Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), mayo-junio 2024,
Volumen 8, Número 3.

https://doi.org/10.37811/cl_rcm.v8i3

CIBERSEGURIDAD: IMPACTO Y DETECCIÓN DE EVENTOS DE SEGURIDAD MEDIANTE PROTOTIPO DE MONITOREO

CYBERSECURITY: IMPACT AND DETECTION OF SECURITY EVENTS THROUGH MONITORING PROTOTYPE

Enrique Alanis Hernández
Tecnológico Nacional de México, México

Eduardo López Sandoval
Tecnológico Nacional de México, México

José Manuel Colín Morales
Tecnológico Nacional de México, México

Samuel Viñas Álvarez
Tecnológico Nacional de México, México

Alejandro Sosa Sales
Tecnológico Nacional de México, México

DOI: https://doi.org/10.37811/cl_rcm.v8i3.11511

Ciberseguridad: Impacto y Detección de Eventos de Seguridad Mediante Prototipo de Monitoreo

Enrique Alanis Hernández[1]
isc.enrique.alanis@outlook.com
https://orcid.org/0000-0001-5288-9321
Tecnológico Nacional de México
Campus Zitácuaro
México

Eduardo López Sandoval
eduardo.ls@zitacuaro.tecnm.mx
https://orcid.org/0000-0002-4777-0470
Tecnológico Nacional de México
Campus Zitácuaro
México

José Manuel Colín Morales
jose.cm@zitacuaro.tecnm.mx
https://orcid.org/0009-0003-5443-4138
Tecnológico Nacional de México Campus Zitácuaro
México

Samuel Viñas Álvarez
samuel.va@zitacuaro.tecnm.mx
https://orcid.org/0000-0001-5891-2801
Tecnológico Nacional de México
Campus Zitácuaro
México

Alejandro Sosa Sales
Alejandro.ss@zitacuaro.tecnm.mx
https://orcid.org/0000-0001-9049-7951
Tecnológico Nacional de México
Campus Zitácuaro
México

RESUMEN

La ciberseguridad se ha convertido en un tema crítico en la era digital, donde los avances tecnológicos han facilitado tanto la vida cotidiana como las actividades delictivas. Este artículo presenta una propuesta de prototipo de herramienta de monitoreo y análisis de eventos informáticos para contar con un componente de seguridad con la finalidad de reforzar nuestra navegación y uso de sistemas web en pequeños negocios, redes domesticas o medias empresas enfocando en la ciberseguridad. Se explora cómo los ciberdelincuentes aprovechan vulnerabilidades en sistemas informáticos y redes para acceder ilegalmente a información sensible o para interrumpir servicios críticos. Además, examinamos la evolución de las tácticas de ataque, destacando la sofisticación creciente de los métodos empleados y su adaptación a las defensas cibernéticas. Se aborda también la importancia de contar con un sistema de detección de eventos que se encuentre al alcance de prácticamente cualquier persona, empresa pequeña o mediana que este preocupada por velar por la integridad de su información y disponibilidad de la misma con el fin de lograr de lograr tener un cerco de seguridad que aporte visión y estrategias de seguridad de lo que fluye dentro de su red y sus dispositivos de cómputo. Finalmente, se concluye resaltando la necesidad de una colaboración continua para el desarrollo de tecnologías innovadoras y regulaciones efectivas para hacer frente al constante cambio y la sofisticación de las amenazas cibernéticas en el futuro.

Palabras clave*:* ciberseguridad, ciberdelincuentes, vulnerabilidad, redes

[1] Autor principal
Correspondencia: isc.enrique.alanis@outlook.com

Cybersecurity: Impact and Detection of Security Events Through Monitoring Prototype

ABSTRACT

Cybersecurity has become a critical issue in the digital age, where technological advancements have facilitated both everyday life and criminal activities. This article presents a proposal for a prototype tool for monitoring and analyzing IT events to provide a security component aimed at enhancing our navigation and use of web systems in small businesses, home networks, or medium-sized enterprises with a focus on cybersecurity. It explores how cybercriminals exploit vulnerabilities in computer systems and networks to illegally access sensitive information or disrupt critical services. Additionally, we examine the evolution of attack tactics, highlighting the increasing sophistication of the methods employed and their adaptation to cybersecurity defenses. The importance of having an event detection system accessible to virtually anyone, including small or medium-sized businesses concerned with the integrity and availability of their information, is also addressed. The goal is to achieve a security perimeter that provides insight and security strategies for what flows within their network and computing devices. Finally, it concludes by emphasizing the need for ongoing collaboration in the development of innovative technologies and effective regulations to counter the constant change and sophistication of cyber threats in the future.

Keywords: cybersecurity, cybercriminal, vulnerabilities, networks

Artículo recibido 20 abril 2024

Aceptado para publicación: 25 mayo 2024

INTRODUCCION

En la era digital, donde la tecnología impregna cada aspecto de nuestras vidas, la ciberseguridad se erige como una preocupación primordial. A medida que aumenta nuestra dependencia de sistemas interconectados, dispositivos y redes, también crece la amenaza planteada por ciberdelincuentes que buscan explotar vulnerabilidades con fines de lucro, espionaje o interrupción. Desde individuos hasta grandes corporaciones y entidades gubernamentales, nadie está inmune a las tácticas en constante evolución de los actores maliciosos en el ciberespacio.

Podemos definir la ciberseguridad como la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. (¿Qué Es la Ciberseguridad? - Soporte Técnico de Microsoft, s. f.).

Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa. Utilizan medidas y herramientas de ciberseguridad para proteger los datos confidenciales del acceso no autorizado, así como para evitar interrupciones en las operaciones empresariales debido a una actividad de red no deseada. Las organizaciones implementan la ciberseguridad al optimizar la defensa digital entre las personas, los procesos y las tecnologías. (¿Qué Es la Ciberseguridad? - Explicación de la Ciberseguridad - AWS, s. f.).

Comúnmente el término de ciberseguridad es empleado intercambiablemente con el término de seguridad de la información; sin embargo, este último tiene mayor alcance que abarca a la información en su estado físico o electrónico.

La Seguridad de la información es la protección de la información contra el acceso, uso, revelación, interrupción, modificación o destrucción por entes externos a la organización. Tiene como objetivo la protección de la integridad, disponibilidad y confidencialidad ya sea física o electrónicamente. (¿Qué Es la Seguridad de la Información (InfoSec)? | Seguridad de Microsoft, s. f.).

La aplicación cuidadosa de controles de seguridad de la información es fundamental para proteger los activos de información de una empresa, así como su reputación, posición legal, personal y otros activos tangibles o intangibles.

Según los datos recabados por FortiGuard Labs, el laboratorio de inteligencia de amenazas de Fortinet, México fue el país latinoamericano que más intentos de ataques recibió (156 mil millones), seguido de Brasil (88.5 mil millones), Perú (11.5 mil millones) y Colombia (11.2 mil millones) (FortiGuard Labs - Threat Intelligence Platform | Fortinet, s. f.).

Se presenta un prototipo de proyecto de investigación para poder monitorear los recursos de red de los dispositivos que ofrecen servicios críticos para nuestro ámbito de navegación diario o de negocios como portales WEB, aplicaciones internas con materiales que están considerados de bajo costo y con una arquitectura escalable que no representa gran inversión monetaria.

Además, exploramos cómo los ciberdelincuentes explotan las debilidades en el software, las redes y el comportamiento humano para infiltrarse en sistemas, robar datos sensibles o interrumpir operaciones. A través de ejemplos del mundo real y estudios de casos, ilustramos las diversas tácticas empleadas por los actores malintencionados para lograr sus objetivos nefastos.

Por otra parte, discutimos la importancia de medidas proactivas de ciberseguridad, incluida la educación, la capacitación y la implementación de protocolos y tecnologías de seguridad sólidos. Al fomentar una cultura de conciencia y preparación en ciberseguridad, los individuos y las organizaciones pueden reducir significativamente su susceptibilidad a las amenazas cibernéticas.

Este artículo subraya la necesidad crítica de vigilancia y colaboración en la lucha continua contra el cibercrimen. Al mantenerse informados, adoptar las mejores prácticas y aprovechar la experiencia colectiva de los profesionales de la ciberseguridad, podemos fortalecer nuestras defensas y mitigar los riesgos planteados por los ciberdelincuentes en un mundo cada vez más interconectado.

Ataques cibernéticos en empresas lideres en su sector

Como parte del antecedente para comprender a detalle algunos de los principales ataques de ciberseguridad suscitados dentro de las principales empresas alrededor del mundo tenemos lo siguiente:

Tabla 1: Principales ataques cibernéticos a empresas lideres en su sector

Ataque	Descripción
Log4j	Es el nombre que se le dio a una vulnerabilidad que permite que un atacante ejecute un código abierto y tome control de los dispositivos afectados. Este ataque afectó a 5 víctimas en las industrias de finanzas, banca y software en países como Israel, Estados Unidos, Corea del Sur, Suiza y Chipre.
Ataque de servidor Exchange	De acuerdo con el ciber reportero Brian Krebs, al menos 30,000 organizaciones en USA, fueron atacadas por una unidad china de espionaje cibernético que se enfoca en robar correo electrónico de sus víctimas. La unidad explotó cuatro fallas descubiertas en el servidor de correo de Microsoft Exchange Server.
SolarWinds	Es una compañía de software basada en USA, la cual proporciona herramientas para monitoreo de redes e infraestructura y otros servicios. Los ciber-actores lograron tener acceso a las redes, sistemas y datos de miles de clientes de SolarWinds, Más de 30,000 organizaciones públicas y privadas usan sus servicios de esta compañía.
Kaseya	Kaseya sufrió un ataque de Ransomware que afectó a varios de sus clientes. De acuerdo con la compañía de mandiant, unos 60 clientes fueron afectados por este ataque. Sin embargo, estos clientes a su vez prestan sus servicios a otras organizaciones, lo que ocasionó una afectación cerca de 1,500 compañías que prestan sus servicios a usuarios finales.
Colonial Pipeline	Una de las más grande compañías de oleoductos en USA sufrió un ataque de Randsomware. Se dice que Darside es una organización detrás de este ataque. Debido a la amenaza de escasez, cuatro estados de EE.UU. (Carolina del Norte, Virginia, Georgia y Florida) declararon el estado de emergencia. Por primera vez desde 2014, el precio promedio de un galón de gasolina en los EE.UU. aumentó a casi $3. Esto es un ejemplo de cómo la infraestructura de servicios críticos de un país puede ser víctima de un ataque y afectar a todo un país.
Twitch	Esto es un ejemplo de lo que se denomina activismo. De acuerdo con la información disponible, la personas que llevó a cabo este ataque, buscaba dañar a la empresa por no haber tomado medidas contra el odio en internet. El atacante publicó en el sitio web 4chan, unos 125GB de datos de Twitch, entre los cuales estaban el código fuente de la compañía, documentos internos, salarios y otra información personal de algunas de las mayores estrellas y operadores de canales de la plataforma.

Santillán, s. f.

METODOLOGÍA

El objetivo del presente articulo tiene como finalidad la posibilidad de crear con bajos recursos monetarios un sistema de monitoreo basado en arquitecturas de micro computadoras Raspberry PI (Raspberry Pi Documentation, s. f.), creado a partir de la necesidad creciente de acercar la ciberseguridad a pequeños negocios, hogares y medianas empresas con la intención de brindar una herramienta adicional de seguridad a su infraestructura al alcance de sus bolsillos.

Para lograr la creación de un prototipo de seguridad para el monitoreo de red y análisis de eventos de eventos de seguridad es necesario seguir un enfoque sistemático, por lo cual se presenta la siguiente metodología:

Definición de requisitos

Identifica los dispositivos que deseas monitorear en este particular caso tendremos computadoras basadas en sistemas operativos linux (¿Qué Es Linux?, s. f.) pudiendo agregar componentes en futuros trabajos como, por ejemplo, servidores, computadoras de escritorio, dispositivos móviles, enrutadores, etc.

Los tipos de eventos de seguridad que estaremos monitoreando son intentos de acceso no autorizado, tráfico de red sospechoso, actividades anómalas de usuarios, etc.

Los objetivos del monitoreo y análisis de eventos de seguridad, por ejemplo, detección temprana de intrusiones, prevención de brechas de seguridad, cumplimiento de normativas, etc.

Selección de herramientas y tecnologías

En este trabajo se estará utilizando herramientas de software libre para poder realizar la integración en un esquema de monitoreo avanzado a bajo coste como será InfluxDB, Telegraf y Grafana para la presentación de resultados de manera gráfica en conjunto con la herramienta de programación Phyton (Welcome To Python.org, 2024) para poder realizar el parceo de eventos y procesamiento de datos.

Diseño de arquitectura

La arquitectura del sistema de monitoreo, se creó de la manera más simple posible sin dejar de lado la consideración de materiales de bajo coste que cumplan con las necesidades para lograr las funciones requeridas siendo el punto focal de la arquitectura una microcumputadora Raspberry PI 4 y un sistema de respaldo de información para evitar perdida de la misma.

Se consideran aspectos como la escalabilidad, la redundancia y de seguridad en la arquitectura.

Implementación del prototipo

Se realizará la implementación del prototipo en pequeñas empresas para validar la funcionalidad y evaluarse en ambiente de calidad para valorar la solución.

Pruebas y ajustes

Realiza pruebas exhaustivas del prototipo para verificar su funcionamiento y detectar posibles problemas.

Ajusta la configuración de las herramientas de monitoreo y análisis según los resultados de las pruebas.

Recopila comentarios de los usuarios y realiza iteraciones en el diseño si es necesario.

Despliegue piloto

Implementa el prototipo en un entorno piloto en producción con un conjunto limitado de dispositivos y usuarios.

Monitorea de cerca el desempeño del sistema y recopila datos sobre su eficacia en la detección y respuesta ante eventos de seguridad.

Evaluación y refinamiento

Evalúa el rendimiento del prototipo en el entorno piloto y recopila retroalimentación de los usuarios.

Realiza ajustes y refinamientos en el prototipo según los resultados de la evaluación.

Prepara documentación detallada sobre la metodología de monitoreo y análisis de eventos de seguridad para su futura implementación a escala.

RESULTADOS Y DISCUSIÓN

Prototipo

Para la creación de nuestro prototipo es necesario contar con software de Open Source (Telegraf, InfluxBd y Grafana), considerando las siguientes definiciones de funcionalidad:

Grafana: Es una plataforma interactiva y open source de visualización de datos desarrollada por Grafana Labs. Dicha plataforma permite a los usuarios ver sus datos a través de tablas y gráficos que se unifican en un panel de control (o en varios) para facilitar la interpretación y la comprensión. También permite realizar consultas y configurar avisos sobre la información y los indicadores desde el

lugar en el que se almacena dicha información, ya sea en entornos de servidores tradicionales, clústeres de Kubernetes y varios servicios de nube, entre otros. (Grafana Labs, s. f.).

InfluxDB: Es una base de datos diseñada para almacenar series de datos temporales, esto quiere decir, que se almacenan una serie de datos en registros asociados a un valor principal o índice, que es la marca de tiempo (fecha y hora). La monitorización es un caso típico de este almacenamiento de datos, donde se guarda la marca de tiempo, el nombre del host y los valores de métricas que se pretenden almacenar (CPU, memoria, IO, red, …). InfluxDB es software libre, y el rendimiento que definen para este tipo de entornos es muy competitivo. (InfluxData, 2021).

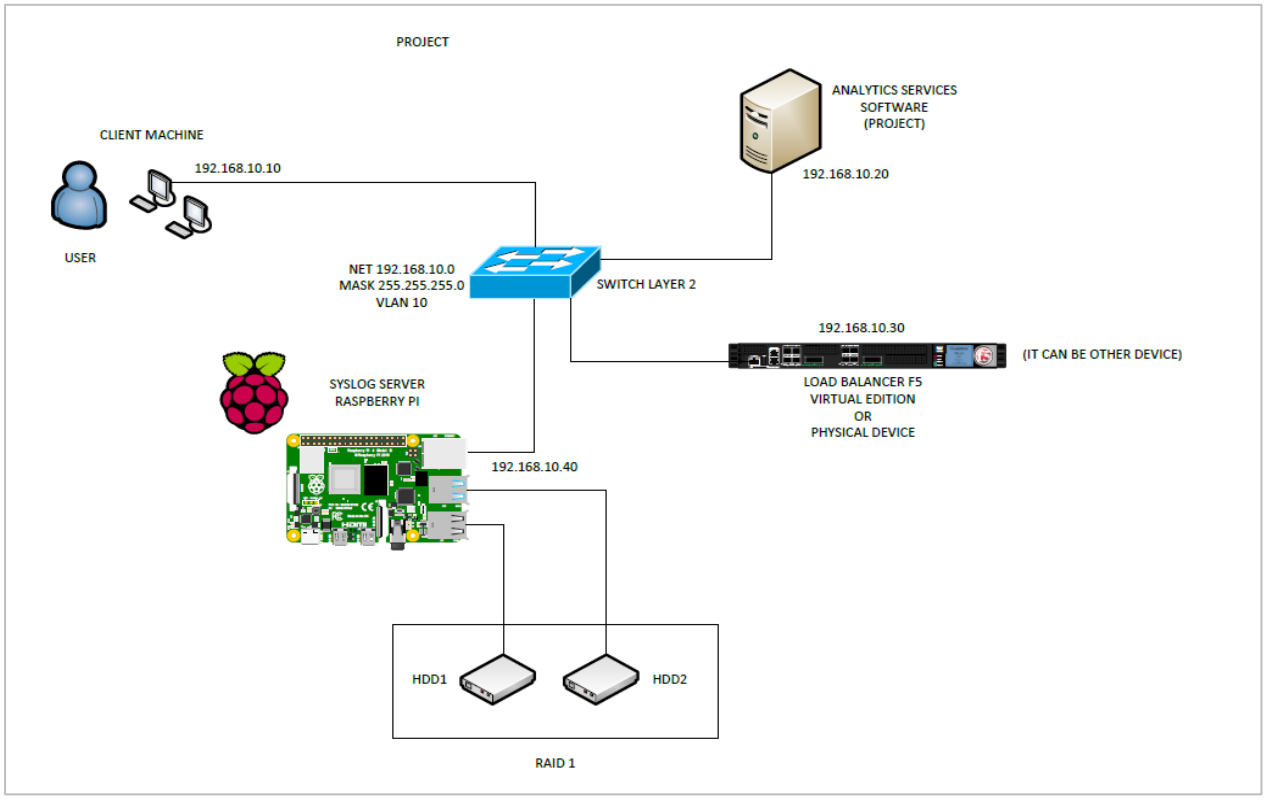
Telegraf: Es un agente que se encarga de recopilar datos/métricas de un determinado sistema y almacenarlos donde le indiquemos. En este caso este agente de Telegraf recopilará datos de sistema tradicionales (uso de memoria, uso de MySQL/Apache, …) y los enviará a la URL con la API de InfluxDB, que se encargará de almacenarlo. Telegraf, al igual que InfluxDB, pertenecen a Influxdata, por lo que la integración entre ambos es totalmente compatible (InfluxData, 2021b).

Todo lo anterior será corriendo en un solo dispositivo de micro computadora Raspberry PI 4 basado en Debian GNU/Linux. (Debian -- The Universal Operating System, 2024).

La integración se llevará a cabo recolectando los eventos a través de Telegraf recolectando los eventos dentro del dispositivo objetivo y realizando el guardado de los mismos en la base de datos especialmente diseñada influxdb para posteriormente utilizar grafana como interfaz gráfica para mostrar los eventos a usuarios creando dashboards personalizados.

A continuación, se presenta mediante un diagrama de red la arquitectura a considerar para nuestro sistema de monitoreo y detección de eventos:

Figura 1. Diagrama de arquitectura. Fuente: Autores.



Materiales por utilizar

- Switch capa 2 (24 puertos cobre)
- Servidor para alojar software prototipo
- Máquina de consulta (endpoint)
- Raspberry PI 4 o superior
- F5 virtual o físico (es posible considerar cualquier dispositivo compatible)
- Dos discos duros (1TB) RAID 0

Relevancia del proyecto de investigación

Contar con un sistema de monitoreo de dispositivos de red y monitoreo de eventos para detección de intrusos es crucial en el panorama actual de ciberseguridad por varias razones:

Detección temprana de intrusiones: Estos sistemas pueden identificar actividades sospechosas o maliciosas en tiempo real, lo que permite a los equipos de seguridad responder de manera rápida y mitigar posibles brechas de seguridad antes de que causen un daño significativo. (¿Qué Es un IPS (Sistema de Prevención de Intrusiones)? | Fortinet, s. f.).

Prevención de pérdida de datos

Al monitorear el tráfico de la red y los eventos en los dispositivos, se pueden detectar intentos de acceso no autorizado o de exfiltración de datos sensibles, lo que ayuda a prevenir la pérdida de información confidencial. (DLP - ¿Qué Es la Prevención de Pérdida de Datos? | Proofpoint ES, 2023).

Análisis de tendencias y patrones

Estos sistemas recopilan datos sobre el comportamiento de la red y de los usuarios, lo que permite identificar tendencias y patrones de actividad que podrían indicar una intrusión o una amenaza potencial. (Análisis de Tendencias y Patrones Actuales del Mercado - FasterCapital, s. f.).

Cumplimiento normativo

Muchas regulaciones y estándares de seguridad, como GDPR, HIPAA y PCI-DSS, requieren la implementación de medidas de monitoreo y detección de intrusos para garantizar la protección de los datos personales y financieros. (Cumplimiento de Normativas - PCI DSS, HIPAA | Trend Micro, s. f.).

Mejora de la postura de seguridad

Al tener visibilidad completa sobre la actividad de la red y los dispositivos, las organizaciones pueden mejorar su postura de seguridad al identificar y remediar vulnerabilidades y puntos débiles en su infraestructura.

Beneficios esperados

Establecer una postura de seguridad avanzada en redes domésticas, empresas pequeñas y medianas con una inversión significativa en comparación con otros sistemas.

Es importante mencionar que el proyecto es escalable por lo que podríamos integrar N cantidad de dispositivos para poder adecuar dependiente las necesidades de cada usuario.

A continuación, se muestras en imagen como se ven los datos representados gráficamente:

Figura 2:Dashboard de datos gráficamente representados

Node Exporter Full | Grafana Labs, s. f.

Para contar con el análisis de eventos de seguridad de la infraestructura, es necesario contar con el proceso de Syslog corriendo dentro de nuestro sistema de Raspberry Pi 4, configurado para poder aceptar conexiones por el puerto 514 protocolo UDP (AIX 7.1, s. f.) de syslog desde cualquier origen que pertenezca al mismo dominio de red.

Mostrándose de la siguiente manera:

Figura 3 Eventos recolectados para detección de eventos de seguridad (Logs).

```
kike — pi@pi: /var/log — ssh pi@192.168.0.101 — 170×48
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + PLUGIN_FILEPATH='/Library/Internet Plug-Ins/JavaAppletPlugin.plugin'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + PREF_PANE_NAME=JavaControlPanel.prefPane
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + PREF_PANE_SRC='/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/deploy/Java
ControlPanel.prefPane'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + PREF_PANE_DEST=/Library/PreferencePanes/
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + APPLICATION_SUPPORT_ORACLE_JAVA='/Library/Application Support/Oracle/Java'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + APPLICATION_SUPPORT_INFO_PLIST='/Library/Application Support/Oracle/Java/Info.plist'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + PLUGIN_ENABLED_INFO_PLIST='/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Enabled.
plist'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + PLUGIN_INFO_PLIST='/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Info.plist'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + APPLICATION_SUPPORT_JAVAWS='/Library/Application Support/Oracle/Java/javaws'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + PLUGIN_JAVAWS='/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/_javaws'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + PLUGIN_JAVAWS_SYMLINK='/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/jav
aws'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + /bin/rm '/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Info.plist'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + /bin/ln -s '/Library/Application Support/Oracle/Java/Info.plist' '/Library/Internet Plug-Ins/Ja
vaAppletPlugin.plugin/Contents/Info.plist'
Apr 22 10:55:37 192.168.0.2 package_script_service[4826]: ./postinstall: + /bin/rm '/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/javaws'
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + /bin/ln -s '/Library/Application Support/Oracle/Java/javaws' '/Library/Internet Plug-Ins/JavaAp
pletPlugin.plugin/Contents/Home/bin/javaws'
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + [[ ! -h /Library/Application Support/Oracle/Java/Info.plist ]]
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + /bin/mkdir -p /Library/PreferencePanes/
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + '[' '!' -h /Library/PreferencePanes//JavaControlPanel.prefPane ']'
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + /bin/ln -s '/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/deploy/JavaCon
trolPanel.prefPane' /Library/PreferencePanes/
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + /usr/sbin/chown -R root:wheel '/Library/Internet Plug-Ins/JavaAppletPlugin.plugin'
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + ./LoadAUDaemons 1.8.411.09
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: Load failed: 5: Input/output error
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: Try running `launchctl bootstrap` as root for richer errors.
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + ./javasettings
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + true
Apr 22 10:55:38 192.168.0.2 javasettings[4863]: No input config file.
Apr 22 10:55:38 192.168.0.2 javasettings[4863]: No input config file.
Apr 22 10:55:38 192.168.0.2 javasettings[4863]: No input config file.
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + JAVA='/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/java'
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + DEPLOY_JAR='/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/deploy.jar'
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + CONFIG_FILE='/Library/Application Support/Oracle/Java/java.settings.cfg'
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + '[' -f install.jar ']'
Apr 22 10:55:38 192.168.0.2 package_script_service[4826]: ./postinstall: + '/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/java' -cp '.:/Library/Int
ernet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/deploy.jar:install.jar' com.oracle.install.InstallOptions -f '/Library/Application Support/Oracle/Java/java.setti
ngs.cfg'
Apr 22 10:55:42 192.168.0.2 package_script_service[4826]: ./postinstall: java.lang.IllegalArgumentException: Invalid argument CFG_FILE: /Library/Application Support/Oracl
e/Java/java.settings.cfg
Apr 22 10:55:42 192.168.0.2 package_script_service[4826]: ./postinstall:       at com.oracle.install.InstallOptions.validateConfigFile(InstallOptions.java:165)
Apr 22 10:55:42 192.168.0.2 package_script_service[4826]: ./postinstall:       at com.oracle.install.InstallOptions.parseArguments(InstallOptions.java:102)
Apr 22 10:55:42 192.168.0.2 package_script_service[4826]: ./postinstall:       at com.oracle.install.InstallOptions.main(InstallOptions.java:46)
Apr 22 10:55:42 192.168.0.2 package_script_service[4826]: ./postinstall: + CONSOLE_USER=root
Apr 22 10:55:42 192.168.0.2 package_script_service[4826]: ./postinstall: + '[' root = root -o -z root ']'
```

Fuente: Autores.

Los resultados de la investigación se centran en lograr la correcta identificación de eventos de seguridad con campos en particular relevantes que podemos obtener, como son:

- Fecha y hora del evento
- Acceso de usuarios
- Cambios dentro de la infraestructura
- Tipo de cambio ejecutado

Con lo anterior se cubre a cabalidad lo buscado, que es tener en vista todos los eventos que a simple vista no nos damos cuenta que están ocurriendo.

Trabajo a futuro

Continuar investigando y monitoreando las tendencias emergentes en ciberseguridad, incluyendo nuevos vectores de ataque, técnicas de evasión de seguridad y amenazas en evolución. Esto podría involucrar la exploración de áreas como el internet de las cosas (IoT) (¿Qué Es IoT? - Explicación del Internet de las Cosas - AWS, s. f.), la inteligencia artificial (¿Qué Es la Inteligencia Artificial o IA? | Google Cloud | Google Cloud, s. f.) aplicada a la seguridad cibernética y la seguridad en la nube.

Trabajar en el desarrollo de tecnologías de seguridad innovadoras que puedan detectar, prevenir y responder a los ataques cibernéticos de manera más eficaz. Esto podría incluir el desarrollo de herramientas de análisis de malware avanzadas, soluciones de autenticación multifactor y sistemas de detección de intrusiones mejorados.

Realizar la integración de nuevas capacidades dentro de nuestro sistema de monitoreo y detección de intrusos integrando un cluster de tarjetas inteligentes Raspberry PI para acortar gastos y poder ofrecer un ambiente con mayores capacidades y robustecer nuestro sistema para poder contar con la mayor compatibilidad, herramientas avanzadas, integración de inteligencia artificial para poder estar a la vanguardia de las tecnologías emergentes.

Contar con un ambiente de respaldo de información más robusto y evitar pérdidas de información considerando integrar nuevos sistemas de repositorio como NAS. (Network Access Storage) (¿Qué Es el Almacenamiento Conectado A la Red (NAS)? | IBM, s. f.).

CONCLUSIONES

El estudio sobre ciberseguridad ha proporcionado una visión integral de las amenazas cibernéticas que enfrentan individuos, organizaciones y la sociedad en general. A través del análisis de diversos vectores de ataque y la evaluación de medidas de mitigación, se han obtenido importantes conclusiones que destacan la necesidad de acciones concretas para fortalecer la seguridad cibernética y proteger contra las amenazas emergentes en el ciberespacio.

Se ha reafirmado la importancia de la concienciación y la capacitación en ciberseguridad tanto para individuos como para organizaciones. La educación del personal y la promoción de buenas prácticas de seguridad son fundamentales para prevenir ataques cibernéticos y mitigar sus impactos.

Se subraya la importancia crítica de la ciberseguridad en la era digital y la necesidad de adoptar un enfoque integral y colaborativo para proteger contra las amenazas cibernéticas. Al abordar los desafíos identificados y tomar medidas proactivas, podemos fortalecer nuestras defensas cibernéticas y salvaguardar la integridad, confidencialidad y disponibilidad de la información en el ciberespacio.

Con lo anterior, ofrecer una herramienta accesible al bolsillo, con componentes actualizados y a la vanguardia podremos estar más cerca de la ciberseguridad obteniendo información donde nuestros ojos no tienen alcance.

La ciberseguridad comienza con el eslabón más débil: los usuarios.

REFERENCIAS BIBLIOGRAFICAS

Análisis de tendencias y patrones actuales del mercado - FasterCapital. (s. f.). FasterCapital. https://fastercapital.com/es/tema/an%C3%A1lisis-de-tendencias-y-patrones-actuales-del-mercado.html

AIX 7.1. (s. f.). https://www.ibm.com/docs/es/aix/7.1?topic=protocols-user-datagram-protocol

Cumplimiento de normativas - PCI DSS, HIPAA | Trend Micro. (s. f.). Trend Micro. https://www.trendmicro.com/es_es/business/capabilities/solutions-for/compliance.html

Debian -- the universal Operating system. (2024, 10 febrero). https://www.debian.org/

DLP - ¿Qué es la prevención de pérdida de datos? | Proofpoint ES. (2023, 21 diciembre). Proofpoint. https://www.proofpoint.com/es/threat-reference/dlp

FortiGuard Labs - Threat intelligence Platform | Fortinet. (s. f.). Fortinet.

https://www.fortinet.com/lat/fortiguard/labs

Grafana Labs. (s. f.). Grafana: The open observability platform | Grafana Labs. https://grafana.com/

InfluxData. (2021, 10 diciembre). InfluxDB: Open-Source Time Series Database | InfluxData. https://www.influxdata.com/

InfluxData. (2021b, diciembre 10). InfluxDB: Open Source Time Series Database | InfluxData. https://www.influxdata.com/time-series-platform/telegraf/

Node Exporter Full | Grafana Labs. (s. f.). Grafana Labs. https://grafana.com/grafana/dashboards/1860-node-exporter-full/

¿Qué es la ciberseguridad? - Explicación de la ciberseguridad - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cybersecurity/

¿Qué es la ciberseguridad? - Soporte técnico de Microsoft. (s. f.). https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390

¿Qué es la inteligencia artificial o IA? | Google Cloud | Google Cloud. (s. f.). Google Cloud. https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419

¿Qué es la seguridad de la información (InfoSec)? | Seguridad de Microsoft. (s. f.). https://www.microsoft.com/es-mx/security/business/security-101/what-is-information-security-infosec

¿Qué es Linux? (s. f.). https://www.redhat.com/es/topics/linux

¿Qué es el almacenamiento conectado a la red (NAS)? | IBM. (s. f.). https://www.ibm.com/mx-es/topics/network-attached-storage

¿Qué es IoT? - Explicación del Internet de las cosas - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/iot/#:~:text=El%20t%C3%A9rmino%20IoT%2C%20o%20Internet,como%20entre%20los%20propios%20dispositivos.

¿Qué es un IPS (Sistema de Prevención de Intrusiones)? | Fortinet. (s. f.). Fortinet.

https://www.fortinet.com/lat/resources/cyberglossary/what-is-an-ips#:~:text=%C2%BFQu%C3%A9%20es%20un%20sistema%20de,y%20actividad%20sospechosa%20o%20maliciosa

Raspberry Pi documentation. (s. f.). https://www.raspberrypi.com/documentation/

(Raspberry Pi Documentation, s. f.)

Santillán, L. F. C. (s. f.). Sistema de Gestión y Capacitación. https://www.educacioncontinua-abm.com.mx/sistema_lms/

Welcome to Python.org. (2024, 8 mayo). Python.org. https://www.python.org/