Convocatoria Colaboración Público-Privada CPP2021-009025

DICYME:
Dynamic Industrial CYberrisk Modelling based on Evidence

Iniciativa Conjunta de:

ENTREGABLE 1.1:
Primer prototipo de módulo de extracción automática de datos internos

Coordinadoras:

Romy R. Ravines (DeNexus Tech)

Marta Beltrán (Universidad Rey Juan Carlos)

Índice

1. INTRODUCCIÓN Y OBJETIVOS

Este breve documento resume los aspectos más importantes de diseño e implementación del entregable 1.1 del proyecto, es decir, del primer prototipo de módulo de extracción automática de datos internos. Este entregable es fruto del trabajo realizado en las tareas 1.1, 1.3 y 1.4 del proyecto, dentro de la Actividad 1 "Sistema de recogida de evidencias".

En las siguientes secciones se explica:

- Qué tipo de datos se van a utilizar en este primer prototipo y cómo se van a recopilar para que puedan transformarse, posteriormente, en información útil como entrada para el cálculo de probabilidades o impactos.
- Qué flujos continuos de evidencias de ciberriesgo provenientes de diferentes fuentes internas de una instalación industrial (*Endpoint Detection Response* ó EDR, *Intrusion Detection and Prevention System* ó IDPS, *Security Information and Event Management* ó SIEM) se han tenido en cuenta para este primer prototipo.
- Qué tipo de transformaciones de estos datos en información útil para el modelado del ciberriesgo industrial u OT se han propuesto.
- Qué datos y código se encuentran disponibles en este entregable (deriskGroup / DICyME Project · GitLab) y cómo pueden emplearse.

2. EXTRACCIÓN AUTOMÁTICA DE EVIDENCIAS INTERNAS

Para la extracción automática de evidencias internas se ha hecho uso de tres sistemas de detección de intrusiones e incidentes, EDR, IDPS y SIEM.

Un EDR, Endpoint Detection and Response, es un sistema de seguridad informática diseñado para proteger y monitorear dispositivos informáticos en una red. Este tipo de herramientas permiten la detección temprana de amenazas para la ciberseguridad, la recopilación de información detallada sobre el comportamiento de los *endpoints* y facilita la respuesta inmediata ante incidentes de seguridad.

Un IDPS o Sistema de Detección y Prevención de Intrusiones, es una tecnología crítica en la defensa cibernética cuya función principal es identificar actividades sospechosas o maliciosas en una red informática y tomar medidas para detener o mitigar estas amenazas. Los IDPS utilizan reglas predefinidas y análisis de tráfico para detectar intrusiones y ataques, como intentos de acceso no autorizado o explotación de vulnerabilidades. Además, pueden tomar medidas proactivas para prevenir ataques, como bloquear el tráfico malicioso.

Por otra parte, un SIEM, Sistema de Gestión de Información y Eventos de Seguridad, es una plataforma integral que recopila, correlaciona y analiza datos de eventos y registros de seguridad de toda la infraestructura de una organización.

Su objetivo principal es proporcionar una visión unificada y en tiempo real de la postura de seguridad de la red. Los SIEM permiten a las organizaciones identificar patrones de actividad sospechosa, detectar amenazas y responder de manera efectiva a incidentes de seguridad. Además, facilitan el cumplimiento normativo al generar informes detallados y almacenar registros de auditoría.

Los EDR son herramientas que funcionan a nivel de dispositivo. Por ese motivo, conocen con seguridad qué usuario está iniciando sesión en ellos, qué servicios y versiones están ejecutando, el estado de sus recursos, etc. Los IDPS, por su parte, actúan a nivel de red y realizan un inventario de los activos y sus características de manera activa o pasiva, pero sin ejecutarse en los mismos (como es el caso de los EDR). Además, realizan una tarea de monitorización de la red, analizando paquetes y decidiendo mitigaciones en caso de descubrir tráfico malicioso. Los SIEM son herramientas de más alto nivel que hacen agregación y correlación de eventos de las herramientas previas, con información más general y de principio a fin.

Para el primer prototipo, se ha optado por utilizar los IDPS por proporcionar una información de un nivel medio, que se puede utilizar directamente en el módulo de visualización para proporcionar indicadores muy relevantes, pero a la vez sencillos de obtener. Utilizar toda la información de los EDR sin ningún tipo de agregación proporcionaría un nivel de detalle también muy útil, pero requeriría un nivel de análisis de los datos y de presentación que sería utilizado únicamente al tratar de examinar comportamientos muy concretos sobre ciertos activos. Por su parte, utilizar la información de los SIEM sería escalar a un alto nivel cuya información no posibilitaría la implementación de indicadores sencillos que alimenten la toma de decisiones para la gestión del ciberriesgo mediante acciones en los activos. Este tipo de herramientas, generalmente, son más útiles para la detección, monitorización y respuesta a incidentes, aunque también podrían utilizarse para agregar indicadores a sucesivas versiones de este prototipo analizando eventos ocurridos en el pasado en los diferentes activos y redes.

En este caso se ha trabajado con datos acerca de los activos en niveles 1, 2 y 3 (o 0, 1 y 2, si se comienza numerando desde el 0) del modelo Purdue, que separa en 5 niveles las redes de entornos industriales. En concreto, podemos encontrar un listado de infraestructuras o facilities, una enumeración de activos con sus direcciones IP y MAC, fabricante, sistema operativo, su nivel de purdue... así como un catálogo de vulnerabilidades y la asociación entre diversas dichas vulnerabilidades y activos en los que han sido encontradas.

Este primer prototipo se ha diseñado teniendo en cuenta cuatro productos o plataformas de tipo IDPS muy extendidos en entornos industriales, en concreto los de Nozomi, Forescout, Claroty, y Dragos. Todos ellos proporcionan los datos antes mencionados y diferentes APIs que facilitan la integración de nuestro prototipo de manera que se puedan extraer automáticamente y emplear como evidencias internas de ciberriesgo.

3. INDICADORES DEFINIDOS Y SIGNIFICADO

Para que los datos en bruto extraídos tal y como se ha explicado en la sección anterior sean de utilidad para la cuantificación del ciberriesgo, deben transformarse en información útil en forma de métricas e indicadores. Este primer prototipo es capaz de manejar los siguientes:

Nombre del indicador	**Expresión para su cálculo**	**Significado y relación con el ciberriesgo**
Recuento de activos informáticos descubiertos pasivamente por la fuente de datos	Suma de activos salvo aquellos que: contengan direcciones IP que no pertenezcan a la empresa; no tengan una red definida; sus direcciones no se correspondan con dispositivos; cuyas fechas de última aparición sean de más de 90 días; y estén duplicados porque se hayan descubierto por más de un sensor o dispositivo.	Proporciona información sobre: visibilidad de activos en la red; detección de actividad no autorizada; exclusión de activos de Internet; evaluación de la efectividad de la seguridad y definición de zonas de seguridad para comprender cómo se distribuyen los activos en la red.
Recuento de activos informáticos en alcance	Suma de activos informáticos para sistemas de control industrial (ICS/OT) y las redes dentro del alcance que ha definido el cliente. Se excluyen redes corporativas e Internet.	Este indicador permite enfocarnos en activos relevantes y en amenazas específicas, pudiendo hacer un seguimiento de la superficie de ataque para una detección y respuesta rápida con priorización de recursos.
Recuento de activos informáticos que han sido evaluados en busca de vulnerabilidades	Suma de activos informáticos cuyas vulnerabilidades hayan sido descubiertas en ICS/OT para evaluar su riesgo gracias a la identificación del sistema operativo, el proveedor o una tarea que incluya los activos informáticos.	La identificación de vulnerabilidades permite a la organización identificar amenazas potenciales antes de ser explotadas, por lo que ayuda a priorizar en la mitigación y la reducción del ciberriesgo.
Recuento de activos informáticos que sufren vulnerabilidades	Suma de activos informáticos que tienen una o más vulnerabilidades.	Permite identificar riesgos de fugas y brechas de datos para poder fijar nuevas medidas de seguridad con las que poder detectar y responder de manera temprana a estas amenazas.
Recuento de vulnerabilidades abiertas actualmente	Suma de todas aquellas vulnerabilidades abiertas extraída de la última muestra de datos.	La identificación de las vulnerabilidades abiertas permite definir el estado de seguridad de una organización en relación a la posibilidad de explotación de estas vulnerabilidades por los atacantes, pudiendo así detectarse las amenazas en tiempo real para reducir el riesgo y corregir dichas vulnerabilidades.
% de activos informáticos que tienen	Tanto por ciento del cociente entre el recuento de activos informáticos que tienen vulnerabilidad de datos y el recuento de activos informáticos	Muestra la proporción de activos informáticos de la organización que tienen una vulnerabilidad de datos, lo que implica la exposición de información confidencial

vulnerabilidad de datos	descubiertos pasivamente por la fuente de datos.	que, a su vez, se relaciona con una posible pérdida de reputación y compromiso de la organización.
Tiempo medio de las vulnerabilidades abiertas	Media de los días transcurridos de cada una de las vulnerabilidades entre que se publica cada vulnerabilidad en la base de datos nacional de vulnerabilidades (National Vulnerability Database o NVD) hasta que se detecta en la organización.	Con una detección rápida, la organización puede responder de manera óptima a las amenazas que se materialicen y futuras amenazas. Esto supone una gestión de riesgos proactiva para anticipar las amenazas emergentes y reducir la superficie de ataque.
Recuento de vulnerabilidades cerradas en el último año	Suma de las vulnerabilidades que se han cerrado/mitigado en el último año.	Una correcta gestión de las vulnerabilidades por parte de la organización permite conocer su capacidad de reacción y respuesta ante estas amenazas. Con el fin de reducir los riesgos y mantener una mejora activa de la seguridad en la organización, conocer las vulnerabilidades y tener capacidad para resolverlas permite preparar a la organización a amenazas futuras.
% de vulnerabilidades cerradas en el último año	Tanto por ciento del cociente entre el recuento de vulnerabilidades cerradas/mitigadas y el recuento de todas las vulnerabilidades descubiertas en el último año.	El porcentaje de vulnerabilidades cerradas en el último año es un indicador que muestra la proporción de vulnerabilidades identificadas en el transcurso del año anterior que han sido abordadas o mitigadas con éxito por una organización en el ámbito del ciberriesgo. Este porcentaje refleja la eficacia de la organización en la gestión de vulnerabilidades, la reducción del riesgo cibernético y la capacidad de responder a amenazas, así como su compromiso con la ciberseguridad y, en algunos casos, el cumplimiento normativo.
Tiempo medio empleado en remediar vulnerabilidades en el último año	Media de los días transcurridos de cada una de las vulnerabilidades entre que se publica cada vulnerabilidad en la base de datos nacional de vulnerabilidades (National Vulnerability Database o NVD) hasta que se cierra dicha vulnerabilidad.	Este indicador refleja la eficacia de una organización en la gestión de vulnerabilidades y su capacidad para reducir el ciberriesgo de manera oportuna. Un tiempo medio corto sugiere una respuesta más rápida y eficiente a las amenazas, lo que contribuye a una menor exposición a ataques y una mayor ciberseguridad.

4. DATOS Y CÓDIGO DISPONIBLES

En el enlace deriskGroup / DICyME Project · GitLab se pueden encontrar los siguientes elementos:

1. Input: Se proporcionan una serie de ficheros en formato CSV que representan datos en bruto, completamente anonimizados, de una instalación industrial cuyo IDPS es el de Nozomi. En concreto, se han utilizado cuatro categorías de datos:
   1.1. Sobre los activos, información como su dirección de red IP, su fabricante, el tipo de dispositivo que es y los protocolos que utiliza, sus versiones, la VLAN y/o zona en que se encuentra, la primera y la última vez que tuvo actividad, y el tenant al que pertenece.
   1.2. Sobre las instalaciones, relación entre un tenant y sus facilities y appliances.
   1.3. Sobre las vulnerabilidades, sus códigos del Common Vulnerabilities and Exposures (CVE) y la fecha en que fueron publicadas.
   1.4. Las vulnerabilidades, según su código CVE, encontradas en los diversos activos monitorizados.
2. Código: Se proporciona un archivo con extensión .py que contiene código en lenguaje de programación Python que, tomando los datos de entrada de los ficheros CSV (punto 1), calcula los diferentes indicadores y genera la salida (punto 3). El código se encuentra comentado para facilitar la comprensión del mismo.
3. Output: Se proporciona la salida que el código entregado genera a partir de la entrada de muestra proporcionada (punto 1). En concreto, incluye un identificador de cada indicador, el valor del mismo y la fecha en que se ha calculado, así como información relacionada con el activo involucrado (como su nivel purdue, severidad de las vulnerabilidades...), el momento en se obtuvo la información utilizada y el estado del indicador.
   Este estado diferencia entre de entre todos los indicadores definidos, aquellos que pueden ser calculados con los datos que proporciona Nozomi actualmente, y los que no. En el caso de los indicadores que sí se pueden calcular, se asigna el valor “PROD”, y para aquellos que no, pero cuyo código ya está preparado para el momento en que se disponga de los datos, el valor “DEV”. Por razones obvias, para este último no existe ningún valor en el fichero de output, ya que no puede generarse el resultado aún.

Cabe aclarar algunos aspectos sobre el entorno de desarrollo empleado para generar el prototipo. Se han utilizado:

- Python 3.9.5
- Databricks Runtime 12.2 LTS
- Apache Spark 3.3.2
- Pandas 1.4.2
- Numpy 1.21.5

También hay que señalar que para poder ejecutar este código sin errores es necesario usar el mismo entorno que el de desarrollo, arriba señalado.

4. CONCLUSIONES Y SIGUIENTES PASOS

En resumen, el prototipo producido en este entregable es capaz de integrarse con el sistema IDPS de Nozomi desplegado en una instalación industrial, extraer evidencias de ciberriesgo de este sistema y transformarlas en información útil para la cuantificación de dicho ciberriesgo mediante el cálculo de una serie de indicadores.

Para la siguiente versión de este módulo se pretende avanzar en las siguientes direcciones:

1. Integrarlo con otros sistemas de tipo IDPS de proveedores o fabricantes diferentes.
2. Completar los indicadores definidos, y si fuera necesario incorporar nuevas fuentes de datos para poder calcularlos, hacerlo mediante integraciones adicionales (por ejemplo, con sistemas de tipo EDR o SIEM).
3. Alimentar desde este módulo a los modelos que cuantifican el ciberriesgo, ya que de momento su salida sólo está pensada para alimentar al módulo de visualización.