SOLUCIONES SEGURAS
CYBERSECURITY
MAGAZINE

Edición No. 24

REVISTA REGIONAL DE CIBERSEGURIDAD

MUJERES EN CIBERSEGURIDAD

SUPERANDO LOS ESTEREOTIPOS Y FORTALECIENDO LA SEGURIDAD DIGITAL

Pág 3.

EN ESTA EDICIÓN:

2024
VOLUMEN 1

SOLUCIONES SEGURAS
TRAINING CENTER
SOLUCIONES SEGURAS CYBERSECURITY REGIONAL TOUR
SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE

SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE

CONTENIDO

Randol Chen
Soluciones Seguras
Editor de la Revista SS CSM

SOLUCIONES SEGURAS
Empresas Protegidas, Empresas Tranquilas

PALABRAS DE EDICIÓN

Hola a todos,

Es un gusto dirigirme a ustedes en esta nueva edición de nuestro Cibersecurity Magazine, que nuestro editor y nuestros ingenieros se esmeran mucho por hacerles llegar con temas de mucho interés y relevancia.

Me gustaría poder decir que ya la marea de ataques y vulnerabilidades ha bajado y estamos mucho más tranquilos... pero por supuesto no se puede decir eso 😨. Los ataques siguen, con más frecuencia y más impacto. ¿Qué hacemos entonces?

Prepararnos

Tener nuestras herramientas al día y bien configuradas, tener un plan de respuesta a incidentes y un plan de recuperación de desastres serán la diferencia entre sobrevivir o ahogarse en un ciberataque.

Nuestra industria sigue cambiando. La inteligencia artificial y los nuevos NPU nos permitirán hacer muchas tareas rápidamente que antes no podíamos. También es importante hablar y tomar nota del aporte de todos los géneros a la ciberseguridad, donde más puntos de vista siempre mejora la seguridad final.

Aprovecho también para agradecer a CyberArk, que recientemente nos nombró como el **2023 LATAM Partner of the Year para el Caribe y Centroamérica**. Un gran honor que nos hacen y esperamos seguir creciendo la relación que tenemos con ellos.

El 2024 nos ha recibido con muchos eventos: A inicio de año tuvimos nuestro Soluciones Seguras Kickoff 2024, donde casi todos los colaboradores de los diferentes países participamos en 3 días muy reinvigorantes en Cancún, alistándonos para el 2024. También participamos en Febrero del Radware Latam Summit, con una delegación de 15 personas a Bogotá, en el Check Point Experience 2024, con una delegación de 22 personas a Las Vegas. En el CPX, nuestro cliente **Elcatex** fue reconocido como el **Most Innovative Customer Project of the Year**, un excelente reconocimiento a ellos por su visión holística de ciberseguridad, en la que nos ayudaron a implementar un ecosistema completo basado en Check Point Infinity.

También participamos del evento Inspire de TD Synnex en Cancún, y esperamos participar del RSA Conference en San Francisco y del CyberArk Impact en Nashville. También esperamos verlos a ustedes en los diferentes Tech Day e Infosecurity que se darán en Panamá, Costa Rica, Guatemala El Salvador y Honduras, donde participaremos para compartir con ustedes experiencias y proyectos.
¡Y eso es solo en la primera mitad del año!

¡Les deseo lo mejor, que tengan éxito y ciberseguridad en todos sus proyectos, y como siempre, seguimos a sus órdenes!

¡Saludos!

Eli Faskha
CEO

MUJERES EN CIBERSEGURIDAD:
SUPERANDO LOS ESTEREOTIPOS Y FORTALECIENDO LA SEGURIDAD DIGITAL

En un mundo cada vez más dependiente de la tecnología, la ciberseguridad se ha convertido en un aspecto fundamental para proteger nuestros datos, identidades y sistemas. Sin embargo, este campo ha sido tradicionalmente dominado por hombres, lo que ha perpetuado estereotipos de género y ha creado barreras para la participación activa de las mujeres. Pero ¿qué sucede cuando las mujeres irrumpen en este terreno? La respuesta es clara: empoderamiento, reducción de la brecha de género y un fortalecimiento significativo de la seguridad digital.

Empoderamiento y Reducción de la Brecha de Género

La presencia de mujeres en el ámbito de la ciberseguridad no solo representa un paso crucial hacia la igualdad de género, sino que también enriquece de manera significativa el panorama de la seguridad digital. Las mujeres aportan perspectivas únicas y una diversidad de enfoques que son esenciales para abordar la complejidad de las amenazas cibernéticas en la era digital. Su inclusión no solo rompe con los estereotipos arraigados sobre roles de género en la tecnología, sino que también desafía la noción de que ciertas habilidades están inherentemente ligadas a un género específico.

Además, la participación activa de las mujeres en ciberseguridad sirve como un catalizador para reducir la brecha de género en la industria tecnológica en su conjunto.

Al ver a mujeres líderes y expertas en ciberseguridad, se envía un mensaje poderoso a las generaciones futuras, inspirándolas a seguir carreras afines y desafiando la percepción de que estos roles son exclusivamente masculinos. Esta diversidad de género no solo es esencial para la representación equitativa en el lugar de trabajo, sino que también es fundamental para garantizar que las soluciones de seguridad digital sean inclusivas y consideren una amplia gama de perspectivas y experiencias.

En última instancia, el empoderamiento de las mujeres en ciberseguridad no solo fortalece la seguridad digital en sí misma, sino que también contribuye a un cambio cultural más amplio hacia la igualdad de género en la sociedad. Al desafiar los estereotipos de género y crear oportunidades equitativas en la ciberseguridad, estamos construyendo un futuro más justo, seguro y diverso para todos.

Rompiendo Barreras y Creando Oportunidades

La inclusión de mujeres en roles de liderazgo y técnicos en el campo de la ciberseguridad no solo representa un avance hacia la igualdad de oportunidades, sino que también desencadena una serie de beneficios tangibles para la industria en su conjunto. La diversidad de género en estos roles no solo enriquece la perspectiva de las soluciones de seguridad digital, sino que también fomenta un ambiente laboral más colaborativo y creativo. Al romper las barreras de género, se amplía el acceso a oportunidades de crecimiento profesional y se abre la puerta a una mayor innovación, ya que se aprovechan al máximo las diversas experiencias y habilidades que cada individuo, independientemente de su género, aporta al equipo.

Además, la presencia de mujeres en roles de liderazgo en ciberseguridad también desempeña un papel crucial en la creación de modelos a seguir para las generaciones futuras. Al ver a mujeres ocupando posiciones destacadas en la industria, las jóvenes son inspiradas a perseguir sus aspiraciones profesionales sin verse limitadas por estereotipos de género obsoletos. Esta representación

diversa no solo impulsa la innovación en la seguridad digital, sino que también contribuye a la construcción de una cultura laboral más inclusiva y equitativa para las generaciones venideras.

Ventajas

Alianza para el Futuro de la Seguridad Digital

La colaboración entre hombres y mujeres en ciberseguridad es fundamental para enfrentar los desafíos digitales del futuro. Esta alianza fortalece la protección de la información y la privacidad en línea, garantizando un entorno digital más seguro y confiable para todos.

Fuerza Imparable en la Protección de la Información Digital

Las mujeres en ciberseguridad son una fuerza imparable en la protección de la información digital. Su compromiso, habilidades técnicas y capacidad para pensar de manera innovadora las convierten en activos inestimables en la lucha contra las amenazas cibernéticas.

Empodera la Resiliencia de la Industria de la Ciberseguridad

La participación activa de las mujeres en ciberseguridad representa una oportunidad única para promover la diversidad y la inclusión en la industria. Al fomentar un entorno laboral donde todas las voces son escuchadas y valoradas, se construyen equipos más fuertes y resilientes capaces de enfrentar los desafíos del mundo digital actual.

Lucha Conjunta para Reducir la Brecha de Género

La reducción de la brecha de género en la industria de la seguridad digital es una responsabilidad compartida. Al trabajar juntos para eliminar los obstáculos y crear oportunidades equitativas, podemos construir un futuro donde la igualdad de género sea la norma, no la excepción.

Alianza para la Protección de la Privacidad y la Seguridad Digital

La colaboración entre hombres y mujeres en ciberseguridad es fundamental para proteger la privacidad y la seguridad digital. Al unir fuerzas, podemos desarrollar soluciones más completas y sofisticadas que aborden las complejas amenazas que enfrentamos en el mundo digital.

De hecho, en Soluciones Seguras contamos con una considerable participación de la mujer en ciberseguridad, con 12 mujeres dentro de nuestro equipo de soporte técnico. Esta diversidad en nuestra fuerza laboral no solo demuestra nuestro compromiso con la igualdad de género, sino que también nos brinda la voz de la experiencia para resaltar la importancia y las ventajas de incluir a la mujer en el ámbito de la ciberseguridad.

En resumen, la participación activa de las mujeres en ciberseguridad no solo es una cuestión de justicia y equidad, sino también de eficacia y seguridad. Al romper con los estereotipos de género y crear entornos laborales más inclusivos, estamos fortaleciendo la seguridad digital para todos y construyendo un futuro más seguro y confiable en línea.

Randol Chen
Editor de la Revista
Soluciones Seguras Panamá

SOLUCIONES SEGURAS RECONOCIDA COMO SOCIO DEL AÑO 2023 DE CYBERARK EN CENTROAMÉRICA Y EL CARIBE

Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica, se enorgullece en anunciar que ha sido galardonada con el prestigioso premio "LATAM 2023 - Partner of the Year, Caribbean and Central America" por nuestro partner Cyberark, líder mundial en seguridad de la identidad y gestión de acceso.

Este reconocimiento refleja el arduo trabajo y la dedicación de todo nuestro equipo en Soluciones Seguras. Queremos expresar nuestro sincero agradecimiento a Cyberark por este honor y por su continua colaboración y apoyo. Este premio no habría sido posible sin la confianza y el compromiso de nuestros colaboradores, cuya pasión y esfuerzo son fundamentales para nuestro éxito.

Además, queremos extender nuestro más profundo agradecimiento a nuestros valiosos clientes, cuya confianza en nuestros servicios y soluciones nos impulsa a seguir innovando y ofreciendo lo mejor en seguridad cibernética. En Soluciones Seguras, nuestra misión es clara: brindarle a nuestros clientes tranquilidad a través de asesoría y las mejores soluciones de ciberseguridad en la región.

Nuestro lema, "empresas protegidas, empresas tranquilas", refleja nuestro compromiso inquebrantable de proporcionar a nuestros clientes la tranquilidad que necesitan para centrarse en sus operaciones comerciales sin preocupaciones por la seguridad de sus datos y sistemas.

Estamos emocionados por este reconocimiento y comprometidos a seguir siendo líderes en el campo de la ciberseguridad en Centroamérica y el Caribe. Continuaremos trabajando en estrecha colaboración con Cyberark y nuestros clientes para brindar soluciones innovadoras y efectivas que protejan los activos más críticos de sus organizaciones.

UN PROMETEDOR INICIO 2024

El año 2024 comenzó con un espíritu de entusiasmo y determinación en Soluciones Seguras, compañía líder en ciberseguridad en Centroamérica. Del 5 al 8 de enero, los colaboradores de toda la organización regional se reunieron en Cancún, México, para el evento Soluciones Seguras Kick-Off 2024. Fue una experiencia enriquecedora que no solo reconoció los logros del pasado, sino que también trazó el camino hacia un futuro emocionante y comprometido con nuestros clientes.

Revisión de Metas y Objetivos Logrados

Uno de los aspectos destacados del Kick-Off 2024 fue la oportunidad de revisar y celebrar los logros del año anterior. Se reconoció el arduo trabajo y dedicación de los colaboradores que contribuyeron al éxito de la empresa en el 2023. Durante el evento, se llevaron a cabo ceremonias de reconocimiento para homenajear a los colaboradores que se destacaron por su compromiso, antigüedad, creatividad y excelencia en sus funciones.

Estos reconocimientos no solo son un testimonio de la dedicación de nuestros empleados, sino que también inspiran a todos a superar sus límites y alcanzar nuevos niveles de excelencia.

Alineamiento de Objetivos para el 2024

El evento Soluciones Seguras Kick-Off 2024 también sirvió como plataforma para establecer las metas y objetivos para el nuevo año. Se llevaron a cabo sesiones de trabajo en grupo y presentaciones estratégicas que permitieron a todos los empleados comprender la visión de la empresa para el 2024. La alineación de objetivos garantiza que todos estemos enfocados en la misma dirección y trabajemos juntos hacia un objetivo común.

Fortalecimiento de la Sinergia Internacional

Después de las sesiones de trabajo, se asignó tiempo para el esparcimiento y la interacción entre los colaboradores de diferentes países. Este momento de integración fue invaluable, ya que permitió que los equipos se conocieran mejor, compartieran experiencias y crearan lazos más estrechos. Esta interacción transfronteriza no solo refuerza la sinergia entre países, sino que también enriquece nuestra capacidad para brindar un servicio de ciberseguridad global excepcional.

Compromiso con Nuestros Clientes

Uno de los pilares fundamentales de Soluciones Seguras es el compromiso con la satisfacción y seguridad de nuestros clientes. Durante el evento, se reafirmó nuestro compromiso de proporcionar soluciones de ciberseguridad de alta calidad y un servicio de soporte excepcional. Se anunciaron iniciativas para fortalecer aún más nuestras relaciones con los clientes y brindarles la confianza y la protección que merecen.

En Conclusión

El evento Soluciones Seguras Kick-Off 2024 en Cancún marcó el comienzo de un año prometedor para Soluciones Seguras. Con un equipo unido, objetivos claros, una sinergia internacional fortalecida y un compromiso inquebrantable con nuestros clientes, estamos preparados para alcanzar nuevas alturas en el campo de la ciberseguridad. Nuestra pasión por la seguridad cibernética y nuestra dedicación a la excelencia nos impulsarán a superar los desafíos que se presenten en el 2024 y más allá. Juntos, construiremos un futuro más seguro para nuestros clientes y la sociedad en general.

IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN LA VIDA DE LAS PERSONAS: LAPTOPS Y CELULARES CON UNIDAD DE PROCESAMIENTO NEURONAL INTEGRADO (NPU)

En la última década, la inteligencia artificial (IA) ha dejado de ser una promesa futurista para convertirse en una realidad palpable, integrándose en el tejido de nuestra vida cotidiana. Una de las innovaciones más recientes en este ámbito es la incorporación de Unidades de Procesamiento Neuronal (NPU, por sus siglas en inglés) en dispositivos móviles y laptops de consumo personal. Esta tecnología no solo ha revolucionado la forma en que interactuamos con nuestros dispositivos, sino que también ha presentado nuevos desafíos y oportunidades en el campo de la ciberseguridad.

Para proporcionar un marco más claro, es importante entender que históricamente, los ordenadores —incluyendo dispositivos móviles, portátiles, de escritorio y servidores— han estado equipados principalmente con CPU (Unidad de Procesamiento Central) y GPU (Unidad de Procesamiento Gráfico). Tradicionalmente, las GPU, aunque originalmente diseñadas para optimizar el procesamiento de gráficos, han sido adaptadas para emular redes neuronales, sentando las bases para el desarrollo de las inteligencias artificiales que conocemos hoy en día. Sin embargo, a pesar de su utilidad, las GPUs no están especializadas en el manejo de redes neuronales. Reconociendo esta limitación, ha surgido una innovación tecnológica significativa: la Unidad de Procesamiento Neuronal (NPU). Esta unidad está específicamente diseñada para manejar redes neuronales, optimizando así el procesamiento de tareas de inteligencia artificial directamente en los dispositivos del usuario.

La NPU y su Impacto en la Experiencia del Usuario

Las NPUs son circuitos integrados especializados diseñados para ejecutar algoritmos de IA de manera eficiente, lo que permite a los dispositivos móviles y laptops procesar tareas relacionadas con la IA directamente en el dispositivo, en lugar de depender de la nube. Esto se traduce en mejoras significativas en velocidad, eficiencia energética y privacidad, ya que los datos sensibles pueden procesarse localmente sin necesidad de enviarlos a servidores remotos.

Ciberseguridad en la Era de las NPUs

Mientras que las NPUs ofrecen ventajas significativas, también introducen nuevos vectores de ataque y desafíos para la ciberseguridad. La capacidad de procesar datos sensibles localmente puede ser una espada de doble filo; si bien mejora la privacidad al reducir la necesidad de transmitir datos a la nube, también significa que un dispositivo comprometido podría permitir a un atacante acceder a información altamente sensible procesada por la NPU.

Además, la IA en sí misma puede ser objeto de manipulación. Los ataques de envenenamiento de datos, por ejemplo, en los que los atacantes introducen datos malintencionados para entrenar maliciosamente modelos de IA, pueden ser particularmente preocupantes en dispositivos con NPUs. Esto podría llevar a que la IA actúe de manera no deseada, comprometiendo la seguridad y privacidad del usuario.
Por otro lado, la integración de NPUs también abre nuevas avenidas para fortalecer la ciberseguridad. Las capacidades avanzadas de procesamiento permiten implementar algoritmos de IA más sofisticados para detectar y prevenir amenazas en tiempo real, directamente en el dispositivo. Esto incluye la detección de malware, análisis de comportamiento para identificar patrones sospechosos y la autenticación biométrica avanzada, ofreciendo un nivel de protección personalizado y altamente eficiente.

Desafíos Regulatorios y Éticos

La incorporación de IA y NPUs en dispositivos cotidianos también plantea importantes consideraciones éticas y regulatorias. La capacidad de estos dispositivos para procesar y almacenar grandes cantidades de datos personales exige un marco regulatorio robusto que garantice la protección de la privacidad del usuario. Además, la transparencia en el funcionamiento de los algoritmos de IA es crucial para evitar sesgos y garantizar que los beneficios de esta tecnología sean accesibles para todos.

En resumen, la integración de Unidades de Procesamiento Neuronal en dispositivos personales como laptops y celulares está remodelando nuestra interacción con la tecnología, ofreciendo mejoras significativas en eficiencia, privacidad y experiencia del usuario. Sin embargo, esta innovación también presenta desafíos únicos en el ámbito de la ciberseguridad. A medida que avanzamos hacia una era cada vez más dominada por la IA, es fundamental abordar estos desafíos de manera proactiva, garantizando que la ciberseguridad evolucione al mismo ritmo que la tecnología que busca proteger.

Randol Chen
Editor de la Revista
Soluciones Seguras Panamá

CHECK POINT RESEARCH UNVEILS CRITICAL #MONIKERLINK VULNERABILITY IN MICROSOFT OUTLOOK WITH A 9.8 CVSS SEVERITY SCORE

Recurso: Check Point Blog, Feb, 2024
https://blog.checkpoint.com/research/check-point-research-unveils-critical-monikerlink-vulnerability-in-microsoft-outlook-with-a-9-8-cvss-severity-score/

Key Findings:
– Hyperlink Handling in Outlook: The research demonstrates that "file://" hyperlinks can be manipulated in a certain way which results in a bypass of the Outlook's security measures such as Protected View.
– The Vulnerability's Impact: The #MonikerLink bug allows for a wide and serious impact, varying from leaking of local NTLM credential information to arbitrary code execution. This is due to the misuse of the Component Object Model (COM) on Windows, where Outlook incorrectly parses a specially crafted hyperlink to access COM objects. This process can bypass the Office Protected View, significantly increasing the risk of exploitation for remote code execution without the user's knowledge.
– Microsoft's Acknowledgement and CVSS Severity Score: Microsoft has acknowledged the vulnerability, and the flaw has received a CVSS severity score of 9.8 out of 10, underlining its critical nature.

Recent research by Check Point Research has brought to light a significant security vulnerability in Microsoft Outlook, referred to as the #MonikerLink bug. This flaw, thoroughly detailed on the Check Point Research blog post could allow an attacker to execute arbitrary code on the victim's machine. The #MonikerLink bug specifically exploits the way Outlook processes certain hyperlinks, leading to severe security implications.

It is worth noting that recent CPR's blog "The Obvious, the Normal, and the Advanced: A Comprehensive Analysis of Outlook Attack Vectors," highlights this and other various attack vectors within Outlook, aiming to enhance the industry's awareness of the security risks posed by the popular email application.

Defense and Mitigation:

The vulnerability has been confirmed on the latest Windows and Microsoft Office Outlook, and Check Point has reported the issue to the Microsoft Security Response Center. While awaiting Microsoft's response, Check Point has developed detection and protection mechanisms for its customers, safeguarding them ahead of public disclosure.

Check Point Customers Remain Protected

Check Point has developed various protections for our customers as soon as we discovered the security vulnerability internally, Check Point customers were protected many months ahead of this disclosure time. The protections are:

Check Point Email Security has deployed protection for customers since October 25, 2023.
Check Point IPS developed and deployed a signature named "Microsoft Outlook Malicious Moniker Link Remote Code Execution (CVE-2024-21413)" to detect and protect against this vulnerability, released on November 15, 2023.
Check Point Research continues to monitor the activities for potential attacks exploiting this bug/attacker vector in the wild through our telemetry data.

The Bigger Picture:

The #MonikerLink bug underscores a broader security risk associated with the use of unsafe APIs, such as MkParseDisplayName/ MkParseDisplayNameEx, potentially affecting not only Outlook but other software that uses these APIs insecurely. The discovery of this bug in Outlook serves as a call to action for the security and developer communities to identify and rectify similar vulnerabilities in other applications, ensuring the safety of the Windows/COM ecosystem.

The #MonikerLink vulnerability discovered in Microsoft Outlook by Check Point Research highlights a significant security flaw that could have profound implications if exploited. This vulnerability stems from the way Outlook processes specially crafted hyperlinks that utilize the "file://" protocol, followed by a specific path, an exclamation mark, and additional arbitrary characters. Unlike standard hyperlinks that prompt security warnings or error messages when deemed unsafe, these manipulated hyperlinks bypass Outlook's existing security mechanisms, leading to two primary concerns: the leakage of local NTLM credentials and the potential for arbitrary code execution.

Leakage of Local NTLM Credentials

The vulnerability allows for the leakage of local NTLM credential information, a critical security issue. NTLM (NT LAN Manager) is a suite of Microsoft security protocols intended to provide authentication, integrity, and confidentiality to users. When a user clicks on a malicious hyperlink crafted to exploit the #MonikerLink bug, it initiates a connection using the SMB (Server Message Block) protocol to a remote server controlled by the attacker. This process inadvertently sends the user's NTLM credentials to the attacker's server, compromising the user's authentication details without their knowledge. Such information can be used for further attacks, including accessing restricted areas of a network or executing privileged operations under the guise of the compromised user.

Potential for Arbitrary Code Execution

More alarmingly, the #MonikerLink bug opens the door for arbitrary code execution on the victim's system. This aspect of the vulnerability takes advantage of the Component Object Model (COM) in Windows. By misleading Outlook into processing the malicious hyperlink as a "Moniker Link," attackers can invoke COM objects and execute code on the victim's machine remotely. This process does not involve the Protected View mode in Office applications, which is typically a security measure to prevent potentially harmful documents from executing code without user consent. As a result, attackers can bypass this protective layer, running malicious code at the Medium integrity level, which could lead to full system compromise. It should be noted that Microsoft themselves call this issue a Remote Code Execution and gives it the highest possible rating of 'critical'.

Read full article at
blog.checkpoint.com

SOLUCIONES SEGURAS EN LAS NOTICIAS

EL PERIÓDICO CR: CIBERSEGURIDAD: LA ASIGNATURA QUE SE APRENDE DESDE CASA

EL PERIODICOCR

EL CAPITAL FINANCIERO: SOLUCIONES SEGURAS BRINDA RECOMENDACIONES PARA INICIAR EL 2024 PROTEGIENDO SU INFORMACIÓN

El Capital Financiero

TELEMETRO: AUMENTAN LOS CIBERATAQUES, UN 20% SE GENERAN EN PANAMÁ

telemetro.com

INTERCENTRO: CIBERSEGURIDAD: LA ASIGNATURA QUE SE APRENDE DESDE CASA

Intercentro

LA REPÚBLICA: 5 CONSEJOS PARA QUE NO SEA VICTIMA DE LOS HACKERS ESTE 2024

SOLUCIONES PARA PROFESIONALES LA REPUBLICA.net

DIARIO DE CENTROAMÉRICA: DEFINEN PRINCIPALES RETOS DE CIBERSEGURIDAD PARA 2024

Diario de Centro América

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

INFORME AÉREO: PROTEJA LOS DATOS EN SUS DISPOSITIVOS ELECTRÓNICOS MIENTRAS DISFRUTA DEL CARNAVAL

INFORME AÉREO

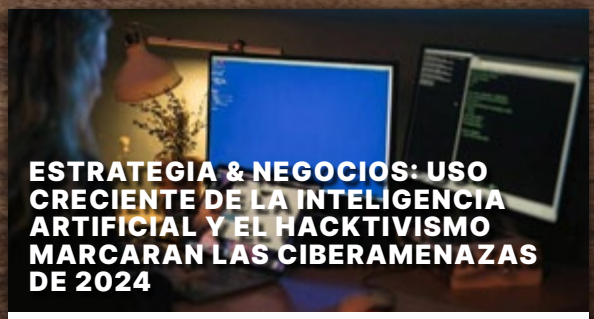
PRENSA LIBRE: 4 DE CADA 10 ATAQUES CIBERNÉTICOS EN GUATEMALA HAN SIDO CONTRA EMPRESAS EN 2023

PRENSA LIBRE

Periódico líder de Guatemala

TICO URBANO: COSTA RICA TIENE UN PROMEDIO DE 819 CIBERATAQUES POR SEMANA

TICO URBANO



ESTRATEGIA & NEGOCIOS: USO CRECIENTE DE LA INTELIGENCIA ARTIFICIAL Y EL HACKTIVISMO MARCARAN LAS CIBERAMENAZAS DE 2024

E&N

LA PRENSA: MARTES FINANCIERO: CÓMO MANTENER UN INTERNET SEGURO EN EL HOGAR

MARTES FINANCIERO

LA REVISTA FINANCIERA DE PANAMÁ

IT NOW: TENDENCIAS DE CIBERSEGURIDAD PARA 2024: DESAFÍOS EMERGENTES Y ESTRATEGIAS DE DEFENSA

IT NOW

INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD: ¿UN FUTURO PROMETEDOR O UN NUEVO DESAFÍO?

El avance tecnológico ha sido una constante en la sociedad moderna, trayendo consigo un sinfín de beneficios, pero también nuevos desafíos. Uno de los campos más impactados por estas innovaciones es la ciberseguridad, donde la inteligencia artificial (IA) se está posicionando como una herramienta fundamental. Este artículo explorará cómo la IA está cambiando el panorama de la ciberseguridad, abordando tanto sus promesas como los desafíos que presenta.

El Impacto de la Inteligencia Artificial en la Ciberseguridad

La IA ha revolucionado la forma en que las organizaciones abordan la ciberseguridad. Su capacidad para aprender de grandes volúmenes de datos y detectar patrones hace posible identificar y neutralizar amenazas de manera más eficiente que los métodos tradicionales. Esto ha permitido una mejora significativa en la Detección y Respuesta a Ataques, ya que los sistemas basados en IA pueden analizar rápidamente grandes conjuntos de datos para identificar comportamientos sospechosos y responder a ellos en tiempo real.

Prevención de Ataques Cibernéticos

La prevención es un aspecto crucial de la ciberseguridad. La IA contribuye en este frente al permitir a las organizaciones anticiparse a los ataques antes de que ocurran. Mediante el análisis predictivo, los sistemas de IA pueden identificar vulnerabilidades potenciales y sugerir medidas correctivas, lo que representa un cambio paradigmático de una postura reactiva a una proactiva en la ciberseguridad.

Gestión del Riesgo y la Resiliencia

La resiliencia se ha convertido en un objetivo clave para las organizaciones que buscan mantenerse a flote ante las crecientes amenazas cibernéticas. La IA juega un papel crucial en la Gestión del Riesgo y la Resiliencia, ayudando a las empresas a entender mejor sus riesgos cibernéticos y a desarrollar estrategias más robustas para resistir y recuperarse de los ataques.

Protección de la Identidad Digital y la Privacidad

En un mundo cada vez más digitalizado, la protección de la identidad digital y la privacidad es fundamental. La IA ofrece soluciones avanzadas para autenticar la identidad de los usuarios de manera segura y proteger su información personal. Esto es esencial para prevenir el robo de identidad y garantizar la confidencialidad de la información sensible.

Prevención y Respuesta a Ataques Cibernéticos en la Nube

Con la adopción masiva de la computación en la nube, la seguridad de estos entornos se ha vuelto crítica. La IA facilita la Prevención y Respuesta a Ataques Cibernéticos en la Nube, proporcionando herramientas que pueden adaptarse y escalar según las necesidades de seguridad específicas de los entornos en la nube.

Pero la inteligencia artificial se ha convertido en un arma de doble filo...

¿UN FUTURO PROMETEDOR O UN NUEVO DESAFÍO?

En la carrera hacia la digitalización, la inteligencia artificial se ha convertido en un doble filo. Mientras sus promesas en el campo de la ciberseguridad son indiscutibles, los riesgos y desafíos que introduce no pueden ser ignorados. La misma tecnología que promete defender nuestras infraestructuras digitales también puede ser armada por ciberdelincuentes, creando un juego del gato y el ratón en el ciberespacio. Este equilibrio precario entre beneficio y riesgo plantea una pregunta inquietante:

¿Estamos preparados para los desafíos que la IA trae consigo?

La posibilidad de que la IA sea utilizada para desarrollar ataques cibernéticos más sofisticados es una realidad que ya estamos comenzando a ver. Los ciberdelincuentes, armados con herramientas de IA, pueden automatizar la creación de malware y phishing, personalizando ataques a una escala y con una precisión sin precedentes. Esto no solo aumenta el volumen de amenazas, sino que también mejora su eficacia, desafiando las defensas tradicionales de la ciberseguridad y exigiendo nuevas estrategias de protección.

Además, la dependencia de la IA en la ciberseguridad plantea interrogantes sobre la privacidad y la seguridad de los datos. Los sistemas de IA requieren acceso a enormes volúmenes de información para aprender y adaptarse. Esta necesidad abre nuevas avenidas para la explotación de datos, donde incluso una brecha de seguridad menor podría resultar en la exposición de información sensible a actores maliciosos. La pregunta sobre cómo equilibrar la eficacia de la IA con la protección de la privacidad de los usuarios se convierte en un dilema central.

Otro desafío significativo es la creación de sistemas de IA resilientes y seguros. A medida que la IA se integra más profundamente en los sistemas de ciberseguridad, la necesidad de asegurar que estos sistemas sean inmunes a la manipulación y capaces de operar incluso bajo ataque se vuelve crítica. La posibilidad de que la IA sea engañada o comprometida por técnicas de adversarios, como los ataques de envenenamiento de datos, subraya la importancia de desarrollar IA robusta y segura, capaz de resistir los intentos de explotación.

Estos desafíos destacan una realidad compleja: mientras que la IA ofrece herramientas poderosas para mejorar la ciberseguridad, también introduce vulnerabilidades que podrían ser explotadas. La clave para navegar este futuro incierto será la capacidad de adaptarse rápidamente, desarrollar defensas que puedan evolucionar al mismo ritmo que las amenazas y establecer marcos éticos y legales que guíen el uso responsable de la IA. Solo así podremos aprovechar plenamente el potencial de la IA para protegernos en el ciberespacio, sin caer en las trampas que nos tiende.

Resumiendo, al contemplar el vasto paisaje que la inteligencia artificial promete remodelar dentro de la ciberseguridad, nos encontramos en la encrucijada de "¿Un Futuro Prometedor o Un Nuevo Desafío?". A medida que avanzamos, la balanza se inclina precariamente entre el optimismo y la cautela, reflejando una era de transformación sin precedentes. La IA, con su inmenso potencial para proteger nuestros mundos digitales, también porta consigo semillas de desafíos inéditos que podrían florecer en amenazas complejas.

Nos hallamos apenas en las etapas tempranas de comprender y navegar por este nuevo dominio, lo que nos deja ante un futuro repleto de posibilidades tan prometedoras como inciertas. En esta aurora de la era digital, la pregunta permanece abierta, invitándonos a reflexionar profundamente sobre el papel que deseamos que la IA juegue en nuestras vidas y cómo podemos moldear este futuro para asegurar que sus promesas superen a sus desafíos. La incertidumbre del impacto de la IA en nuestras vidas subraya la importancia de proceder con precaución, inteligencia y un compromiso inquebrantable con la seguridad y la ética, mientras navegamos por este territorio desconocido juntos.

Randol Chen
Editor de la Revista
Soluciones Seguras Panamá

CYREBRO BLOG: CÓMO PREPARARSE CON ÉXITO PARA UNA AUDITORÍA DE CIBERSEGURIDAD

Recurso: Cyrebro Blog, Feb, 2024
https://www.cyrebro.io/es/blog/como-prepararse-con-exito-para-una-auditoria-de-ciberseguridad/

La Ley Dodd-Frank para la Reforma de Wall Street y la Protección al Consumidor, aprobada en 2010, exigía a la Reserva Federal de los Estados Unidos que realizara pruebas de estrés anuales a los bancos con un volumen mínimo de activos. Los directivos de estos bancos se toman muy en serio estas auditorías de estrés y dedican amplios recursos y esfuerzos a prepararse para estas inspecciones. Esto incluye sus propias evaluaciones internas de riesgos para identificar posibles vulnerabilidades.

Aunque no sea a la misma escala, muchas empresas deben someterse periódicamente a auditorías de ciberseguridad. Estas auditorías son pruebas de estrés esenciales para determinar si una organización es capaz de hacer frente a los ataques dirigidos contra las vulnerabilidades más comunes. En algunos casos, una auditoría puede descubrir una amenaza grave, como una puerta trasera. Al igual que ocurre con las auditorías bancarias, no superarlas tiene graves repercusiones. Eso significa que es fundamental una preparación absoluta y eso requiere una estrategia.

Realización de una auditoría preliminar

Seamos realistas, la única manera de asegurarse de que su empresa está preparada para una auditoría es una auditoría real. Una auditoría preliminar examina las superficies de ataque de su hardware y software y revisa las políticas y controles de seguridad para protegerlos. El primer paso es determinar qué tipo de auditoría necesita realizar, porque no todas las auditorías son iguales. Por ejemplo, una auditoría recurrente mensual incluiría sólo aspectos básicos como:

- Garantizar que todos los sistemas y aplicaciones estén totalmente parcheados y actualizados.
- Revisar al personal y sus responsabilidades asignadas.
- Asegurarse de que todas las bases de datos y repositorios de datos están debidamente protegidos.

Si nunca ha realizado una auditoría preliminar o ha transcurrido mucho tiempo desde la última, deberá incluir pasos adicionales como:

- Realizar una evaluación de riesgos para identificar los riesgos a los que se enfrenta su organización.
- Realizar un inventario de todos los dispositivos y aplicaciones de software conectados a la red.
- Identificar y clasificar todos los datos alojados a través de su red para comprender qué datos necesitan ser priorizados en términos de seguridad.
- Realizar un análisis de deficiencias para comparar sus políticas de seguridad actuales con los mejores estándares del sector, como NIST, CIS Controls o ISO 27001.

Una auditoría posterior a una brecha de seguridad a menudo requiere herramientas de seguridad avanzadas que puedan hacer una prueba exhaustiva de la postura de seguridad de su empresa. Los conjuntos de herramientas también vienen determinados por requisitos normativos específicos. Por ejemplo, las empresas que deben cumplir la normativa PCI DSS están obligadas a realizar evaluaciones trimestrales de vulnerabilidad y una prueba de penetración anual.

Auditorías internas o externas

Una vez que haya determinado el tipo de auditoría que necesita realizar, debe decidir si puede llevarla a cabo adecuadamente de forma interna o si necesita recurrir a especialistas externos. Si su empresa opera en un entorno de bajo riesgo y dispone de personal informático interno con los conocimientos adecuados, una auditoría interna le resultará menos costosa y le dará más control sobre el proceso.

Prepararse para la realidad

Ahora que ya ha realizado una prueba para prepararse, llega el día del encuentro. Lo más probable es que quiera complacerles en todo lo posible y agilizar el proceso. Le gustaría saber lo que quieren averiguar antes de su visita para tener todos los documentos necesarios a su disposición. Del mismo modo, es una buena idea tenerlo todo preparado para una auditoría real.

Confirme con antelación el alcance del proyecto con el auditor. Esto es especialmente útil si va a contratar a un equipo de auditores externos para evitar que el proyecto se desvíe y contener los costes. Saber de antemano qué partes de la red examinarán los auditores y qué tipo de documentación necesitarán le permitirá estar mejor preparado para facilitar información y responder a las preguntas. Averigüe qué personal, en su caso, debe estar disponible para las entrevistas.

Organice sus políticas de ciberseguridad en un documento único que pueda presentar al auditor. Este documento debe incluir la política de contraseñas, la política de seguridad de la información, las restricciones de cuentas de usuario, las políticas de control de acceso, las políticas de uso de Internet y las políticas BYOD. Asegúrese de incluir una copia completa de su plan de respuesta a incidentes, ya que es de vital importancia. Tenga sus archivos de registro y copias de seguridad organizados y fácilmente accesibles, ya que el auditor los solicitará en algún momento.

La importancia de un SOC

Estar totalmente preparado para una auditoría también reducirá el estrés de todo el proceso y le permitirá estar menos nervioso en la siguiente. Las PYMES que utilizan un centro de operaciones de seguridad (SOC) conocen la mayor confianza que puede aportar un equipo de seguridad SOC antes de una auditoría. Dado que un equipo SOC supervisa y analiza su red 24 horas al día, 7 días a la semana, conoce su red mejor que la mayoría. Su trabajo consiste en eliminar las vulnerabilidades detectadas y las vías de ataque aprovechables, su red ya estará segura antes de la auditoría. También podrán ayudarle a facilitar cualquier dato que requiera un auditor de cumplimiento de seguridad, facilitándole así el trabajo preparatorio.

NAVIGATING THE FUTURE: RADWARE CUSTOMERS CALL OUT 2024 CYBERSECURITY TRENDS

Recurso: Radware Blog, Feb, 2024
https://www.radware.com/blog/customers/2024/02/navigating-the-future-radware-customers-call-out-2024-cybersecurity-trends/

As we embark on the journey through 2024, the digital realm continues to evolve at a rapid pace, shaping a landscape where security challenges abound. In this ever-changing world, knowledge is your most potent ally. That is why we invite you to join us in uncovering the insights and predictions from the front lines of cybersecurity—insights brought to you by none other than our knowledgeable Radware Link members. From the pitfalls of ransomware to the rise of artificial intelligence, these predictions paint a vivid portrait of what to expect in 2024.

2023 to 2024: What a Difference a Year Makes

Let us look at the hottest topics for the new year, starting with a quick 2023 recap for each before turning to our exclusive customer insight.

Automation and AI Maturation

In 2023, the acceleration in technological advancements was undeniable. With the ever-growing complexity of cyberthreats, organizations sought efficiency. It is no wonder automation started making waves as a viable solution.

Diego Del Portillo, Informatics Infrastructure Analyst at PUERTO DE BARRANQUILLA, anticipates the significance of AI automation in 2024:

"With the acceleration in technology and the scarcity of cybersecurity personnel, 2024 will focus on automation, accompanied by AI. While AI holds a promise, entrusting tasks to it poses challenges. Implementing it cautiously is crucial, but undoubtedly, it's a technology that should be implemented quickly."

Ransomware Resilience

In 2023, cybercriminals targeted corporations with a vengeance, exploiting vulnerabilities and demanding ransoms. The need for robust backup solutions and employee training became increasingly evident.

Horacio Quiteno, Information Security Specialist at LIFEMILES, shares insights on how threat resilience will evolve in 2024:

"Cybercriminals will target critical infrastructure, making robust backup solutions, employee training, and vulnerability assessments paramount. AI will play a prominent role in cyberattacks, demanding cybersecurity professionals stay one step ahead. Addressing IoT vulnerabilities is essential, with a call for manufacturers and consumers to prioritize security features, firmware updates, and robust authentication mechanisms."

AI's Growing Role in Cybersecurity

Throughout 2023, the integration of AI with cybersecurity operations gained momentum. AI-driven tools proved crucial in identifying and mitigating threats.

Rajesh Garg, EVP & Chief Digital Officer at YOTTA INFRASTRUCTURE SOLUTIONS LLP, envisions the integration of AI with compliance efforts in 2024:

"Huge surge in cyber insurance across enterprises will be visible. AI and ML (Machine Learning) will promise to streamline compliance efforts in organizations. Integrating AI with SOC services will be a cybersecurity imperative to manage new and increasingly complex threats."

Evolving Cyberthreats and Regulations

The cyberthreat landscape evolved rapidly in 2023, demanding advanced measures for protection.

Parveen Shishodia, Senior Consultant Infrastructure and Security, RELAXO FOOTWEAR LTD, sees a need for comprehensive cybersecurity regulations and compliance standards, painting a nuanced picture of the future:

"Cybersecurity threats will continue to evolve, leading to increased demand for advanced measures such as AI-powered security systems and comprehensive data encryption methods. The increased focus on cybersecurity regulations and compliance standards is essential to protect sensitive information."

Cyber Warfare Complexity

The geopolitical conflicts of 2023 spilled into cyberspace, intensifying cyber warfare scenarios.

Humberto Castillo, Systems Engineer at PUERTO DE BARRANQUILLA, explores the impact of geopolitical conflicts on cybersecurity in 2024:

"Due to different scenarios generated by global conflicts, cyber warfare has emerged, intensifying attacks. Artificial Intelligence will be increasingly used by both defenders and attackers, and there will be a surge in attacks on IoT devices. More regulations and policies regarding appropriate usage will be more prevalent than ever."

Unpredictability and Continuous Vigilance

The unpredictability of cybersecurity events in 2023 emphasized the need for continuous vigilance.

Sujit Kumar Sahoo, System Expert, THE ODISHA COMPUTER APPLICATION CENTRE (OCAC), provides a pragmatic perspective, stressing the importance of adapting to 2024's evolving trends:

"Predicting specific events is challenging. Trends suggest increased focus on AI-driven attacks, evolving ransomware sophistication, growing concern for supply chain security, and heightened emphasis on quantum-resistant encryption. Continuous vigilance and proactive measures will be crucial in this dynamic landscape."

As we put down our crystal ball, we invite you to turn to Radware to fortify your defenses and prepare for the challenges that await us 2024. Reach out to a Radware expert to find out how to make this year a safer one for your organization.

En conmemoración del Día Internacional de Internet Segura (Safer Internet Day) , Soluciones Seguras se une a esta iniciativa global destacando la importancia de la ciberseguridad en el entorno digital desde la niñez.

“La era digital ofrece a los menores innumerables oportunidades de aprendizaje y conexión, pero también plantea desafíos en términos de seguridad en línea. Es esencial que los padres desempeñen un papel activo en la protección de sus hijos e hijas mientras exploran el vasto mundo de Internet” comentó Joey Milgram, Gerente General de Soluciones Seguras en Costa Rica.

Según el experto, los niños, niñas y jóvenes enfrentan varios riesgos significativos mientras navegan en internet, entre los cuales destaca el ciberacoso infantil (Cyberbullying), donde pueden ser víctimas de acoso, intimidación o amenazas por parte de otros menores o adultos.

Otros peligros incluyen la exposición a contenidos nocivos o inapropiados en línea, la publicación inocente de información privada que los expone a riesgos de phishing, juegos o retos virales peligrosos, y el Grooming, una estrategia utilizada por adultos para establecer relaciones con menores con malas intenciones.

Con el objetivo de promover prácticas seguras a temprana edad y desde el hogar, la organización comparte valiosos consejos dirigidos a los padres de familia, reconociendo su papel crucial en la educación de sus hijos e hijas en materia de ciberseguridad.

Comunicación abierta: Fomente un diálogo abierto con sus hijos e hijas sobre la importancia de la seguridad en línea. Anímelos a compartir sus experiencias y preocupaciones, creando un ambiente donde se sientan cómodos buscando orientación.

Establezca límites y normas: Defina límites claros sobre el tiempo de pantalla y el acceso a ciertos contenidos. Establecer normas desde una edad temprana ayudará a formar hábitos seguros y responsables.

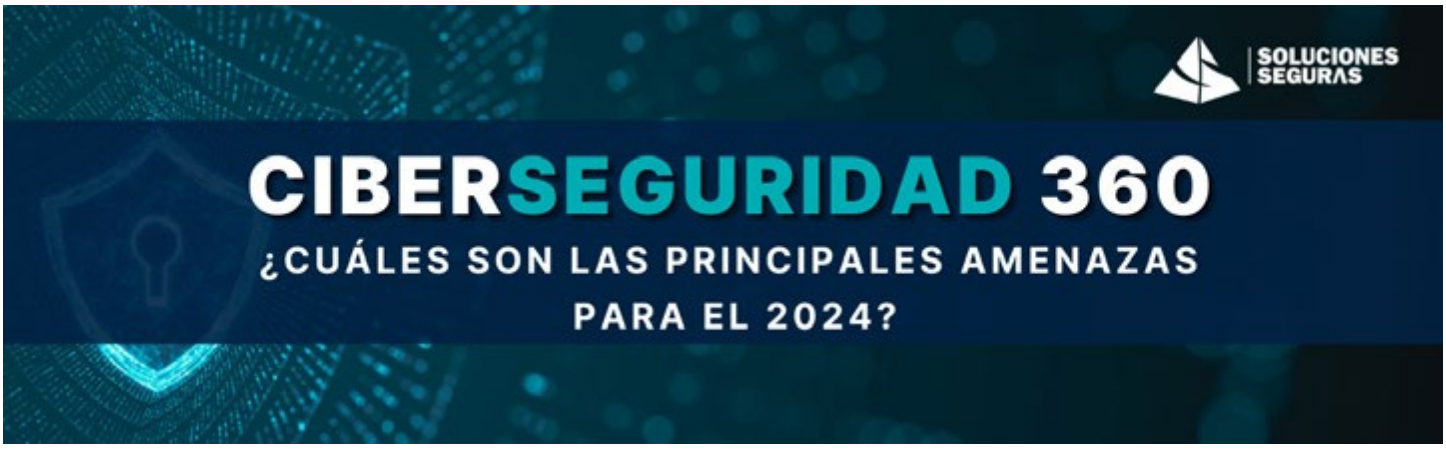
Aprendizaje conjunto: Explore Internet junto con los menores. Participar activamente en sus actividades en línea les permitirá comprender mejor los posibles riesgos y enseñarles cómo tomar decisiones seguras.

Controles parentales: Utilice las herramientas de control parental disponibles en dispositivos y aplicaciones para limitar el acceso a contenido inapropiado y supervisar las actividades en línea de sus hijos e hijas.

Concientización sobre peligros en línea: Hable con sus hijos e hijas sobre los posibles peligros en línea, como el ciberacoso y el contacto con desconocidos. Enseñe estrategias para identificar situaciones de riesgo y cómo buscar ayuda cuando sea necesario.

Monitoreo activo: Realice un seguimiento regular de las actividades en línea de sus hijos. Manténgase informado sobre las plataformas y aplicaciones que utilizan, y esté alerta a posibles cambios en su comportamiento en línea.

Milgram enfatiza que la educación en ciberseguridad es una herramienta poderosa para empoderar a los niños y niñas y garantizar que disfruten de una experiencia segura en línea. “Al equipar a nuestros hijos con conocimientos y habilidades, les proporcionamos las herramientas necesarias para navegar por Internet de manera responsable tanto en su niñez, como juventud y adultez”, concluyó.



En el marco del Día Internacional de la Seguridad de la Información, expertos de Soluciones Seguras resaltan las principales tendencias y retos de seguridad que enfrentarán las empresas durante el 2024.

El panorama que definirá la ciberseguridad en el año 2024 estará marcado por el aumento de amenazas sofisticadas, el uso creciente de tecnologías como la inteligencia artificial y el hacktivismo.

La ciberdelincuencia ha experimentado un crecimiento significativo en el último año, destacando un aumento del 8% en los ciberataques semanales a nivel global en el segundo trimestre, según datos de Check Point Research (CPR). Estos indicadores marcan el volumen más alto en dos años, evidenciando una evolución y sofisticación de amenazas conocidas como ransomware y hacktivismo, con grupos criminales modificando sus métodos y herramientas para afectar a organizaciones a nivel mundial.

Uno de los desarrollos más significativos ha sido la evolución del panorama de ransomware, donde más de 48 grupos informaron sobre la extorsión a más de 2,200 víctimas en el primer semestre del 2023.

Soluciones Seguras, junto a su partner Check Point, afirman que casos de los ataques de alto perfil han impactado en la percepción de la seguridad cibernética, generando consecuencias financieras significativas.

Las predicciones de ciberseguridad de Check Point, partner de Soluciones Seguras, para el 2024 abarcan siete categorías principales:

Inteligencia Artificial y Aprendizaje Automático:

- Ascenso de ciberataques dirigidos por IA: Los actores de amenazas adoptarán IA para acelerar y expandir su arsenal, desde el desarrollo eficiente de nuevas variantes de malware hasta el uso de tecnologías deepfake para ataques de phishing y suplantación de identidad.
- Uso de IA en defensa cibernética: La inversión en IA para ciberseguridad se intensificará, siendo vital para la protección contra amenazas avanzadas.

GPU Farming y la Nube:

- El enfoque de hackers en recursos de IA en la nube: Los hackers verán las recursos de IA basados en la nube como oportunidades lucrativas, centrando sus esfuerzos en establecer granjas de procesamiento gráfico (GPU) para financiar sus actividades cibernéticas.

Ataques a la cadena de suministro y la infraestructura crítica:

- Confianza cero en la cadena de suministro: Ante el aumento de ciberataques, habrá un desplazamiento hacia modelos de "confianza cero" que requieran verificación para cualquier conexión a un sistema, independientemente de la red en la que se encuentren.

Ciberseguro y AI:

- Transformación en la evaluación de resiliencia cibernética: La IA transformará la manera en que las compañías de seguros evalúan la resistencia cibernética de sus clientes potenciales.

Ataques de Estados Nación y Hacktivismo:

- Persistencia de la guerra cibernética: La inestabilidad geopolítica será un factor que influya en actividades hacktivistas, con el objetivo de perturbar y desestabilizar.

Utilización de tecnología Deepfake como arma para propósitos espurios:

- Avances en tecnología deepfake. Estas herramientas serán empleadas para crear contenido que pueda influir en opiniones o alterar precios de acciones.

Amenazas de Phishing Continúan:

- Tácticas avanzadas de phishing: Se prevé un aumento en campañas de phishing más personalizadas y efectivas.

Eli Faskha, CEO de Soluciones Seguras, comenta: "La transición a utilizar la IA en ciberseguridad es innegable. Debemos innovar más rápido que las amenazas que enfrentamos para mantenernos un paso adelante. Aprovechemos todo el potencial de la IA para la ciberseguridad, con un enfoque en el uso responsable y ético".

Asimismo, "con el aumento de ciberataques mejorados por IA, modelos de confianza cero y la tecnología deepfake, la inversión en soluciones de ciberseguridad colaborativas, completas y consolidadas es crucial. En un panorama de amenazas en constante expansión, es imperativo mantenerse vigilantes y ágiles, trabajando juntos para crear una defensa efectiva contra los riesgos cibernéticos", finalizó Faskha.

CHECK POINT

SOLUCIONES SEGURAS

2024 CYBER SECURITY REPORT

El Informe de Seguridad de 2024 indica un aumento del 90% en el número de víctimas de ataques de Ransomware extorsionadas públicamente. Estos ataques ahora representan el 10% de todo el malware detectado por los sensores de Check Point.

Los adversarios explotan vulnerabilidades de día cero, emplean limpiadores disruptivos y tácticas emergentes de RaaS (ransomware como servicio).

La inteligencia artificial emerge como un defensor formidable, remodelando la forma en que prevenimos, detectamos y respondemos a los ataques cibernéticos.

DESCARGAR INFORME

CCSA

CHECK POINT

Check Point Certified SECURITY ADMINISTRATOR

Este curso proporciona una base sólida para aquellos que desean administrar y mantener la seguridad de las redes utilizando los productos de Check Point. La certificación CCSA es reconocida en la industria y demuestra la competencia en la implementación y administración de soluciones de seguridad de red.

Resumen de los temas clave cubiertos en el curso:

- Introducción a Check Point y FireWall-1
- Gestión de objetos y configuración de VPN
- Monitoreo y resolución de problemas:
- Network Address Translation (NAT)
- Gestión avanzada de conexiones y resolución de problemas
- Implementación de políticas de seguridad avanzadas
- Configuración y administración de servicios de red
- Configuración de VPN avanzada.

CCSE

CHECK POINT

Check Point Certified SECURITY EXPERT

El curso CCSE proporciona conocimientos especializados en la administración y configuración avanzada de soluciones de seguridad de Check Point. La certificación CCSE valida la experiencia y competencia en la implementación de políticas de seguridad avanzadas y la resolución de problemas en entornos complejos.

Resumen de los temas clave cubiertos en el curso:

- Conceptos avanzados de VPN
- Gestión avanzada de políticas de seguridad
- Resolución de problemas avanzada
- Configuración avanzada de ClusterXL
- Configuración avanzada de SecureXL y CoreXL
- Auditoría y monitorización avanzada
- Implementación de políticas de seguridad en entornos complejos

Es importante tener en cuenta que los detalles específicos del curso pueden cambiar con el tiempo, por lo que se recomienda verificar la información más reciente en el sitio web oficial de Check Point.

Consúltenos para obtener más información:

entrenamiento@sseguras.com

www.sseguras.com

SOLUCIONES SEGURAS TRAINING CENTER

CHECK POINT PARTNER ELITE

PROTECCIÓN DE REDES, ENDPOINTS Y MOVILES

Check Point ofrece la más reciente protección de seguridad de redes en una plataforma integrada. Con protección para su centro de datos, empresa, móviles, estaciones de trabajo y oficina en el hogar, Check Point tiene una solución para usted.

SEGURIDAD DE CUENTAS PRIVILEGIADAS

CyberArk es líder y experto en seguridad de cuentas privilegiadas. Gestión de privilegios, análisis de amenazas privilegiadas y registro de sesiones. Las contraseñas privilegiadas se mantienen en una bóveda segura.

MITIGACIÓN DE ATAQUES | ENTREGA DE APLICACIONES

Soluciones para seguridad, disponibilidad, balanceo y rendimiento de infraestructura y aplicaciones web. Sistema Mitigador de Ataques para protección perimetral y alta disponibilidad en sus aplicaciones web manteniéndolas seguras y optimizadas.

PROTECCIÓN DE BASE DE DATOS Y APLICACIONES WEB

Soluciones de auditoría y protección a datos críticos mediante protección de Bases de Datos, además de protección para aplicativos web (WAF). Brindando una protección completa lo más cerca de la fuente de información.

SEGURIDAD Y SERVICIOS DNS, DHCP & IPAM

Servicios DNS, DHCP & IPAM en una sola plataforma. Elimine la interrupción del servicio DNS mediante una defensa automatizada contra ataques volumétricos basados en DNS y exploits.

VISIBILIDAD Y CONTROL DE ACCESO A LA RED

Descubra dispositivos, contrólelos y organice respuestas de amenazas en instalaciones cableadas e inalámbricas, centros de datos, campus, nube y tecnología operativa con o sin agentes.

SEGURIDAD DE DATOS DE MISIÓN CRÍTICA EN PREMISAS Y NUBE

Varonis crea una vista prioritaria única del riesgo para sus datos, lo que le ayuda a eliminar de forma proactiva y sistemática el riesgo de las amenazas internas y ataques cibernéticos.

SOLUCIONES DE CIFRADO Y SEGURIDAD DE SERVIDORES Y DATOS

Soluciones que frecen seguridad de servidores y datos mediante mecanismos de cifrado, enmascaramiento y tokenización. Además provee de auditoría y control de acceso a datos sensitivos.

DEFENSA DISEÑADA PARA AMENAZAS AVANZADAS

Solución que le muestra no solo a dónde van los intrusos, sino dónde han estado. Brinda visibilidad completa en la nube, el centro de datos y la IoT, incluso cuando el tráfico está cifrado.

MONITOREO DE RENDIMIENTO DE REDES Y SERVIDORES

Monitoreo completo de su infraestructura. De rápida implementación brindando alertas proactivas y vistas, permitiendo resolver incidencias de red lo más rápido posible.

FILTRADO DE CONTENIDO Y ARCHIVADO DE DATOS

Le birnda una única fuente para proteger todos sus vectores de amenazas, incluidos el correo electrónico, sitios web, aplicaciones web, y el rendimiento de la red, ya sea en el sitio o en la nube.

EVALUACIÓN CONTINUA DE COMPROMISO

Descubra su nivel de compromiso en minutos. Mida el compromiso con rapidez y presición.

PLATAFORMA DE EVALUACIÓN Y FORMACIÓN EN CIBERSEGURIDAD

Cympire ayuda a las organizaciones a aumentar la resiliencia cibernética y mitigar el riesgo de ataques graves a través de capacitación y evaluación continuas.

DESCUBRIMIENTO & GESTIÓN DE ACTIVOS Y PROVEEDORES

La Plataforma de Descubrimiento & Gestión de Activos y Proveedores de Proactivanet permite conocer al instante y de manera exhaustiva el inventario de todo el parque informático.

SISTEMA INMUNE DE LAS EMPRESAS

Detección de amenazas en tiempo real, visualización de la red y capacidades avanzadas de investigación en un solo sistema unificado.

IPS Y PROTECCIÓN AVANZADA PARA REDES Y SERVIDORES

Soluciones que frecen alta tecnología en prevención de intrusiones para proteger contra toda la gama de amenazas en cualquier lugar de su red y servidores en ambientes físicos, virtuales y en la nube.

SIEM BASADO EN LA NUBE | ANÁLISIS DE VULNERABILIDADES

Solución SIEM basado en la nube con User Behavior Analytics y Deception Technology (HOneypot). Además de solución para análisis de vulnerabilidades.

ADMINISTRACIÓN PROACTIVA DE SEGURIDAD

Plataforma con integración profunda a dispositivos críticos, pre-cargada de instrucciones de remediación fácil de leer.

ASEGURE, EVALÚE Y ANALICE SU CÓDIGO FUENTE ANTES DE LANZAR

Asegure, evalúe y analice su código fuente en tiempo de desarrollo. Encuentre y solucione vulnerabilidades en su código de manera más rápida y sencilla.

PLATAFORMA DE CAPACITACIÓN Y CONCIENTIZACIÓN

Plataforma de capacitación y concientización de usuarios. Establezca sus metas y deje que Smartfense haga el resto.

SEGURIDAD Y FIRMA ELECTRÓNICA DE CORREOS Y DOCUMENTOS

Seguridad de documentos y formularios, cumplimiento y aceleración del lugar de trabajo: rastrear, corroborar, firmar electrónicamente, cifrar, compartir, certificar, controlar, todo en uno.

INTELIGENCIA PROACTIVA Y RESPUESTA RÁPIDA A INCIDENTES

Sistema de mando centralizado de ciberseguridad online que le permite integrar todos los eventos con monitoreo estratégico, inteligencia proactiva de amenazas y respuesta rápida a incidentes cibernéticos.

PLATAFORMA EXTENDIDA DE GESTIÓN DE POSTURA DE SEGURIDAD

Plataforma para capacitar a los profesionales y líderes de la seguridad para que administren, conozcan y controlen su postura de ciberseguridad de un extremo a otro.

PROTECCIÓN CONTRA RIESGOS DIGITALES ASOCIADOS A LA MARCA

La sólida tecnología de BrandShield escanea Internet, analiza amenazas potenciales y detecta amenazas de phishing, abuso de marca en línea, infracciones de TM y ventas falsificadas.

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

ACERCA DE SOLUCIONES SEGURAS

Con 20 años de experiencia en la gestión de seguridad de redes, aplicaciones y telecomunicaciones, Soluciones Seguras es la compañía líder en ciberseguridad en Centroamérica. Nuestra reputación se ha creado en base al excelente servicio que ofrecemos, el total conocimiento de las líneas que manejamos, y los productos líderes que representamos.

PERSONAL EXPERTO Y CERTIFICADO

Somos un equipo de profesionales del más alto nivel, certificados por los fabricantes más reconocidos de la industria de seguridad.

CENTRO REGIONAL DE ENTRENAMIENTO AUTORIZADO

Centro Regional de Entrenamiento Autorizado Check Point número uno en la región, con profesionales expertos que forman parte del equipo de desarrollo del contenido de los entrenamientos.

CHECK POINT GOLD ATC PARTNER 2024

CHECK POINT ELITE PARTNER

SOLUCIONES SEGURAS TRAINING CENTER

LÍDER EN CIBERSEGURIDAD EN CENTROAMÉRICA

PRESENCIA REGIONAL

PANAMÁ
Tel: +507 317-1312
infopa@sseguras.com

COSTA RICA
Tel: +506-4000 0885
infocr@sseguras.com

GUATEMALA
Tel: +502 2261-7101
infogt@sseguras.com

EL SALVADOR
Tel: +503 7870-6319
infosv@sseguras.com

HONDURAS
Tel: +504 9469-9999
infohn@sseguras.com

Alianzas

SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

Panamá | Costa Rica | Guatemala | El Salvador | Honduras

www.sseguras.com

SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE