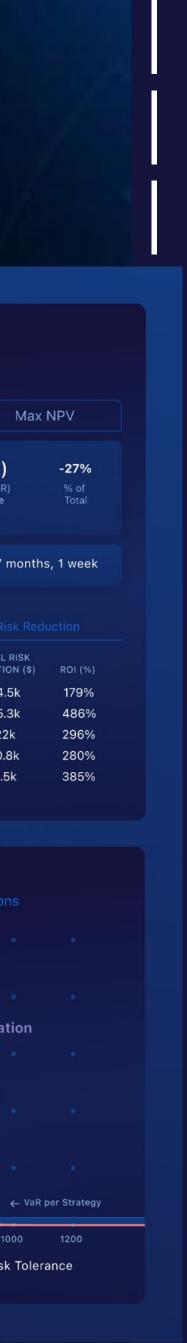
Risk Reduction

-53%				Max ROI			
% of Total	Expe Li	5.6k ected oss ?	()	Valu	S215.5 ue at Risk (V 5th Percent	/aR)	
Capex \$47.3	k Ope	x \$46.	2k	Implem	nentation	7 mont	
			3				
MATURITY	0 1	2	3	4		AL RISK TION (\$)	
DE.CM-7 🔞					\$3	34.5k	
PR.IP-1 🕐					\$2	25.3k	
PR.PT-4 🕐					\$	22k	
PR.AC-4					\$1	0.8k	
RS.IM-2 🕐					\$	8.5k	

Mitigation Strategies

Loss Exceedance vs Mitigation Recommendations





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

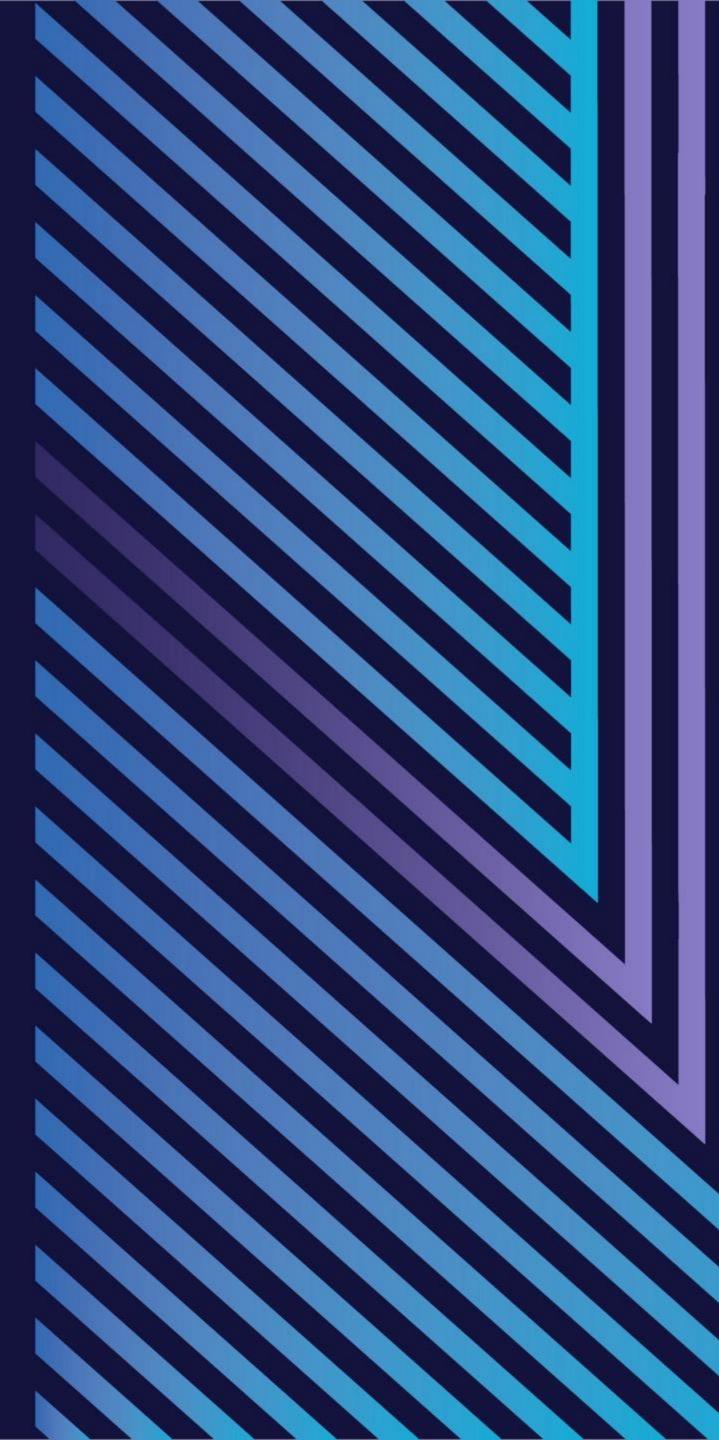


Confidential & Proprietary. Copyright © by DeNexus, Inc.





Why Do We Need Cyber Catastrophe Models?





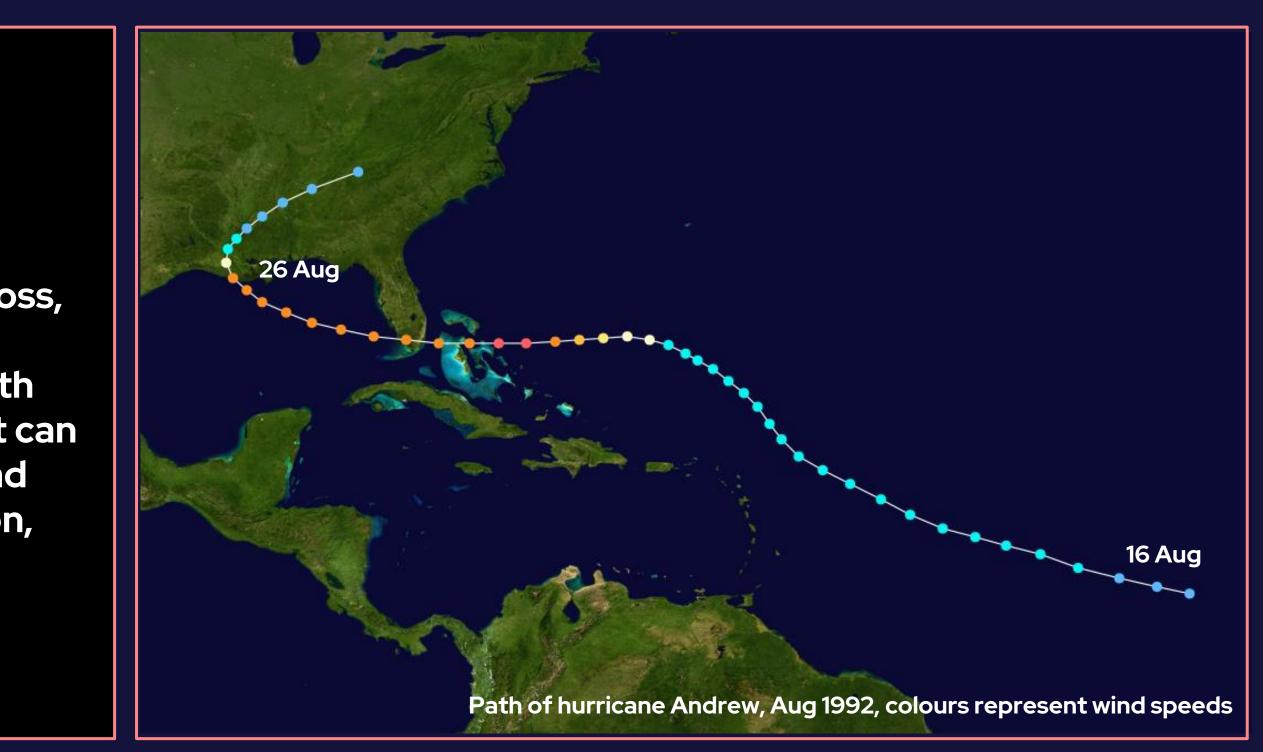


[Nat] CAT: definition



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)

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



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)

LOW FREQUENCY **EVENTS**

SCARCE HISTORICAL DATA

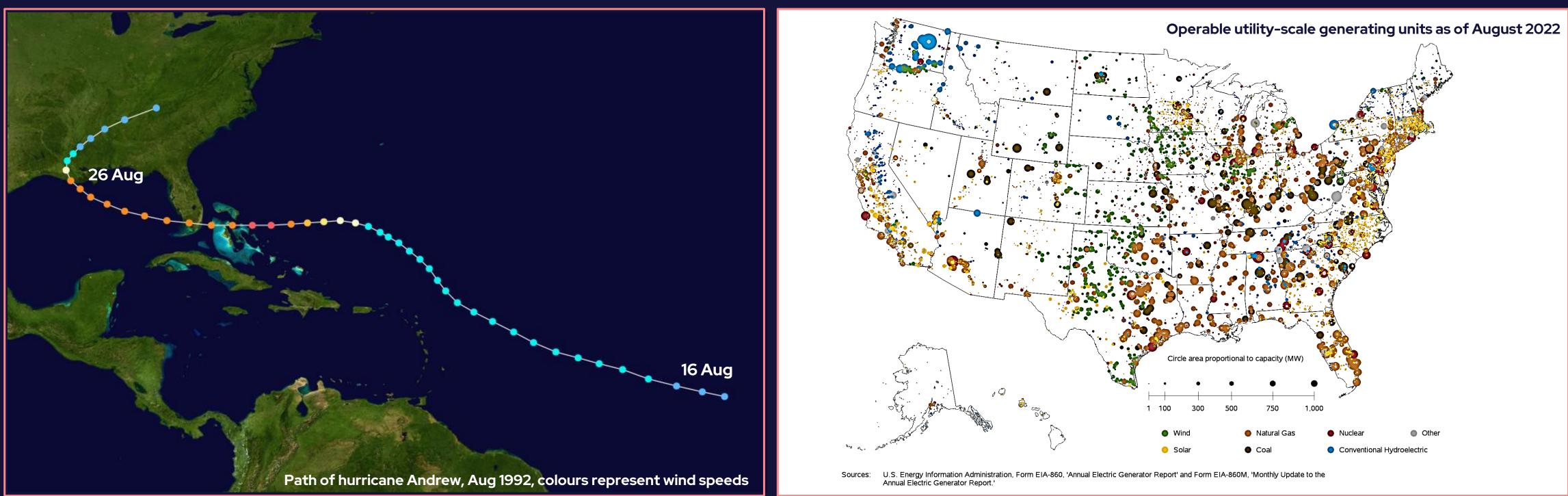


[SPATIAL] CORRELATION

RELIABLE MODELS



Cyber CAT: even more challenging





MANY MANIFESTATIONS **OF LOSS**

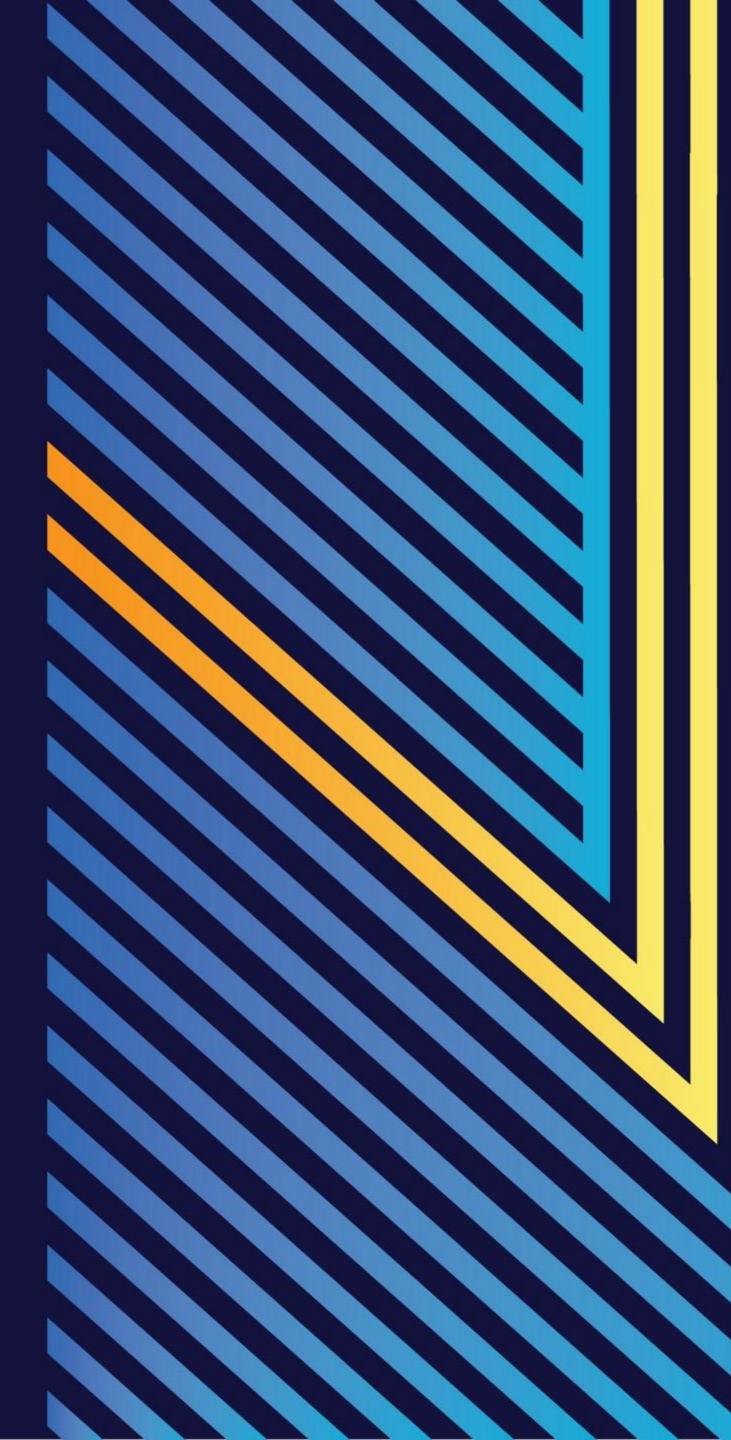
1st GENERATION FAILED







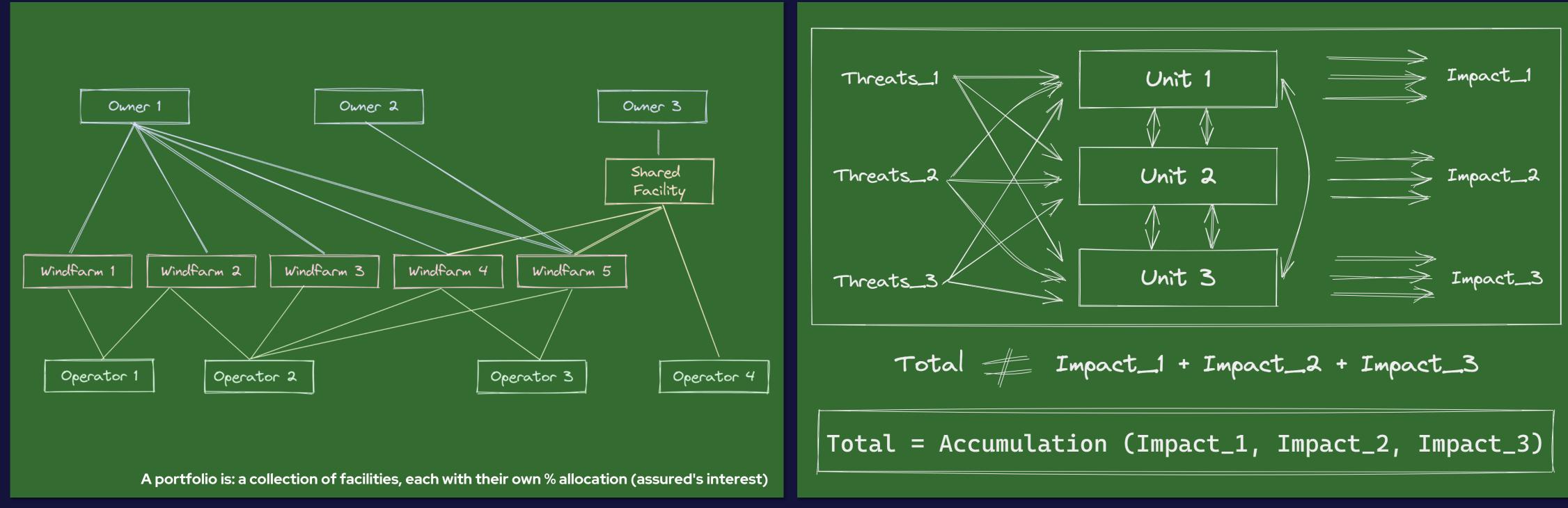
Data is the foundation







Cyber CAT: Accumulation and Portfolio



A <u>large loss</u> happens in isolation, either by accident or as the result of a sophisticated attack An <u>accumulation</u> 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



PORTFOLIO ACCUMULATION

BOTTOM-UP



- 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

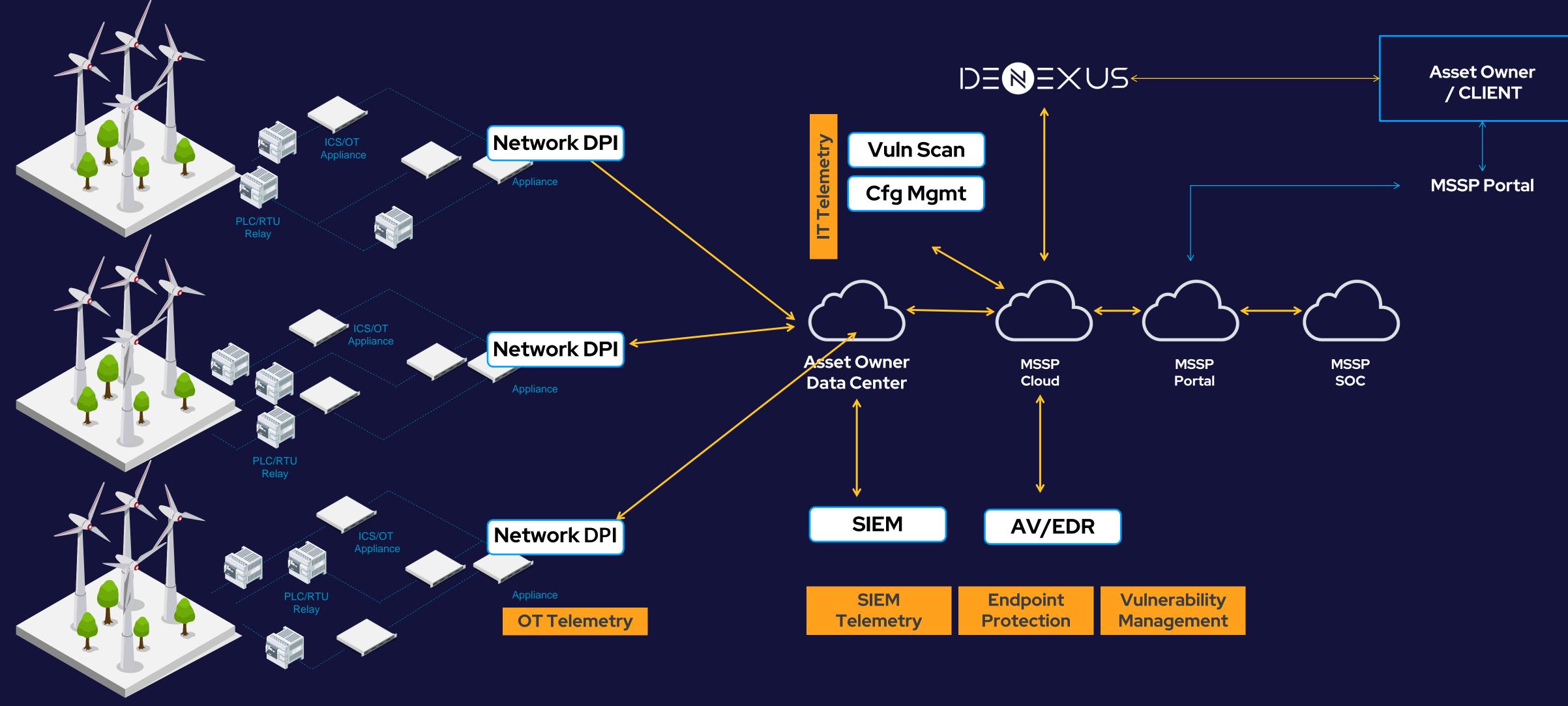
FIT-FOR-PURPOSE





One Client in US >60 Sites

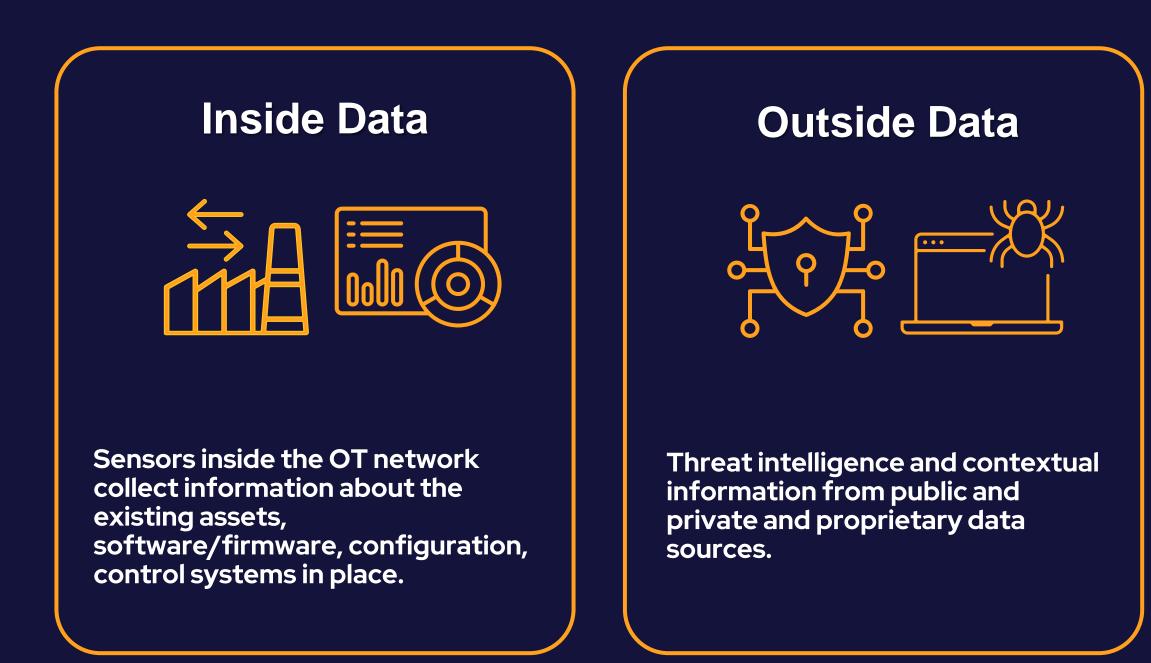
Inside-Out and Outside-in Risk Visibility, RT Quantification, 24x7 Management





Built for Purpose: OT Inside Out Data

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



INDUSTRIAL CRQM

Firmographics

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



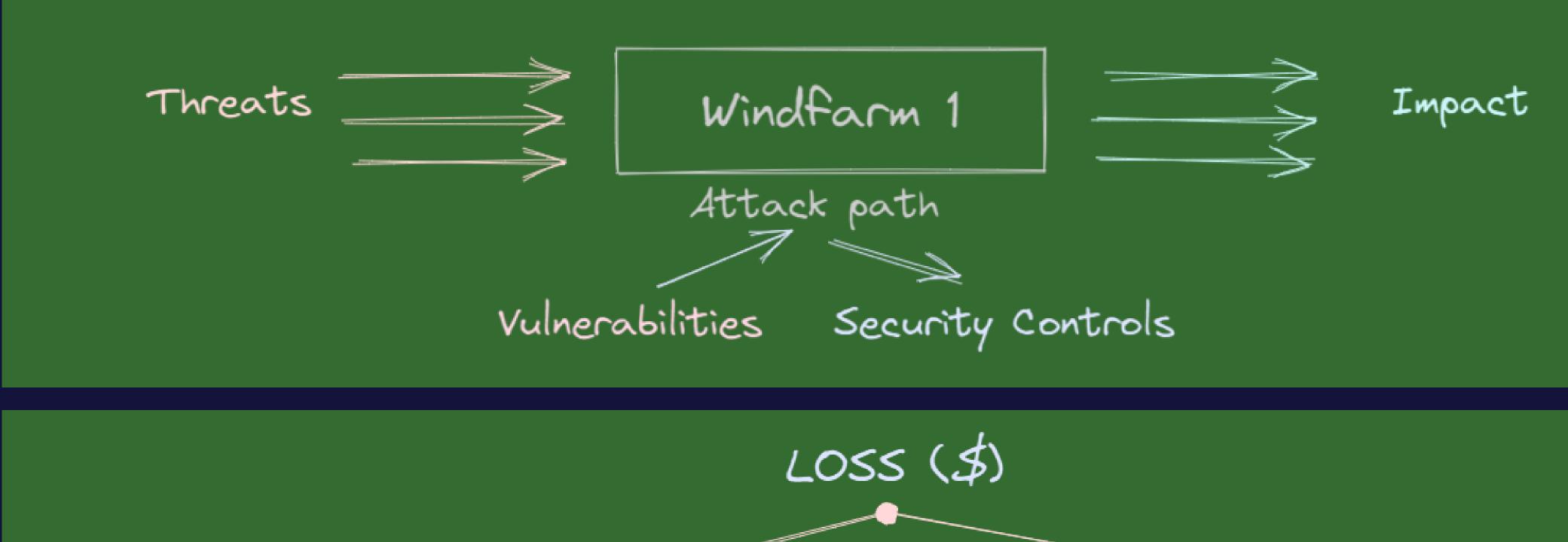
DeNexus Knowledge Center

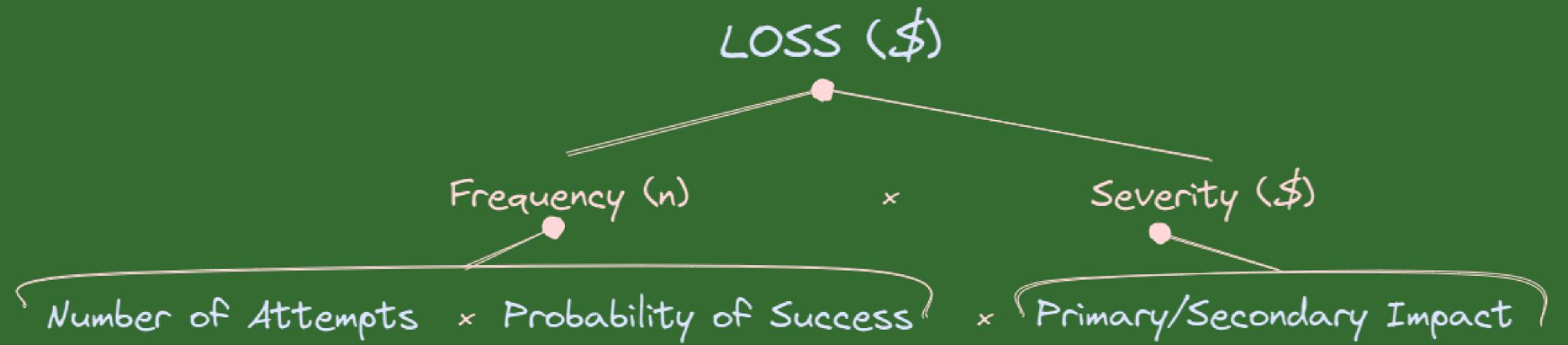
FIT-FOR-PURPOSE





Risk Quantification: putting data in context





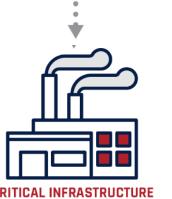


DeNexus Modeling System – Uniquely Approach

Number of Attempts

How many attempts in a year?

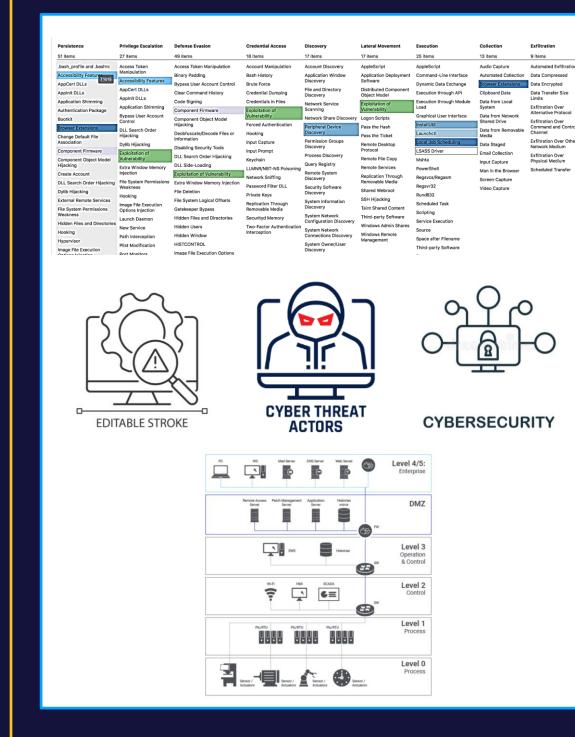
Initial Access 9 techniques	s	Initial Access 12 techniques	
Drive-by Compromise		Drive-by Compromise	
Exploit Public- Facing		Exploit Public- Facing Application	CYBER THREAT ACTORS
Application		Exploitation of Remote Services	0
External Remote Services		External Remote Services	۲ ۲ ۲
Hardware Additions		Internet Accessible Device	
Phishing (0/3)	Ш	Remote Services	Deploy malicious tools
Replication Through Removable		Replication Through Removable Media	to reach their targets
Media	_	Rogue Master	
Supply Chain Compromise _(0/3)	II	Spearphishing Attachment	
Trusted Relationship		Supply Chain Compromise	
Valid Accounts _(0/4)	II	Transient Cyber Asset	
		Wireless Compromise	



Powered by **Outside-in Data**

Attack Path Simulator

How can an incident propagate and cause a loss event?



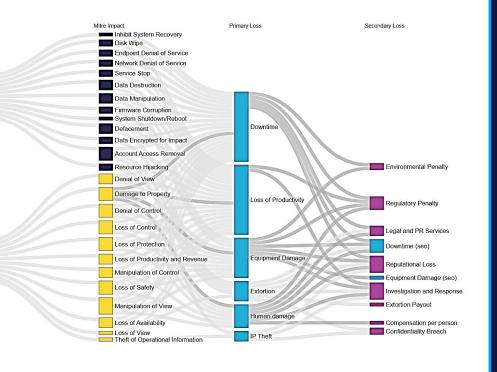
Powered by Inside-Out & Outside-In Data

Loss / Severity / Impact

What is the financial impact (\$)?

Mitigation Recommendations

How to Mitigate? **Unit Risk Level**

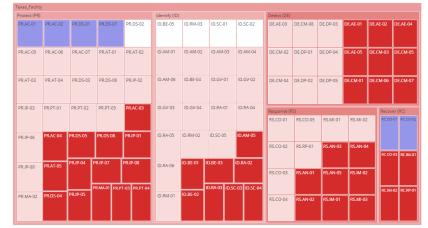


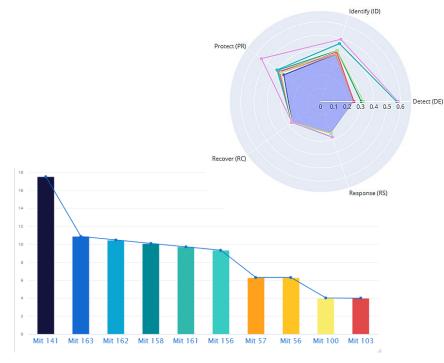




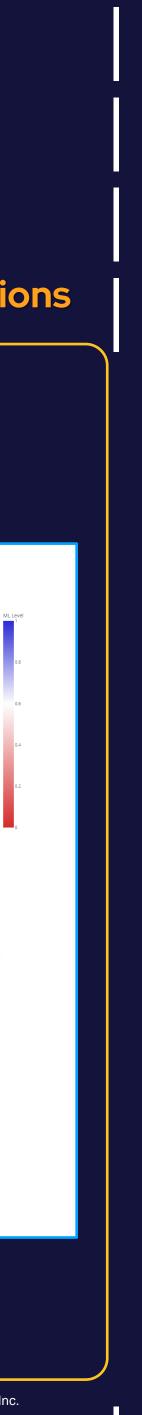
CYBERSECURITY

Powered by Business-Risk-Loss Data





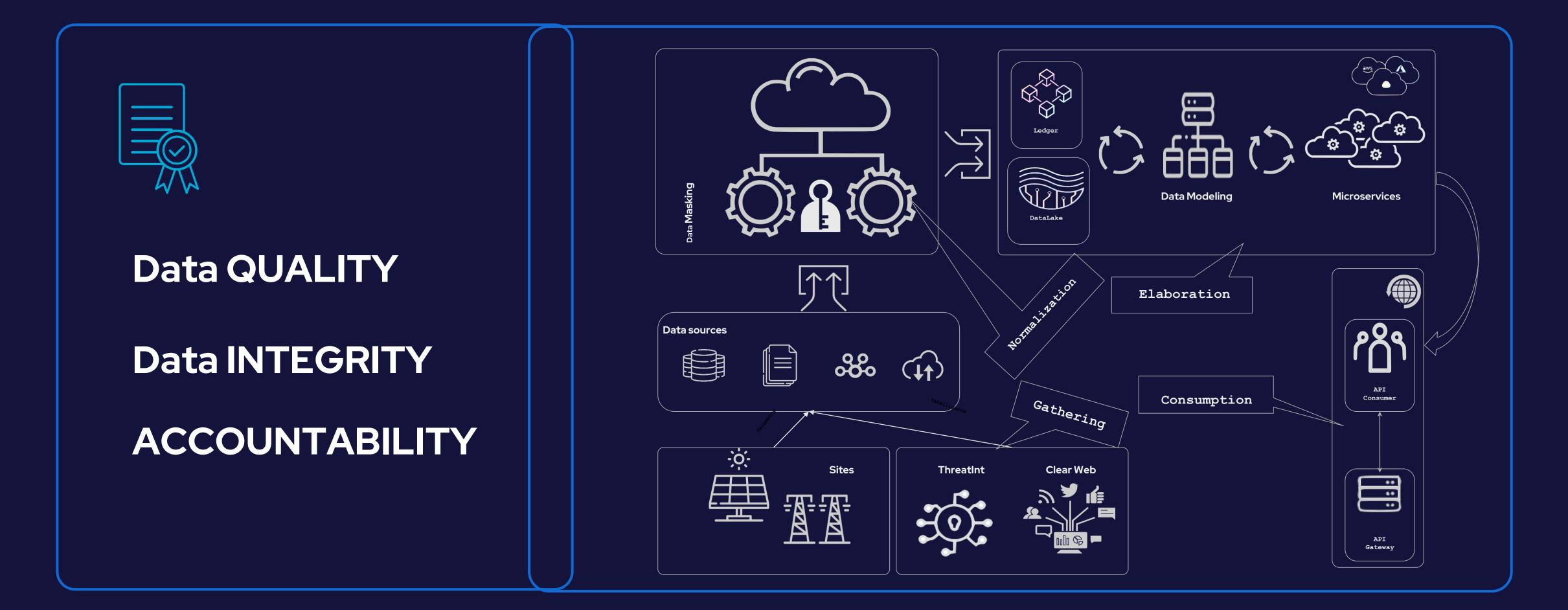
Powered by **Business-Risk-Loss Data**





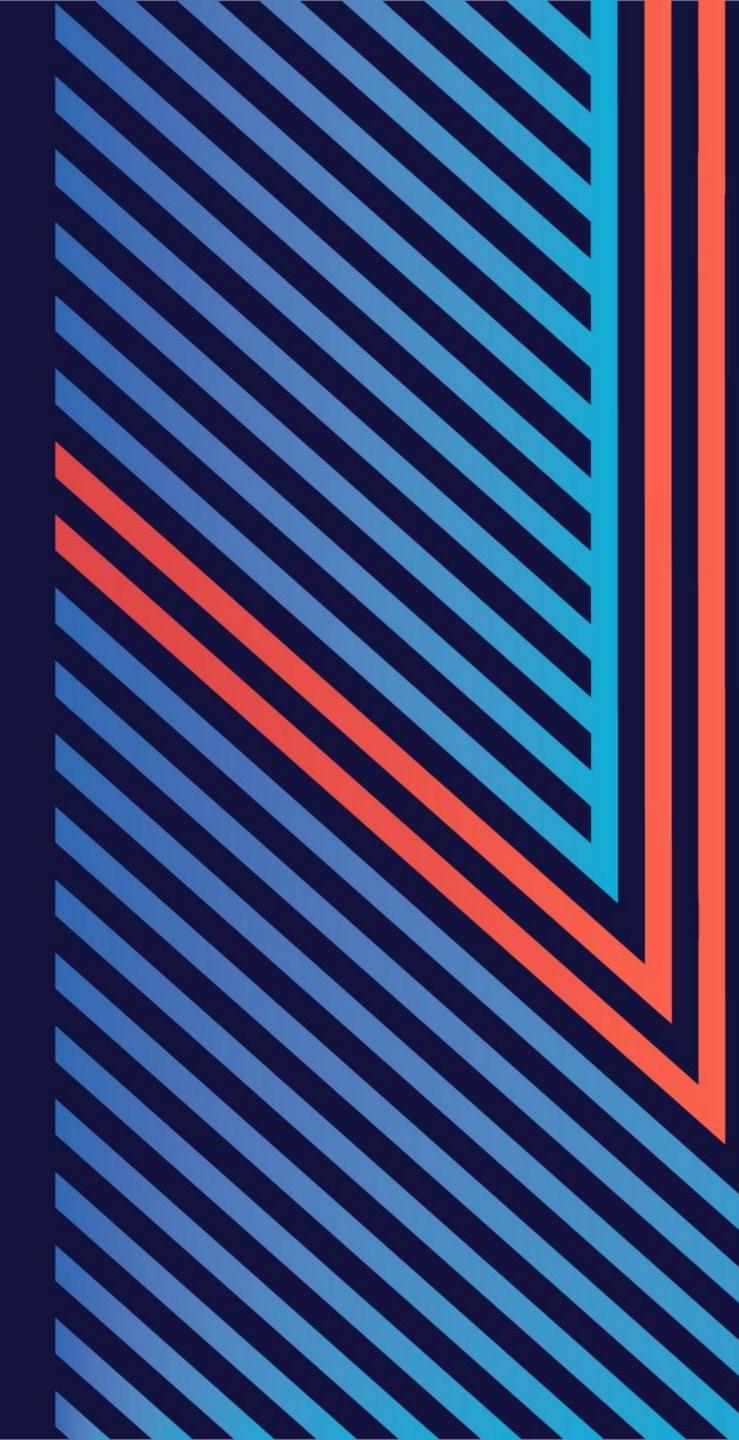
Trusted Ecosystem

Only one option to make it real





Unlocking the value





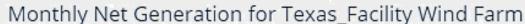


The site: Texas Facility

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



Country: US	Owner: Demo Wind Ventures	Number of Turbines: 125 Vestas V100/2000
GPS: 32° 32' 25.152'' N	Operator: Demo Operating Company	Turbine Capacity (MW): 2.0
GPS: 99° 43' 8.112'' W	OEM: VestasWind	Farm Capacity (MW): 250
Operating since: 2010	Developer: Demo Clean Power	Fuel Type: Wind





Capabilities Assessment - Cyber Security Framework

Strength: Identify | Weakness: Recover



• 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

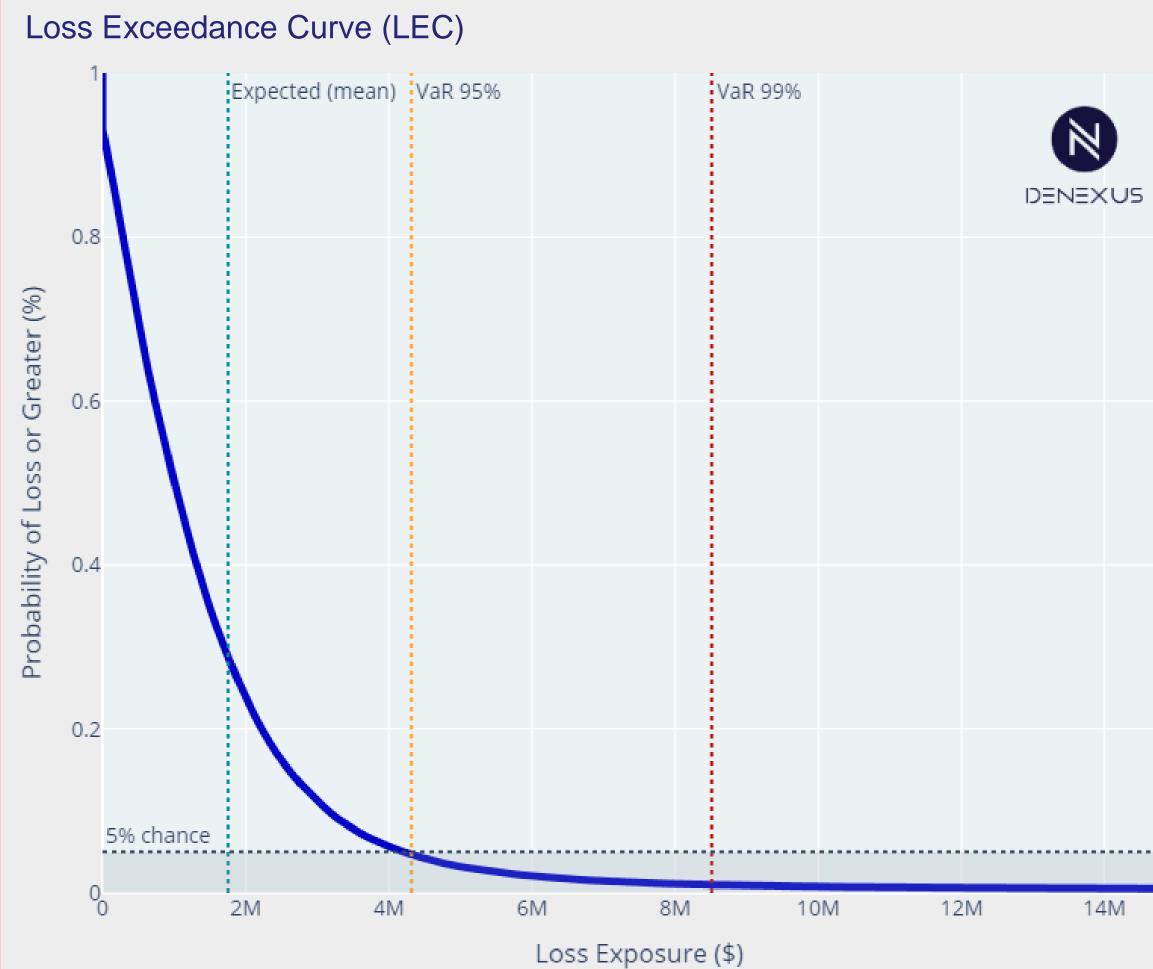
Protect Function contains the most advanced capabilities. Many security controls not initiated

Protect (PR)						Identify (ID)				Detect (DE)					
PR.AC-01	PR.AC-02	PR.DS-01	PR.DS-07	PR.DS-02	PR.IP-11	ID.BE-05	ID.RM-03	ID.SC-01	ID.SC-02	DE.AE-03	DE.CM-08	DE.DP-03	DE.AE-01	DE.AE-05	DE.CM-01
PR.AC-05	PR.AT-04	PR.DS-03	PR.DS-06	PR.IP-02	PR.IP-03	ID.AM-01	ID.AM-02	ID.AM-03	ID.AM-04	DE.CM-02	DE.DP-01	DE.DP-04	DE.AE-02	DE.CM-03	DE.CM-06
PR.AC-06	PR.IP-06	PR.PT-05	PR.AC-03	PR.AC-04	PR.AT-05	ID.AM-06	ID.BE-04	ID.GV-01	ID.GV-02	DE.CM-04	DE.DP-02	DE.DP-05	DE.AE-04	DE.CM-05	DE.CM-07
PR.AC-07	PR.IP-09	_				ID.GV-03	ID.RA-05	ID.RA-06	ID.RM-01	Response (R	۱ ۲۶)			Recov	ver (RC)
	111.11-05	PR.DS-04	PR.IP-04	4 PR.IP-05	PR.IP-07					RS.CO-01	RS.CO-05	RS.MI-01	RS.MI-02	2 RC.CO	D-01 RC.CO-02
PR.AT-01	PR.MA-02	_				ID.GV-04	ID.RM-02	ID.BE-01	ID.BE-02						
		PR.DS-05	PR.IP-08	3 PR.IP-12	PR.MA-01					RS.CO-02	RS.RP-01	RS.AN-03	RS.AN-04		D-03 RC.IM-01
	_					ID.RA-01	ID.SC-05	ID.BE-03	ID.RA-03					ne.ee	
PR.AT-02	PR.PT-01	PR.DS-08								RS.CO-03	RS.AN-01	RS.AN-05	RS.IM-02	2	
			PR.IP-10) PR.PT-03	PR.PT-04				ID.SC-03					RC.IM	I-02 RC.RP-01
PR.AT-03	PR.PT-02	PR.IP-01				ID.RA-04	ID.AM-05	ID.RA-02	ID.SC-04	RS.CO-04	RS.AN-02	RS.IM-01	RS.MI-03	3	
									10.50-04						



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

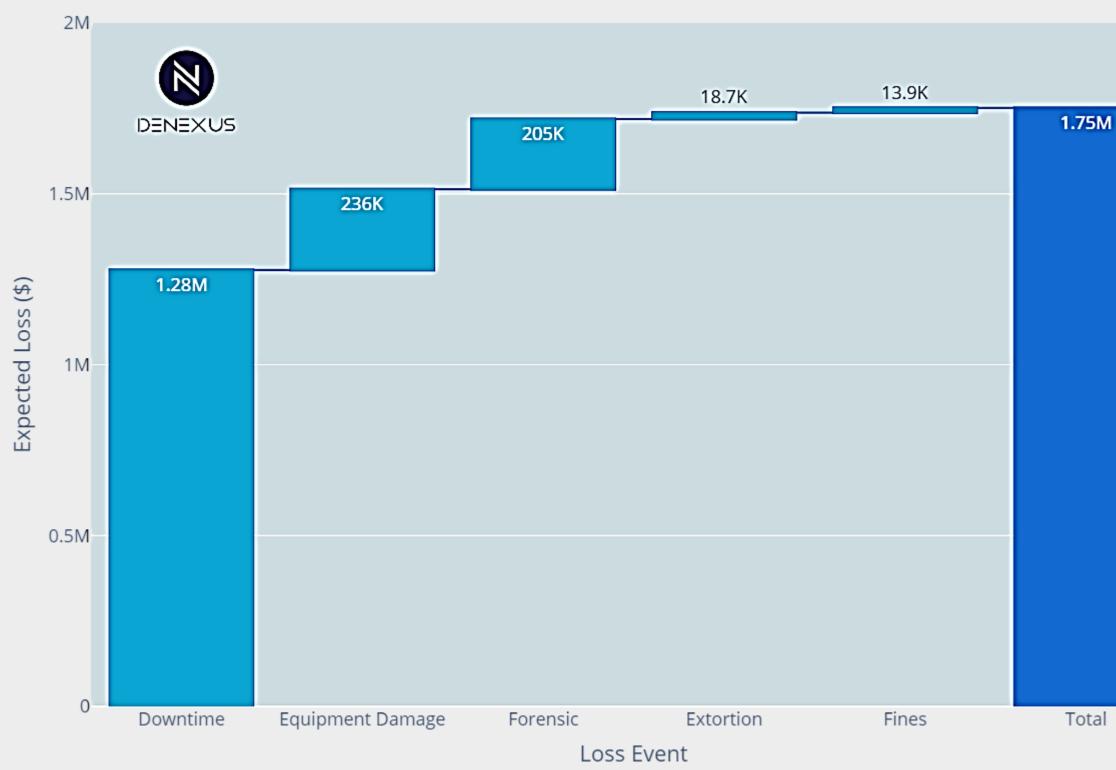
Metric	Value	Description
Revenue	\$35.9M	DeNexus sourced starting number for site. Update for specificity.
Expected Loss	\$2.0MM	In statistical terms, the expected loss is the mean loss that we would expect over a given period of time (year). The expected loss is an average used for provisioning.
Unexpected 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.

Proje	ct 0: (Curre	ent s [.]	tatus			
Texas_F	acility						
Protect	: (PR)						
PR.AC-01	PR.IP-11	PR.AT-02	PR.IP-02	PR.PT-01	PR.PT-02	PR.PT-05	PR.AC-03
PR.AC-02	PR.AC-05	PR.AT-03	PR.IP-03	PR.AC-04	PR.DS-08	PR.IP-01	PR.IP-04
PR.DS-01	PR.AC-06	PR.AT-04	PR.IP-06	PR.AT-05	PR.IP-05	PR.IP-10	PR.IP-12
PR.DS-07	PR.AC-07	PR.DS-03	PR.IP-09	PR.DS-04	PR.IP-07	PR.MA	-01
PR.DS-02	PR.AT-01	PR.DS-06	PR.MA-02	PR.DS-05	PR.IP-08	PR.PT-	03
Identify	Identify (ID) Detect (DE)						
ID.BE-05	ID.RM-03	ID.SC-01	ID.SC-02	D.AM-01	DE.AE-03	DE.CM-02	DE.CM-04
ID.AM-02	ID.GV-01	ID.GV-02	ID.GV-03 I	D.GV-04	DE.CM-08	DE.DP-01	DE.DP-02
ID.AM-03	ID.RA-01	ID.RM-01	ID.RM-02	D.SC-05	DE.DP-03	DE.DP-04	DE.DP-05
ID.AM-04	ID.RA-04	ID.AM-05	ID.BE-03	ID.RA-02	DE.AE-01	DE.AE-05	DE.CM-01
ID.AM-06	ID.RA-05	ID.BE-01	ID.RA-0	3 0.504	DE AE-02	DE.CM-03	DE.CM-06
ID.BE-04	ID.RA-06	ID.BE-02	ID.SC-0	3	DE.AE-04	DE.CM-05	DE.CM-07
Respor	nse (RS)					Recove	er (RC)
RS.CO-01 RS.	CO-03 RS.CO-05	5 RS.MI-02 F	rs.an-01 rs.an	103 RSAN-05	RS.IM-01	RC.CO-01	RC.CO-02
RS.CO-02 RS.0	20-04 RS.MI-0	I RS.RP-01 F	rsan-02 rsan	HO4 RSJM-02	RS.MI-03	RC.CO-03	RC.IM-02
						RC.IM-01	RC.RP-01

Project 1: OT_DPI

OT_DPI							
Protect	t (PR)						
PR.AC-05	PR.PT-01	PR.DS-07	PR.AT-02	PR.IP-02	PR.IP-03	PR.IP-06	PR.IP-09
PR.DS-02	PR.PT-04	PR.IP-11	PR.AT-03	PR.PT-02	PR.AT-05	PR.DS-04	PR.DS-05
PR.IP-01	PR.AC-01	PR.AC-06	PR.AT-04	PR.PT-05	PR.DS-08	PR.IP-07	PR.IP-08
	PR.AC-02					PR.IP-	
PR.MA-02	PR.DS-01	PR.AT-01	PR.DS-06	PR.AC-04	PR.IP-05	PR.MA	01
Identif	y (ID)				Detect	(DE)	
ID.AM-01	ID.AM-02	id.am-03	D.RA-01 ID).RA-02	DE_AE-01	DE AE-02	DE_AE-03
ID.BE-05	ID.AM-06	ID.BE-04 I	D.GV-01 ID).GV-02	DE.AE-05	DE.CM-01	DE.CM-04
ID.RM-03	ID.GV-03	ID.RA-06	ID.RM-01 ID	D.RM-02	DE.CM-06	DE.CM-07	DE.CM-08
ID.SC-01	ID.GV-04	ID.SC-05	ID.BE-02 I	D.BE-03	DE.DP-02	DE.DP-01	DE.DP-03
	ID.RA-04		ID.RA-03		DE.DP-04	DE.DP-05	DE.CM-03
ID.AM-04	ID.RA-05	ID.BE-01	ID.SC-03	3	DE.CM-02	DE.AE-04	DE.CM-05
Respor	nse (RS)					Recove	er (RC)
RS.AN-03 RS.	CO-02 RS.CO-0	4 RS.MI-01 RS	S.RP-01 RSAN	02 RSAN-05	RS.IM-01	RC.CO-01	RC.CO-02
RS.CO-01 RS.	CO-03 RS.CO-0	5 RS.MI-02 RS	SANIOT RSANI	04 RS.IM-02	RS.MI-03	RC_CO-03	RC.IM-02
						RC.IM-01	RC.RP-01

Project 2: Authentication

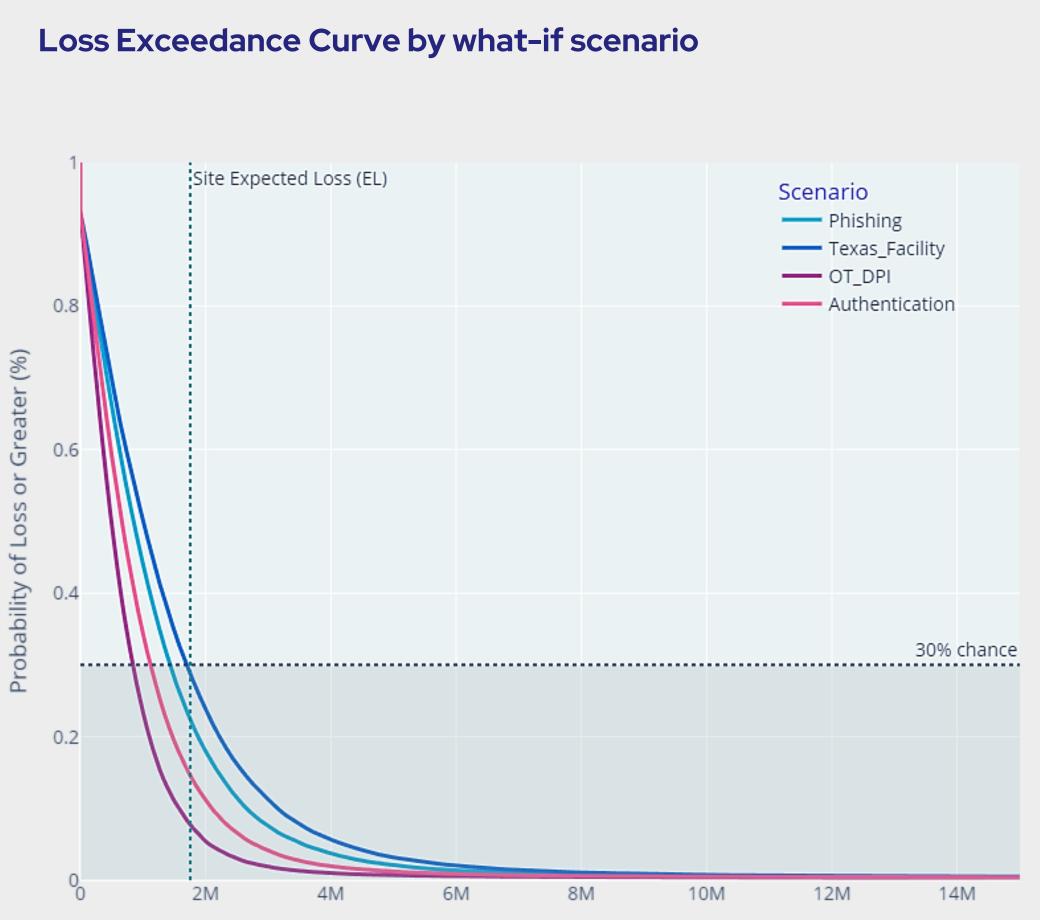


Project 3: Phishing Assessment



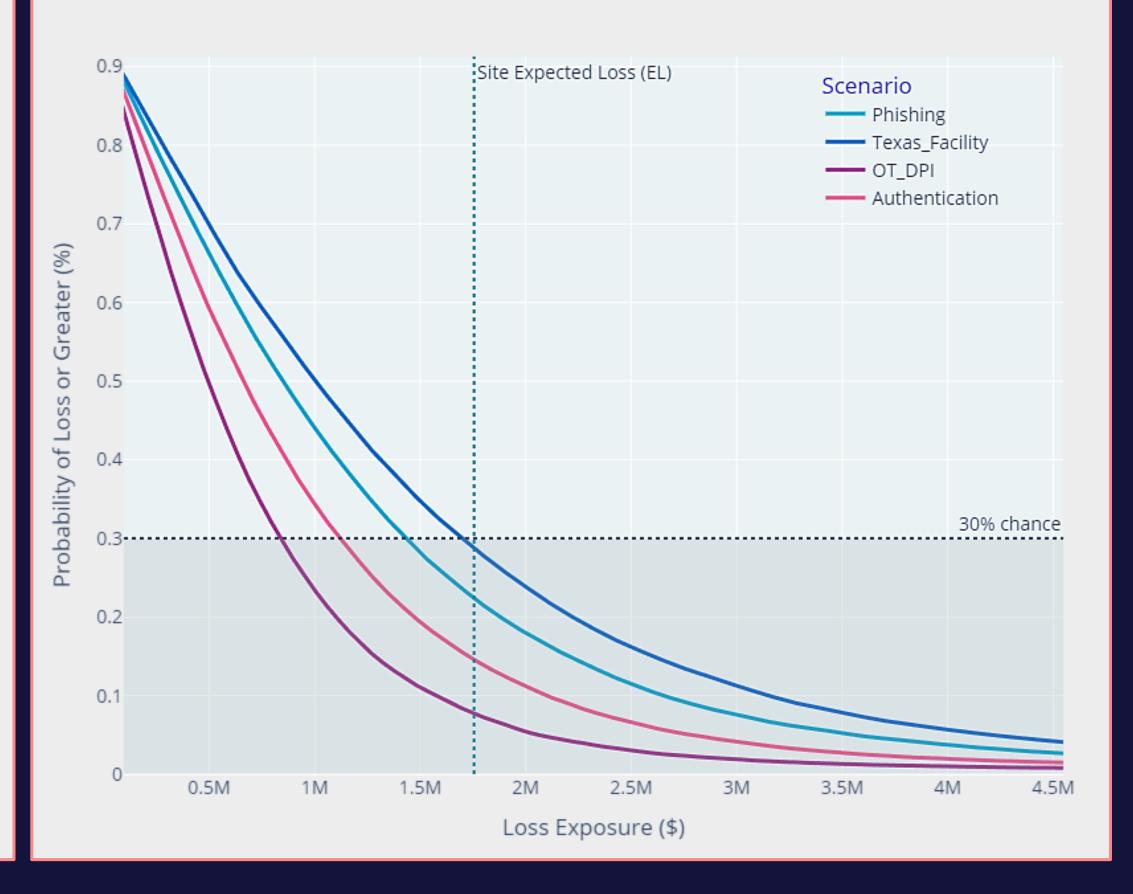
What scenario provides the most risk reduction

OT-DPI provides the biggest risk reduction



Loss Exposure (\$)

Risk Reduction – 30% chance



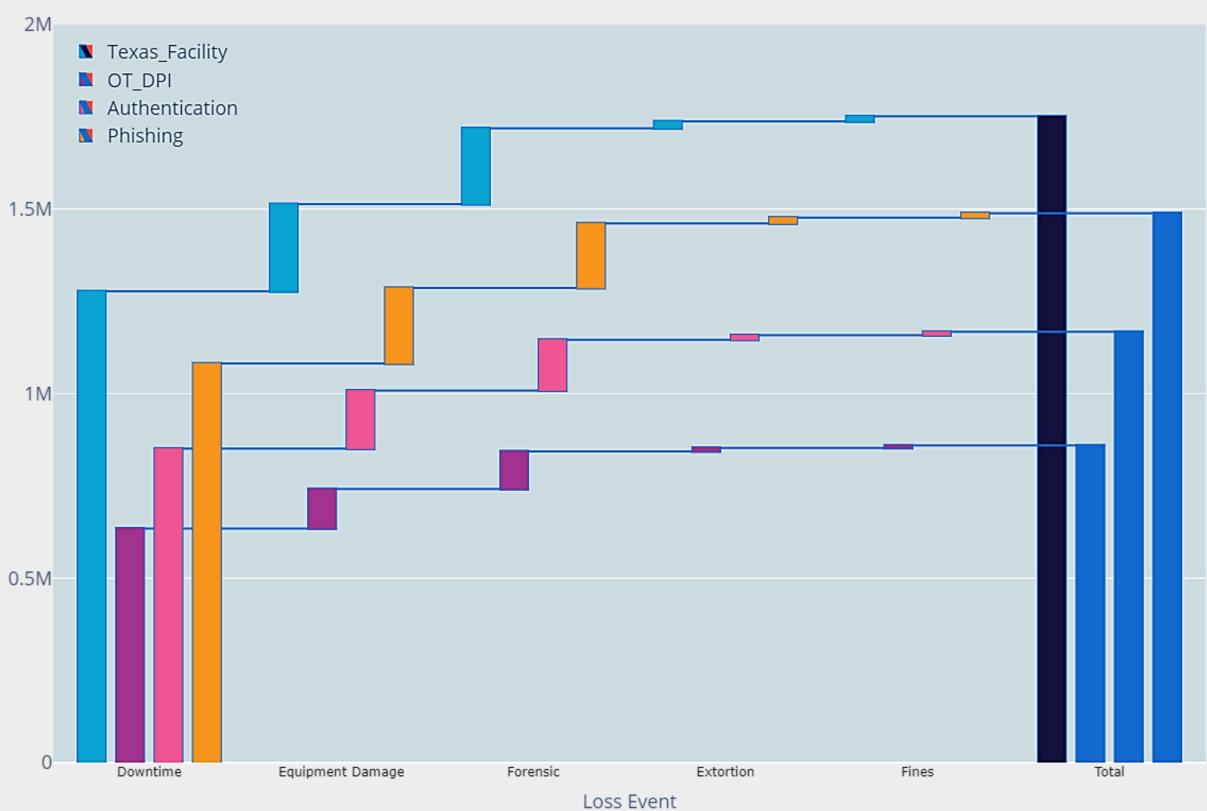


What scenario provides the most risk reduction?

Different initiatives | Different risk reduction



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



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



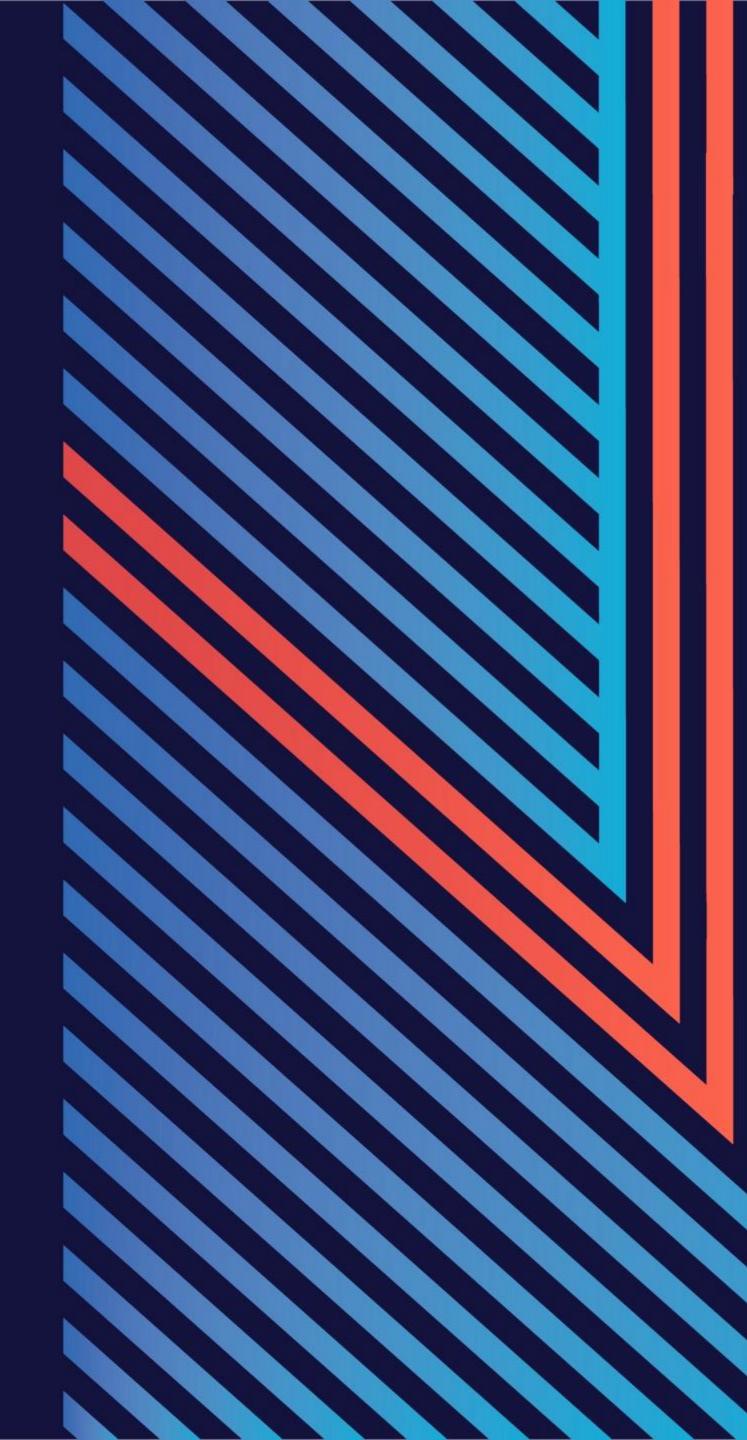








With DeRISK ...







Unlocking the value in data

Costly Unanswered Questions for Industrial Underwriters



Mitigation Strategies

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 Answei

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



Thank You Learn more @: DeNexus.io

DENEXUS Denet Construction Denet Constructio

ortfolio Navigator	
	and a second

Texas Wind Central			
	WAT PERSONNEL		
	INGS YOURS	100	
		-	

	LANY DAMAGE IN 17 JUL
30 Sites in Partfolio	

\$0	\$1.5M	\$3.3M
Notes and Notes	Late	Vote of Red 114 S105 Percentle
		\$1.54
	\$2558 (17%)	

\$0	\$255k	\$797k
All a frances	Experime Loss	Nature at Black (The Black Party and B
Texas Wind Ce	etral	Sile vs Peers

11/104 10/104013 10/10/102 10/10/102	D (-14)	\$25x (37%) \$325x (47%)
riige Notesta p Notesta p		882.8k (19%)

	THE PARTY OF THE P	
present ()		
	0 (-%) 518,2% (7%)	
	0(-40)	

ey Risk Controls 🙁

Completion to Yearly Target	Completion to Final Target
Identity .	
ABRE? MANAGEMENT.	10.00
	0.15
	101 EN
	1114
	111 - Hills
Pistect	
	19.42
AMARTINE AND TRAINING	11.47 No.

	tegies			
\mathcal{X}				
11		Pre Milli	gation	
		Fastest		
		MAX RO		
		Max NP	K.	
~				
_/				
-	1.1			
	110			eer Dis seraes

Romy Rodriguez-Ravines Risk Modeling

rr@denexus.io



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



Confidential & Proprietary. Copyright © by DeNexus, Inc.

