Dynamic Industrial CYberrisk Modelling based on Evidence (DICYME)

Alberto Fernández-Isabel, Isaac Martín de Diego, Emilio L. Cano,
Rubén R. Fernández, Javier García-Ochoa,
Romy R. Ravines, Ovidio López, Jaume Puigbó

Rey Juan Carlos University & DeNexus Inc.

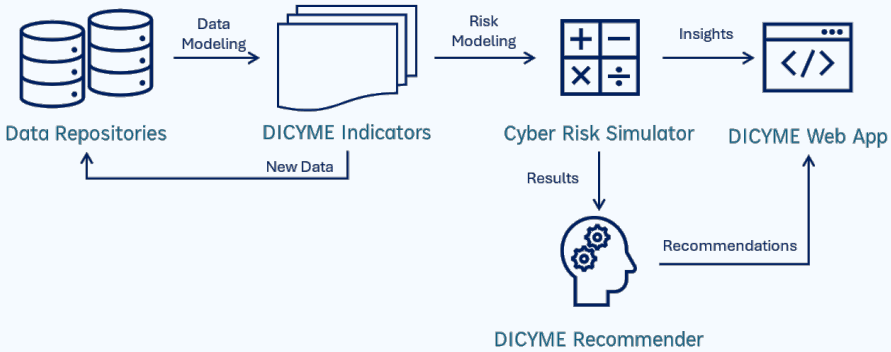
Jornadas Nacionales de Investigación en Ciberseguridad, 4 June 2025

- **Javier Sánchez García-Ochoa**
  - Researcher at DSLAB group, Rey Juan Carlos University (URJC), Spain. `www.datasciencelab.es`
  - `javier.garciaochoa@urjc.es`
- **Public-Private Collaboration** (CPP) project
  - **URJC** & **DeNexus Inc.**
  - Spanish Ministry of Science, Innovation and Universities (MICIU) under the **CPP2021-009025** call.

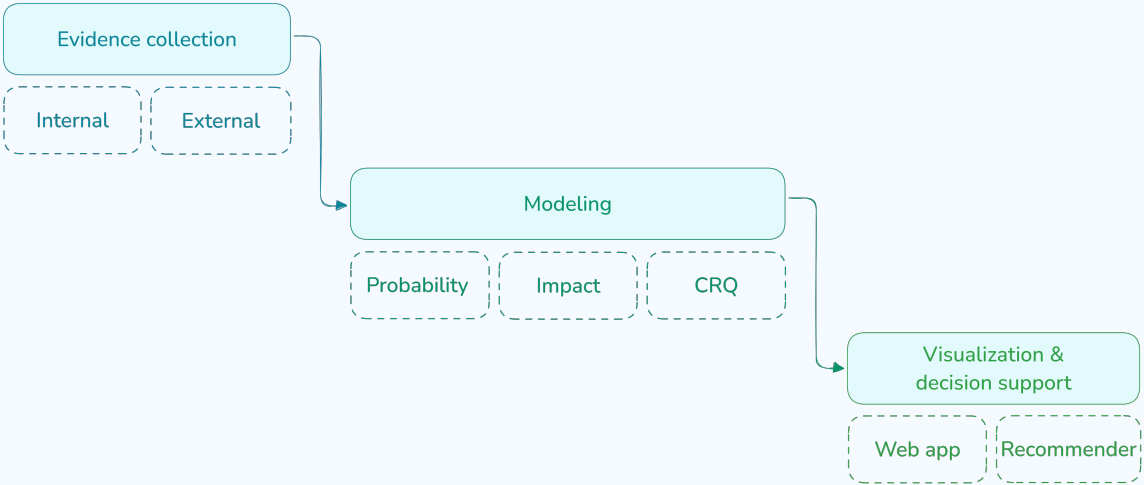
Contenido

- OT systems are vulnerable to cyberattacks.
- Current cybersecurity frameworks (e.g., NIST CSF, NIST SP 800-82, ISO 27019) do not fully address industrial needs.
- DeRISK^{TM} translates OT cyber risk exposures and vulnerabilities into business metrics.
- DICYME proposes a new approach for cyber risk quantification (CRQ).

- Evidence collection → Modeling → Visualization and decision support.
- Uses real and synthetic entities.
- Empowered by LLMs to translate data into actionable knowledge.



2. System workflow

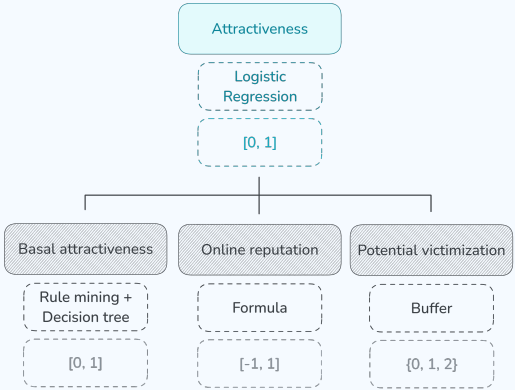


- **Cyber incidents:** multi-source incident data using NLP to remove duplicates and structure information.
- **Victim profile:** entity-level dataset with financials, reputation, and exposure signals for risk modeling (firmographics).
- **IDS telemetry:** anonymized sample of internal security data capturing vulnerabilities, assets, and threat activity.

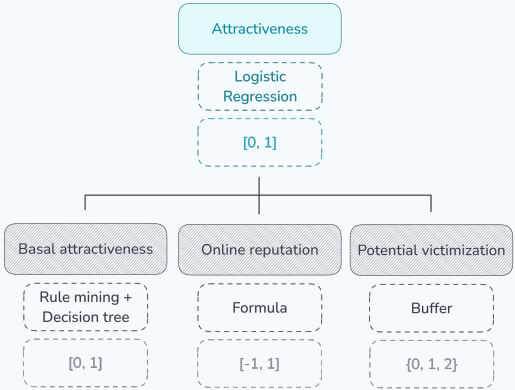
- **Cyber incidents:** multi-source incident data using NLP to remove duplicates and structure information.
- **Victim profile:** entity-level dataset with financials, reputation, and exposure signals for risk modeling (firmographics).
- **IDS telemetry:** anonymized sample of internal security data capturing vulnerabilities, assets, and threat activity.

- **Cyber incidents:** multi-source incident data using NLP to remove duplicates and structure information.
- **Victim profile:** entity-level dataset with financials, reputation, and exposure signals for risk modeling (firmographics).
- **IDS telemetry:** anonymized sample of internal security data capturing vulnerabilities, assets, and threat activity.

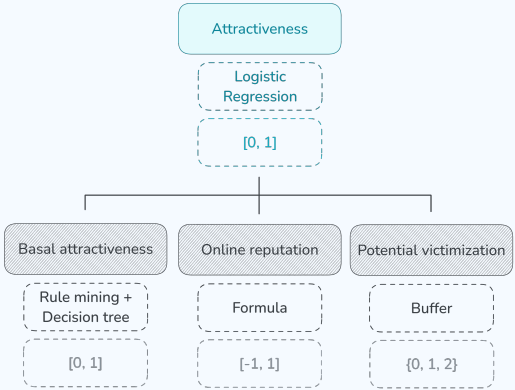
- **Attractiveness:** likelihood of being targeted.
- **THRACT:** threat actor profiling over time.
- **CVE2TTs:** CVE to MITRE ATT&CK mapping.



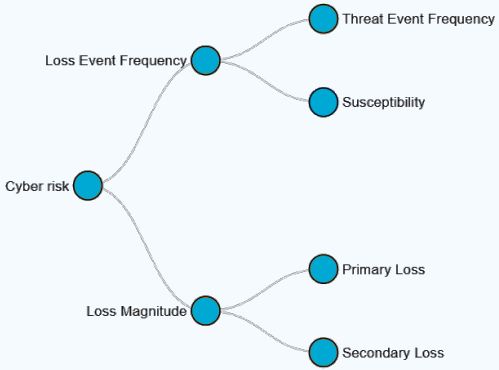
- **Attractiveness:** likelihood of being targeted.
- **THRACT:** threat actor profiling over time.
- **CVE2TTs:** CVE to MITRE ATT&CK mapping.



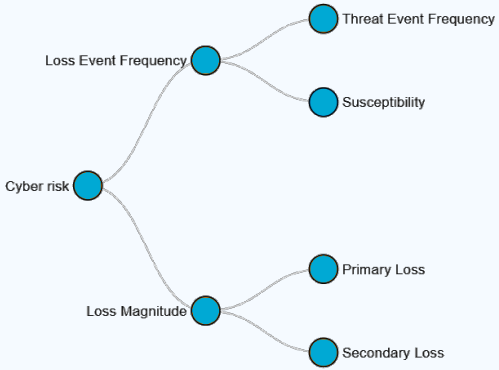
- **Attractiveness:** likelihood of being targeted.
- **THRACT:** threat actor profiling over time.
- **CVE2TTs:** CVE to MITRE ATT&CK mapping.



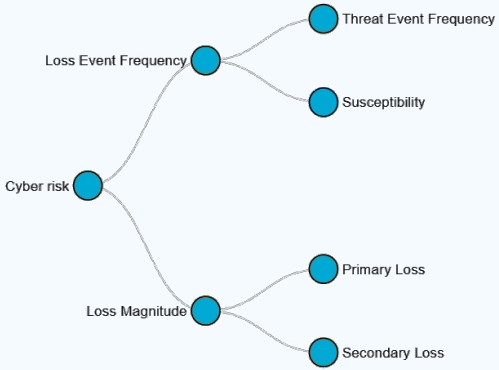
- Based on FAIR taxonomy.
- Combines: frequency × magnitude.
- Uses data and indicators, as well as some inputs.
- Uses Monte Carlo simulations and probabilistic distributions.



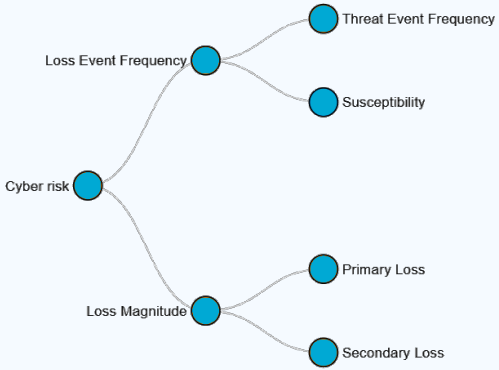
- Based on FAIR taxonomy.
- Combines: frequency $\times$ magnitude.
- Uses data and indicators, as well as some inputs.
- Uses Monte Carlo simulations and probabilistic distributions.

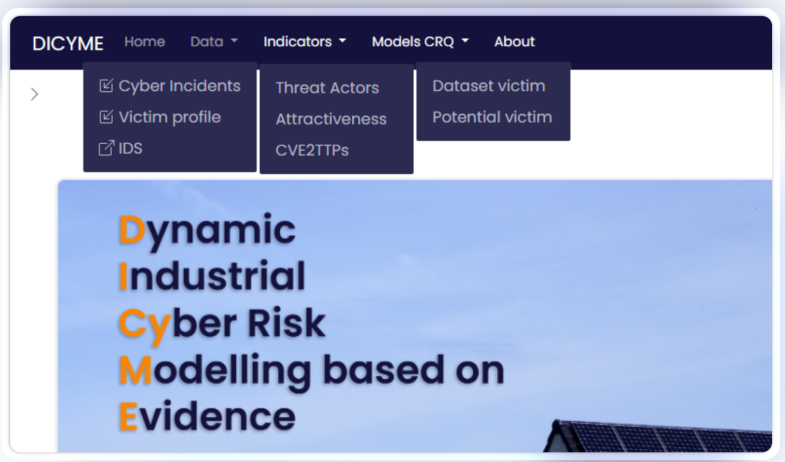


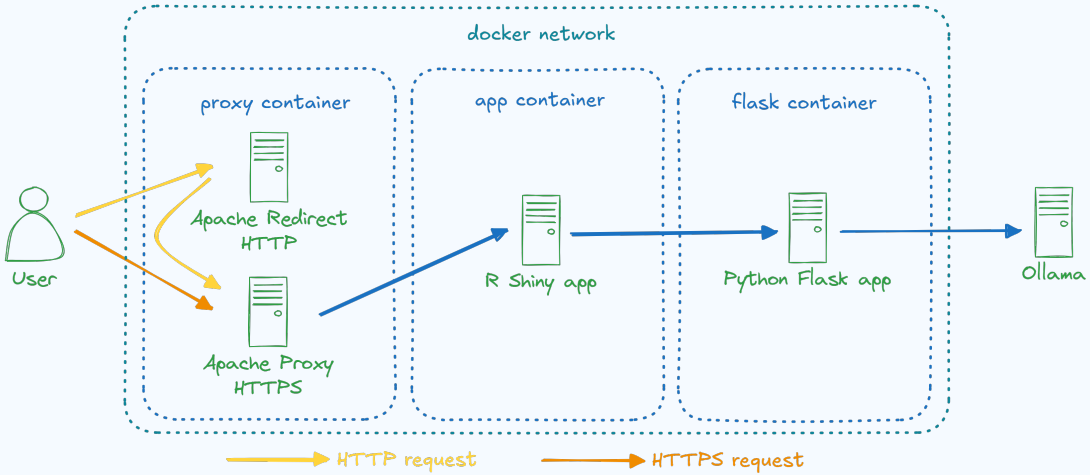
- Based on FAIR taxonomy.
- Combines: frequency $\times$ magnitude.
- Uses data and indicators, as well as some inputs.
- Uses Monte Carlo simulations and probabilistic distributions.



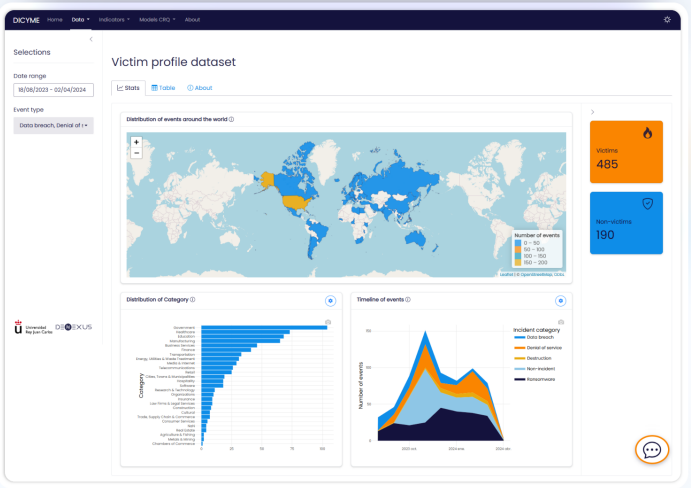
- Based on FAIR taxonomy.
- Combines: frequency $\times$ magnitude.
- Uses data and indicators, as well as some inputs.
- Uses Monte Carlo simulations and probabilistic distributions.



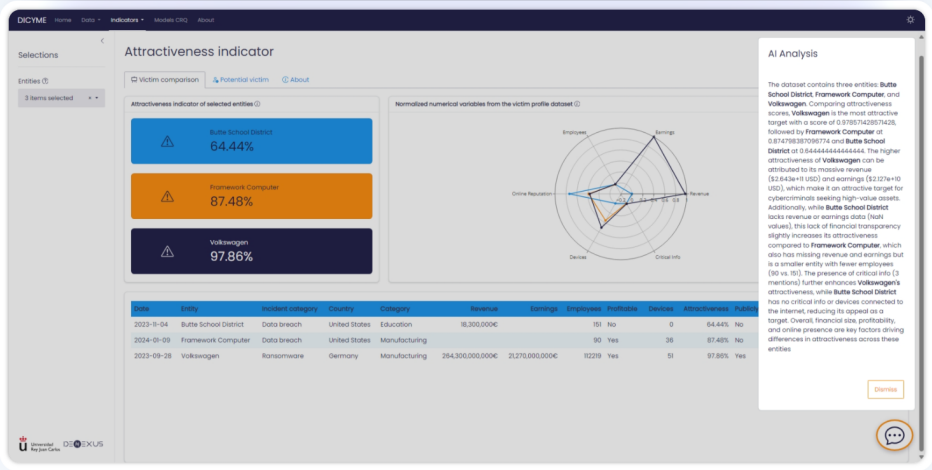

DICYME
Home
Data
Indicators
Models CRQ
About
Cyber Incidents
Victim profile
IDS
Threat Actors
Attractiveness
CVE2TTPs
Dataset victim
Potential victim
Dynamic
Industrial
Cyber Risk
Modelling based on
Evidence


docker network
proxy container
app container
flask container
User
Apache Redirect
HTTP
Apache Proxy
HTTPS
R Shiny app
Python Flask app
Ollama
HTTP request
HTTPS request

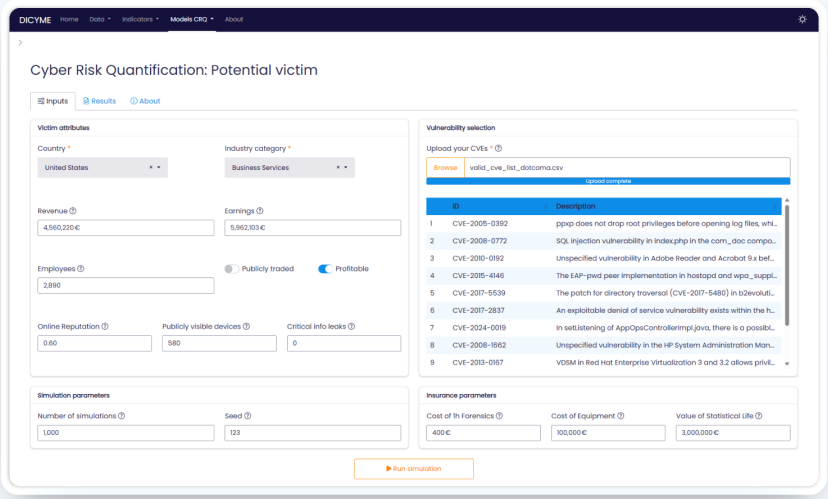
4. Visualization & decision support

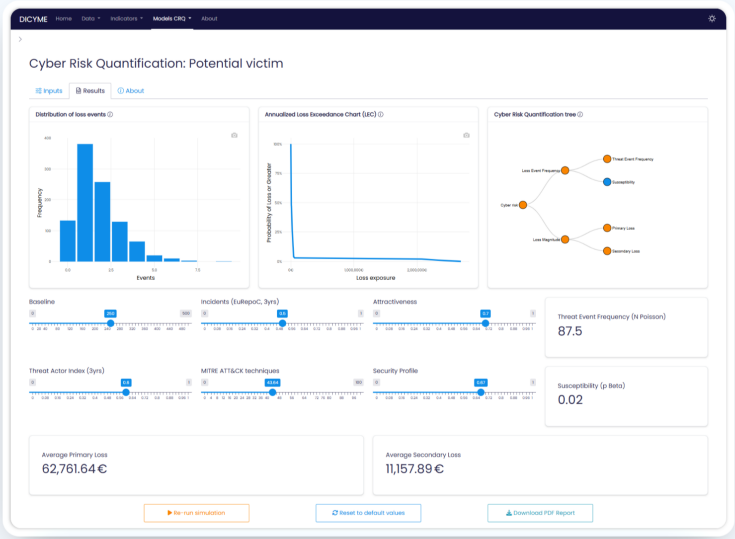


4. Visualization & decision support



4. Visualization & decision support




DICYME
Home
Data
Indicators
Models CRQ
About
Cyber Risk Quantification: Potential victim
Inputs
Results
About
Distribution of loss events
Frequency
Events
Annualized Loss Exceedance Chart (LEC)
Probability of Loss or Greater
Loss exposure
Cyber Risk Quantification tree
Loss Event Frequency
Threat Event Frequency
Susceptibility
Cyber risk
Loss Magnitude
Primary Loss
Secondary Loss
Baseline
Incidents (EuRepoC, 3yrs)
Attractiveness
Threat Event Frequency (N Poisson)
87.5
Threat Actor Index (3yrs)
MITRE ATT&CK techniques
Security Profile
Susceptibility (p Beta)
0.02
Average Primary Loss
62,761.64 €
Average Secondary Loss
11,157.89 €
Re-run simulation
Reset to default values
Download PDF Report

- **Curated datasets:** Aggregated from public, private and telemetry sources to ensure coverage and reliability.
- **Novel indicators:** Metrics such as *Attractiveness*, *THRACT* and *CVE2TTs* provide actionable, data-driven insights.
- **CRQ integration:** Quantification models aligned with FAIR are embedded into a modular platform.
- **Support for insurers:** The system enables more informed underwriting and risk pricing decisions.
- **Explainable AI:** LLM-powered modules enhance transparency for non-expert users.

- **Curated datasets:** Aggregated from public, private and telemetry sources to ensure coverage and reliability.
- **Novel indicators:** Metrics such as *Attractiveness*, *THRACT* and *CVE2TTs* provide actionable, data-driven insights.
- **CRQ integration:** Quantification models aligned with FAIR are embedded into a modular platform.
- **Support for insurers:** The system enables more informed underwriting and risk pricing decisions.
- **Explainable AI:** LLM-powered modules enhance transparency for non-expert users.

- **Curated datasets:** Aggregated from public, private and telemetry sources to ensure coverage and reliability.
- **Novel indicators:** Metrics such as *Attractiveness*, *THRACT* and *CVE2TTs* provide actionable, data-driven insights.
- **CRQ integration:** Quantification models aligned with FAIR are embedded into a modular platform.
- **Support for insurers:** The system enables more informed underwriting and risk pricing decisions.
- **Explainable AI:** LLM-powered modules enhance transparency for non-expert users.

- **Curated datasets:** Aggregated from public, private and telemetry sources to ensure coverage and reliability.
- **Novel indicators:** Metrics such as *Attractiveness*, *THRACT* and *CVE2TTs* provide actionable, data-driven insights.
- **CRQ integration:** Quantification models aligned with FAIR are embedded into a modular platform.
- **Support for insurers:** The system enables more informed underwriting and risk pricing decisions.
- **Explainable AI:** LLM-powered modules enhance transparency for non-expert users.

- **Curated datasets:** Aggregated from public, private and telemetry sources to ensure coverage and reliability.
- **Novel indicators:** Metrics such as *Attractiveness*, *THRACT* and *CVE2TTs* provide actionable, data-driven insights.
- **CRQ integration:** Quantification models aligned with FAIR are embedded into a modular platform.
- **Support for insurers:** The system enables more informed underwriting and risk pricing decisions.
- **Explainable AI:** LLM-powered modules enhance transparency for non-expert users.

- **CRQ simulation refinement:** Improve accuracy of probabilistic models.
- **Recommender system:** Suggest optimal mitigation actions based on cost-effectiveness and risk impact.
- **AI for data processing:** Use machine learning models to improve data collection, multi-source merging, and missing value imputation.
- **Web platform rollout:** Public demo version with real-time interactions and downloadable reports.
- **Academic dissemination:** Ongoing publications and use in educational cybersecurity programs.
- **Commercial integration:** Modules will be integrated into DeRisk™.

- **CRQ simulation refinement:** Improve accuracy of probabilistic models.
- **Recommender system:** Suggest optimal mitigation actions based on cost-effectiveness and risk impact.
- **AI for data processing:** Use machine learning models to improve data collection, multi-source merging, and missing value imputation.
- **Web platform rollout:** Public demo version with real-time interactions and downloadable reports.
- **Academic dissemination:** Ongoing publications and use in educational cybersecurity programs.
- **Commercial integration:** Modules will be integrated into DeRisk™.

- **CRQ simulation refinement:** Improve accuracy of probabilistic models.
- **Recommender system:** Suggest optimal mitigation actions based on cost-effectiveness and risk impact.
- **AI for data processing:** Use machine learning models to improve data collection, multi-source merging, and missing value imputation.
- **Web platform rollout:** Public demo version with real-time interactions and downloadable reports.
- **Academic dissemination:** Ongoing publications and use in educational cybersecurity programs.
- **Commercial integration:** Modules will be integrated into DeRisk™.

- **CRQ simulation refinement:** Improve accuracy of probabilistic models.
- **Recommender system:** Suggest optimal mitigation actions based on cost-effectiveness and risk impact.
- **AI for data processing:** Use machine learning models to improve data collection, multi-source merging, and missing value imputation.
- **Web platform rollout:** Public demo version with real-time interactions and downloadable reports.
- **Academic dissemination:** Ongoing publications and use in educational cybersecurity programs.
- **Commercial integration:** Modules will be integrated into DeRisk™.

- **CRQ simulation refinement:** Improve accuracy of probabilistic models.
- **Recommender system:** Suggest optimal mitigation actions based on cost-effectiveness and risk impact.
- **AI for data processing:** Use machine learning models to improve data collection, multi-source merging, and missing value imputation.
- **Web platform rollout:** Public demo version with real-time interactions and downloadable reports.
- **Academic dissemination:** Ongoing publications and use in educational cybersecurity programs.
- **Commercial integration:** Modules will be integrated into DeRisk™.

- **CRQ simulation refinement:** Improve accuracy of probabilistic models.
- **Recommender system:** Suggest optimal mitigation actions based on cost-effectiveness and risk impact.
- **AI for data processing:** Use machine learning models to improve data collection, multi-source merging, and missing value imputation.
- **Web platform rollout:** Public demo version with real-time interactions and downloadable reports.
- **Academic dissemination:** Ongoing publications and use in educational cybersecurity programs.
- **Commercial integration:** Modules will be integrated into DeRisk^{TM}.

Thank you! Any questions?

javier.garciaochoa@urjc.es

DSLAB DATA SCIENCE LABORATORY
Universidad Rey Juan Carlos
DENEXUS
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
AGENCIA ESTATAL DE INVESTIGACIÓN