DENEXUS

Standards in Quantified Industrial Cyber Risk #3

DeNexus Knowledge Center
Part 2 – Driving Value from Data

In Part 2 of the DeNexus Knowledge Center- **Driving Value from Data**, Romy Rodriguez Ravines and Juan Carlos Cortinas Abad describe how we leverage data to **understand, quantify and manage Industrial OT cyber risk exposure, impact and ROI-based mitigation options.**

Our Standards in Quantified Industrial Cyber Risk series continues with DeNexus' Head of Research & Modelling Strategies, Romy Rodriguez Ravines and our Sr Director of Cybersecurity, Juan Carlos Cortinas Abad, presenting how we derive value from our ***DeNexus Knowledge Center***, the 'brain' of the ***Second Generation DeRISK Platform*** that has revolutionized the industrial cyber-risk modeling, quantification, and management industry.

In Part 2 of the DeNexus Knowledge Center- **Driving Value from Data**, we describe how we leverage data to **understand, quantify and manage Industrial OT cyber risk exposure, impact and ROI-based mitigation options.**

Our next paper in the series, **Part 3- Multi-Site Portfolio Solutions**, we will describe how the data in the DeNexus Knowledge Center is used to calculate **Multi-Site Risk, Portfolio Accumulation and Cyber-CAT Risk.**

The Data Difference Recap

In Part 1 The Data Difference we addressed some of the major challenges that quantifying cyber risk consistently presents: the data available for modeling is incomplete and sparse, and cyber risk requires rich models to capture the potential impact of events that occur in different industrial sectors.

The data challenges are exacerbated when it comes to Industrial OT organizations, where metadata about cyber incidents is lacking, especially when we try to account for the state of the company's security at the time of the incident.

On the flip side, Romy and Juan Carlos highlighted the variety of newly available data sources in the cyber threat, monitoring and vulnerability landscapes and the opportunities that technology opens for us; especially when it comes to leveraging Inside-Data.

"Combining critical data from inside an Industrial clients OT network (Inside-Data), together with outside threat, loss and vulnerability data (Outside-Data) opens an entirely new world of CRQM to the Industrial OT/ ICS landscape. That's why we call DeRISK the Second-Generation of Industrial Cyber Risk Quantification, Modelling and Management." Romy Rodriguez Ravines

Driving Value from Data-An Introduction

The ***DeNexus Knowledge Center*** is a unique OT CRQM knowledge base. It is built with structured and unstructured data from a global consortium of public, private, and proprietary threat intelligence and cyber breach data sources that bring together a 360 view of cyber risk.

Before we can drive value from that data, we must address the challenges that inherently come with such diverse data sources, types of data, granularities of that data, when and how often that data is updated and then we can approach enriching the data from each of those sources.

Each data source is thoroughly investigated and securely processed to generate the intelligence necessary to obtain each risk factor. In other words, we enrich information from many databases to provide a more complete understanding of the status of cyber incidents and their consequences.

How do we create intelligence? DeNexus utilizes data science and advanced analytics to model the cyber risk possibilities specific to the Industrial OT environment. DeNexus is transforming raw data into useful information about cyber risk complexity, contextualizing the available data and using it to drive valuable intelligence.

As a result, the DeRISK platform can derive the value necessary to feed meaningful indicators and dashboards that deliver OT stakeholders:

- Single Site Cyber Risk Quantification
- Multi-Site Cyber Risk Quantification
- Mitigation Recommendations
- Industry Peer Comparisons
- Portfolio Accumulation Analysis
- ICS/OT Cyber risk for the risk transfer industry
- Continuous Calibration and Validation

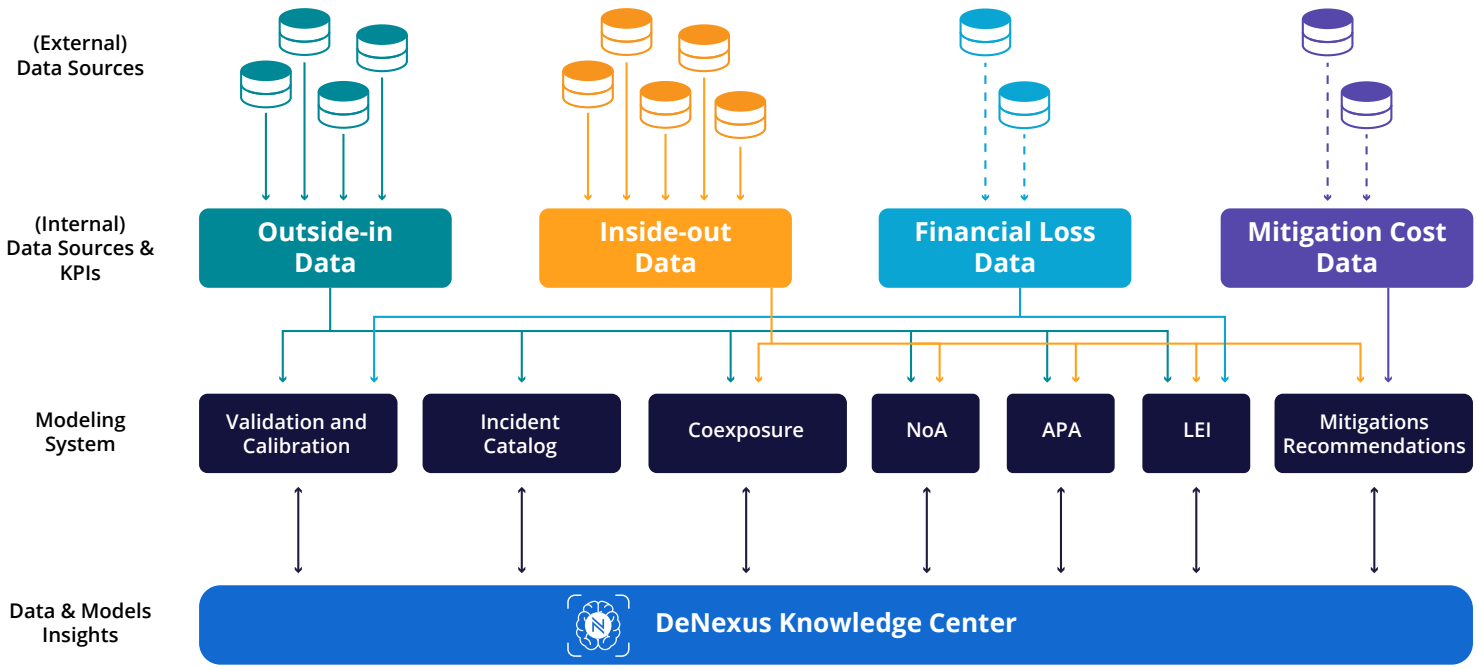

Figure 1: Data flow

NoA: Number of Attacks | APA: Attack Path Algorithms | LEI: Loss Event Impact | MRS: Mitigations Recommendations

Single-Site Cyber Risk Quantification

The core of ***DeRISK Platform*** is the single-site modeling system where the accumulated intelligence within the ***DeNexus Knowledge Center*** is used to simulate how a cyber-attack can spread and impact an organization, using a realistic representation of its OT network, along with near real time evidence-based inside-out and outside-in data.

Overall, we use data and mathematical models combined with cyber security domain knowledge to estimate (i) how many attempts could an organization face in a year; (ii) how likely is that an attack will succeed; and (iii) what is the dollar value for each successful attack?

It sounds simple on paper, but if we think about the kinds of threats, how many entry points, how many attack paths, which platforms, what vulnerabilities, what's the cyber impact… driving meaningful answers becomes very complicated.

The ***DeNexus Knowledge Center*** holds the answers we need in the cyber threat landscape. We have information about the attack surface, the supply chain exposure, dark web information threat actors use about your organization and employees, and information about the threat actors themselves.

We also have data about past incidents studied by the cyber community with detailed descriptions of the techniques used along with the platforms and vulnerabilities exploited. In other words, with the ***DeNexus Knowledge Center*** we can describe the dynamic cyber threats related to an organization, **from the adversary side of the equation**.

But, what about vulnerabilities and safeguards? ***DeNexus Knowledge Center*** also contains asset level information by Purdue Levels (Proximity to cyber-physical systems), the list of vulnerabilities by asset, Common Vulnerabilities & Exposures (CVEs), Common Vulnerability Scoring System (CVSS) and Security Control indicators and Maturity Level indicators, data retrieved from Inside-out sources (and informed by the organization). This information is crucial for a comprehensive understanding of how likely an attack is, **from the defender side**.

DeNexus Knowledge Center – Uniquely Rich

Data and CRQ (as for Jan 2023)

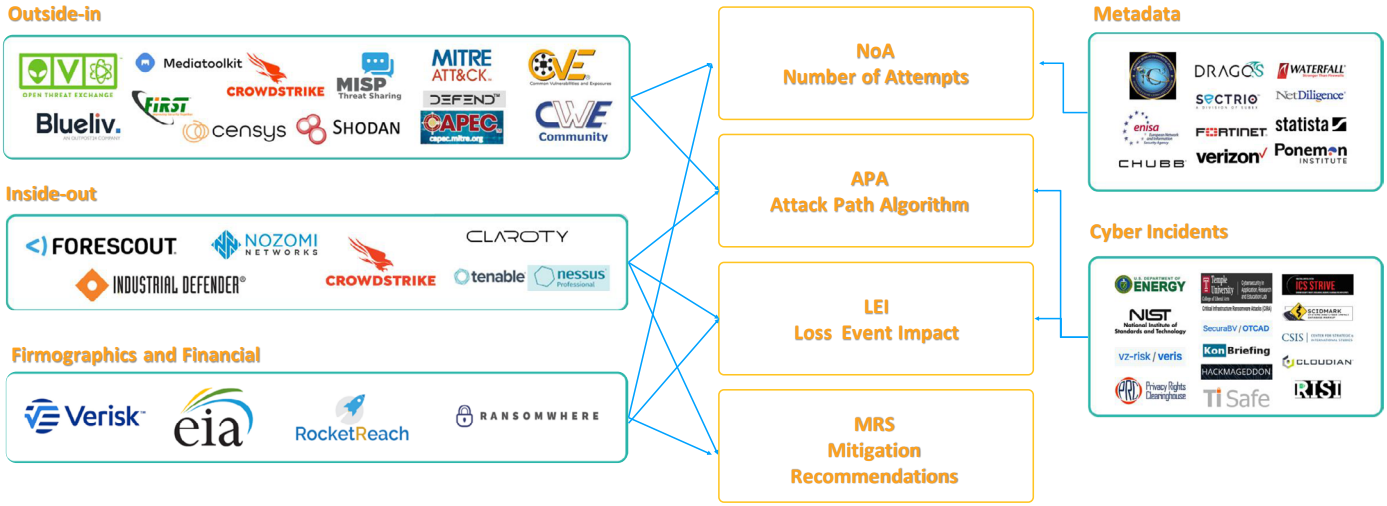

Figure 2: Example of data flow between sources and DeRISK models – January '23

DeRISK Platform builds the bridge that links adversary and defender data to enable industrial enterprises to understand their cyber risk at a granular level. Now they can see which loss events contribute most to their risk (productivity loss, equipment damage, extortion), what is the proportion of risk attributed to each access vector (phishing, supply chain), how vulnerabilities found in their system affect risk beyond overall scores, and so forth.

DeRISK Platform provides detailed information to answer the hard questions:

- *How much risk do I have?*
- *What is my Expected Loss, or my Value at Risk, or my tail risk?*
- *How likely is a given financial loss?*
- *Where is the risk coming from?*
- *How does it evolve over time?*
- *How do my risk factors compare with my industry peers?*

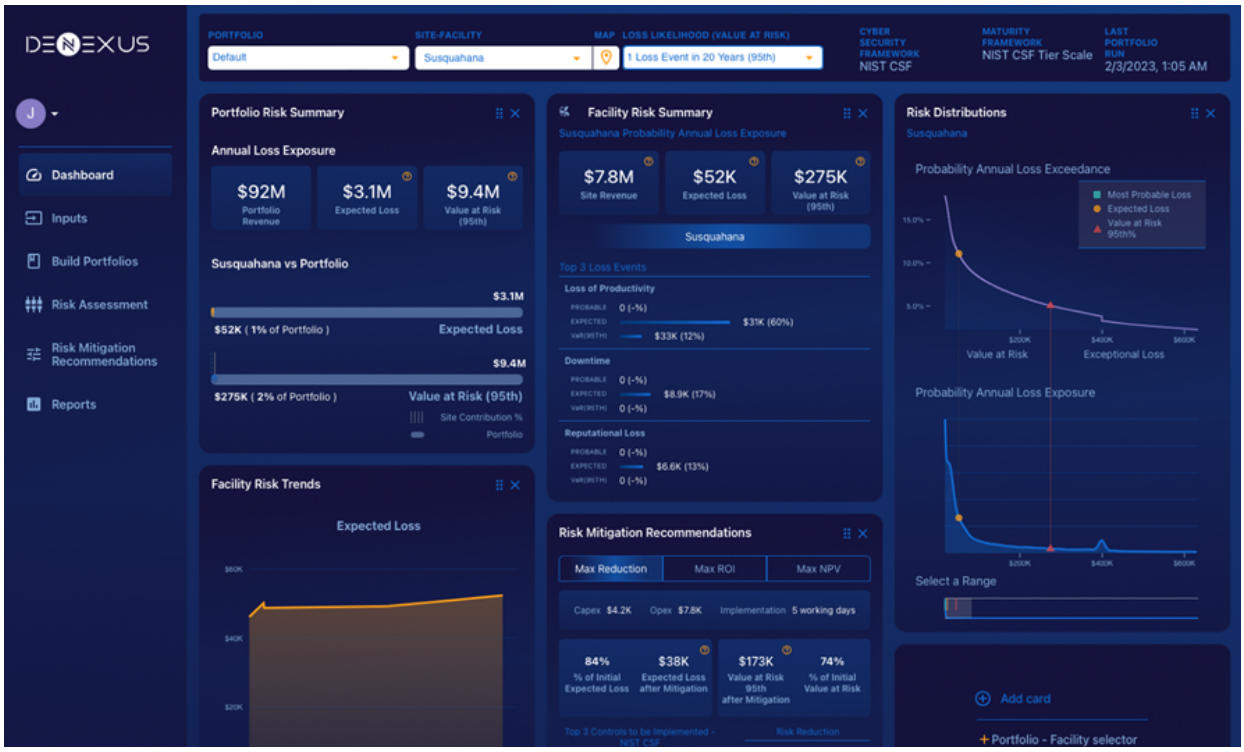

Figure 3: DeRISK Platform dashboard (v5.1.3)

Mitigation Recommendations – Remediation Projects

One of the advantages of having a robust modeling system is that we can ask and answer complex questions. One of the first questions involves what happens to risk factors once mitigation measures are implemented. ***"What if…?"***

- What if I invest my budget in a two-factor authentication program?
- What if I implement the network segmentation?
- What if we increase the Phishing detection?
- What if we implement new intrusion detection and monitoring solutions?

All of them are questions related to a security profile and investment in security controls.

DeRISK Platform enables risk reduction assessment within the context of customizable cyber-security improvement projects. The residual risk resulting from those projects is compared to the current assessment to help form before and after expectations.

"In other words, DeRISK provides new and relevant information to support ROI-based decision making for OT cyber risk investments based on performance or financial KPIs." Juan Carlos Cortinas Abad

DeNexus Knowledge Center allows you to define specific projects and determine the costs of the controls involved. A few project-specific use-cases that our clients utilize include:

- Projects that mature capabilities identified by low cost or high-risk reduction.
- Projects that align with organizational objectives and preferred strategies.
- Projects that ensure compliance objectives are met.

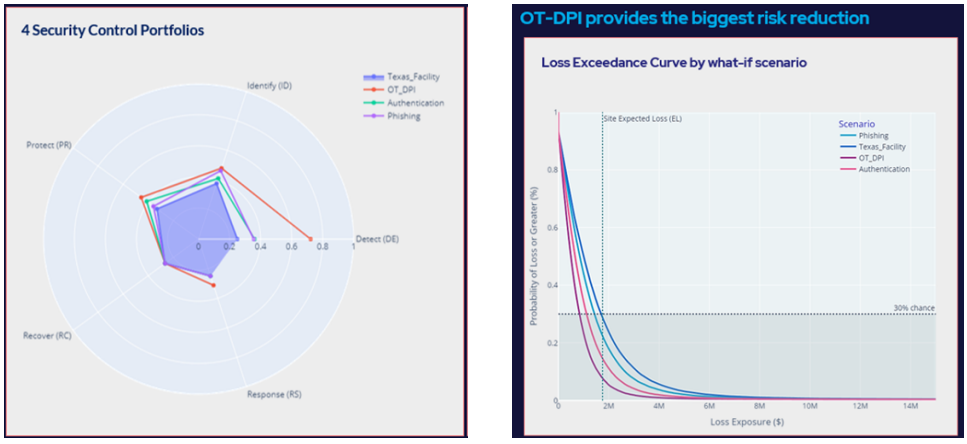

Figure 4: Security Controls and Risk Reduction

Mitigation Recommendations – Controls

Implementing controls to answer the question *"How can I mitigate my risk?"* involves evaluating the risk reduction obtained with many combinations of security controls, potentially millions of combinations! This is where complex recommendation algorithms come into place.

DeRISK Platform includes a unique module that finds the portfolio of security controls that minimizes the expected loss or maximizes the expected outcome of a selected strategy (ROI, NPV, or Fastest risk reduction), by a frontier level optimization mathematical algorithm. The solution incorporates concepts from risk aversion within a utility function so that the portfolio with maximum expected utility is chosen.

In other words, with the obtained in-depth understanding of the risks that the organization faces, we can lead to informed and optimized decisions on risk-control adoption which can reduce the likelihood of a cyber threat occurring or improve the capability to mitigate different types of impact.

Armed with the in-depth knowledge that comes from the DeRISK platform, OT stakeholders can answer the questions coming from the C-suite and the Board:

- *What mitigation options maximize my risk reduction?*
- *What mitigation options maximize my return on investment?*
- *What are the top 5 mitigations that provide the greatest risk reduction?*

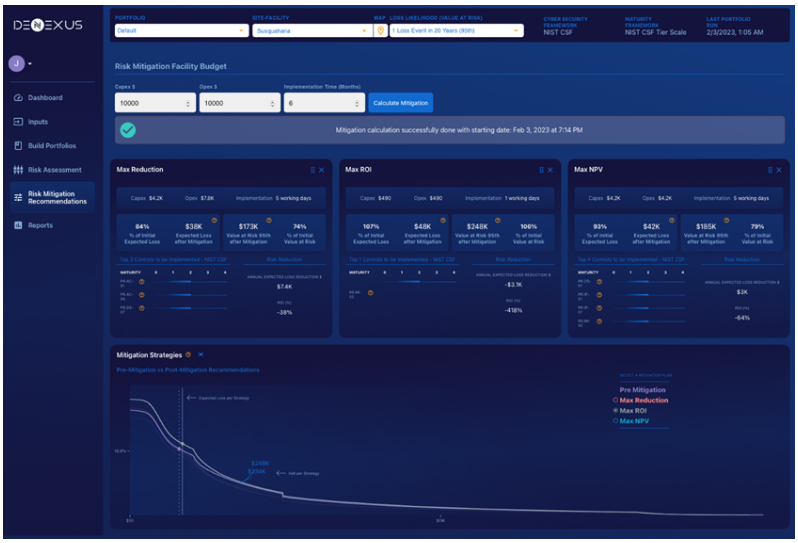

Figure 5: DeRISK Platform – Mitigation Recommendations (v5.1.3)

Powerful Data Drives Powerful Solutions

The ***DeNexus Knowledge Center*** is a pinnacle part of what makes ***DeRISK Platform*** the global standard in Industrial Cyber Risk Quantification and Management. All the critical information accumulated in the ***DeNexus Knowledge Center*** is stored, secured, and shared through our proprietary ***DeNexus Trusted Ecosystem***.

Together, they enable the ***DeRISK Platform*** to deliver **the world's first evidence-based, data-driven, real-time, and self-adaptive cyber risk quantification and management tool** that is purpose-built for Industrial OT stakeholders and the Underwriters, (re)Insurers and ILS Funds that insure them!

Our comprehensive approach to Risk Quantification delivers inside-out, outside-in and bottom-up visibility into an industrial asset's Exposure to cyber risk, the Probability of a breach, their financial Impact, ROI-based Mitigation Options, the in-depth analysis of internal and external drivers of risk and potential options for risk transfer.

Simply put, there is no **Second-Generation Cyber Risk Quantification and Management platform** for Industrial environments other than ***DeRISK Platform***.

DeRISK - DeNexus Knowledge Center - DeNexus Trusted Ecosystem

The global standard of industrial cyber risk quantification for Industrial OT stakeholders, investors, boards and the risk transfer market

Quantify Cyber Risk. Save Money.

We are DeNexus

DeNexus is the leading provider of cyber risk modeling for ICS/OT organizations and global (re)insurers. Our platform empowers the industrial enterprise and risk underwriters to quantify cyber risk exposure on a continuous, self-adaptive basis using the world's first evidence-based data analytics software and services. The DeRISK Platform from DeNexus is the world's first self-adaptive, cloud-based platform that uses evidence-based data to predict where and how breaches are likely to occur, what their business impact will be and how to mitigate them. DeNexus is headquartered in Sausalito, California with engineering based in Madrid, Spain.

Fortune 500 companies rely on Denexus to understand their bespoke cybersecurity economics and optimize their risk reduction ROI with the SOC 2, type 1 compliant solutions. Leverage DeNexus and our DeRISK Platform to make asset, vulnerable, configuration, operational anomaly, supply chain and cyber intrusion data work for you.

DENEXUS

DeNexus.io
@DeNexusInc1