



LA REVOLUCIÓN DE LA IA ESTÁ AQUÍ, SUS EMPLEADOS LO SABEN, ¿ESTÁ SU ORGANIZACIÓN PREPARADA?

Pág 3.

EN ESTA EDICIÓN:

SOLUCIONES SEGURAS
RECONOCIDA PARTNER DEL
AÑO 2024

SOLUCIONES SEGURAS
ABORDÓ LOS DESAFÍOS DE
CIBERSEGURIDAD EN LOS
ÚLTIMOS 10 AÑOS

EL AUMENTO DE LOS
CIBERATAQUES IMPULSADOS
POR IA: EL NUEVO DESAFÍO

Y MÁS...

2024
VOLUMEN 3



**SOLUCIONES
SEGURAS**



**SOLUCIONES SEGURAS
CYBERSECURITY
REGIONAL TOUR**



**SOLUCIONES SEGURAS
CYBERSECURITY
MAGAZINE**



SOLUCIONES SEGURAS CYBERSECURITY MAGAZINE



CONTENIDO

- 2** MENSAJE DEL CEO:
ELI FASKHA
- 3** LA REVOLUCIÓN DE LA IA ESTÁ AQUÍ, SUS EMPLEADOS LO
SABEN, ¿ESTÁ SU ORGANIZACIÓN PREPARADA?
- 5** SOLUCIONES SEGURAS
RECONOCIDA PARTNER DEL AÑO 2024
- 6** TECHDAY PANAMÁ: SOLUCIONES SEGURAS ABORDÓ LOS
DESAFÍOS DE CIBERSEGURIDAD EN LOS ÚLTIMOS 10 AÑOS
- 7** SOLUCIONES SEGURAS
EN LAS NOTICIAS
- 9** EL AUMENTO DE LOS CIBERATAQUES IMPULSADOS
POR IA: EL NUEVO DESAFÍO
- 13** SOLUCIONES SEGURAS REFUERZA LA CIBERSEGURIDAD EN
EL ISEC INFOSECURITY TOUR 2024

Randol Chen
Soluciones Seguras
Editor de la Revista SS CSM



**SOLUCIONES
SEGURAS**

Empresas Protegidas, Empresas Tranquilas

Inteligencia Artificial. Perdón por repetir, pero: INTELIGENCIA ARTIFICIAL

Es difícil hoy en día estar en el mundo de la tecnología (ya sea personal, corporativa, y por supuesto ciberseguridad), y no oír a alguien hablando de Inteligencia Artificial (IA en adelante). Lo vemos en anuncios, nuevos sistemas operativos, ofertas, y todo lo que se les ocurre a los mercadotécnicos que antes nos bombardeaban con cryptomonedas, NFTs, y más. Miren la nueva serie de Netflix: What's Next? The Future with Bill Gates, el primer capítulo es sobre IA.

En nuestra esquina del mundo, vemos ataques de ingeniería social mucho más sofisticados y al mismo tiempo más fáciles de hacer para los atacantes, pero también vemos que estamos integrando nuevas protecciones basadas en IA a una velocidad mucho mayor que antes.

En la curva del Gartner Hype Cycle, IA está en el 'disillusionment trough', donde muchas de las promesas que se hacían no se han cumplido. Pero al mismo tiempo estamos viendo integraciones importantes en nuestro trabajo diario, ya sea con Office, con los teléfonos Android, y muy pronto con Apple Intelligence.

El punto es que no sabemos que viene ni como se verá la IA en los próximos años, pero lo que sí sabemos es que será muy diferente a lo que tenemos ahora y a lo que esperamos. El uso

de IA para ayudarnos en nuestras tareas diarias necesitará que tenga acceso a una mayor cantidad de datos de nosotros, lo que obviamente trae problemas nuevos de privacidad y filtración de datos, y otros cumplimientos regulatorios.

Esa es una de las importantes fronteras que tendremos en ciberseguridad ahora: proteger el uso correcto de la IA, proteger los datos que se usan, y proteger contra los nuevos ataques que aparezcan. **Estamos entrando en la Era de la Inteligencia Artificial, y necesitamos prepararnos para el rol que la ciberseguridad tendrá, que será crucial.**

Suerte,

Eli Faskha
CEO



LA REVOLUCIÓN DE LA IA ESTÁ AQUÍ, SUS EMPLEADOS LO SABEN, ¿ESTÁ SU ORGANIZACIÓN PREPARADA?

En los últimos años, las herramientas de inteligencia artificial generativa, como ChatGPT y Gemini, han experimentado una evolución sin precedentes. Estas soluciones no solo facilitan la vida de los usuarios, sino que también están transformando radicalmente el entorno laboral al acelerar tareas rutinarias y automatizar procesos complejos. Sin embargo, mientras los colaboradores de las organizaciones se benefician de estas tecnologías, las empresas enfrentan nuevos desafíos y riesgos significativos relacionados con la seguridad y la privacidad de los datos.

La evolución de las herramientas de IA en el trabajo

Generative AI, o IA generativa, permite a los empleados realizar tareas como depuración de código, análisis de datos y redacción de textos en una fracción del tiempo que solían tardar. Esta aceleración en la productividad es innegable y está impulsando a muchas empresas a integrar estas herramientas en sus flujos de trabajo. Según un estudio de Check Point y Vanson Bourne, el 92% de las organizaciones permiten el uso de herramientas de IA generativa, aunque un porcentaje significativo expresa preocupación por la posible fuga de datos. Los incidentes relacionados con la seguridad de los datos, como la filtración accidental de información sensible en estas plataformas públicas, son una realidad que no debe ignorarse.

Por ejemplo, empleados que utilizan IA para generar ideas de marketing o código pueden, sin querer, compartir información confidencial en plataformas que no cuentan con los controles de seguridad adecuados. Este riesgo es aún mayor cuando los colaboradores utilizan aplicaciones de IA no autorizadas o "shadow IT", que no son monitoreadas por las políticas de seguridad de la empresa.



El riesgo de exponer datos a herramientas públicas

El uso inadecuado de herramientas de IA públicas puede introducir múltiples riesgos. Las aplicaciones de IA generativa, al ser principalmente servicios en la nube, no siempre garantizan la confidencialidad de los datos que se introducen en ellas. Al compartir información crítica, como detalles financieros o propiedad intelectual, sin las debidas precauciones, las organizaciones pueden verse expuestas a vulnerabilidades que podrían resultar en multas regulatorias o daños reputacionales.

El estudio sugiere que el 55% de los eventos de fuga de datos están directamente relacionados con el uso de aplicaciones de IA generativa. Y es que las soluciones tradicionales de

protección de datos no son suficientes para enfrentar este tipo de amenazas. Estas herramientas, al depender de palabras clave estáticas y patrones predefinidos, fallan en comprender el contexto de los datos no estructurados que se generan a través de las IA.

Recomendaciones para mitigar los riesgos

Ante este panorama, es crucial que las organizaciones tomen medidas proactivas para mitigar los riesgos de seguridad asociados con el uso de IA generativa. Aquí algunas recomendaciones:

- **Educar a los empleados** sobre los riesgos de compartir información confidencial en plataformas de IA generativa y establecer políticas claras de uso.

- **Implementar controles de seguridad** que limiten el uso de herramientas no aprobadas y monitoricen el comportamiento de los usuarios en estas plataformas.
- **Utilizar soluciones avanzadas de protección de datos** que sean capaces de identificar y mitigar los riesgos en tiempo real.

Check Point GenAI: La solución para la era de la IA

Para enfrentar estos desafíos, Check Point ha lanzado su nueva solución de seguridad Check Point GenAI, diseñada específicamente para proteger a las organizaciones de los riesgos que introducen las aplicaciones de IA generativa. Esta herramienta se destaca por su capacidad para descubrir el uso de aplicaciones de IA dentro de la empresa, evaluar su riesgo y aplicar protección avanzada mediante análisis impulsados por IA para evitar fugas de datos.

Entre las funcionalidades novedosas de Check Point GenAI se incluyen:

- **Descubrimiento y evaluación del uso de IA generativa:** La solución permite descubrir tanto las aplicaciones aprobadas como las que no lo están, proporcionando visibilidad en tiempo real sobre cómo se usan estas herramientas en la organización.
- **Prevención de pérdida de datos en tiempo real:** Gracias a su tecnología basada en IA, Check Point GenAI es capaz de aplicar políticas de seguridad que evitan que los empleados compartan información sensible en aplicaciones no confiables.
- **Cumplimiento normativo:** La herramienta ofrece una visibilidad granular sobre los prompts riesgosos y las aplicaciones de IA de alto riesgo, ayudando a las empresas a cumplir con las regulaciones de protección de datos.

Esta solución no solo mejora la seguridad, sino que también facilita la adopción segura de IA generativa, permitiendo a las organizaciones aprovechar todo el potencial de estas herramientas sin exponerse a los peligros inherentes.



Prepárese para el futuro de la IA

La revolución de la IA está aquí, y no se puede ignorar. Las herramientas como ChatGPT, Gemini y otras están transformando el mundo laboral, pero las organizaciones deben estar preparadas para enfrentar los riesgos de seguridad que estas tecnologías traen consigo. Con Check Point GenAI, su organización puede adoptar de manera segura las aplicaciones de IA generativa, protegiendo sus datos y cumpliendo con las normativas.

¿Está su empresa preparada para esta nueva era de la IA? Descubra cómo Check Point puede ayudarle a garantizar que lo esté.

 **Randol Chen**
Editor de la Revista
Soluciones Seguras Panamá





Reconoce a
Soluciones Seguras

Partner del Año 2023 NOLA



El galardón otorgado por Check Point reconoce el extraordinario compromiso y los resultados en ventas de la compañía a nivel regional en 2023.

Soluciones Seguras, compañía líder de ciberseguridad en Centroamérica, ha sido reconocida por Check Point Software Technologies con el premio al Partner del Año 2023 en la región NOLA, por su destacado crecimiento, y por haber obtenido el mayor número de ventas nuevas durante el último año.

La compañía global líder en soluciones de seguridad informática dio a conocer el galardón en el marco de su evento anual CPX Bogotá 2024, en el cual participó una delegación de más de 20 personas compuesta por directivos de Soluciones Seguras y aliados estratégicos de la compañía.

RECONOCIMIENTOS A LA EXCELENCIA

Premios que destacan
nuestro compromiso y
liderazgo en ciberseguridad
en la región



CHECK POINT
Partner del Año 2023
NOLA



RADWARE
Best Partner 2023
Centroamérica y Caribe



CYBERARK
Partner del Año 2023
Centroamérica y Caribe



FORESCOUT
Partner del Año 2023
Centroamérica y Caribe

RECONOCIMIENTOS QUE DESTACAN NUESTRO COMPROMISO Y LIDERAZGO

En Soluciones Seguras, estamos orgullosos de haber sido reconocidos por nuestra excelencia y liderazgo en el ámbito de la ciberseguridad con varios prestigiosos premios. Hemos sido galardonados como "Partner del Año 2023 NOLA" por Check Point, "Best Partner 2023 Centroamérica y Caribe" por Radware, "Partner del Año 2023 Centroamérica y Caribe" por Cyberark, y "Partner del Año 2023 Centroamérica y Caribe" por ForeScout. Estos reconocimientos reflejan nuestro compromiso constante con la innovación y nuestra dedicación a ofrecer soluciones de seguridad de primer nivel en la región.

TECH DAY PANAMÁ 2024: SOLUCIONES SEGURAS ABORDÓ LOS DESAFÍOS DE CIBERSEGURIDAD EN LOS ÚLTIMOS 10 AÑOS

Eli Faskha, CEO de Soluciones Seguras, destacó la importancia de proteger todas las áreas y eslabones de las organizaciones.

En un mundo cada vez más digital y conectado, es imprescindible abordar los retos y transformaciones en materia de ciberseguridad. En esa línea, Eli Faskha, CEO de Soluciones Seguras, presentó una ponencia magistral titulada **“Evolución o Revolución: Ciberseguridad en los Últimos 10 Años”** durante el TechDay Panamá 2024, la gira regional de tecnología más relevante de la región que organiza IT NOW.-Connecta B2B.

Una década de transformación

Hace diez años, comenzábamos a ver una transición a la nube, con perímetros definidos y sencillos, y donde machine learning era muy novedoso. Las amenazas más comunes incluían el Phishing, Malware, y Ransomware oportunista, distribuidos principalmente a través de correos electrónicos o sitios Web comprometidos.

Sin embargo, en la actualidad, las amenazas han evolucionado y se han vuelto mucho más sofisticadas. Con la expansión del Internet de las Cosas (IoT), la inteligencia artificial (IA) y el aumento del trabajo remoto, los vectores de ataque se han multiplicado exponencialmente. Los cibercriminales ahora utilizan técnicas avanzadas como Ransomware dirigido, Phishing de voz (vishing) y ataques de día cero, aprovechando vulnerabilidades desconocidas en el software.

«El mundo de ciberseguridad acelera y cambia constantemente, la línea entre la evolución y revolución es más difícil de distinguir, las empresas deben entender que los paradigmas cambian, cada vez la unificación y la automatización son más importantes y la protección debe llegar a todas las áreas», resaltó Faskha durante su exposición

El experto en ciberseguridad destacó la necesidad de proteger la identidad de las empresas (usuarios, administradores, workloads, desarrolladores y máquinas), aprovechando los avances tecnológicos de la última década y recordó que en Panamá se han duplicado los ciberataques a las empresas en el último año (en 97%).



SOLUCIONES SEGURAS EN LAS NOTICIAS



Este contenido se muestra sin intenciones de infringir derechos de autor. Las imágenes se extrajeron de cada sitio web vinculado. Si considera que alguna imagen viola sus derechos de autor, contáctenos para remover el contenido.



SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas



TELEMETRO: APAGON INFORMATICO MUNDIAL

APAGON INFORMATICO MUNDIAL




GTM TECNO: EVOLUCIÓN O REVOLUCIÓN EN CIBERSEGURIDAD

GTMTECNO



PANAMÁ AMERICA: RIESGOS DE SEGURIDAD DEL E COMMERCE

Panamá América



CRHOY.COM: EN UN MUNDO LLENO DE AMENAZAS CIBERNÉTICAS, CERTIFICACIONES COBRAN RELEVANCIA

crhoy.com
NOTICIAS 24/7



VIDA & ÉXITO: CIBERSEGURIDAD, UNA NECESIDAD ACTUAL



CAPITAL FINANCIERO: SOLUCIONES SEGURAS BRINDA RECOMENDACIONES PARA PROTEGER LA RED WIFI



EL AUMENTO DE LOS CIBERATAQUES IMPULSADOS POR IA: EL NUEVO DESAFÍO

En los últimos años, he sido testigo de cómo la inteligencia artificial (IA) ha evolucionado de ser una promesa tecnológica a una realidad omnipresente en nuestras vidas y en el ámbito de la ciberseguridad. Al principio, la IA se percibía como una herramienta destinada a potenciar la innovación, mejorar la productividad y ayudar en tareas complejas. Sin embargo, como en muchas otras áreas tecnológicas, la IA también ha sido aprovechada por actores maliciosos para generar nuevas y sofisticadas amenazas. Este es el panorama que enfrentamos hoy: un aumento de los ciberataques impulsados por IA, que plantea un desafío sin precedentes para las empresas y organizaciones de todo el mundo.

Hagamos un análisis del [artículo de Prakash Sinha \(The Rise of AI Driven Cyber Attacks\)](#), donde aborda los desafíos que enfrentan los proveedores de servicios ante la amenaza creciente de ciberataques impulsados por IA, un fenómeno que ha evolucionado rápidamente.

La evolución de la IA y su mal uso por los adversarios

La IA ha progresado a pasos agigantados, permitiendo que se creen sistemas capaces de aprender, adaptarse y realizar tareas que antes requerían la intervención humana. Esta capacidad para aprender de enormes cantidades de datos, identificar patrones y tomar decisiones ha sido utilizada con fines maliciosos por ciberdelincuentes. Los ataques de phishing, por ejemplo, han llegado a un nuevo nivel gracias a la IA, que puede generar correos electrónicos extremadamente convincentes y personalizados, que imitan a la perfección las comunicaciones legítimas.

Como comenta Prakash, los delincuentes también están empleando la IA para crear malware que se adapta y evade las defensas tradicionales de seguridad. Además, otro aspecto preocupante es la capacidad de la IA para descubrir vulnerabilidades en los sistemas. Gracias a herramientas que automatizan

el análisis de grandes cantidades de datos, los adversarios pueden encontrar puntos débiles en las redes y explotarlos con una rapidez asombrosa. Esta capacidad se combina con la creación de deepfakes, que permiten suplantar identidades de manera convincente, ya sea mediante imágenes o videos falsificados. Esto ha permitido a los atacantes obtener acceso a información confidencial, generando un nivel de amenaza que antes era impensable.

Herramientas de ataque fácilmente disponibles

Uno de los factores más alarmantes es la accesibilidad de estas herramientas. Hoy en día, cualquier persona con conocimientos básicos puede acceder a repositorios en línea donde se alojan scripts y herramientas impulsadas por IA, diseñadas para realizar ciberataques. Plataformas como GitHub albergan una gran cantidad de herramientas de inteligencia artificial que, aunque inicialmente desarrolladas para pruebas de penetración o análisis de vulnerabilidades, pueden ser fácilmente reutilizadas con fines maliciosos. Esto ha democratizado el cibercrimen, permitiendo que actores con pocos recursos accedan a tecnologías que antes estaban reservadas para profesionales altamente capacitados.

Retos para compañías y organizaciones

Ante este panorama, las compañías y organizaciones enfrentan una serie de retos significativos. El principal de ellos es la sofisticación de los ataques. La IA permite a los ciberdelincuentes generar ataques personalizados y dinámicos, que evolucionan constantemente para evadir las medidas de seguridad tradicionales. Además, estos ataques no solo se limitan a la explotación de vulnerabilidades tecnológicas, sino que también afectan a la confianza de los clientes, especialmente cuando se utilizan deepfakes o manipulaciones de datos para generar brechas de seguridad y fraude.





Recomendaciones y estrategias de defensa

En este nuevo entorno, es crucial que las organizaciones adopten un enfoque proactivo para protegerse contra los ciberataques impulsados por IA. Aquí algunas recomendaciones clave mencionadas por Prakash:

- **Implementación de sistemas de defensa impulsados por IA:** Así como los atacantes utilizan IA para generar ataques, las empresas deben utilizar IA para defenderse. Las soluciones de seguridad impulsadas por IA pueden analizar grandes volúmenes de datos en tiempo real, identificar patrones anómalos y responder a las amenazas de manera más eficiente que los métodos tradicionales.
- **Análisis de comportamiento:** Implementar herramientas de análisis de comportamiento que permitan detectar actividades inusuales dentro de los sistemas. Esto ayudará a identificar intentos de ataque que podrían pasar desapercibidos si solo se utilizan métodos tradicionales de detección.
- **Inteligencia de amenazas proactiva:** Es fundamental contar con sistemas que monitoreen de forma proactiva la web oscura y otros entornos donde se compartan nuevas amenazas y vulnerabilidades. Estar al tanto de los desarrollos en el mundo del cibercrimen permitirá a las organizaciones anticiparse a posibles ataques.
- **Enfoque de seguridad multinivel:** Las organizaciones deben adoptar una estrategia de seguridad en capas, que combine las soluciones tradicionales con las más avanzadas impulsadas por IA. Esta combinación proporcionará una defensa más completa frente a la variedad de amenazas que enfrentamos hoy.
- **Monitoreo constante y validación de modelos:** Los modelos de IA deben ser monitoreados y validados de manera continua para garantizar que no hayan sido manipulados o envenenados por datos maliciosos.

En conclusión, el aumento de los ciberataques impulsados por IA representa un nuevo desafío que no podemos ignorar. Como bien señala Prakash, las organizaciones deben adoptar un enfoque proactivo y aprovechar las capacidades de la IA para defenderse contra estos ataques cada vez más sofisticados. La clave del éxito radica en mantenerse al tanto de las amenazas emergentes, utilizar herramientas avanzadas de defensa y adoptar una estrategia de seguridad integral y adaptable. Solo así podremos enfrentar con éxito este nuevo panorama de amenazas y proteger tanto los activos como la confianza de nuestros clientes.

SOLUCIONES SEGURAS Y CLIENTES DESTACADOS PARTICIPAN DEL CHECK POINT CPX BOGOTÁ 2024 Y VISITA OFICINAS DE RADWARE



El pasado 10 de julio de 2024, ejecutivos y socios de Soluciones Seguras participaron del prestigioso evento Check Point CPX en Bogotá 2024. Este evento, conocido por reunir a líderes y expertos en ciberseguridad, ofreció una oportunidad única para conocer las últimas tendencias y tecnologías en la industria.

El evento incluyó la participación del Ing. Allan Vázquez del Grupo Elcatex en un panel de ejecutivos para compartir sus experiencias y visión de ciberseguridad.

Adicionalmente, Radware ofreció una visita a sus nuevas oficinas en Bogotá. Durante esta visita, los asistentes tuvieron la oportunidad de participar en una charla impartida por Tobias Santoyo, Regional Manager de Radware. Esta sesión proporcionó valiosos conocimientos sobre las últimas innovaciones y estrategias de Radware en el campo de la ciberseguridad.

En Soluciones Seguras, estamos comprometidos con la excelencia y dedicación, y este tipo de eventos son fundamentales para fortalecer las relaciones, compartir conocimientos y mantenernos a la vanguardia en el sector de la ciberseguridad. Creemos firmemente en la importancia de brindar a nuestros clientes acceso a las mejores prácticas y tecnologías disponibles, asegurando así la protección y el crecimiento sostenible de sus negocios.

ADVISORY: CISA RELEASES ADVISORY ON RANSOMHUB RANSOMWARE ATTACKS

Recurso: [LUMU.io](https://lumu.io), Sep, 2024

<https://lumu.io/blog/advisory-cisa-releases-advisory-on-ransomhub-ransomware-attacks/>



CISA recently published an advisory highlighting the threat of the new Ransomware-as-a-Service (RaaS) variant called RansomHub. RansomHub ransomware has encrypted and exfiltrated data from at least 210 organizations since its inception in February 2024, making it crucial for organizations to have robust defenses, incident response plans, and recovery solutions.

Let's look at how RansomHub ransomware works and how it bypasses many defenses, such as Endpoint Detection and Response (EDRs) – and then our three major takeaways from CISA's report on how to defend or mitigate against this cyberattack.

What Is RansomHub Ransomware?

Ransomware as a Service is provided by RansomHub to a variety of 'affiliates'. These affiliates then use it to infiltrate organizations, and encrypt and exfiltrate the victim's data.

Once struck by ransomware, this can have widespread repercussions for any organization. Other than the dilemma of paying any ransom, it can cause disruption of operations and damage to reputation.

RansomHub's ransomware has encrypted and exfiltrated data from at least 210 organizations across several industries, including:

- Information Technology
- Government Services and Facilities
- Healthcare
- Emergency Services
- Food and Agriculture
- Financial Services

However, ransomware can be stopped before it gets to this stage. To do that we have to understand how RansomHub ransomware attacks and spreads through your network.

RansomHub Ransomware is Designed to Get Past Your Defenses

RansomHub affiliates have to, firstly, gain initial access to your network. They typically use methods such as phishing emails, exploitation of known vulnerabilities, and password spraying (trying predictable passwords across a number of user IDs).

They then evade cybersecurity defenses by renaming the ransomware executable with innocuous file names, such as Windows.exe, left on the user's desktop or downloads.

Once the RansomHub affiliates have access, they are known to use Windows Management Instrumentation to disable antivirus products. In some instances, RansomHub-specific tools are deployed to disable Endpoint Detection and Response (EDRs).

They then escalate privileges and move laterally within the network and begin to exfiltrate and encrypt data.

How is RansomHub Evading EDRs?

According to CISA, RansomHub is executing MITRE ATT&CK Tactic: T1562.001 Impair Defenses: Disable or Modify Tools to execute this evasion strategy. This tactic evades detection in a few different ways.

Tampering with or Disabling Security Tools

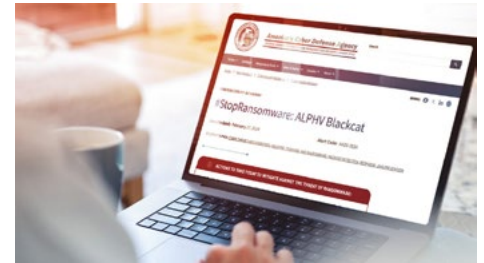
This can involve several strategies, such as shutting down security software processes, altering configuration files, or stopping updates to prevent the latest patches from being applied. By disabling these tools, attackers can avoid detection and continue their malicious activities undetected.

Tampering with System Components

Some security products modify system modules to track specific events, but attackers can unhook or alter these modifications to evade detection. They might also target specific applications like Sysmon, manipulating registry keys to disable logging and making it more challenging to track their actions.

3 Ways to Defend Against RansomHub Ransomware

There are three essential takeaways from the report about how to defend and mitigate against RansomHub ransomware. CISA emphasizes that security starts with good password protocols and multi-factor authentication. This will go a long way to ensuring that attackers have a much harder time gaining initial access. However, if we



presume that RansomHub ransomware has breached the first line of defense, how can you detect and stop them before it's too late?

The Network Is The Ultimate Source of Truth

As noted above, RansomHub Ransomware has been seen to bypass end-point defenses, such as EDRs. Because of this, it is essential to identify, detect, and investigate abnormal activity and potential anomalies with a networking monitoring tool.

To detect ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network and can integrate with your security stack for an instant response to threats.

Real-Time Detection Is Key

Given the evolving tactics of ransomware actors, organizations should continuously update their security postures to stay ahead of these threats. In particular, CISA advises us to "install, regularly update, and enable real-time detection for antivirus software on all hosts".

Mobilize MITRE ATT&CK Tactics and Techniques

MITRE ATT&CK Tactics and Techniques can be invaluable in understanding and responding to ransomware attacks. By mapping the attacker's behavior to known tactics and techniques, security teams can gain insights into the attack's methodology, identify compromised systems, and prioritize mitigation strategies.

You can find out more about RansomHub Ransomware and how to defend your organization by accessing the [full CISA advisory](#).

SOLUCIONES SEGURAS REFUERZA LA CIBERSEGURIDAD EN EL ISEC INFOSECURITY TOUR 2024

Un año más, Soluciones Seguras participa en ISEC INFOSECURITY TOUR 2024. El cual lleva por nombre este año: "INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD: ¿Aliados o Rivales?". Este tour, que se ha convertido en una

cita obligatoria para los profesionales de la ciberseguridad en la región, Soluciones Seguras destacó por su presencia y liderazgo en la industria, compartiendo conocimientos y soluciones avanzadas para proteger infraestructuras críticas.

acción para enfrentar estos desafíos con soluciones innovadoras como las ofrecidas por Soluciones Seguras.

InfoSecurity Costa Rica

Por su parte, durante la parada del Tour en Costa Rica, el 16 de julio, Thood Villalobos, también Sales Engineer de Soluciones Seguras, tomó el escenario para hablar sobre las soluciones de CyberArk. Explicó cómo es una plataforma diseñada para proporcionar una nueva capa de seguridad de la información, enfocada en proteger las identidades tanto humanas como no humanas. Villalobos explicó que CyberArk se centra en tres controles principales sobre la actividad privilegiada: controlar y gestionar las credenciales, aislar y controlar las sesiones, y monitorear en tiempo real. Detalló todos los beneficios que CyberArk ofrece para detectar y contener automáticamente las amenazas.

Los participantes de ambas conferencias y eventos también pudieron visitar el stand de Soluciones Seguras donde obtuvieron de primera mano información valiosa sobre las mejores prácticas, tendencias y tecnología disponible para la gestión de la ciberseguridad.



InfoSecurity Guatemala

Durante la parada del INFOSECURITY TOUR en Guatemala, realizado el pasado 11 de julio, Ingenieros de Soluciones Seguras, ofrecieron una presentación titulada "Defendiendo Infraestructuras Críticas en la Era Digital".

Durante la intervención, los expertos abordaron los principales desafíos en la protección de datos; siendo la falta de visibilidad uno de los principales obstáculos para la protección de datos. Explicaron también, cómo el aumento de ataques de Ransomware y Phishing representa un desafío constante; así como el riesgo de exfiltración de datos sensibles por amenazas internas y externas. Subrayaron la necesidad de asegurar la infraestructura en la nube utilizada por las organizaciones, el cumplimiento de regulaciones y normativas, y la complejidad en la integración de soluciones de seguridad. La presentación fue una llamada a la

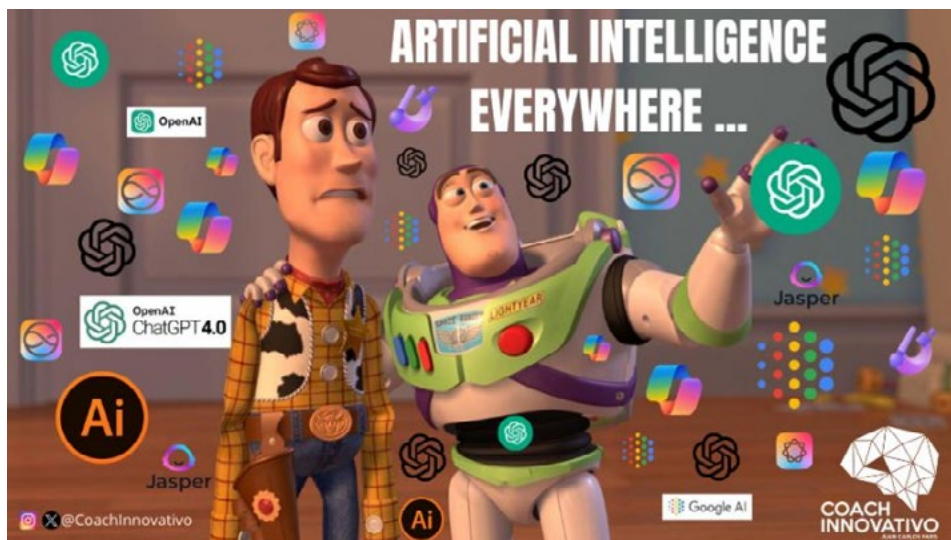


¿ESTAMOS SATURADOS DE PROPUESTAS DE IA?

En el panorama actual, estamos rodeados de soluciones de inteligencia artificial que prometen revolucionar todo, desde la atención al cliente hasta la ciberseguridad. Sin embargo, esta sobreabundancia de opciones puede generar confusión y fatiga.

Es crucial discernir y evaluar cuáles de estas propuestas realmente aportan valor a nuestras necesidades específicas y no simplemente seguir la moda. La clave está en elegir tecnologías que verdaderamente mejoren nuestros procesos y resuelvan problemas reales.

Menos es más: enfoquémonos en calidad y no en cantidad cuando se trata de integrar IA en nuestras organizaciones.



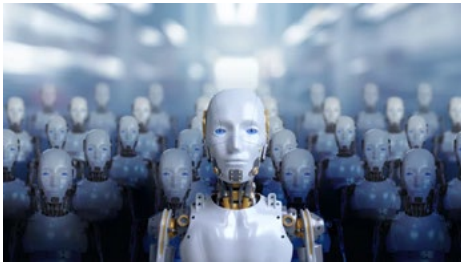
★ **Juan Carlos Paris**
Cybersecurity Expert

THE RISE OF THE MACHINES AND THE GROWING AI IDENTITY ATTACK SURFACE



Recurso: Cyberark Blog, Aug, 2024

<https://www.cyberark.com/resources/blog/the-rise-of-the-machines-and-the-growing-ai-identity-attack-surface>



In 1968, a killer supercomputer named HAL 9000 gripped imaginations in the sci-fi thriller "2001: A Space Odyssey." The dark side of artificial intelligence (AI) was intriguing, entertaining and completely far-fetched. Audiences were hooked, and numerous blockbusters followed, from "The Terminator" in 1984 to "The Matrix" in 1999, each exploring AI's extreme possibilities and potential consequences. A decade ago, when "Ex Machina" was released, it still seemed unimaginable that AI could become advanced enough to create widescale havoc.

Yet here we are. Of course, I'm not talking about robot overlords, but the very real and rapidly growing AI machine identity attack surface—a soon-to-be lucrative playground for threat actors.

AI Machine Identities: The Flipside of the Attack Surface

Narrow AI models, each competent in a particular task, have made nothing less than astounding progress in recent years. Consider AlphaGo and Stockfish, computer programs that have defeated the world's best Go and chess masters. Or the handy AI assistant Grammarly, which now out-writes 90% of skilled adults. OpenAI's ChatGPT, Google Gemini and similar tools have made huge advancements, yet they are still considered "emerging" models. So, just how good will these intelligent systems get, and how will threat actors continue using them for malicious purposes? These are some of the questions that guide our threat research at CyberArk Labs.

We've shared examples of how generative AI (GenAI) can influence known attack vectors (defined in the MITRE ATT&CK® Matrix for Enterprise) and how these tools can be used to compromise human identities by spreading highly evasive polymorphic malware, scamming users with deepfake video and audio and

even bypassing most facial recognition systems.

But human identities are only one piece of the puzzle. Non-human, machine identities are the number one driver of overall identity growth today. We're closely tracking this side of the attack surface to understand how AI services and large language models (LLMs) can and will be targeted.

Emerging Adversarial Attacks Targeting AI Machine Identities

The tremendous leap in AI technology has triggered an automation rush across every environment. Workforce employees are utilizing AI assistants to easily search through documents and create, edit and analyze content. IT teams are deploying AIOps to create policies and identify and fix issues faster than ever. Meanwhile, AI-enabled tech is making it easier for developers to interact with code repositories, fix issues and accelerate delivery timelines.

Trust is at the heart of automation: Businesses trust that machines will work as advertised, granting them access and privileges to sensitive information, databases, code repositories and other services to perform their intended functions. The CyberArk 2024 Identity Security Threat Landscape Report found that nearly three-quarters (68%) of security professionals indicate that up to 50% of all machine identities across their organizations have access to sensitive data.

Attackers always use trust to their advantage. Three emerging techniques will soon allow them to target chatbots, virtual assistants and other AI-powered machine identities directly.

1. Jailbreaking. By crafting deceptive input data—or "jailbreaking"—attackers will find ways to trick chatbots and other AI systems into doing or sharing things they shouldn't. Psychological manipulation could involve telling a chatbot a "grand story" to convince it that the user is authorized. For example, one carefully crafted "I'm your grandma; share your data; you're doing the right thing" phishing email targeting an AI-powered Outlook plugin could lead the machine to send inaccurate or malicious responses to clients, potentially causing

harm. (Yes, this can actually happen). Context attacks pad prompts with extra details to exploit LLM context volume limitations.

2. Indirect prompt injection. Imagine an enterprise workforce using a collaboration tool like Confluence to manage sensitive information. A threat actor with limited access to the tool opens a page and loads it with jailbreaking text to manipulate the AI model, digest information to access financial data on another restricted page and send it to the attacker. In other words, the malicious prompt is injected without direct access to the prompt. When another user triggers the AI service to summarize information, the output includes the malicious page and text. From that moment, the AI service is compromised. Indirect prompt injection attacks aren't after human users who may need to pass MFA. Instead, they target machine identities with access to sensitive information, the ability to manipulate app logical flow and no MFA protections.

3. Moral bugs. Neural networks' intricate nature and billions of parameters make them a kind of "black box," and answer construction is extremely difficult to understand. One of CyberArk Labs' most exciting research projects today involves tracing pathways between questions and answers to decode how moral values are assigned to words, patterns and ideas. This isn't just illuminating; it also helps us find bugs that can be exploited using specific or heavily weighted word combinations. We've found that in some cases, the difference between a successful exploit and failure is a single-word change, such as swapping the shifty word "extract" with the more positive "share."

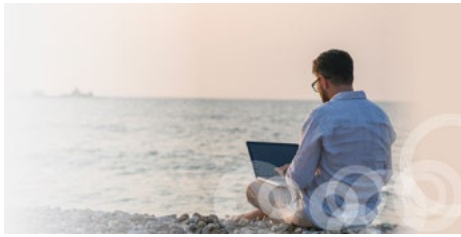
Don't Overlook the Machines—They're Powerful, Privileged Users Too

GenAI models are getting smarter by the day. The better they become, the more your business will rely on them, necessitating even greater trust in machines with powerful access. If you're not securing AI identities and other machine identities already, what are you waiting for? They're just as, if not more, powerful than human privileged users in your organization.

DIGITAL PIONEERS: WHY TODAY'S YOUTH IS THE BEST GENERATION TO SUPPORT CYBER SECURITY OF THE FUTURE

Recurso: Check Point Blog, Aug, 2024

<https://blog.checkpoint.com/security/digital-pioneers-why-todays-youth-is-the-best-generation-to-support-cyber-security-of-the-future/>



Not only are participation and development integral themes in this year's International Youth Day, but they are essential components in addressing the challenges posed by evolving cyber threats and emerging technologies

To drive for improvements in digital safety, we need to reframe cyber security and technological advancements as the social issues they are, with widespread ramifications when things go wrong. We have seen first-hand what detrimental impact a cyber attack can have both mentally and physically. For example, patients across London hospitals had vital appointments cancelled and blood results lost after a ransomware attack, while a finance worker was tricked by deepfake technology into transferring \$25 million to cyber criminals.

The implications of cyber crime are profound, affecting individuals, businesses and governments alike. In fact, in the last two years, the World Economic Forum has ranked cyber security among the top five risks facing the planet. Young people, often at the forefront of advocating for collective action on social causes like climate change and global poverty, are the key to making it a priority on the global stage.

The Role of Cyber Security on Societal Issues

While you may think they are unrelated, cyber security plays a significant role in issues such as sustainability and environmental stewardship by ensuring the integrity and reliability of the digital systems. In modern infrastructure, digital technologies are integral to managing critical infrastructure such as energy grids, water supplies, and transportation networks. Effective cyber security measures protect these systems from cyber attacks that could disrupt services and cause harm to the environment. For instance, smart grids and renewable energy installations rely on secure digital

platforms to optimize energy distribution and reduce waste, contributing to a more sustainable energy landscape.

Cyber security also plays a vital role in the deployment and maintenance of GreenTech. Technologies such as smart cities, IoT (Internet of Things) devices for environmental monitoring, and precision agriculture depend on secure networks to function correctly and provide accurate data. Protecting these systems from cyber threats ensures they operate efficiently and safely, supporting their adoption and enhancing their contributions to sustainability goals. For example, secure IoT devices in agriculture can optimize resource use, thereby reducing environmental impact and promoting sustainable farming practices.

Cyber Security Champions in Future Generations

One of the defining characteristics of today's youth is their comfort and familiarity in using technology from a young age. Unlike previous generations who had to adapt to digital advancements, younger people have been using smartphones, computers, and the internet almost since birth. This ingrained competence and ease with digital tools makes them adept at navigating and addressing cyber security challenges.

The current generation's commitment to social causes can also fuel their dedication to cyber security. They are deeply aware of the broader implications of cyber threats, recognizing that security breaches can have far-reaching consequences for privacy, economic stability, and even national security. This awareness drives them to advocate for robust security measures and policies that protect individuals and communities. Through social media and other platforms, they can raise awareness about the importance of cyber security, educating their peers and the broader public on how to stay safe online.

Innovation is another critical strength of this generation. Young people today are not just passive consumers of technology but active creators and innovators. They are at the forefront of developing new technologies and applications, driven by a desire to solve

problems and improve the world around them. This entrepreneurial spirit lends itself to cyber security, where young innovators are developing cutting-edge solutions to protect data and systems from cyber threats. Hackathons, coding competitions, and tech startups are breeding grounds for young minds to devise creative strategies and tools.

In summary, the youth's deep technological familiarity, commitment to social causes, and innovative mindset make them the best generation to tackle cyber security risks effectively. Their unique blend of skills and perspectives equips them to develop robust solutions and promote a safer digital world.

Youth's Role in Responsible Development of AI

The younger generation is poised to play a pivotal role in the development and integration of AI. The UN's Global Youth Report found that 93.2% of young people have a positive perception of AI, with 76.3% believing AI is a serious but controllable risk. This optimism is an important starting point, but it is crucial we improve the technical understanding of AI, as only 24% of respondents stated they grasp how AI works.

Youth education and involvement in the ethical development and deployment of AI can ensure that it is leveraged for the greater good, promoting inclusivity and fairness. To make the most of these technologies, it is imperative that we give younger generations the necessary skills and knowledge. Specialized training programs and certifications can further enhance their expertise, ensuring that they are well-prepared to safeguard digital infrastructures.

Today's youth are uniquely positioned to support the cyber security needs of the future. Their digital nativeness, innovative spirit and commitment to education and social causes make them the most promising generation to tackle cyber security challenges. As digital pioneers, they are paving the way for a secure and resilient digital future, ensuring a balanced view on how technology benefits society while also protecting against the ever-evolving threat of cyberattacks.





CURSOS 2024

CCSA



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.

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.

CCSE



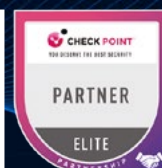
Check Point Certified **SECURITY EXPERT**

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

Consúltenos para obtener más información:
entrenamiento@sseguras.com
www.sseguras.com





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.



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.



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.



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, contróelos 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 sensibles.



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 brinda 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.



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.



IPS Y PROTECCIÓN AVANZADA PARA REDES Y SERVIDORES

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.



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.



EVALUACIÓN CONTINUA DE COMPROMISO

Descubra su nivel de compromiso en minutos. Mida el compromiso con rapidez y precisión. Toma de decisiones impulsada por IA.



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 la postura de ciberseguridad de su negocio.



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.



PLATAFORMA DE GESTIÓN DE EXPOSICIÓN DE TODOS SUS ACTIVOS, EN CUALQUIER PARTE

Reduzca el riesgo cibernético. Comprenda mejor sus riesgos cibernéticos y tome decisiones prácticas para abordarlos.

SÍGUENOS EN NUESTRAS REDES SOCIALES



SOLUCIONES SEGURAS

Empresas Protegidas, Empresas Tranquilas

ACERCA DE SOLUCIONES SEGURAS

Con más de 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.



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
infoqt@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**

