Convocatoria Colaboración Público-Privada CPP2021-009025

DICYME:

Dynamic Industrial CYberrisk Modelling based on Evidence

Iniciativa Conjunta de:

DENEXUS

Universidad Rey Juan Carlos

ENTREGABLE 5.2:

Informe final de presentación de resultados

Coordinadores:

Romy R. Ravines (DeNexus Tech)
Isaac Martín de Diego (Universidad Rey Juan Carlos)
Alberto Fernández Isabel (Universidad Rey Juan Carlos)

MINISTERIO DE CIENCIA E INNOVACIÓN

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

AGENCIA ESTATAL DE INVESTIGACIÓN

Contenido

1 INTRODUCCIÓN Y OBJETIVOS

Este documento describe las actividades de comunicación, difusión y uso de los resultados del proyecto DICYME por parte de las dos instituciones involucradas.

2 ESTRATEGIAS DE COMUNICACIÓN Y DIFUSIÓN

Este primer bloque de actividades engloba las acciones orientadas a dar visibilidad y transferir el conocimiento generado en el marco del proyecto DICYME. La estrategia busca garantizar que los avances se comuniquen de manera efectiva al público general y especializado, reforzando la percepción del valor añadido del proyecto y fomentando su impacto en la comunidad científica, profesional e industrial. La comunicación se centra en ofrecer información clara y accesible, mientras que la difusión está orientada a la comunidad académica, técnica y a los usuarios potenciales de las soluciones desarrolladas.

2.1 Actividades de comunicación

Las actividades de comunicación tienen como objetivo asegurar la presencia del proyecto en canales públicos de alta visibilidad, facilitando el acceso a información actualizada y atractiva para audiencias amplias:

2.1.1 Página web del proyecto

Se constituye como el eje central de la estrategia de comunicación, ofreciendo una descripción general del proyecto, sus objetivos, socios participantes y los dominios de aplicación. Además de servir como repositorio de entregables públicos, funciona como escaparate para logros, avances y novedades. Está disponible tanto en inglés como español, combinando el idioma oficial del proyecto (al estar financiado por el Ministerio de Ciencia e Innovación a través de la Agencia Estatal de Investigación) con la lengua de referencia en la relación con clientes, usuarios, y cualquier otra forma de comunicación y difusión internacional.

Ambas versiones de la web contienen la misma estructura:

- **Página principal**: presenta una visión general del proyecto, incluyendo la financiación asignada y las entidades financiadoras (junto con sus respectivos logotipos obligatorios), los integrantes de los equipos de la URJC y DeNexus, así como una sección dedicada a las últimas novedades, que recoge publicaciones recientes tanto en el blog como en redes sociales. Disponible en la versión en inglés y la versión en español.
- **El proyecto**: ofrece una descripción detallada que abarca las cinco actividades principales, junto con sus respectivas tareas y los entregables definidos en cada una. Además, se especifican las fechas previstas para la disponibilidad de dichos documentos, y se facilita el acceso a los entregables ya finalizados, disponibles en formato PDF para su descarga por parte de los visitantes de la página web. Disponible también tanto en la versión en inglés y la versión en español.

- **Blog**: la página web también contiene el enlace al blog del proyecto, detallado en la Blog del proyecto.

2.1.2 Blog del proyecto

Este espacio permite la publicación periódica de contenidos sobre avances técnicos, modelos desarrollados y casos de uso, favoreciendo la transparencia y la generación de interés continuado. Hasta septiembre de 2025 se han publicado un total de 15 entradas, divididas en dos categorías:

- **Investigación y desarrollo (*Research & Development*, R&D)**: engloba artículos centrados en los avances metodológicos y técnicos del proyecto, como la descripción de nuevos conjuntos de datos, nuevos modelos de estimación de ciberriesgo o la integración de técnicas de visualización para la toma de decisiones.
    - *A Dynamic Approach to Data-Driven Insights on Cyber Threat Actors* (15/12/2023): explica el indicador de actores de amenazas desarrollado durante las actividades 1 y 2 del proyecto y su visualización e integración en el prototipo final a lo largo de las actividades 3 y 4. Disponible en el blog del proyecto.
    - *Defining the Basal Attractiveness Concept for Cybercriminals* (06/05/2024): detalla el indicador del atractivo basal de una organización, desarrollado también durante las actividades 1 y 2 del proyecto. Disponible en el blog del proyecto.
    - *AI to Map Software Vulnerabilities to Cyberattack Techniques* (15/07/2024): aborda cómo se emplean modelos de inteligencia artificial, en concreto redes neuronales, para relacionar CVEs con las tácticas y técnicas de MITRE ATT&CK. Disponible en el blog del proyecto.
    - *Exploring the visual interface of the DICYME web app* (15/12/2024): ofrece una visión general sobre la navegación y estructura de la aplicación web desarrollada en las actividades 3 y 4 para integrar y facilitar al usuario la comprensión de todos los resultados de las actividades 1 y 2, así como la integración en modelos de cuantificación del ciberriesgo. Disponible en el blog del proyecto.
    - *Harnessing LLMs for cybersecurity risk assessment in DICYME* (03/02/2025): aporta detalles sobre las técnicas y tecnologías empleadas para ofrecer a los usuarios de la aplicación web una explicación en texto natural de las visualizaciones mostradas en cada pestaña, así como datos o detalles importantes de los modelos. Disponible en el blog del proyecto.
    - *DICYME Cyber Risk Calculator* (03/03/2025): desgrana cómo integramos todos los resultados del proyecto para lograr la cuantificación del ciberriesgo, basándonos en la metodología FAIR pero empleando simulaciones y elementos propios, como los indicadores de atractivo o actores de amenazas, el conjunto de datos de perfil de víctimas, etc. Disponible en el blog del proyecto.

- *VISCA: A data-driven approach to victim profiling and attractiveness modeling* (01/09/2025): expone el sistema VISCA, que automatiza la extracción a gran escala de atributos sobre víctimas de ciber incidentes desde diferentes fuentes de información, combina duplicados y normaliza el resultado para generar un conjunto de datos que nutra los modelos de Atractivo. Disponible en el blog del proyecto.
- *DICYME at Computer Science and Information Systems*. Publicación del paper "Defining the Attractiveness Concept for Cyber Incident Forecasting". Disponible en el blog del proyecto.

- **Actividad**: incluyen entradas relacionadas con la participación en congresos, jornadas y eventos especializados, así como noticias sobre publicaciones aceptadas en congresos y revistas científicas.
  - *About DeNexus* (02/01/2023): introducción a los principios y objetivos de DeNexus, así como su principal producto, denominado DeRISK™. Disponible en el blog del proyecto.
  - *About URJC DSLAB* (01/02/2023): descripción del grupo de investigación, sus objetivos y principales líneas de investigación. Disponible en el blog del proyecto.
  - *URJC at RootedCON y T3chFest* (01/04/2024): presentación de la asistencia de miembros del equipo de la URJC a los eventos RootedCON y T3chFest 2024. Disponible en el blog del proyecto.
  - *Knowledge transfer in the DICYME project: R and cybersecurity risk analysis* (01/11/2024): descripción de cómo el proyecto DICYME utiliza el lenguaje R para desarrollar herramientas avanzadas de análisis de riesgos en ciberseguridad, destacando la aplicación web basada en Shiny. Incluye las menciones realizadas al proyecto en la 92ª reunión del Grupo de Usuarios de R de Madrid, la conferencia *useR!* en Salzburgo y el Congreso de Usuarios de R en Sevilla, celebrados todos durante 2024. Disponible en el blog del proyecto.
  - *DeNexus at III Cybersecurity week at UAX* (10/04/2025): reseña de la participación del equipo de DeNexus en la III Semana de la Ciberseguridad de la Universidad Alfonso X el Sabio (UAX), donde presentaron la charla "*Leveraging Data & AI for Cyber Risk Management*". En ella, mostraron cómo la ciencia de datos y la inteligencia artificial pueden generar indicadores útiles para gestionar el ciberriesgo, como el índice de actores de amenaza y el mapeo de vulnerabilidades con MITRE ATT&CK, ambos casos de éxito del proyecto. Disponible en el blog del proyecto.
  - *DICYME project featured at JNIC 2025 conference* (05/06/2025): presentación de artículos en el congreso nacional JNIC 2025. Disponible en el blog del proyecto.
  - *DICYME - DeNexus at International Congress of Cybersecurity: Companies, Research and Society*. Participación en la mesa redonda *"Empresas: retos, investigación e innovación en Ciberseguridad"* el 01 de octubre de 2025. Disponible en el blog del proyecto.

2.1.3 Blog y redes sociales del DSLAB

A través de los canales institucionales del grupo de investigación Data Science Lab, al que pertenecen los investigadores de la URJC del equipo DICYME, se ha reforzado la visibilidad del proyecto mediante la difusión de publicaciones científicas, participación en congresos y resultados intermedios, alcanzando así a una audiencia especializada y a una comunidad más amplia interesada en ciberseguridad y ciencia de datos, manteniendo los detalles más técnicos del proyecto en su blog propio.

- **Cuenta** @DSLAB_URJC **en X**
    - 07/03/2024: coworking interno del equipo de la URJC sobre el proyecto. Disponible en la red social X.
    - 24/10/2024: información sobre la 92ª reunión del Grupo de Usuarios de R de Madrid sobre el uso de R en el DSLAB, en la que se expone el proyecto DICYME. Disponible en la red social X.
    - 30/10/2024: fotografías sobre la 92ª reunión del Grupo de Usuarios de R de Madrid sobre el uso de R en el DSLAB. Disponible en la red social X.
    - 07/11/2024: presentación de la herramienta CRAS, desarrollada por Emilio López, miembro del equipo de la URJC, que ha servido como base de la aplicación web de DICYME y del modelo de cuantificación del ciberriesgo. Disponible en la red social X.
    - 04/06/2025: presentación de artículos en el congreso nacional JNIC 2025. Disponible en la red social X.
    - 03/09/2025: anuncio de la publicación del artículo *Defining the Attractiveness Concept for Cyber Incidents Forecasting* en *Computer Science and Information Systems* (ComSIS). Disponible en la red social X. También se ha replicado la comunicación en la cuenta de LinkedIn del DSLAB.

- Blog del DSLAB alojado en su sitio web oficial (www.datasciencelab.es)
    - *RootedCON y T3chFest* (18/03/2024): asistencia de miembros del equipo de la URJC a los eventos RootedCON y T3chFest 2024. Disponible en el blog del DSLAB.
    - *Uso de R en el DSLAB* (30/10/2024): información sobre la 92ª reunión del Grupo de Usuarios de R de Madrid sobre el uso de R en el DSLAB, en la que se expone el proyecto DICYME. Disponible en el blog del DSLAB.
    - *Analizando datos en ciberseguridad* (03/06/2025): información sobre el webinar en el que se expuso el proyecto DICYME como caso de éxito del uso del Big Data y la Ciencia de Datos en ciberseguridad. Disponible en el blog del DSLAB.
    - *El proyecto DICYME, protagonista en el congreso JNIC 2025* (04/06/2025): presentación de artículos en el congreso nacional JNIC 2025. Disponible en el blog del DSLAB.

2.1.4 Charlas y eventos de comunicación

- *III Semana de la Ciberseguridad en la UAX*: la participación en este evento por miembros del equipo de DeNexus supone una oportunidad para acercar el proyecto a la comunidad universitaria y académica de una universidad vecina, reforzando su posicionamiento en el ecosistema de ciberseguridad en España y creando un espacio de intercambio con actores clave.
- *Webinar Ciberseguridad para un Futuro Conectado*: parte del equipo de la URJC participó en este evento, organizado por el Centro Demostrador TIC de Extremadura (CDTIC) en el marco del proyecto TriRuralTech, abordando por qué el análisis de datos es una pieza clave para reforzar la ciberseguridad en el panorama actual. Entre los casos de éxito expuestos, destacó DICYME como ejemplo de aplicación de diversas técnicas de Ciencia de Datos y *Machine Learning* para resolver problemas y crear modelos novedosos para cuantificar el ciber riesgo.

2.2 Actividades de difusión

Las actividades de difusión se orientan a la comunidad científica y técnica, así como a profesionales y potenciales clientes interesados en los resultados de DICYME. La finalidad es promover la transferencia de conocimiento, fortalecer colaboraciones y aumentar la visibilidad del proyecto en foros especializados.

2.2.1 Entregables públicos

Todos los documentos públicos generados están disponibles en la web del proyecto, tanto en la versión en inglés y la versión en español, siguiendo un enfoque de acceso abierto que garantice su conocimiento y reutilización por la comunidad investigadora y profesional.

2.2.2 Publicaciones científicas

Se han publicado un total de tres artículos durante la duración del proyecto, además de una aceptación adicional en un congreso internacional. Dos de los artículos publicados corresponden a las Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2025), de los cuales uno tiene formato póster, mientras que tercero forma parte de la revista internacional *Computer Science and Information Systems* (ComSIS). La última contribución, que se encuentra en estado aceptado, corresponde al congreso internacional IDEAL 2025.

- *Defining the Basal Attractiveness Concept for Cybercriminals* (JNIC 2025, formato póster): describe el concepto de atractivo basal, ampliamente abordado en los diversos entregables de la actividad 2 del proyecto. Este concepto categoriza a las víctimas potenciales de ciber incidentes según su ubicación, tamaño, ganancias... El póster se encuentra adjunto en el ANEXO A: Póster JNIC 2025. Publicado en las actas de las jornadas, estando disponible el libro completo.

- *Dynamic Industrial Cyber risk Modelling based on Evidence (DICYME)* (JNIC 2025): aborda el Sistema complete desarrollado en el proyecto como una aplicación web interactiva de acceso público que permite explorar los conjuntos de datos e interactuar con los modelos de datos de manera independiente, así como realizar una cuantificación del ciber riesgo de una entidad, tanto de las existentes en los *datasets* como de una cualquiera que defina el usuario. Publicado en el libro completo de actas.
- *Defining the Attractiveness Concept for Cyber Incidents Forecasting* (ComSIS): define de una manera más extensiva el concepto de atractivo, incluyendo nuevas variables como la reputación en redes sociales y visibilidad en la red de dispositivos de las entidades, con nuevos modelos de *Machine Learning* para combinar todos los atributos y predecir el valor final. Accesible desde DOISerba.
- *Using LLM Agents for Data Integration in Cybersecurity Incidents* (IDEAL 2025): explora una novedosa utilidad de los modelos grandes de lenguaje (*Large Language Models*, LLMs), construyendo una arquitectura multi-agente que se encarga de obtener de diferentes fuentes de información atributos sobre víctimas de ciber incidentes, combinar duplicados y normalizar el resultado para generar un conjunto de datos a gran escala que nutra los modelos de atractivo.

2.2.3 Colaboraciones con otros proyectos, consorcios o grupos

A lo largo del desarrollo de DICYME se han impulsado diversas acciones de colaboración con otros grupos de investigación y entidades, con el objetivo de enriquecer los resultados, fortalecer sinergias y facilitar la transferencia de conocimiento entre equipos especializados en ciberseguridad:

- *Grupo de Ingeniería de Medios de la Universidad de Extremadura*: la colaboración se consolidó a través de la estancia de investigación de uno de los investigadores principales de la URJC en este grupo, lo que permitió un intercambio directo de metodologías, resultados y enfoques en torno al modelado de riesgos en entornos industriales. El *Grupo de Ingeniería de Medios* de la UEx cuenta con una amplia trayectoria en proyectos de ciberseguridad y participa en una Cátedra de Ciberseguridad en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE), lo que facilita un marco idóneo para el trabajo conjunto y la aplicación práctica de resultados, como el citado *webinar Ciberseguridad para un Futuro Conectado*.
- *Computer Security Lab de la Universidad Carlos III de Madrid*: la colaboración surge en el marco académico de la codirección de una tesis doctoral, en la que participan un investigador de la UC3M y una investigadora de la URJC vinculada al proyecto DICYME. El *Computer Security Lab* es un referente en la investigación del cibercrimen, analizando desde técnicas forenses y de detección de amenazas hasta la caracterización de atacantes y sus motivaciones. La interacción con este grupo ha aportado nuevas perspectivas en torno a la dimensión del comportamiento criminal en ciberseguridad, complementando las líneas de trabajo de actores de amenazas y Atractivo de DICYME y contribuyendo a la generación de resultados con mayor alcance interdisciplinar.

2.2.4 Participación en congresos y ferias

Además de la participación en las JNIC 2025, dentro de las labores de difusión los miembros han participado en eventos de referencia, como RootedCON, en sus ediciones de 2024 y 2025, TechFest 2024 y AWS Summit 2025, en las que los investigadores han podido compartir con otros profesionales del sector los avances el proyecto y aprender nuevas tendencias y avances tecnológicos disponibles que posteriormente han aplicado al desarrollo de DICYME.

2.3 Monitorización de impacto

Con el fin de evaluar el alcance de las actividades de comunicación y difusión desarrolladas en el marco de DICYME, empleando las propuestas del entregable E5.1, se han definido y recopilado una serie de indicadores que permiten medir tanto la presencia del proyecto en canales públicos como su impacto en la comunidad científica, profesional y social. Los resultados se presentan en dos tablas diferenciadas: la Tabla 1. Indicadores de impacto de las actividades de comunicación recoge las métricas relacionadas con comunicación (visibilidad en web, blog, redes sociales y charlas), mientras que la

Tabla 2. Indicadores de impacto de las actividades de difusión resume los indicadores de difusión (publicaciones científicas, colaboraciones, participación en congresos y entregables públicos). Cabe señalar que no se incluyen métricas de visitas al blog del DSLAB, ya que actualmente no se dispone de los recursos técnicos y administrativos necesarios para implementar mecanismos de análisis de tráfico que, además de ser fiables, garanticen una correcta gestión de la privacidad de los usuarios.

Tabla 1. Indicadores de impacto de las actividades de comunicación

Indicador	Resultado
Visitas web proyecto	700
Visitas blog proyecto	500
Posts blog del proyecto	15 publicaciones
Posts blog del DSLAB	4 publicaciones
Publicaciones en X (DSLAB)	6 publicaciones
Visualizaciones en X	537
	291
	108
	1033
	612
	61
Charlas impartidas	2

Impacto de las charlas	1 charla grabada con 99 asistentes en directo

Tabla 2. Indicadores de impacto de las actividades de difusión

Indicador	Resultado
Publicaciones científicas	4
Citas de publicaciones científicas	1 artículo con 1 cita
Participación en congresos y ferias	4 congresos
Impacto de los congresos y ferias	*RootedCON* 2024: 6.000 asistentes
	RootedCON 2025: 8.000 asistentes
	AWS Summit 2025: 10.000 asistentes
Entregables públicos	10 entregables disponibles
Colaboraciones	2 grupos de investigación universitarios

3 ESTRATEGIAS DE EXPLOTACIÓN

DeNexus ha incorporado parte de los conceptos desarrollados en DICYME en su plataforma DeRISK. En particular, indicadores a partir de información inside-out (IDS), indicador de actores de amenazas y el mapeo de CVEs a técnica MITREse han adaptado a DeRISK. En otras palabras, las ideas originales DICYME han sido la base de alguno de los indicadores que actualmente usa DeRISK.

Debido a los tiempos de desarrollo que tiene DeNexus, a la fecha de redacción de este informe no se terminado la integración de VISCA. DeNexus está definiendo su propia infraestructura de aplicaciones Gen-AI donde tendrá cabida VISCA. Por otro lado, las ideas discutidas para la co-exposición de compañías a los mismos ataques cibernéticos han sido utilizada para desarrollar un prototipo, que será la base del algoritmo de acumulación de riesgo de DeRISK.

Cabe mencionar que la propia aplicación web DICYME sirve como ambiente de prueba para entender como se pueden visualizar los datos e indicadores propuestos.

En consecuencia, la explotación de resultados de parte de DeNexus es a través de la mejora cualitativa de los datos que alimentan su sistema DeRISK.

3.1 Actividades de explotación y oportunidades comerciales

3.1.1 Aplicación web DICYME

La propia herramienta DICYME, accesible públicamente en Internet, supone una actividad de difusión al mostrar los resultados del proyecto de manera interactiva y contener secciones con explicaciones detalladas de los procesos y modelos desarrollados. Este elemento constituye un puente entre la difusión académica y la explotación comercial, pues combina el objetivo de explicar los resultados con la preparación para su adopción práctica e integración en DeRISK y clientes con escenarios más completos y complejos.

3.2 Monitorización de impacto

Indicador	Resultado
Número de versiones de la aplicación web	12 versiones con prototipos y cambios incrementales
Usuarios de la aplicación web	Se empieza a monitorizar una vez finalizado el proyecto el 30 de septiembre y se realiza la publicación oficial de la aplicación web.
Usuario indirectos vía DeRISK	No se puede determinar el número exacto. Se afirma que todos los usuarios activos de DeRISK se benefician directamente de la mejor calidad de la salida del producto ya que reciben mejores inputs.

4 CONCLUSIONES

El proyecto ha alcanzado los objetivos propuestos, logrando avances significativos en el modelado dinámico del ciber riesgo en entornos industriales. Los equipos involucrados han trabajado de manera coordinada, enriqueciendo las misiones y perspectivas de cada uno, lo que ha permitido generar sinergias valiosas entre investigación, desarrollo y aplicación práctica.

Durante el desarrollo se han afrontado numerosos desafíos, tanto tecnológicos como relacionados con la alineación de planes y el ritmo de trabajo entre las instituciones participantes. Superar estas dificultades ha fortalecido la colaboración y ha permitido establecer procesos más eficientes y adaptativos.

Este contexto colaborativo ha sido especialmente beneficioso para la formación de profesionales en ciberseguridad, aportando conocimientos especializados y experiencia real en un ámbito crítico para la industria. Además, el proyecto ha contribuido a mejorar la calidad de los datos utilizados por la empresa en su producto, afinando procesos y garantizando mayor fiabilidad en la toma de decisiones.

En definitiva, DICYME ha demostrado ser un espacio de innovación y aprendizaje que refuerza la importancia de la cooperación entre instituciones académicas y empresas para afrontar los retos presentes y futuros de la ciberseguridad.

ANEXO A: Póster *JNIC 2025*

Defining the Basal Attractiveness Concept for Cybercriminals

Javier García-Ochoa[1], Alberto Fernández-Isabel[1], Isaac Martín de Diego[1],
Clara Contreras[1], Romy R. Ravines[2], Ovidio López[2]

[1]Data Science Lab, Rey Juan Carlos University, Spain, www.datasciencelab.es, javier.garciaochoa@urjc.es, [2]DeNexus Inc., United States, www.denexus.io

Abstract

Companies face increasing cyber incidents with significant risks. This paper proposes *Basal Attractiveness*, which measures how appealing is a target for threat actors based on inherent and stable attributes (firmographics). The approach consists of 3 stages:

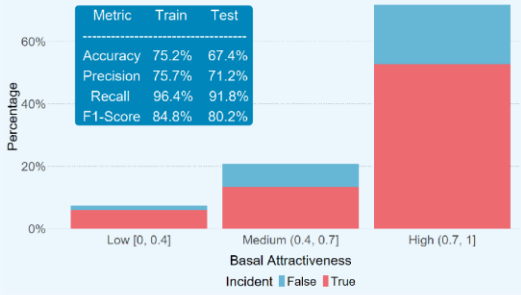
1. Rule Mining to identify patterns in historical cyber incident victims.
2. Rules attributes (e.g., support, confidence, lift) to generate features for classification.
3. Decision Tree classifier to predict the likelihood of an incident based on these features.

Test on a dataset with firmographic variables (country, sector, revenue, earnings, publicly traded, employees, profitable), experiments show promising results. This approach aids in assessing a company's exposure to non-targeted cyber risk.

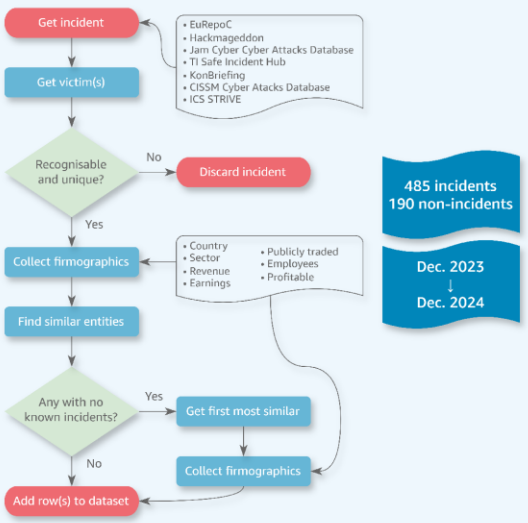
Methodology & experiments

1. **Rule Mining (FP-Growth):** Train **only on 80% incident data**. Generates association rules.
   - 8,214 rules generated (min confidence & support = 0.01)
2. **Feature generation:** Apply rules to all data, getting amount of rules met, total support, total confidence, total lift.
3. **Classification (Decision Tree):** Train on Rule Mining features (80 % incidents & 80% non-incidents). Predicts incident probability $[0, 1]$ = *Basal Attractiveness* score.
   - Tuned via grid search: `max depth = 5, min samples = 10`.

Metric	Train	Test
Accuracy	75.2%	67.4%
Precision	75.7%	71.2%
Recall	96.4%	91.8%
F1-Score	84.8%	80.2%



Dataset



Upcoming developments

- **Data quality & representativeness:** Minimize missing/unknown data and address imbalance (more incidents than non-incidents).
  - Currently developing a LLM-based system designed for scalable data gathering and intelligent imputation of missing or uncertain values.
- **Feature expansion:** Include dynamic variables (real-time threat intelligence, social media visibility, dark web mentions, public security posture).
- **Model comparison:** Benchmark against a diverse set of Machine Learning models (e.g., ensembles, Random Forest, Gradient Boosting) to assess robustness, validate predictive consistency, and uncover potential areas for improvement.

Conclusions

- Present a novel concept, *Basal Attractiveness*, which uses stable firmographic attributes to measure threat actors' victim willingness.
- Approach successfully integrates Rule Mining for feature extraction from disclosed incidents and a Decision Tree for classification.
- Experiments show **promising results**, linking higher Basal Attractiveness scores to increased incident likelihood.
- This method helps companies **prioritize cybersecurity resources** and improve both risk quantification and long-term management.
- Future work will focus on **improving data**, incorporating **dynamic threat features**, and **comparing Machine Learning models**.

References

[1] Shinichi Kamiya, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3):719–749, 2021.

[2] Malik Shahzad K Awan and Laila Dahabiyeh. Corporate attractiveness index: A measure for assessing the potential of a cyber attack. In *2018 9th International Conference on Information and Communication Systems (ICICS)*, pages 1–6. IEEE, 2018.

[3] Muriel F Franco, Erion Sula, Alberto Huertas, Eder J Scheid, Lisandro Z Granville, and Burkhard Stiller. Secriskai: A machine learning-based approach for cybersecurity risk prediction in businesses. In *2022 IEEE 24th Conference on Business Informatics (CBI)*, volume 1, pages 1–10. IEEE, 2022.

[4] Wentian Cai and Huijun Yao. Research on information security risk assessment method based on fuzzy rule set. *Wireless Communications and Mobile Computing*, 2021(1):9663520, 2021.

ANEXO B: Artículo ComSIS

ComSIS Computer Science and Information Systems

Defining the Attractiveness Concept for Cyber Incidents Forecasting

Javier García-Ochoa[1], Alberto Fernández-Isabel[1], Clara Contreras[1], Rubén R. Fernández[1], Isaac Martín de Diego[1] and Marta Beltrán[1]

1. Rey Juan Carlos University Department of Computing, ETSII
C/ Tulipán, s/n, 28933, Móstoles, Madrid (Spain)
{javier.garciaochoa, alberto.fernandez.isabel, clara.contreras, ruben.rodriguez, isaac.martin, marta.beltran}@urjc.es

Abstract

Cyber incident forecasting has several applications within the security field, such as attack projection, intention recognition, attack prediction, or situational awareness. One of the main challenges of these issues lies in analysing the proneness of an entity to be attacked by an adversary evaluating the relevance of different target features or behaviours. This paper presents a methodology that defines the Attractiveness concept to address this issue. Attractiveness is the possession of features or the exhibition of behaviours in entities that raise interest for potential adversaries. Thus, the more significant the Attractiveness value is, the greater the proneness of attacking could be considered. The concept is decomposed into three main branches: basal attractiveness (relevance of the entity in the world), online reputation (the opinion of the individuals and the reach of the entity), and potential victimisation (the interest that the entity arouses for potential attackers). Machine Learning (ML) methods in combination with Information Retrieval (IR) and text mining techniques have been proposed to gather relevant information and identify hidden patterns and relations in past security incidents. With this approach, potential targets could reduce their Attractiveness, focusing on those aspects that can be remedied. Alternatively, future risky situations could be predicted to better prepare for proactive protection, detection, and response. The proposal has been validated through several experiments.

Key words

Attractiveness, Cyber incidents, Victimisation, Online reputation, Forecasting