JNIC - Programa de Transferencia

Ficha de reto científico

Edición 2017

1 FICHA DE RETO

El mero hecho de proponer un reto a través del presente formulario implica la aceptación de las bases del Programa de Transferencia JNIC.

El formulario o Ficha Reto para documentar la propuesta de reto contiene los siguientes campos.

FICHA DE RETO JNIC

A. INFORMACIÓN SOBRE LA EDICIÓN DEL PROGRAMA EN LA QUE SE PRESENTA EL RETO

A.1 Edición Programa Transferencia JNIC: **2017**

B. INFORMACIÓN SOBRE EL RETADOR

B.1 Nombre de la Organización: ElevenPaths. Telefónica Cyber Security Unit.

B.2 Portal web: (de la organización o aquel en el que haya información sobre el reto propuesto)
www.elevenpaths.com

B.3 Persona de contacto: Nombre, cargo, email, teléfono contacto.
Marcos Arjona, Consultor de Investigación e Innovación, marcos.arjona@11paths.com, 666985706.

B.4 Información de soporte (buzón de email / teléfono u otros) para dar respuesta a las dudas que los investigadores puedan plantear sobre el reto:
marcos.arjona@11paths.com

C. CARACTERÍSTICAS RELATIVAS AL RETO

C.1 Tipo de reto (abierto / restringido): Restringido

C.2 Se facilitará información confidencial que requiera un acuerdo previo formal (SI/NO): SI

C.3 Tipo de incentivo:

Nota: Es objetivo del Programa la publicación de los resultados obtenidos fruto de la investigación realizada para la solución del reto.

- ☐ Sin incentivos
- ☐ Premio en metálico mejor/es propuesta/s
- ☐ Financiación de la investigación para generación de prototipo o una PoC
- ☒ Reconocimiento para la mejor/es propuesta/s
- ☒ Utilización de instalaciones/equipos del retador durante la investigación
- ☒ Otros

Comentarios sobre los incentivos seleccionados:
ElevenPaths realizará un esfuerzo de difusión en sus medios de comunicación, así como en eventos y jornadas de índole científica donde se podrán presentar conjuntamente con el equipo de investigación, los avances actuales y el progreso de la solución al reto. Además, ElevenPaths apoyará en todo momento la hoja de ruta, facilitando el uso de las instalaciones, sistemas y datos necesarios para cumplir con los objetivos de la solución.

El vínculo entre la entidad investigadora junto a ElevenPaths podrá generar un proceso colaborativo propicio para ambas instituciones, mejorando el clima de cooperación y facilitando investigaciones y desarrollos relacionados con el reto en curso.
Los equipos investigadores que trasladen el conocimiento y producción de los retos a iniciativas empresariales propias o spin-offs podrán optar de manera privilegiada al programa de emprendimiento y aceleración de Wayra, una iniciativa de Telefónica a través de Open Future que se facilitará a las empresas siempre que cumplan con las características de admisión necesarias.
Pese a no tener un fondo de financiación definido, ElevenPaths realizará un seguimiento proactivo de la solución al reto, agilizando e incentivando su desarrollo, fomentando nuevas colaboraciones en el ámbito de la solución. Finalmente, según el progreso del reto podrían establecerse contratos privados de investigación sobre el reto para la creación del PoC o su continuidad.

C.4 (si procede) Cuantía económica para el premio a la mejor propuesta
Haga clic aquí para escribir texto.

C.5 (si procede) Cuantía económica para la financiación (1 año de trabajo investigador).
Haga clic aquí para escribir texto.

C.6 Se solicita revisión previa de cualquier publicación científica generada en la resolución del reto (SI/NO):
SI

C.7 Servicios que se ponen a disposición (utilización de hardware/software, posibilidad de estancias en las instalaciones del retador para conocer el reto, etc.):
- Acceso a las plataformas pertinentes.
- Asistencia y tutorial de uso de las plataformas.

C.8 Requisitos de confidencialidad (tanto para los investigadores, como para los miembros del Comité que evalúen la propuesta):
Acuerdo de Confidencialidad sobre la documentación y software utilizado por los investigadores durante la ejecución del reto.

C.9 Condiciones de aceptación (limitaciones para la aceptación de solicitudes):
- Posesión de experiencia en el ámbito del reto bien sea a través de publicaciones en conferencias o revistas.
- Se valorará muy positivamente cualquier solución que proponga un enfoque de amplio espectro y que automatice el proceso de evaluación del impacto en el negocio.
- Se valorará positivamente desarrollos previos y PoC realizados por el mismo equipo científico en áreas científicas similares o cuyo conocimiento pueda proporcionar valor añadido a la solución.

C.10 Condiciones de rechazo (cuestiones que quieran evitarse en las solicitudes):
- Equipo de investigación no consolidado o sin trayectoria científica demostrable.
- La solución debe ser capaz de definir modelos aplicables a distintos tipos de empresas y entornos corporativos heterogéneos.

D. RETO PROPUESTO

D.1 Título del reto:
Técnicas de análisis del alcance e impacto de los incidentes de ciberseguridad en las empresas

D.2 Antecedentes:
Las amenazas de seguridad se han convertido en un desafío constante para las empresas que deben realizar esfuerzos constantes en la supervisión del conjunto de vulnerabilidades que contienen sus sistemas, a la par que protegen sus activos, incrementan la consciencia

de los empleados en materia de seguridad e introducen herramientas preventivas y reactivas en sus sistemas.

La experiencia dictamina de manera acertada que tarde o temprano toda empresa será objeto de un ciberataque y en ese momento toda la inversión en el entrenamiento y en la protección de los equipos adquiere el sentido más justificado. Por tanto, resulta viable poder trasladar cuantitativamente a las empresas las consecuencias de sus carencias en cuanto a sus medidas de ciberseguridad e incluso disponer de herramientas de diagnóstico personalizadas que a posteriori sean capaces de realizar una valoración global del impacto producido en el negocio. Todo ello en un lenguaje claro y conciso y que pueda cuantificar económicamente el impacto.

D.3 Motivación:

Tanto analistas de seguridad, auditores como consultores respaldan sus informes de ciberseguridad especificando el potencial impacto en el negocio de las carencias existentes en la empresa, realizando un estudio formado por cientos de parámetros y fundamentando sus conclusiones en factores procedentes de la empresa que está siendo evaluada. Entre las cualidades más susceptibles de tener en consideración podemos encontrar la infraestructura de red, la formación de los trabajadores, los recursos económicos y humanos destinados a la supervisión de los activos, políticas de seguridad, mecanismos de autenticación, el tipo de supervisión realizada por el equipo de IT, etc.

Fruto de esta magnitud tan elevada de variables y características que configuran las empresas, es necesario encontrar modelos de estimación y de análisis que permitan pronosticar y evaluar el impacto que puede provocar en la empresa un ciberataque, atendiendo a dicho compendio de cuestiones. Estos modelos totales o parciales podrán ser trasladados a las empresas en las etapas tempranas previas a un plan director de seguridad. También es posible adjuntarlas en las auditorías de seguridad destinadas a evaluar el cumplimiento normativo. Pero sobretodo, como medida representativa del impacto que ha provocado en la empresa algún suceso de ciberseguridad o ciberataque determinado.

Lo ideal por tanto sería por tanto realizar una evaluación del impacto utilizando modelos **precisos, realistas, entrenados y adaptados a las características de la empresa.**

D.4 Descripción del reto:

Este reto trata de abordar la problemática real existente en el sector corporativo a la hora de cuantificar los daños y efectos que podría provocar o ha provocado un incidente de ciberseguridad. Este análisis del impacto debe combinar un estudio que permita parametrizar una serie de variables correspondientes a la configuración empresarial, con unos modelos matemáticos que permitan realizar una valoración comprensible por los clientes. Todo esto enmarcado en un proceso lo más automatizado posible.

Dependiendo de la experiencia de los equipos investigadores, el enfoque adquirirá un enfoque diferenciado, pero todos ellos deben centrarse en identificar las características a considerar y desarrollar modelos, procedimientos o metodologías aplicables para realizar el pronóstico o la evaluación.

La solución debe integrar una componente de aprendizaje que permita reforzar su capacidad predictiva y analítica, retroalimentando sus técnicas de cálculo conforme a casos reales donde ésta haya sido aplicada previamente y se hayan podido obtener datos reales y concluyentes del impacto.

Del amplio conjunto de tecnologías aplicables a la solución, la propuesta debe demostrar la viabilidad, capacidad de evolución y una estimación del impacto con una desviación aceptable. Entre los elementos esperados de las propuestas podríamos esperar:

- Modelos matemáticos y estadísticos para el cálculo del impacto
- Capacidad de aprendizaje a partir de medidas de impacto de casos reales.
- Valoración del riesgo de ciberseguridad existente en la empresa
- Capacidad de configurar los cálculos de acuerdo a múltiples parámetros como el tipo de empresa, su diseño y su tipo de negocio.

- Modelos predictivos de la evolución de ataques en la empresa.
- Correlación entre el potencial impacto y tendencias externas de amenazas de ciberseguridad.
- Cuantificación del impacto en el negocio empresarial
- Clasificación de tipo de amenazas y ataques y el tipo de alcance e impacto que podrían provocar.
- Pronósticos de recuperación y grado de contención y respuesta logrado.
- Proceso o metodología automatizada para el análisis del impacto.
- Otros.

El presente reto no debe entenderse como una verificación del cumplimiento normativo o de estándares industriales, pero sí tendrá que utilizar ciertas estipulaciones normativas para poder extrapolar aquellas características útiles y sensibles de ser computadas en los modelos matemáticos de la propuesta. Con un enfoque claramente automatizado, los resultados obtenidos de los modelos matemáticos y el entrenamiento tendrán que arrojar unas cifras acordes a la realidad y que permitan fundamentar cualquier enfoque comercial relativo a clientes y empresas.
El hecho de poder proporcionar una valoración del daño a posteriori no debería requerir ningún análisis en profundidad de tipo forense, pese a la posible pérdida de precisión, los modelos matemáticos deben ser aproximados y no requerir un estudio tan profundo de los daños.

D.5 Recursos de apoyo que se pondrán a disposición de los investigadores (data-sets, etc.):
Según la solución, alcance y tipo de enfoque se proporcionará al equipo de investigación acceso a la información, conjuntos de datos y APIs necesarias para la resolución del reto. Esta cesión documental puede estar sujeta a un acuerdo de confidencialidad debido a su naturaleza privada y corporativa.
ElevenPaths trata de ligar ciertos aspectos cuantitativos del presente reto a algunas de sus soluciones de ciberseguridad. De esta forma el presente reto podrá verse favorecido del estrecho trato con clientes de ElevenPaths y Telefónica Digital España de cara a la obtención de cifras y casos de uso reales.

D.6 Avances realizados actualmente por el retador:
ElevenPaths realiza numerosas consultorías de ciberseguridad técnica y también normativa, de hecho, herramientas como SandaS GRC ayudan a las empresas en la automatización del cumplimiento legislativo y regulatorio. ElevenPaths desea mejorar sus procesos automáticos de evaluación gracias al presente reto, y que los modelos matemáticos o estadísticos refuercen de manera precisa, fundamentada y adaptada al cliente el proceso de valoración.

D.7 Alcance:
Este reto sustenta su éxito en un minucioso estudio durante la fase inicial que defina claramente el proceso y arquitectura necesarias para ejecutar la solución. Pero este ciclo de investigación tendrá que ser constante a lo largo de las futuras fases de desarrollo, requiriendo un constante avance en el plano científico. Debido principalmente a que existen características como la posible incorporación de nuevas variables a los modelos o la mejora de las técnicas de aprendizaje a lo largo del tiempo.
Por tanto, el alcance podremos establecerlo de acuerdo a una serie de posibles objetivos acordados previamente. Entre el conjunto más deseable podríamos destacar.

- Generación de modelos matemáticos y estadísticos con una sólida justificación científica.
- Categorización, identificación y evaluación de cuáles son las variables cuyas métricas pueden arrojar mayor información valiosa al análisis preventivo.

- Diseño de mecanismos de aprendizaje y entrenamiento de mejora y optimización de los modelos.
- Mecanismos de captura e identificación de daños para la valoración del impacto de acuerdo a criterios económicos.
- Correlación entre tipos de amenazas/vulnerabilidades y el tipo de impacto que podría provocar en la infraestructura de las empresas.
- Proceso automatizado del análisis del impacto.

D.8 Casos de uso:

CU1:

Precondición: ElevenPaths desea ampliar cobertura a uno de sus clientes que utiliza un conjunto de herramientas de ciberseguridad, pero ésta carece de un conjunto de utilidades preventivas y reactivas que mejorarían sustancialmente las capacidades de protección relativas a su infraestructura de red. Para ello, al margen de enumerar las características técnicas de los nuevos servicios y módulos, sería deseable poder presentar un informe cuantitativo y fundamentado, además de personalizado a la configuración del cliente sobre el impacto que causaría en sus activos la carencia de estos nuevos servicios propuestos.

Descripción: Gracias al análisis de impacto en el negocio del cliente abordado por este reto se utilizaría un vector de características extraído de la configuración de la empresa para generar la valoración del impacto. La oferta comercial podrá incorporar este análisis para que el cliente pueda opinar, conforme a un criterio del alcance de pérdidas económicas, del interés en contratar o no los nuevos servicios.

Secuencia:

1) ElevenPaths tiene información detallada de la empresa o podría solicitar a la misma una serie de datos de interés para el estudio.
2) Utilizando los modelos matemáticos y los procesos de análisis, ElevenPaths incorpora estas variables para realizar el estudio del estado actual del cliente
3) ElevenPaths presenta junto a su propuesta comercial el informe realizado a la empresas del cliente cuya base científica y formulación matemática respaldará el potencial peligro para el cliente.
4) El cliente podrá verificar los datos integrados en el informe y las conclusiones, pudiendo verificar el alcance, expansión del impacto, la valoración del riesgo presente y las cifras de pérdidas económicas en caso de producirse algún incidente de ciberseguridad

Postcondición: Gracias a la precisión de los modelos matemáticos de este proceso y a que incorpora las características del cliente, este análisis contendrá una escasa desviación respecto a la realidad, permitiendo al cliente tomar una decisión, con pleno conocimiento y de forma fundamentada, de los riesgos que conllevaría no contratar los nuevos servicios que ElevenPaths le sugiere.

CU2:

Precondición: Una central eléctrica ha recibido un ataque de ransomware y esto ha provocado un perjuicio a los servicios internos además de exponer a la opinión pública la fragilidad de sus sistemas debido a un protocolo de respuesta lento y erróneo. Algunas de las medidas reactivas no fueron tomadas a tiempo y además de cara a la opinión pública se trató de ocultar cualquier indicio del ataque para mitigar en lo posible el impacto en los medios. Finalmente, los fallos en los servicios al cliente provocó el descubrimiento del incidente y las decisiones ejecutadas durante el suceso.

Descripción: Las centrales eléctricas son un tipo de infraestructura crítica, por tanto no solo se ha visto comprometido el servicio a los clientes sino la propia actividad habitual de la población ha puesto en entredicho la empresa y su gestión. Es por esto que para resumir el análisis de los daños ocasionados y cómo se ha repelido, se necesita una valoración global de cuántas pérdidas económicas y de recursos ha provocado el incidente. Algo que permitirá ofrecer una cuantificación realista del daño de cara a la opinión pública y al equipo directivo.

Secuencia:

1) La empresa eléctrica solicita a ElevenPaths el análisis del impacto en su negocio que ha provocado el incidente de seguridad.
2) ElevenPaths dispone del expertise y conocimiento del tipo de incidente, a nivel técnico y con pleno conocimiento de sus características en cuanto al daño, forma de actual y consecuencias
3) ElevenPaths integra en los modelos matemáticos el compendio de características de la central eléctrica además de los detalles técnicos necesarios para caracterizar el ataque. De acuerdo a características como la cantidad de gente afectada, tiempo de respuesta y número de equipos afectados.
4) El informe cuantifica los daños en 10M€ respecto a daños provocados y unos 2M€ respecto a los recursos humanos invertidos en recuperar la normalidad y los ficheros dañados durante el ataque.

Postcondición: La empresa eléctrica recibe la valoración del impacto económico en su negocio que ha sido generado de acuerdo a sus características y tipología, tanto a nivel interno como a nivel gubernamental, ante quién tendrán que responder, estando ahora en posesión de datos fiables y fundamentados. La propia empresa decidirá si el impacto de 12M€ de euros debe suponer la revisión de sus protocolos de ciberseguridad.

D.9 Soluciones actuales que dan cobertura parcial al reto:

Normalmente estas soluciones se integran en la hoja de servicio de consultoras que realizan un estudio con mayor o menor capacidad automática. Algunos ejemplos son:
https://www.escgs.com/services/cyber-security/services/business-impact-analysis
https://www2.deloitte.com
https://www.pwc.com/us/en/cybersecurity.html
https://www.ibm.com/es-es/marketplace/business-impact-analysis

D.10 Estudios/Investigaciones relacionados:

A. Santos Olmo Parra, L. E. Sanchez Crespo, E. Alvarez, M. Huerta and E. Fernandez Medina Paton, "Methodology for Dynamic Analysis and Risk Management on ISO27001," in IEEE Latin America Transactions, vol. 14, no. 6, pp. 2897-2911, June 2016.
doi: 10.1109/TLA.2016.7555273 (PDF)
The cost of incidents affecting CIIs (Link)
H. Yadav and S. Gour. “Cyber Attacks: An impact on Economy to an organization” International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 9 (2014), pp. 937-940 (PDF)
The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment (2013) by Afcea Cyber Committee (PDF)

D.11 Documentación/Bibliografía de interés:

T. Okubo, H. Kaiya and N. Yoshioka, "Effective Security Impact Analysis with Patterns for Software Enhancement," 2011 Sixth International Conference on Availability, Reliability and Security, Vienna, 2011, pp. 527-534.
doi: 10.1109/ARES.2011.79
S. Tjoa, S. Jakoubi and G. Quirchmayr, "Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology," 2008 Third International Conference on Availability, Reliability and Security, Barcelona, 2008, pp. 179-186.
doi: 10.1109/ARES.2008.206
The Total Economic Impact Of EnCase® Cybersecurity For Incident Response (Link)

D.12 Otras consideraciones a tener en cuenta:

Los equipos de investigación que aborden estas soluciones no deben limitar su enfoque científico ni acotar su ambición tecnológica a los términos expresados en este reto si esto supone un perjuicio de cara a la ambición o a las expectativas alcanzables por los investigadores. Se valorará positivamente la incorporación de factores de valor diferenciales que permitan trazar una hoja de ruta mucho más ambiciosa e innovadora.

E. SEGUIMIENTO

E.1 Hitos esperados (puntos de seguimiento de la investigación):

La lista de milestones serán factores que se acordarán adecuadamente con los equipos de investigación implicados, de esta manera se podrán adaptar las expectativas a criterios reales tales como la experiencia de los investigadores y el tipo de solución propuesta. Sin embargo, varios hitos serían deseables para el control de la investigación:

1) Compendio de variables y características para plasmar la configuración de la empresa objetivo
2) Modelos matemáticos y estadísticos para la ejecución del análisis.
3) Motor de entrenamiento conforme a datos reales.
4) PoC del automatismo para realizar el análisis de impacto

E.2 **TRL** objetivo para el primer año (Nivel de madurez que se espera que tengan las propuestas de solución recibidas): TRL2

F. EVOLUCIÓN DEL RETO

F.1 **TRL** objetivo para el final de la investigación (Nivel de madurez final que desea el retador para dar por finalizado el reto de forma exitosa):

TRL5

F.2 **Plazo** del reto (fecha límite para alcanzar el TRL final de investigación):

18 meses

http://2017.jnic.es/