Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

Tipo de artículo : Artículo original
Temática : Seguridad Informática
Recibido: 30/06/2021| Aceptado: 01/10/2021

Arquitectura para la detección violaciones a políticas de seguridad

Architecture for the detection of security policy violations

Yohandra Echeverria Castillo[1*] https://orcid.org/0000-0001-6163-2819

Mónica Peña Casanova [1] https://orcid.org/0000-0003-2500-4510

Bárbara Laborí de la Nuez [1] https://orcid.org/0000-0001-8114-0969

[1] Facultad 2, Universidad de las Ciencias Informáticas. Carretera a San Antonio Km 2 ½ Torrens. Boyeros. La Habana. Cuba.{yoha, monica, barbaral}@uci.cu

[*] Autor para correspondencia.(yoha@uci.cu)

RESUMEN

Las trazas poseen una gran relevancia en la gestión de la seguridad informática, debido a que la información que en ellas se registran contribuye en las actividades de auditoría y análisis forense, en el apoyo a investigaciones internas, establecimiento de líneas base y en la identificación de tendencias operacionales y problemas de comportamiento de los sistemas de información. Entre las trazas asociadas a la seguridad se encuentran las trazas generadas por el acceso a los servicios de red, específicamente a internet a través de un proxy. El proceso de detección de violaciones de seguridad a partir del análisis de trazas de la navegación de Internet de los usuarios, requiere de variantes que normalicen los formatos existentes. Se deben definir estrategias de análisis y búsquedas que permitan la generación de alarmas y reportes ante la detección de alguna violación de seguridad a las políticas establecidas en la organización. En el presente artículo se

expone un análisis de los diferentes formatos para definir la estructura de las trazas. Se propone una arquitectura para la detección de violaciones de seguridad a partir del análisis de trazas de navegación de internet de los usuarios, así como los componentes necesarios como resultado del análisis desarrollado. Se determina un formato común para la estandarización de la estructura de las trazas, permitiendo una mayor capacidad de análisis. Se evalúan las herramientas necesarias para la implantación de la arquitectura propuesta.

Palabras clave: trazas; usuarios; violaciones; seguridad; Internet.

ABSTRACT

Logs are highly relevant in the management of computer security, because the information recorded in them contributes to auditing and forensic analysis activities, supporting internal investigations, establishing baselines and identifying operational trends and behavior problems of information systems. Among the logs associated with security are the logs generated by access to network services, specifically the internet through a proxy. The process of detecting security violations from the analysis of logs of users' Internet browsing requires variants that standardize the existing formats. Analysis and search strategies must be defined that allow the generation of alarms and reports in the event of the detection of any security violation to the policies established in the organization. This article presents an analysis of the different formats to define the structure of the Logs. An architecture is proposed for the detection of security violations from the analysis of Internet browsing Logs of users, as well as the necessary components as a result of the analysis developed. A common format is determined for the standardization of the structure of the logs, allowing a greater capacity for analysis. The tools necessary for the implementation of the proposed architecture are evaluated.

Keywords: log; users; violations; security; Internet.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

Introducción

Las trazas poseen una gran relevancia en la gestión de la seguridad informática, debido a que la información que en ellas se registran contribuye en las actividades de auditoría y análisis forense, en el apoyo a investigaciones internas, establecimiento de líneas base y en la identificación de tendencias operacionales y problemas de comportamiento de los sistemas de información. Según el tipo de aplicaciones, se tienen trazas de software asociadas directamente a la seguridad y trazas relativas a los sistemas operativos, las aplicaciones y servicios que se encuentran en ejecución (Schipper et al., 2019).

Entre las trazas asociadas a la seguridad se encuentran las generadas por el proxy. Un proxy en una red informática, es un servidor, que hace de intermediario en las peticiones de recurso que realiza un cliente a otro servidor (Chen et al., 2020). Dentro de las trazas generadas por el proxy se encuentran las trazas generadas por el acceso a los servicios de red, específicamente a internet.

Según una encuesta realizada por el Instituto SANS la mayoría de las organizaciones, independientemente de su dimensión y las soluciones que tengan implantadas, no hacen uso en su totalidad de la información contenida en las trazas (Dale, Chris,*2020*). Muchas de las herramientas que utilizan los especialistas de seguridad informática para obtener información a partir de las trazas obtenidas, no generan alarmas relacionada a las violaciones que cometen los usuarios cuando acceden a internet a través de la red de las organizaciones, específicamente, las violaciones relacionadas a robo de credenciales y accesos a sitios comprometidos.

Generalmente la revisión de las trazas, especialmente las de la navegación en internet de los usuarios, ocurre ante la notificación de un evento, lo que hace que se proceda a buscar evidencia digital y no a detectar en tiempo real la ocurrencia de dicho evento. Debido a que el cúmulo de datos que se almacena en las trazas es tan grande y sus formatos pueden ser diferente, en reiteradas ocasiones el especialista no encuentra la información necesaria en tiempo o para poder analizarlas deben auxiliarse de un conjunto de herramienta que no están integradas entre sí.

El proceso de detección de violaciones de seguridad a partir del análisis de trazas de la navegación de Internet de los usuarios, requiere de variantes que normalicen los formatos existentes. Se deben definir estrategias de análisis y búsquedas que permitan la generación de alarmas y reportes ante la detección de

alguna violación de seguridad a las políticas establecidas en la organización. En el presente artículo se expone un análisis de los diferentes formatos para definir la estructura de las trazas.

Se propone una arquitectura para la detección de violaciones de seguridad a partir del análisis de trazas de navegación de internet de los usuarios, así como los componentes necesarios como resultado del análisis desarrollado. Se determina un formato común para la estandarización de la estructura de las trazas, permitiendo una mayor capacidad de análisis. Se evalúan las herramientas necesarias para la implantación de la arquitectura propuesta.

Métodos o Metodología Computacional

En el presente trabajo se utilizó como métodos de investigación: el analítico - sintético para descomponer el problema de investigación en elementos, profundizar en su estudio y luego sintetizarlos en la solución propuesta; y el histórico – lógico con el fin de realizar un estudio crítico sobre la evolución de los diferentes enfoques relativos a la gestión de trazas. Como método empírico se empleó el análisis comparativo para detectar similitudes y diferencias en marcos de referencia asociados a la gestión de trazas.

Resultados y discusión

Las trazas son registros en el cual se almacenan los diferentes eventos que se realizan dentro de un sistema, red o aplicación. Se encuentran compuestos de campos, dónde cada una de estos representan información sobre un evento o suceso que haya ocurrido en el sistema. El procesamiento de las trazas a través de los mecanismos adecuados podría convertirse en una base de datos de eventos con utilidad en diversos fines, entre los cuales se encuentra: administración de recurso, detección de incidentes de seguridad y de violaciones a las políticas de seguridad establecidas en la organización, análisis forense, registrar las diferentes acciones que realice un usuario y auditorías.

Tipos de trazas

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

Según el tipo de aplicaciones, se tienen trazas de software asociadas directamente a la seguridad y trazas relativas a los sistemas operativos, las aplicaciones y servicios que se encuentran en ejecución. Por lo que se pueden dividir en tres grandes grupos *(Cigdem BAKIR, V. H, 2020)*. Los registros asociados a las categorías mencionadas se muestran en la Tabla 1.

Tabla 1 -Agrupación de las fuentes de generación de trazas según el tipo de aplicación *(Cigdem BAKIR, V. H, 2020)*

Trazas de seguridad	**Trazas de sistemas operativos**	**Trazas de aplicaciones**
Software antimalware	Eventos del sistema	Peticiones en aplicaciones tipo cliente servidor
Sistemas de detección y previsión de incidentes	Registros de auditorias	Información de auditoria
Software de acceso remoto		Información de utilización de las aplicaciones
Proxy		Trazas de funcionamiento y operaciones significativas
Software de gestión de vulnerabilidades		
Routers		
Firewall		

La selección de las fuentes de trazas para el monitoreo de seguridad, debe estar en correspondencia con la utilización que se le dará a la información recolectada, ya sea para el monitoreo, respuesta a incidentes de seguridad o cumplimiento de regulaciones y análisis forenses.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

Estructura de las trazas

Los datos específicos que contiene cada una de las trazas varía en función de su forma de generación. Hoy en día, cada aplicación tiene su propio formato de archivo de registro. Tal variedad de formatos complica el análisis de registro y causa problemas a los administradores de sistemas, desarrolladores de sistemas de detección de intrusión (IDS) y analistas de seguridad. Sin embargo, existen formatos de referencias para la normalización de la estructura de las trazas.

El Formato de Expresión Común de Eventos (por sus siglas en inglés CEE) estandariza la forma en que se describen, registran e intercambian las trazas. Al utilizar un lenguaje y una sintaxis comunes, CEE elimina las conjeturas en los campos (Danyliw et al., 2007). El propósito del Formato de intercambio de mensajes de detección de intrusiones (por sus siglas en inglés IDEMF) es definir formatos de datos e intercambiar procedimientos para compartir información de interés para los sistemas de detección y respuesta de intrusos y para los sistemas de gestión que puedan necesitar interactuar con ellos.

El Formato intercambio de descripción de objetos de incidentes (por sus siglas en inglés IODEF) está especialmente diseñado para incidentes de seguridad informática, así como el Formato de Evento Común (por sus siglas en inglés CEF) desarrollado como parte del sistema de detección de intrusos A pesar de que los formatos mencionados tienen diferentes propósitos, cada uno de ellos podría usarse para la normalización de la estructura de las trazas. Su principal semejanza es que ofrecen un número limitado de opciones para analizar con precisión la descripción textual del evento, afectando directamente a la normalización de los detalles del evento (Danyliw et al., 2007) y (*Buczak, Anna L., et al., 2017*).

El perfil de registro de trazas (RLP por sus siglas en inglés) proporciona las capacidades de gestión para representar los datos de las trazas de los sistemas gestionados, se modela haciendo referencia a los datos a los elementos del sistema administrado. El perfil de registro de trazas (RLP por sus siglas en inglés) forma parte del Modelo Común de Información (CIM por sus siglas en inglés) para el entorno de TI, su función es describir la asociación entre los elementos del sistema gestionado y las trazas generadas a través de clases.

Permitiendo la neutralidad tecnológica y la interoperabilidad de sistemas de diferentes fabricantes (*Distributed Management Task Force*, 2008). El inconveniente de este perfil es que no tiene en cuenta la normalización de los campos que se almacenan en las trazas.

Por otra parte, el Esquema Común de Elastic (ECS por sus siglas en inglés), es una especificación de código abierto que proporciona una forma personalizable para que las organizaciones estructuren sus datos de eventos. ECS facilita el análisis unificado de trazas de diversas fuentes, lo que respalda una amplia gama de casos de uso, incluidos el registro, el análisis de seguridad y la supervisión del rendimiento de las aplicaciones. ECS también agiliza el desarrollo de contenido analítico. En lugar de crear nuevas búsquedas y paneles cada vez que una organización agrega una fuente de datos con un nuevo formato, los usuarios pueden seguir aprovechando las búsquedas y los paneles compatibles. Además, hace que sea mucho más fácil para las organizaciones adoptar directamente contenido analítico de otras partes que usan ECS *(Rakhmetova1, 2021*).

Gestión de trazas

La gestión de trazas es el proceso que se enfoca en las actividades que se llevan a cabo para identificar los datos necesarios, procesarlos, manipularlos y mostrarlos de forma organizada, contribuyendo a la detección de incidentes y a la toma de decisiones por parte de los especialistas de seguridad. Además, contribuye en las actividades de auditoría y análisis forense, en el apoyo a investigaciones internas, establecimiento de líneas base y en la identificación de tendencias operacionales y problemas de comportamiento de los sistemas de información.

El proceso de gestión de traza se encuentra compuesto de los siguientes subprocesos: generar, transmitir, almacenar y analizar

Generación de trazas: Este primer subproceso se encuentra integrado por los diferentes equipos que generan los registros de las trazas.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

Transmisión: Permite él envió de las trazas recolectadas hacia los servidores de almacenamiento.

Almacenamiento: Servidores que reciben las trazas recolectadas.

Monitoreo: En esta etapa puede que se realicen tareas de procesamiento para poder incluir mecanismos especializados de búsquedas. Además, se incorporan herramientas que permiten visualizar los datos que se encuentran en los archivos y generar reportes. Con el objetivo de brindar información sobre el uso de los servicios de navegación, detectar y responder ante ataques, robo de información u otro evento. Además, permiten informar a los especialistas sobre fallos o posibles acciones que deben ser ejecutadas.

Actualmente se utilizan herramientas para gestionar la información almacenada en las trazas, debido a volumen de información almacenada, el acceso y reconocimiento, las operaciones que intervienen requeridas en la aplicación de herramientas de análisis de trazas son: filtrado, normalización, correlación y reporte.

Las trazas se clasifican dependiendo de su fuente de generación y la selección de estas fuentes debe estar en correspondencia con el objetivo a seguir. El proceso de gestión de traza, que se encuentra dividido por varios subprocesos que determinan las fases de tratamiento de las trazas, los cuales son: generación de traza, recolección de traza, filtrado, monitorización y reporte. Es de vital importancia para las organizaciones que el proceso de gestión de trazas se realice en tiempo real, permitiendo la detección temprana de incidentes y violaciones de seguridad a los procedimientos establecidos.

Principios que rigen el funcionamiento de la arquitectura propuesta

Los principios de esta arquitectura se pueden resumir en los siguientes puntos:

1. **Escalable**: posibilita que se puedan incorporar nuevos elementos de seguridad u otros equipos a la arquitectura
2. **Tolerante a fallos:** Después de un fallo se tarde el menor tiempo posible en la recuperación o pérdida de la menor cantidad de información o datos posibles.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

3. **Eficiente:** todos los sistemas de la arquitectura funcionen a su nivel óptimo, sin sobrecargarse, pero sin infrautilizarse.
4. **Segura:** lo más importante, que garantice el máximo posible la seguridad en cada una de sus capas.
5. **Generalizable**: podrá ser desplegada en cualquier organización que requiera la realización del análisis de trazas.
6. **Independiente:** la arquitectura es independiente de la tecnología que se emplee en cada organización para puesta en funcionamiento de los sistemas y servicios.
7. **Bajo Acoplamiento:** la arquitectura posibilita la modificación de una capa sin afectar a otras.

Estructura organizativa de la arquitectura

La arquitectura para la detección automática de violaciones a políticas de seguridad, está sustentado en el proceso de análisis de trazas identificado en el epígrafe 1.3 con el análisis documental de las principales regulaciones, decretos, normas y guías de buenas prácticas. Como se describe en la figura 2.1 la arquitectura se ha dividido en cinco capas (generación, recolección y envió, normalización, almacenamiento, análisis, visualización de información y monitoreo).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

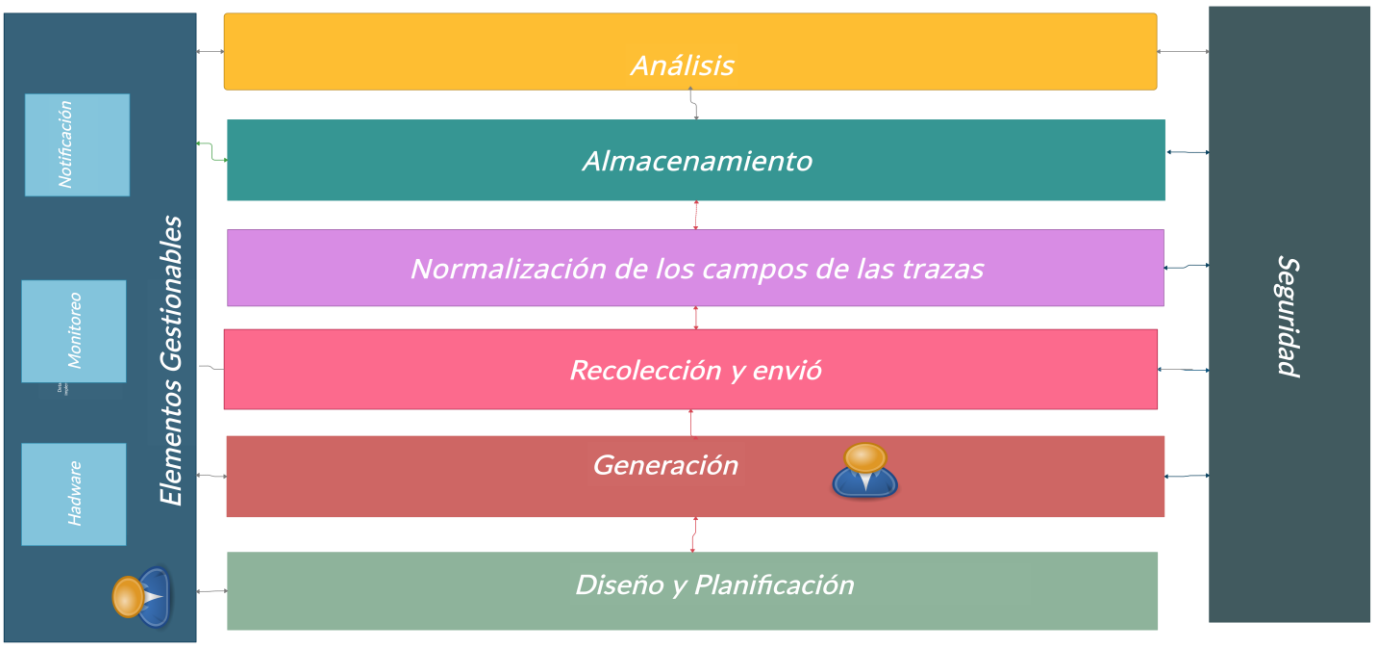

Fig. 1 - Componentes general de la arquitectura para la detección de violaciones a políticas de seguridad.

Las comunicaciones entre cada uno de las capas se realizan en banda o fuera de banda en función de los requisitos de seguridad de cada organización. En el primer caso se utilizará la red de la organización que se está monitorizando, en este caso deben tomarse medidas adicionales de seguridad durante el proceso de recolección de las trazas para no inducir vulnerabilidades. También puede desplegarse una red independiente para la comunicación entre las capas de la infraestructura. Una vez generadas las trazas, una herramienta se encarga de recolectarlos y enviarlos para su posterior almacenamiento e indexación, permitiendo las funciones de visualización y análisis de las trazas. Cada uno de las capas de la arquitectura están formado por herramientas que trabajan de forma integrada. La utilización de varias herramientas y su instalación requiere del manejo de múltiples ficheros de configuración.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

Descripción de las capas

A continuación, se describen las funciones de cada una de las capas que forman parte de la arquitectura, así como la manera en que debe ocurrir la interacción entre ellas.

1. **Capa de Diseño y planificación:** Tiene como objetivo realizar un diagnóstico de la infraestructura tecnológica de la organización. Detectando los elementos gestionables y su impacto en la organización. Se definen las herramientas para la instanciación de la arquitectura en dependencia de las necesidades y de la infraestructura de la organización
2. **Capa de Generación:** contiene las trazas generadas por los sistemas operativos, dispositivos de seguridad, almacenamiento y aplicaciones, se debe diseñar la infraestructura de las trazas de manera que sea escalable.
3. **Capa de Recolección y envió:** se encarga de recolectar las trazas de interés para su posterior almacenamiento y análisis.
4. **Capa de Análisis:** es la responsable de revisar de manera frecuente y en tiempo real las trazas generadas, permitiendo la detección de eventos y violaciones de seguridad. El resultado de este análisis permite conocer en detalle la actividad de los usuarios y/o equipos dentro de la red, registrada en las trazas del proxy utilizado, datos que serán visualizados en las capas de monitoreo y visualización.
5. **Capa de Almacenamiento:** en esta capa se debe definir cómo será almacenada y el tiempo de retención de la información. Las trazas deben almacenarce en una infraestructura de almacenamiento segura y bien administrada, se debe proveer accesos basados en roles para tener una auditoria confiable. El almacenamiento puede ser federado integrado en una base de datos común o desde el punto de vista tecnológico puede realizarse en la nube o en un servidor dedicado a esta tarea.
6. **Capa de Elementos Gestionables**: esta capa se integra con las subcapas de hardware, monitoreo y notificación.
7. **Subcapa de Hardware:** permite la comunicación con los distintos elementos que conforma el sistema operativo.

8. **Supcapa de Monitoreo**: provee todos los servicios que brinda la arquitectura a través de una interfaz. Posibilita el diseño de las opciones de búsqueda avanzada sobre los campos de las trazas que intervienen en la capa de almacenamiento, brindando una variedad de información.
9. **Supcapa de Notificación**: posibilita las funciones de notificación a ante la ocurrencia de la detección de una violación o evento de seguridad.
10. **Capa de Normalización:** Tiene como objetivo normalizar los campos de las trazas, permitiendo la búsqueda, visualización y análisis uniformes de trazas de diferentes fuentes de datos dispares. Estos datos son normalizados una vez recolectados. Para la normalización de las trazas se utiliza la especificación ECS.
11. **Capa de Seguridad:** la premisa de esta capa es asegurar la disponibilidad, confidencialidad de las trazas a través de todo su ciclo de vida. Las trazas son susceptibles a su alteración o eliminación, si no se tienen los controles durante su almacenamiento y en su transmisión. Se debería tener procesos y procedimientos seguros sobre los activos o sistemas que generan los las trazas, mediante control de accesos, roles y responsabilidades bien definidos, políticas y procedimientos sobre control de cambios. Las herramientas que conforman la arquitectura deben configurarse siguiendo las buenas prácticas de seguridad.

Normalización de los campos de las trazas utilizando ECS

La especificación ECS presenta los siguientes conjuntos de campos: el conjunto de campos bases, conjunto de campos de categorización y el conjunto de campos generales. El conjunto de campos bases son definidos en dependencia de las trazas. ECS utiliza el conjunto de campos de categorización para identificar y agrupar las trazas similares de múltiples fuentes de datos. Basándose en los siguientes principios de categorización *Rakhmetova1, 2021*) :

1. Son agrupados en un mismo grupo las trazas de múltiples fuentes que pueden ser analizados juntos debido a la similitud de sus datos.
2. Las acciones específicas del dominio son agrupadas en campos separados del resto de los datos.
3. Existencia de valores permitidos para algunos campos de clasificación.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

Especificaciones de ECS para la definición de los campos *Rakhmetova1, 2021*)**:**

1. Los nombres de los campos deben estar en minúsculas.
2. Se deben combinar palabras con guion bajo, siendo este el único carácter especial permitido.
3. Las trazas deben contener campo de tiempo en presente, al menos que describa información histórica.
4. Se debe utilizar nombres en singular y plural correctamente, para reflejar el contenido de los campos.
5. Utilizar prefijos para todos los campos, excepto para los campos bases.
6. Evitar las abreviaturas.
7. El ID y los códigos son palabras claves no números enteros

Cuando las trazas recibidas que se encuentran en otro formato, se analiza el encabezado y se establece el valor de la marca de tiempo. Luego se aplica el procesador para analizar los datos codificados. Los datos codificados se describen en campo de objeto. Por último, se completan los datos de los campos según las especificaciones determinadas en ECS. En la tabla 1 se muestra la instanciación de la arquitectura para la detección de violaciones a políticas de seguridad a partir del análisis de las trazas de navegación de Internet de los usuarios.

Tabla 2 -Descripción de la herramientas para el despliegue de la arquitectura.

Herramienta	**Descripción**
Elasticsearch	Es una base de datos no relacional de almacenamiento con funciones incorporadas de búsqueda de texto y análisis de datos. Entre sus principales características están el acceso y el análisis de los datos en tiempo real, escalabilidad a través de una arquitectura distribuida y alta disponibilidad (*Elasticsearch Guide [7.14] | Elastic*, s. f.).
Filebeat	Filebeat se instala como agente en los servidores, posibilitando la monitorización de las trazas específicas y de interés para el especialista de seguridad. Utiliza módulos para fuentes de datos de seguridad que simplifican la recopilación, el análisis y la visualización de los formatos de trazas comunes. Algunos módulos se encuentran configurados con aprendizaje automático. Filebeat utiliza un protocolo sensible a la contrapresión, cuando envía datos a Logstash o Elasticsearch para tener mayores volúmenes de datos (*Filebeat Overview | Filebeat Reference [7.14] | Elastic*, s. f.).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 265-280

Kibana	Provee un interfaz de búsqueda gráfica para los registros de trazas almacenados en Elasticsearch. Permite la creación de tablas, gráficos y múltiples tipos de visualización para los resultados de las búsquedas realizadas. La configuración de los gráficos descritos conforma los distintos paneles de mando para el análisis de las trazas almacenadas por parte de los especialistas de seguridad (*Kibana Guide [7.14] | Elastic*, s. f.).

Conclusiones

En una organización con acceso a Internet es fundamental realizar una adecuada gestión de las trazas, principalmente las de navegación de los usuarios. Para lograr este objetivo deben contar con mecanismos de detección de violaciones de seguridad, que a su vez generen alarmas y reportes a los especialistas de seguridad. Del análisis de la gestión de traza y los formatos de comunes para la estructura de las trazas se obtuvieron los elementos fundamentales y las especificaciones necesarias para analizar y normalizar las trazas de navegación de internet de los usuarios. Las trazas deben almacenarce en una infraestructura de almacenamiento segura y bien administrada, se debe proveer accesos basados en roles para tener una auditoria confiable. La arquitectura propuesta va a proveer a los especialistas de seguridad y administradores del sistema, la normalización de los datos almacenados en las trazas, posibilitando un mayor criterio de búsquedas en trazas de diferentes formatos. Además, provee de reportes, datos y alarmas acelerando los tiempos de búsquedas y respuestas ante la ocurrencia de alguna violación a las políticas establecidas en la organización. La arquitectura de despliegue propuesta agrupa e integra los componentes de la gestión de trazas, tratando de usar el menor número de herramientas, en un sistema único donde se garantiza la recolección, normalización, almacenamiento, análisis y monitoreo de las trazas de navegación de los usuarios Debido a su flexibilidad, la integración de las herramientas puede variar partiendo de los recursos y necesidades concretas de las organizaciones.

Referencias

Dale, Chris. (2020). *2020 SANS Enterprise Cloud Incident Response Survey | SANS Institute*. (s. f.). Recuperado 5 de septiembre de 2021, de https://www.sans.org/white-papers/39805/

Chen, L., Yang, M., Wimmer, H., & Wilbert, B. (2020, enero 1). *A Practical Low-Cost Security Solution for Log Management and File Integrity Monitoring*. https://doi.org/10.4108/eai.27-8-2020.2294894

Cigdem BAKIR, V. H. (2020). *Classifying Database Users for Intrusion Prediction and Detection in Data Security*. 6. *Tehnički vjesnik, 27*(6), 1857-1862. https://doi.org/10.17559/TV-20190710100638

Danyliw, R., Meijer, J., & Demchenko, Y. (2007). The Incident Object Description Exchange Format. *International Journal of High Performance Computing Applications - IJHPCA. IETF Request For Comments, 5070.*

Rakhmetova1, Evelina , Combi, Carlo, Fruggi, Andrea (2021) *Conceptual Modelling of Log Files: From a UML-based Design to JSON Files, CEUR Workshop Proceedings, 2958, ISSN 1613 0073* http://ceur-ws.org/Vol-2958/

Elasticsearch Guide [7.14] | Elastic. (s. f.). [Learn/Docs/Elasticsearch/Reference/7.14]. Recuperado 7 de septiembre de 2021, de https://www.elastic.co/guide/en/elasticsearch/reference/7.14/index.html

Filebeat overview | Filebeat Reference [7.14] | Elastic. (s. f.). [Learn/Docs/Filebeat/Reference/7.14]. Recuperado 7 de septiembre de 2021, de https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html

Kibana Guide [7.14] | Elastic. (s. f.). [Learn/Docs/Kibana/Reference/7.14]. Recuperado 7 de septiembre de 2021, de https://www.elastic.co/guide/en/kibana/7.14/index.html

Record Log Profile (Specification N.º DSP1010; p. 25). (2008). Distributed Management Task Force. https://www.dmtf.org/documents/dash/record-log-profile-100

Schipper, D., Aniche, M., & van Deursen, A. (2019). Tracing Back Log Data to its Log Statement: From Research to Practice. *2019 IEEE/ACM 16th International Conference on Mining Software Repositories (MSR)*, 545-549. https://doi.org/10.1109/MSR.2019.00081

Buczak, Anna L., et al. Using sequential pattern mining for common event format (CEF) cyber data. En *Proceedings of the 12th annual conference on cyber and information security research*. 2017. p. 1-4. https://dl.acm.org/doi/abs/10.1145/3064814.3064822

Conflicto de interés

Declaro ser autora del presente artículo y reconozco a la Universidad de las Ciencias Informáticas los derechos patrimoniales del mismo, con carácter exclusivo.

Contribuciones de los autores

1. Conceptualización: Mónica Peña Casanova y Bárbara Laborí de la Nuez
2. Curación de datos: Yohandra Echeverria Castillo
3. Análisis formal: Yohandra Echeverria Castillo
4. Investigación: Yohandra Echeverria Castillo
5. Metodología: Yohandra Echeverria Castillo
6. Administración del proyecto: Mónica Peña Casanova y Bárbara Laborí de la Nuez
7. Recursos: Mónica Peña Casanova y Bárbara Laborí de la Nuez
8. Supervisión: Mónica Peña Casanova y Bárbara Laborí de la Nuez
9. Validación: Mónica Peña Casanova y Bárbara Laborí de la Nuez
10. Visualización: Yohandra Echeverria Castillo
11. Redacción – borrador origina: Yohandra Echeverria Castillo
12. Redacción – revisión y edición: Mónica Peña Casanova y Bárbara Laborí de la Nuez