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: INCIBE

B.2 Portal web: (de la organización o aquel en el que haya información sobre el reto propuesto)
Haga clic aquí para escribir texto.

B.3 Persona de contacto: Nombre, cargo, email, teléfono contacto.
Enrique Redondo Martínez

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:
apoyo.investigacion@incibe.es indicando "`[Reto SCI]`" en el título del correo

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:
Otros incentivos ofrecidos:
La propuesta de solución ganadora, recibirá una invitación para presentar y exponer su propuesta en la siguiente edición del evento ENISE (organizado por INCIBE), dentro del espacio dedicado a emprendimiento. Igualmente, si la solución obtiene una puntuación superior a 25 puntos (de los 60 posibles) y con no menos de 3 puntos en cada criterio de valoración, obtendrá una plaza como finalista en la próxima edición del certamen de

emprendimiento incubadora Ciberemprende (promovido por INCIBE). En dicho certamen se ofrecen servicios de formación y mentoring para ayudar, de forma práctica, en la constitución y lanzamiento de spin-offs en ciberseguridad.

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.):
Determinados dispositivos del Laboratorio SCI de INCIBE

C.8 Requisitos de confidencialidad (tanto para los investigadores, como para los miembros del Comité que evalúen la propuesta):
Acuerdo de Confidencialidad

C.9 Condiciones de aceptación (limitaciones para la aceptación de solicitudes):
Haga clic aquí para escribir texto.

C.10 Condiciones de rechazo (cuestiones que quieran evitarse en las solicitudes):
Haga clic aquí para escribir texto.

D. RETO PROPUESTO

D.1 Título del reto:
Conjunto de datos para experimentación en ciberseguridad SCI

D.2 Antecedentes:
A día de hoy no existen conjuntos de datos actualizados y representativos en Sistemas de Control industrial para la investigación en aplicación de técnicas IDA (Intelligent Data Analysis) orientadas a la detección de anomalías en redes de datos.
La mayor parte de los estudios (además estudios importantes) están basados en el conjunto de datos KDD99 y NSL-KDD (ligera evolución) que publicó DARPA en el año 1999 y que, aparte de estar muy desactualizados y haber recibido múltiples críticas por parte de la comunidad científica, no son de carácter industrial, si no que corresponden a redes TIC.

D.3 Motivación:
Poder disponer de un conjunto de datos necesario para la investigación en la aplicación de técnicas IDA para la detección de anomalías o novedades que puedan indicar presencia de un ataque determinado en una Red de Control Industrial. Esto permitiría generar una futura herramienta “detector pasivo de amenazas” basado en técnicas IDA que permitiera detectar gran parte de los ataques que se llevan a cabo, incluso aquellos que fueran no conocidos.

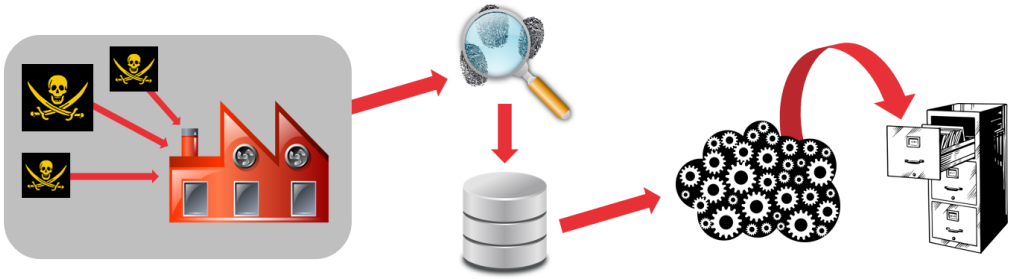
D.4 Descripción del reto:
Una tentativa de etapas para llevar a cabo este proyecto sería la siguiente:

1. Definición de una arquitectura válida para la obtención del conjunto de datos. Se debe tener en cuenta que en este etapa se debe construir tanto una arquitectura industrial representativa de la realidad, como una arquitectura robusta de adquisición y almacenamiento de datos (número y tipo de sondas (tap?, port mirroring?, datos router?), colocación de las mismas, tipo de base de datos (SQL?,

Mongo?, Hadoop?, Cassandra?), etc). Para esta etapa se podría utilizar el Laboratorio Industrial de INCIBE si fuera necesario por parte de los investigadores.

2. Definición de un set de ataques a llevar cabo sobre los elementos de la arquitectura. Estos ataques deben ser lo más representativos posibles de la realidad, y se deben seleccionar varios y desde diferentes ubicaciones del atacante.
3. Selección de los datos que se van a adquirir y almacenar, y de sus características. Existen múltiples opciones: Por ejemplo, datos derivados de los niveles de transporte y de red (al igual que en los conjuntos KDD), datos derivados del nivel de aplicación (protocolo industrial) o datos únicamente de proceso. También habría que llevar a cabo una selección de las características de los datos representativas y útiles para la detección de las anomalías.
4. Proceso de adquisición de los datos. El conjunto tendría que tener representación de datos normales del proceso y de datos que correspondan a ataques (anomalías).
5. Proceso de etiquetado de los datos.
6. Pre-procesado y limpieza de los datos para eliminación de muestras erróneas y presentación de los datos de la forma más limpia y ordenada posible y en un formato adecuado (por ej. csv.)

1. **ARQUITECTURA:** Diseño arquitectura industrial realista (definición de nº y tipo de sondas, etc.) que permita la obtención del conjunto de datos y su almacenamiento.
2. **ATAQUES:** Definición de ataques representativos, que varíen en cuanto a origen, tipo de ataque, impacto, etc.
3. **DATOS:** Selección de los datos más relevantes a recoger, así como el tipo de datos (de red, transporte, aplicación, proceso, etc.)
4. **ADQUISICIÓN:** Recopilación de datos con ataques y también normales (sin ataques).
5. **ETIQUETADO:** Distribución de los datos en categorías/familias/grupos…
6. **PRE-PROCESADO:** Sanitización y normalización de la información recopilada y adecuación de los datos para poder ofrecerse en formatos adecuados para su posterior utilización (por ejemplo, CSV)



D.5 Recursos de apoyo que se pondrán a disposición de los investigadores (data-sets, etc.):
Dispositivos industriales necesarios del Laboratorio Industrial de INCIBE

D.6 Avances realizados actualmente por el retador:
Haga clic aquí para escribir texto.

D.7 Alcance:
Construcción de un conjunto de datos adecuado teniendo en cuenta las características que se exponen a la finalización de la línea de investigación.

D.8 Casos de uso:
Aplicación del Conjunto de Datos para la investigación de técnicas IDA orientadas a la detección de posibles ataques en una red industrial.

D.9 Soluciones actuales que dan cobertura parcial al reto:
Haga clic aquí para escribir texto.

D.10 Estudios/Investigaciones relacionados:
Haga clic aquí para escribir texto.

D.11 Documentación/Bibliografía de interés:
Haga clic aquí para escribir texto.

D.12 Otras consideraciones a tener en cuenta:
Haga clic aquí para escribir texto.

E. SEGUIMIENTO

E.1 Hitos esperados (puntos de seguimiento de la investigación):
Se propone establecer un hito a la finalización de cada una de las fases establecidas en el apartado D.4 y, adicionalmente, un hito final, que supondrá la entrega final de todo el proyecto, con las versiones más recientes de todos sus documentos asociados, código, BBDD, categorías, etc.
A parte, el retador realizará un seguimiento continuo de la evolución del reto con reuniones periódicas a convenir con los investigadores.

E.2 **TRL** objetivo para el primer año (Nivel de madurez que se espera que tengan las propuestas de solución recibidas): TRL4

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):
TRL6

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

http://2017.jnic.es/