24 de noviembre 2021
Online

¿Ransomware ha cambiado las reglas de la ciberseguridad?

Forthcoming events

e-crime & cybersecurity GERMANY 20th January 2022 Frankfurt	PCI LONDON 26th January 2022 London	e-crime & cybersecurity CONGRESS 2nd & 3rd March 2022 London	e-crime & cybersecurity CONGRESS 9th March 2022 Dubai
e-crime & cybersecurity FRANCE 22nd March 2022 Paris	e-crime & cybersecurity NORDICS 12th May 2022 Stockholm	e-crime & cybersecurity GERMANY 2nd June 2022 Munich	e-crime & cybersecurity CONGRESS 7th June 2022 Doha
SECURING FINANCIAL SERVICES 6th July 2022 London	e-crime & cybersecurity CONGRESS 21st September 2022 Abu Dhabi	e-crime & cybersecurity SWITZERLAND 28th September 2022 Zurich	e-crime & cybersecurity MID-YEAR 19th October 2022 London
e-crime & cybersecurity NORDICS 1st November 2022 Copenhagen	e-crime & cybersecurity SCOTLAND 9th November 2022 Edinburgh	e-crime & cybersecurity SPAIN 16th November 2022 Madrid	e-crime & cybersecurity BENELUX 8th December 2022 Amsterdam

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

El año pasado, las organizaciones españolas se vieron muy afectadas por los ciberataques y, como es el caso a nivel mundial, el ransomware es la amenaza número uno.

Todos los sectores, incluidos los elementos cruciales de la CNI, como el gobierno, las finanzas y la atención médica, se han visto afectados. En marzo de 2020, justo cuando comenzó la pandemia, un hospital de Madrid fue desconectado por ransomware. Desde entonces, gigantes regionales como Mapfre, SegurCaixa Adeslas, Adif y muchos otros han sido víctimas.

El Servicio Público de Empleo del Estado, que gestiona las prestaciones por desempleo y ha sido fundamental durante la pandemia, fue "paralizado" por ransomware a principios de este año, poco seguido por el Ministerio de Trabajo y Economía Social.

El hecho de que algún nivel de tolerancia estatal (si no apoyo real) para los criminales de ransomware está claramente involucrado, finalmente, también está comenzando a ser reconocido. Las agencias de inteligencia estadounidenses recibieron instrucciones de investigar el ataque de Kaseya y las conversaciones sobre el ciberespionaje se están volviendo comunes. Los gobiernos se dan cuenta de que dejar la ciberseguridad en manos del sector privado puede no ser suficiente.

La investigación realizada por proveedores de seguridad muestra que los expertos cibernéticos españoles son muy conscientes de la amenaza, y el 85% ya ha sufrido al menos un ataque de ransomware en el último año o lo espera. La propia investigación de AKJ indica que el perfil del CISO dentro del negocio, y los recursos asignados a la ciberseguridad, han aumentado para igualar el riesgo. Pero con los equipos aún sin personal y bajo presión, la pregunta en la mente de todos es: ¿será suficiente?

Veremos esto y mucho más en este último Congreso de e-Crime & Cybersecurity España en línea. El evento es una oportunidad fantástica para escuchar estudios de casos de la vida real y sesiones técnicas detalladas de colegas sobre cómo la digitalización acelerada requiere un nuevo tipo de seguridad. Aproveche esta oportunidad para establecer contactos con sus compañeros en la sala de networking, plantear preguntas a los oradores en el auditorio y visitar la sala de exposiciones para relacionarse con los proveedores de soluciones. Esperamos que disfrute del evento, por favor visite nuestro equipo en el mostrador

Simon Brady | Editor

@eCrime_Congress **#ecrimecongress**

24 de noviembre 2021

Online

Editor:
Simon Brady
e: simon.brady@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
t: +44 (0) 20 7242 7820
e: simon.brady@akjassociates.com

© AKJ Associates Ltd 2021. All rights reserved. Reproduction in whole or part without written permission is strictly prohibited.

Articles published in this magazine are not necessarily the views of AKJ Associates Ltd. The publishers and authors of this magazine do not bear any responsibility for errors contained within this publication, or for any omissions. This magazine does not purport to offer investment, legal or any other type of advice, and should not be read as if it does.

Those organisations sponsoring or supporting e-Crime & Cybersecurity Spain VR bear no responsibility, either singularly or collectively, for the content of this magazine. Neither can those organisations sponsoring or supporting e-Crime & Cybersecurity Spain VR, either singularly or collectively, take responsibility for any use that may be made of the content contained inside the magazine.

Ransomware de doble extorsión

Hace un año y medio, el ransomware de "doble extorsión" estaba siendo utilizado por un solo ciberdelincuente conocido. Actualmente, más de 16 grupos de ransomware utilizan activamente esta táctica. Entonces, ¿qué es y por qué se ha vuelto tan popular?

Par Brianna Leddy

¿Qué es el ransomware de doble extorsión?

La historia tradicional del ransomware era la de un código malicioso que cifraba rápidamente archivos con encriptación RSA de clave pública y luego los borraba si la víctima no pagaba el rescate.

Sin embargo, después del infame ransomware WannaCry y NotPetya durante 2017, las empresas intensificaron su ciberdefensa. Se puso más énfasis en las copias de seguridad y los procesos de restauración, para que incluso si los archivos fuesen destruidos, las organizaciones tuvieran copias en su lugar y pudieran restaurar fácilmente sus datos.

Sin embargo, a su vez, los ciberdelincuentes también han adaptado sus técnicas. Ahora, en lugar de simplemente encriptar archivos, el ransomware de doble extorsión extrae primero los datos. Esto significa que si la empresa se niega a pagar, la información puede filtrarse en línea o venderse al mejor postor. De repente, todas esas copias de seguridad y planes de recuperación de datos se volvieron obsoletos.

Maze ransomware y amigos

A finales de 2019, Maze ransomware surgió como el primer caso de alto perfil de doble extorsión. Pronto siguieron otras cepas, con el ataque Sodinokibi, que paralizó a la empresa de cambio de divisas Travelex, en el último día de ese año.

A mediados de 2020, cientos de organizaciones fueron víctimas de ataques de doble extorsión, varios sitios web en la *dark net* filtraban datos de la empresa y el negocio de Ransomware-as-a-Service estaba en auge a medida que los desarrolladores vendían y alquilaban nuevos tipos de malware.

Además, las regulaciones de ciberseguridad comenzaron a ser armadas por ciberdelincuentes que podían aprovechar la amenaza de tener que pagar una fuerte multa de cumplimiento (regulaciones CCPA, RGPD, NYSDFS) para alentar a sus víctimas a guardar silencio ofreciéndoles un rescate menor que la multa.

A pesar de que se redactan regularmente nuevas leyes para tratar de mitigar estos ataques, no se están ralentizando. Según un estudio reciente realizado por RUSI, hubo 1.200 incidentes de ransomware de doble extorsión solo en 2020 en 63 países diferentes. El 60% de estos estaban dirigidos a organizaciones con sede en los EE. UU., y el Reino Unido sufrió el segundo mayor número de infracciones.

Hace unos meses, la banda de ciberdelincuentes conocida como REvil publicó detalles sobre la nueva Macbook Pro de Apple en su sitio "Happy Blog", amenazando con publicar más planos y exigiendo un rescate de $50 millones. Colonial Pipeline supuestamente pagó $5 millones en bitcoin para recuperarse de un devastador ataque de ransomware de OT.

Anatomía de un ataque de ransomware de doble extorsión

Darktrace ha detectado un gran aumento en las amenazas de ransomware de doble extorsión en el último año, más recientemente en una empresa de energía con sede en Canadá. Los hackers claramente habían hecho su tarea, adaptando el ataque a la empresa y moviéndose rápida y clandestinamente una vez dentro.

Darktrace detectó cada etapa de la intrusión y notificó al equipo de seguridad con alertas de alta prioridad. Si Darktrace Antigena hubiese estado activo en el entorno, el servidor atacado habría sido aislado tan pronto como comenzara a comportarse de manera anómala, evitando que la infección se propagara.

Cifrado y exfiltración

Se desconoce el vector de infección inicial, pero la cuenta de administrador se vio atacada muy probablemente por un enlace de phishing o una implementación de vulnerabilidad. Esto es indicativo de una tendencia a alejarse de las campañas generalizadas de ransomware "spray and pray" de la última década hacia un enfoque más específico.

La IA de Autoaprendizaje identificó un servidor interno que participaba en un escaneo de red inusual y un intento de movimiento lateral utilizando el Protocolo de escritorio remoto (RDP). Las credenciales de administrador comprometidas se utilizaron para propagarse rápidamente desde el servidor a otro dispositivo interno, "serverps".

El dispositivo "serverps" inició una conexión saliente a TeamViewer, un servicio de almacenamiento de archivos legítimo, que estuvo activo durante casi 21 horas. Esta conexión se utilizó para el control remoto del dispositivo y para

Es importante defenderse de estos ataques antes de que sucedan, implementando de manera proactiva medidas de ciberseguridad que puedan detectar y responder de manera autónoma a las amenazas tan pronto como surjan.

facilitar las etapas posteriores del ataque. Aunque TeamViewer no operaba por completo en el entorno digital de la empresa, ninguna de las defensas heredadas lo bloqueó.

Luego, el dispositivo se conecta a un servidor de archivos interno y **descargó 1,95TB de datos** y subió el mismo volumen de datos a pcloud [.]com. Esta exfiltración tuvo lugar durante las horas de trabajo para combinarse con la actividad administrativa habitual.

También se vio que el dispositivo descargaba el software Rclone, una herramienta de código abierto, que probablemente se aplicó para sincronizar datos automáticamente con el servicio de almacenamiento de archivos legítimo pCloud.

La credencial de administrador atacada permitió que el ciberdelincuente se moviera lateralmente durante este tiempo. Una vez completada la exfiltración de datos, el dispositivo "serverps" finalmente comenzó a cifrar archivos en 12 dispositivos con la extensión *.06d79000.

Como ocurre con la mayoría de los incidentes de ransomware, el cifrado ocurrió fuera del horario de oficina (durante la noche en hora local) para minimizar la posibilidad de que el equipo de seguridad responda rápidamente.

Investigación impulsada por IA

Cyber AI Analyst informó sobre cuatro incidentes relacionados con el ataque, destacando el comportamiento sospechoso al equipo de seguridad y proporcionando un informe sobre los dispositivos afectados para su reparación inmediata. Estos informes concisos permitieron al equipo de seguridad identificar rápidamente el alcance de la infección y responder en consecuencia.

Cyber AI Analyst investiga on-demand

Tras un análisis más detallado, el día 13 de marzo, el equipo de seguridad contrató a Cyber AI Analyst para realizar investigaciones a demanda sobre la credencial de administrador comprometida en Microsoft 365, así como sobre otro dispositivo que se identificó como una amenaza potencial.

Cyber AI Analyst creó un incidente para este otro dispositivo, que resultó en la identificación de un escaneo de puertos inusual durante el período de tiempo de la infección. El dispositivo se eliminó rápidamente de la red.

Doble problema

El uso de herramientas legítimas y técnicas de "Living off the Land" (utilizando RDP y una credencial de administrador comprometida) permitió a los ciberdelincuentes llevar a cabo la mayor parte del ataque en menos de 24 horas. Al implementar TeamViewer como una solución de almacenamiento de archivos legítima para la exfiltración de datos, en lugar de depender de un dominio conocido como "malo" o registrado recientemente, los hackers eludieron fácilmente todas las defensas existentes basadas en firmas.

Si Darktrace no hubiera detectado esta intrusión y hubiera alertado de inmediato al equipo de seguridad, el ataque podría haber resultado no solo en una "negación del negocio" con empleados bloqueados en sus archivos, sino también en la pérdida de datos confidenciales. La IA fue un paso más allá para ahorrarle al equipo un tiempo vital con la investigación automática y los informes a demanda.

Hay mucho más que perder con el ransomware de doble extorsión. La exfiltración proporciona otra capa de riesgo, lo que lleva a comprometer la propiedad intelectual, dañar la reputación y multas por incumplimiento. Una vez que un grupo de amenazas tiene los datos, es posible además que solicite más pagos en el futuro. Por lo tanto, es importante defenderse de estos ataques antes de que sucedan, implementando de manera proactiva medidas de ciberseguridad que puedan detectar y responder de manera autónoma a las amenazas tan pronto como surjan. □

Brianna Leddy, Director of Analysis, Darktrace.

Más información en:
www.darktrace.com

Lucha contra el ransomware con IA

Darktrace es la única tecnología que interrumpe el ransomware de forma autónoma, sin provocar cierres costosos.

darktrace.com/es/ransomware

DARKTRACE

The World Has Changed. Has Your Security?

SentinelOne. The End of Passive Security.

Malware doesn't need a connection to attack, and neither should your cybersecurity. SentinelOne delivers Online/Offline Protection across any platform or OS—because if your security only works online, it doesn't work.

Trusted by the Best

ASTON MARTIN norwegian flex McKESSON

SentinelOne®

sentinelone.com

SentinelOne "reinventa" la ciberseguridad con su solución autónoma basada en inteligencia artificial

Las empresas deben poner en marcha buenas estrategias y soluciones de ciberseguridad para hacer frente a las dificultades y prepararse para el futuro.

Par SentinelOne

La crisis sanitaria ha puesto a prueba la ciberseguridad y alterado una gran cantidad de certidumbres por su envergadura e imprevisibilidad. Las empresas son ahora conscientes de que deben poner en marcha buenas estrategias y soluciones de ciberseguridad para hacer frente a las dificultades y prepararse para el futuro.

Según usted, ¿cómo será el ecosistema de la ciberseguridad en los próximos años?

En la actualidad, los ataques son cada vez más sofisticados y furtivos. Lo hemos visto con el malware Sunburst, que ha afectado a miles de empresas, infraestructuras e instituciones públicas. Los ciberdelincuentes se profesionalizan y emplean kits "listos para utilizar", disponibles en la red oscura, que les permiten lanzar ataques masivos, rápidos y automatizados contra varios puntos de entrada al mismo tiempo.

Con el desarrollo del Internet de las cosas (IoT) y de la transformación digital, las empresas son ahora más vulnerables a los ciberataques, y los antivirus tradicionales ya no son suficientes. La proliferación de dispositivos, junto con el teletrabajo, añade todavía más presión a empresas que carecen del tiempo y los recursos, y el uso de la automatización parece más necesario que nunca para administrarlos y protegerlos. Para seguir prosperando en tiempos de crisis, las empresas deben elaborar una estrategia eficaz de ciberresiliencia.

¿Cómo se trasladará esto en la práctica a las herramientas de seguridad, y en particular, a su área de actividad?

En un mundo dominado por la nube y los dispositivos móviles, donde el sistema de información está cada vez más distribuido, y en el que el teletrabajo se ha convertido en la norma, serán muchas las empresas que van a desplegar la arquitectura de confianza cero (Zero Trust), que permite saber quién, con un determinado dispositivo, accede a qué información, cuándo lo hace y desde dónde.

En los próximos años, las empresas también recurrirán cada vez más a soluciones de seguridad SaaS (Software-as-a-service), fáciles de desplegar a través de la nube y harán un uso más generalizado de servicios gestionados, que les permita externalizar la seguridad de sus sistemas de información.

> El aprendizaje automático y el análisis del comportamiento serán muy pronto parte integral de las soluciones de ciberseguridad para detectar las ciberamenazas y los comportamientos maliciosos en tiempo real y prevenir la propagación de los ataques.

Incluso si tienen que reorganizar su política de seguridad en función del contexto actual, las tecnologías EPP/EDR serán siempre la prioridad de los CISO en lo que a inversión se refiere. La idea es disponer de una vista centralizada de las herramientas necesarias para correlacionar los eventos y bloquear los ataques en tiempo real.

Por último, la inteligencia artificial y la automatización seguirán ganando terreno. El aprendizaje automático y el análisis del comportamiento serán muy pronto parte integral de las soluciones de ciberseguridad para detectar las ciberamenazas y los comportamientos maliciosos en tiempo real y prevenir la propagación de los ataques. Además, la inteligencia artificial permitirá a las empresas paliar la escasez de expertos cualificados en ciberseguridad.

Pero, además de la adquisición de soluciones técnicas avanzadas, la mejora de la seguridad pasa por un comportamiento más responsable de los usuarios, ya que basta una simple negligencia para poner en peligro la seguridad de todo un sistema de la información. Por lo tanto, es esencial que las empresas aumenten sus esfuerzos de formación y concienciación de sus empleados.

¿Cómo va a evolucionar su oferta en este sentido?

SentinelOne utiliza inteligencia artificial para proteger, en cada etapa del ciclo de vida de la amenaza, a las

SentinelOne utiliza inteligencia artificial para proteger, en cada etapa del ciclo de vida de la amenaza, a las empresa más importantes a nivel mundial, así como para evitar que sean víctimas de grandes ciberataques en el futuro.

empresa más importantes a nivel mundial, así como para evitar que sean víctimas de grandes ciberataques en el futuro. A día de hoy, sigue siendo la única solución de ciberseguridad totalmente autónoma que integra funciones de prevención, de detección/respuesta para todos los activos de la empresa, desde las estaciones de trabajo a los dispositivos IoT, pasando por los contenedores y cargas de trabajo en la nube. SentinelOne ofrece a las empresas absoluta transparencia de todas las actividades de red y sustituye eficazmente a los antivirus tradicionales.

Son muchos los reconocimientos que avalan la calidad de su rendimiento. SentinelOne es la única empresa de protección de endpoints, reconocida por su innovadora plataforma XDR basada en inteligencia artificial, que figura en la clasificación AI 100 de CB Insights. El informe MITRE Engenuity ATT&CK ™ de abril de 2021 refleja que se trata del único proveedor de soluciones EDR que ofrece el 100 % de visibilidad de las tácticas de ataque de Carbanak y FIN7. Asimismo, la empresa ha sido incluida por primera vez entre los líderes del Magic Quadrant 2021 de Gartner en la categoría de plataformas de protección para endpoints. Y, por último, por 2° año consecutivo, figura en la lista Disruptor 50 de la CNBC (4º lugar), que demuestra su capacidad de "reinventar" la ciberseguridad a través de una inteligencia artificial patentada.

La división de investigación, SentinelLabs, nos permite además supervisar los nuevos ataques y métodos empleados por los hackers, así como adaptar nuestras soluciones en consecuencia. □

Más información en:
www.sentinelone.com

SentinelOne™

Por que la microsegmentación debe ser una prioridad para los Bancos

Las instituciones financieras necesitan una solución que pueda aumentar la seguridad y al mismo tiempo promover la eficiencia operativa.

Par Guardicore

La microsegmentación permite a las instituciones financieras alcanzar una serie de objetivos clave mientras protegen sus aplicaciones críticas a través de un enfoque único y directo. Las instituciones financieras tienen un fuerte requerimiento de ahorro de costos a través de la automatización, la optimización de recursos y las tecnologías ágiles. Necesitan una solución que pueda aumentar la seguridad y al mismo tiempo promover la eficiencia operativa.

Además, las instituciones financieras siempre han sido los principales objetivos para la delincuencia. Según Forbes, los ataques cibernéticos cuestan más a las instituciones financieras que las empresas de cualquier otra industria. Dado que las transacciones remotas e indirectas son la norma en estos días, los atacantes tienen aún más oportunidades para romper la seguridad del perímetro. Esto aumenta aún más el riesgo de incumplimiento y los costos de remediación.

¿Cómo pueden los bancos usar la microsegmentación para resolver estos problemas? Veamos...

¿Cuáles son los desafíos de Ciberseguridad que enfrentan los bancos?

- La gestión de los controles de seguridad cibernética en los servicios financieros es una tarea compleja. Existen numerosos controladores que hacen que el trabajo requiera mucho tiempo y recursos, como:
- Hay requisitos de Ciberseguridad a nivel de país que deben seguirse, sin mencionar los mandatos de seguridad de los proveedores y diversas regulaciones de privacidad. En conjunto, imponen una gran cantidad de desafíos de informes y gestión de riesgos.
- La banca moderna depende en gran medida de una gran cantidad de aplicaciones de terceros, socios y proveedores externos que acceden al centro de datos a través de una variedad de rutas de acceso.
- La infraestructura de red en evolución deja a las organizaciones con una combinación de tecnología en la nube y sistemas heredados, en un entorno enredado que es difícil de visualizar, auditar y proteger.

Todos esos factores combinados con una multitud de herramientas, usuarios y presiones externas hacen que las instituciones financieras sean especialmente vulnerables al delito cibernético.

Permitir la transformación digital para un mejor servicio al cliente y disponibilidad conduce a más formas para que los bancos sean vulnerables al fraude y a las transacciones no autorizadas. Los clientes son conscientes de estos problemas cada vez mayores y desean asegurarse de que su privacidad y sus finanzas estén protegidas.

> "Los clientes son cada vez más conscientes de las amenazas a la seguridad cibernética y esperan que sus bancos y cooperativas de crédito aseguren y protejan su información financiera privada."
> **Consejo de Cooperativas de Crédito (CUC), FS-ISAC, 2019**

> "Los bancos han validado esta tendencia al informar que las pérdidas debidas a la interrupción operativa y las pérdidas en la confianza de los clientes son más perjudiciales desde el punto de vista financiero que las pérdidas debidas a multas regulatorias."
> **Análisis comparativo de ciberseguridad de Deloitte y FS-ISAC, 2019**

Cuatro maneras en que los bancos pueden beneficiarse de la microsegmentación

La mejor manera de abordar estos desafíos es crear un único panel de seguridad, con visibilidad completa del tráfico de red y aislamiento total de las joyas de la corona digitales. Mediante el uso de controles de microsegmentación flexibles, de despliegue rápido y fáciles de entender, las instituciones financieras pueden proteger sus activos principales de manera simple y efectiva.

Para obtener el máximo provecho de una solución de microsegmentación, hay cuatro pasos críticos a seguir:

1. Simplifique y acelere el cumplimiento normativo

Para lograr este objetivo, comience mapeando todo y aislando todas las aplicaciones y sistemas relacionados con el cumplimiento. La visualización granular lo

ayudará a comprender la mejor manera de reducir el riesgo de violaciones de forma rápida y fácil.

2. Proteja sus sistemas esenciales

Separe las aplicaciones críticas, como transferencias de dinero, pagos y aplicaciones de clientes de la infraestructura de TI general.

3. Evite el movimiento lateral no autorizado

Aísle adecuadamente el acceso a IoT y a terceros. Además, administre las rutas de acceso y finalice el acceso en las aplicaciones de destino, evitando más movimientos dentro del centro de datos.

4. Adopte la nube, PaaS y otras tecnologías emergentes de forma rentable y segura

Utilice un solo panel de administración para obtener visibilidad y establecer políticas de seguridad en todas las infraestructuras. Además, asegúrese de aplicar la seguridad a través de un conjunto unificado de herramientas.

Cómo funciona la microsegmentación en la vida real

¿Necesita pruebas de que el enfoque de microsegmentación funciona? A continuación, se muestra un ejemplo de un cliente de Guardicore, un banco regional de EE. UU., Que pudo producir grandes mejoras utilizando las capacidades de visualización y microsegmentación de Guardicore Centra.

Este banco tenía algunas iniciativas en marcha:

- Cumplir con el mandato de Fedline de aislar cualquier aplicación conectada al servicio Fedline de la TI general.
- Proteja diez de sus aplicaciones más críticas para reducir significativamente los riesgos cibernéticos y garantizar la continuidad del negocio en caso de incumplimiento.
- Limite el acceso de terceros para hacer cumplir los controles de acceso Zero Trust.
- Hacer posible migrar aplicaciones de forma segura a la nube.
- Mantenga un único conjunto de controles de seguridad en toda la infraestructura híbrida.

Con un solo arquitecto de seguridad, en el transcurso de dos meses, el cliente pudo cumplir con todos sus objetivos más allá de las expectativas originales. Al final, pudieron:

- Logre una visibilidad granular del tráfico de este a oeste.
- Proteja sus aplicaciones críticas para el negocio.
- Restringir y enrutar adecuadamente el acceso de terceros.
- Mapear las dependencias de las aplicaciones para una migración a la nube sin problemas.
- Logre la automatización completa de procesos con la integración de DevOps.

¿Buscando por más? Esto es lo que tienen que decir algunos de nuestros otros clientes:

"Guardicore nos permite mejorar nuestra estrategia general de seguridad del centro de datos y ayudar a nuestro equipo de seguridad de TI a evitar las amenazas avanzadas de hoy."
Marino Aguiar, CIO, Santander Brasil

"Deutsche Bank está comprometido con los más altos estándares de seguridad, y una alta prioridad para nosotros es implementar una estricta segmentación de la red en nuestros entornos locales y en la nube. Guardicore nos ofrece una forma eficaz de proteger nuestros activos críticos mediante la segmentación."
Alan Meirzon, director, director de seguridad de la información

Utilice la microsegmentación para proteger sus joyas de la corona hoy

Con controles de microsegmentación simples y fáciles de administrar, las instituciones financieras pueden reducir la superficie de ataque y detectar rápidamente brechas dentro del centro de datos. La visibilidad profunda de las dependencias de las aplicaciones y los flujos de tráfico ayuda a aplicar políticas precisas a nivel de proceso y de red que aíslan las aplicaciones y los sistemas críticos.

No olvide buscar una herramienta que proporcione una cobertura de seguridad completa para las aplicaciones, independientemente de dónde residan. Después de todo, la mayoría de las instituciones financieras necesitan proteger las cargas de trabajo que abarcan plataformas y entornos: locales, heredados y bare metal, máquinas virtuales, contenedores y nubes públicas y privadas (incluidos Infraestructuras Amazon Web Services, Microsoft Azure, Google Cloud y Oracle Cloud). □

Más información en:
www.guardicore.com

Guardicore

¿Sabía que se prevé que cada 11 segundos se produce un nuevo ataque de ransomware?

RANGEFORCE

Upskill in an On-Demand Cyber Range

Experience hands-on and interactive cybersecurity training for you and your team. Start your RangeForce journey today and prove your strength against the latest cyber attacks.

rangeforce.com

© Copyright — RangeForce

Cyber range and simulation-based training use case coverage

How a new generation of e-learning and simulation technologies is changing the way CISOs operationalise cybersecurity.

Next generation training to improve cyber-defence

Everyone is familiar with the three legs of cybersecurity: people, process, and technology. However, most investments of time and money go to just one area – technology. A growing investment in technology should not be a surprise when vendors continue to push technology-only solutions. At the same time, security training focuses mostly on end-users and social-engineering/phishing awareness. On a related note, there has been no easy, unified way to measure cybersecurity process or operational effectiveness. As a result, cyber-incidents continue to grow in number and magnitude.

RangeForce offers the industry's only integrated cybersecurity simulation platform that is focused on improving the skills of each security team member and how they work together. Critical new cybersecurity skills can now be learned in hours, rather than weeks, by team members at any time and anywhere. But the real value of simulation-based cybersecurity training does not stop there – it offers additional value to the cybersecurity organisation across seven important use cases, including visibility, hiring, onboarding, skills-building, and more.

Understanding and reporting cybersecurity effectiveness

Your board wants to know, your CEO wants to know, your compliance team wants to know, and you want to know – Can the security team handle a real cyber-attack that can steal from and even shut down my business? The answer to this question typically comes in the days and weeks following an attack. In its worst outcome, revenue and customers are lost, fines are levied, and careers ended. By focusing on continuous training, assessments, and simulation exercises and by capturing all of these activities in unified reporting, CISOs and security managers can build on strengths and remediate weaknesses. CISOs can then report an accurate assessment of a team's skills and a path to improvement to executives, and compliance teams to achieve confidence across an organisation.

Dealing with staffing shortages

Hiring experienced cybersecurity professionals is difficult and, for many, not an option. A robust approach to countering staffing and skills shortages is to build a flexible team through role-based cross-training. Following a military developed model where each member of a team is trained on multiple positions, CISOs can use RangeForce assessments and learning paths to identify their most proficient cyber-pros and cross-train them into other security areas. Cross-training decisions can be based on skills gaps, processes models, role timing, and technology employed. The goal is to optimise the roles covered by each team member at each stage in the detection and response process, so no one is 'sitting on their hands' at any time during an incident.

> "Due to our company location, we do not have a lot of local security talent to choose from. Utilising RangeForce for cross-training, especially our best IT folks, has allowed us to meet our security team resource requirements."

Improving hiring processes through assessment

When a company is looking to bring on new security talent, **RangeForce can improve the hiring process.** With the existing skills shortage, candidates are likely to be fresh out of school or through a cyber-training certificate programme. The candidates may not have the operational skills needed to effectively fill the role or the aptitude to be trained in the role. For this reason, security managers can no longer rely on a candidate's resume, training certificates, or professional references for qualification. What is needed is a way to assess a candidate's cyber-defence skills across a variety of attack vectors and security tools – RangeForce assesses cyber-defence skills across a variety of attack vectors and security tools.

Getting new hires up to speed quickly

When new cybersecurity team hires come on board, it often takes many months to train them into the role. Often, they are sent to vendor and third-party training, followed by months of on the job training, while shadowing a more senior member of the team already in the role. A recent Ponemon Institute survey[1] found that the time to hire and train one analyst is almost one year.

RangeForce reports

RANGEFORCE

RangeForce has developed a series of Cybersecurity Learning Paths that cover both introductory and advanced role-based skills development.

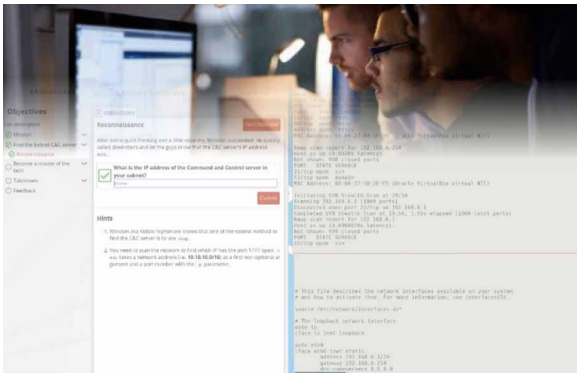
Starting with Security Operations Analyst (Level 1), a new hire completes approximately 30 hours of training customised to match the needs and tools of the role. The Learning Paths include simulation-based assessments so security managers can watch the learner's progress and assure required skills are being developed. Within weeks, the new hire can operate independently in their role, saving significant time and cost for the security team.

Career path development and improved retention

Cybersecurity leaders can improve the retention of valuable staff by building career paths that include increasing responsibility, training, and certificates. **RangeForce delivers learning paths that can be combined to create career paths for security staff.** Because these learning paths can be configured to the roles and tools of any cybersecurity team, they give team leaders a tool to build the career of a young analyst over multiple years and into new roles that the analyst is interested in obtaining.

Optimising security tool investments

RangeForce integrates leading security tools in both its hands-on training module coverage and in its Battle Fortress Cyber Range so that security operators can utilise their security stack. They learn through a series of lessons delivered in RangeForce training modules that take them from introduction to advanced usage. Then they move to the Battle Fortress Cyber Range to test and practice their skills on the tool until they are honed to a razor's edge.



Conclusion

If one of the most significant challenges facing cybersecurity is the shortage of and investment in human capital, then an investment in RangeForce is a wise decision. Initial testing on the RangeForce platform allows CISOs to assess where their company's staff is genuinely prepared for a variety of different cyber-attacks and where improvement is needed. Once employees' skills are assessed, RangeForce provides a turnkey solution: centrally administered training tools help address problem areas using state-of-the-art tools and approaches. Testing without training doesn't offer today's CISO with current data. Testing, followed by training, followed by additional testing, provides CISOs with hard evidence of how they are improving their company's readiness for an eventual cyber-attack.

CISOs at these forward-thinking companies have shifted investment from technology to people and adopted a strategy to improve cyber-readiness focused on:

- Role-based advanced cyber-defence training
- On-demand, interactive, hands-on lessons
- Standards-based (NIST/MITRE/OWASP) learning modules
- Simulated attack scenario training
- Individual & team skills assessments and reporting

What's preventing you from making the same investment in your human capital? □

[1] The Economics of Security Operations Centers: What is the True Cost for Effective Results? Ponemon Institute.© Research Report Sponsored by Respond Software Independently conducted by Ponemon Institute LLC. Publication Date: January 2020.

About RangeForce

RangeForce creates accessible cybersecurity training experiences for you and your team. Powered by the industry's first integrated training platform and virtual cyber range, we help customers operationalise a SaaS-based cybersecurity training program in hours, saving up to 65% over traditional training and up to $1m annually on hosted cyber ranges. RangeForce is revolutionising cybersecurity training with its adaptive learning technology to better train and cross-train DevOps, IT, and security professionals. Train with us to build cyber-resilience, and follow us on LinkedIn and Twitter.

For more information, please visit **www.rangeforce.com**

RANGEFORCE

Patrocinadores

Darktrace | Patrocinadore estratégico

Darktrace es la empresa líder mundial en ciber IA y creadora de la tecnología de Autonomous Response (Autonomous Response). La IA de auto-aprendizaje se ha modelado en el sistema humano y es utilizado por más de 3.500 organizaciones para proteger contra las amenazas dirigidas hacia la nube, correo electrónico, IoT (Internet de las cosas), redes y sistemas industriales.

La empresa tiene más de 1.200 empleados y cuenta con sede en San Francisco y Cambridge, Reino Unido. Cada 3 segundos, la IA de Darktrace defiende contra una amenaza cibernética, evitando que causen daños.

Para obtener más información, visite www.darktrace.com

Guardicore | Patrocinadore estratégico

Guardicore is an innovator in data centre and cloud security that protects your organisation's critical assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security – for any application, in any IT environment. Guardicore was founded in 2013 with the goal of reinventing security to place greater emphasis on security beyond the traditional network perimeter. Guardcore has been entrusted to protect the data centres of enterprises across North America, South America, and EMEA in financial, healthcare and retail industries, including global, blue-chip brands.

For more information, please visit www.guardicore.com

RangeForce | Patrocinadore estratégico

RangeForce develops the world's most comprehensive cybersecurity training and cyber-skills assessment programme. RangeForce believes in the power of skilling up SOC and cybersecurity professionals through advanced cyber-defence training, combining this with the ability to accurately and quantitatively assess your team's genuine preparedness to combat real cyber-attacks. Every day, hackers invent new creative techniques, with regulators administering increasingly significant fines. Using our Battle Skills individual training platform in combination with the Battle Fortress team event cyber-range, we help companies mitigate their cybersecurity risk and boost the effectiveness and efficiency of their security operations. Our advanced threat training covers the very latest attack and defence techniques, all delivered through a browser and on real infrastructure. No prep, no set-up, no testing, no kit, no downtime, no hassle. All you have to do is log in, learn, assess and transform – for a fraction of the cost of traditional learning.

For more information, please visit www.rangeforce.com

Recorded Future | Patrocinadore estratégico

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organisations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organisations around the world.

Learn more at recordedfuture.com

SentinelOne | Patrocinadore estratégico

SentinelOne's cybersecurity solution encompasses AI-powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous platform.

For more information, please visit www.sentinelone.com

Synack | Patrocinadore estratégico

Synack, la plataforma de seguridad de colaboración abierta más confiable, ofrece pruebas de penetración integrales y continuas con resultados de acciones concretas. La compañía combina a los piratas informáticos (hackers) éticos más capacitados y confiables del mundo con tecnología habilitada para inteligencia artificial para crear una solución de seguridad escalable y efectiva. Con sede en Silicon Valley y oficinas regionales en todo el mundo, Synack protege a los principales bancos mundiales, las 10 principales firmas de consultoría y empresas de seguridad mundiales, los activos clasificados del Departamento de Defensa y más de $2 trillones en ingresos de Fortune 500. Synack fue fundada en 2013 por los ex expertos en seguridad de la NSA Jay Kaplan, Director General (CEO), y el Dr. Mark Kuhr, Director de Tecnología (CTO).

Para obtener más información, por favor visítenos en www.synack.com

CybelAngel | Patrocinadore del seminario de educación

CybelAngel provides an innovative solution of data leaks detection on the Internet.

We monitor the Dark Web and the Internet of Things to identify threats that could adversely affect our customers. We identify, in real time, the new risks on the web that target large companies. Every day we detect sensitive data circulating via the Internet without any protection such as passwords, credit cards, confidential documents, etc.

We have automated the entire information search process. This allows us to monitor a large number of sources at a high frequency. When a risk is identified, we perform a detailed human analysis to supplement the detected information. Having eliminated false positives, we then alert the companies, providing them with a precise analysis of the existing risk so they can take appropriate remedial steps.

We offer a service that can be easily integrated into existing security solutions. This service is non-intrusive, does not need to be installed on our customers' IT infrastructure and is based on a list of keywords that includes in particular domain names, IP addresses as well as subsidiary, brand and product names.

When a risk is detected, we alert our customers via a secure interface. This interface makes it possible to manage threats effectively. A control panel facilitates the monitoring of alerts over time, from the detection to the resolution of threats.

For more information, please visit www.cybelangel.com

Kenna Security | Patrocinadore del seminario de educación

Kenna Security es al empresa líder en gestión de vulnerabilidades basadas en riesgos (RBVM). Utilizando la plataforma de Kenna Security, las organizaciones pueden trabajar de forma transversal para determinar y arreglar los riesgos cibernéticos. Kenna se aprovecha de la ciencia de datos y el aprendizaje automático para rastrear y predecir vulnerabilidades del mundo real, de modo que los equipos de seguridad puedan centrarse en lo más importante. Kenna presta servicio a casi todos los sectores importantes y cuenta con CVS, KPMG y muchas otras empresas de la lista Fortune 100 entre sus clientes.

Las puntuaciones de riesgo de Kenna, otra innovación pionera de la RBVM, ofrecen a la seguridad, a las TI, a los ejecutivos, a los miembros de la junta directiva y a otras partes interesadas una forma sencilla y eficaz de evaluar el riesgo relativo de una vulnerabilidad específica, de una clase de activos, de un grupo de trabajo y de las organizaciones en su conjunto.

Recientemente adquirida por Cisco, la aclamada gestión de vulnerabilidades basada en riesgos de Kenna Security se combinará con SecureX, la plataforma que conecta la cartera de seguridad más amplia e integrada de la industria, proporcionando a las organizaciones globales la capacidad de identificar y evaluar las amenazas, identificar las vulnerabilidades con más probabilidades de suponer un riesgo, y dar a los equipos de remediación una orientación clara sobre lo que hay que arreglar primero.

Cisco SecureX aportará capacidades adicionales al integrar las soluciones de gestión de la seguridad de la empresa en una ubicación centralizada, ofreciendo a los equipos una forma integral de acabar con los silos, ampliar las capacidades de detección y respuesta, y orquestar y remediar con confianza.

Al integrar Kenna Security en SecureX, las empresas resolverán una pieza notoriamente difícil del rompecabezas de la seguridad y ofrecerán la pionera plataforma de RBVM de Kenna a más de 7.000 clientes que utilizan Cisco SecureX en la actualidad.

Todo ello refleja la determinación de Cisco de agilizar y simplificar la gestión de seguridad a través de una plataforma abierta y altamente integrada que reúne la gestión de amenazas y vulnerabilidades.

Para obtener más información, consulte las últimas noticias y visite kennasecurity.com

OneLogin | Patrocinadore del seminario de educación

Onelogin, el líder del Control de Acceso Unificado, conecta las personas con la tecnología a través de un inicio de sesión simple y seguro, empoderando a las empresas a acceder al mundo™. La plataforma de Control de Acceso Unificado de Onelogin (UAM) es la clave para desbloquear aplicaciones, dispositivos y datos, mejorando la productividad y facilitando la colaboración. Onelogin da servicio a empresas y partners de multitud de industrias, con mas de 2500 clientes alrededor del mundo.

Para mas información, visita www.onelogin.com

OPSWAT | Patrocinadore del seminario de educación

OPSWAT is a global leader in critical infrastructure cybersecurity that helps protect the world's mission-critical organisations from malware and zero-day attacks. To minimise the risk of compromise, OPSWAT Critical Infrastructure Protection solutions enable both public and private organisations to implement processes that ensure the secure transfer of files and devices to and from critical networks. More than 1,000 organisations worldwide spanning financial services, defence, manufacturing, energy, aerospace, and transportation systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations, and protect their reputation, finances, employees and relationships from cyber-driven disruption.

For more information on OPSWAT, visit www.opswat.com

AGENDA

08:00	Inicio de sesión y redes
08:50	Bienvenida a la conferencia
09:00	**Ransomware: un desafío para la continuidad del negocio, no solo una contingencia de TI** **Maite Avelino,** Jefa de Ciberseguridad, Ministerio de Defensa de España • Identifique sus procesos comerciales críticos y dónde se encuentran alojados • Formas "modernas y cómodas" de realizar copias de seguridad que no funcionan contra el ransomware • La segmentación de la red y los NAC son fundamentales • La importancia de un buen Plan de Comunicación para evitar "ramonguares"
09:20	**El auge del Ransomware en estos tiempos** **Carlos Payés,** Sales Engineer y **Raúl Benito,** Regional Sales Manager Iberia, SentinelOne • ¿Cómo vemos la preparación de las empresas para estos ataques post-COVID? • Estado del arte de soluciones EDR/XDR • Ransomware As A Service • Tipos de partners y conocimeintos. Posicionamiento a nivel global
09:40	**Ransomware en el punto de mira: cómo la IA contiene quirúrgicamente la amenaza** **José Badía López,** Country Manager, España & Portugal, Darktrace • Inmediatamente después de un ataque de ransomware, los ejecutivos se enfrentan con demasiada frecuencia a un dilema difícil: pagar un rescate o cerrar los sistemas y servicios críticos • En los ecosistemas digitales cada vez más complejos de la actualidad, el daño colateral que resulta de los ataques de ransomware puede ser de amplio alcance y destructivo, y las organizaciones tardan días, semanas o incluso meses en recuperarse. Pero, ¿qué pasaría si hubiera otra salida, una forma de contener quirúrgicamente el ransomware en sus primeras etapas, sin interrumpir las operaciones comerciales normales? • Únase a esta presentación para descubrir cómo la IA de Autoaprendizaje está ayudando a miles de organizaciones a luchar contra el ransomware. Hablaremos sobre: El impacto del ransomware de "doble extorsión" y el "ransomware como servicio"; Ejemplos reales de ransomware detectados por la IA de Autoaprendizaje; Cómo la IA de autoaprendizaje responde proporcionalmente al ransomware, gracias a su profundo conocimiento del patrón de vida de una organización
10:00	**Perspectiva del CEO de la ciberseguridad** **Fernando Vegas,** Former CIO & CRO, OHL Group • Visión comparada de la evolución de los costes de la ciberseguridad y de los daños causados por incidentes • Comparación de los datos anteriores con la visión global del World Economic Forum • Visión general de los riesgos más relevantes • Perspectiva estratégica: Contención técnica, Organización y Aseguramiento
10:20	**Seminario de educación | Sesión 1** **CybelAngel** **Cómo romper la cadena del Ransomware** **Vijay Kishnani,** Lead Cyber Security Engineer, CybelAngel **OneLogin** **Aprovechamiento de IAM para una mitigación de amenazas eficaz y eficiente** **Lonnie Benavides,** Head of Infrastructure and Application Security, OneLogin
10:50	Descanso de networking
11:20	**Un enfoque estratégico clave en un periodo de cambio** **María Luz Garin,** Responsable Seguridad de la información, Eroski • Las promesas de los proveedores de servicios en la nube • Matriz de responsabilidades compartida – Incorporando los riesgos y las amenazas de migrar a la nube • Probar una migración y analizar los riesgos
11:40	**Explorando la Microsegmentación: Consiga visibilidad, Detenga el ransomware y Proteja las aplicaciones críticas** **Julen Cordon,** SE for Iberoamerica, Guardicore • ¿Cómo tener una base sólida para detener la propagación del ransomware, lograr proteger las cargas de trabajo y el cumplimiento de la normativa? • Entienda porque la visibilidad, el aislamiento y la segmentación de las aplicaciones de red y sus componentes son factores cruciales. • El Zero Trust como un requisito de seguridad • El panorama actual: el uso de la nube dinámica, entornos híbridos y sistemas heredados y la necesidad de velocidad para hacer cumplir las políticas, escalar sus operaciones y reducir la superficie de ataque

12:00 **Testimonio de Cliente: ODDO-BHF: Prueba de Penetración Colaborativa con Synack**

Gaël Barrez, Sales Director, Synack, **Willem Peerbolt,** ODDO-BHF Group CISO y **Matthew West,** Solutions Architect, Synack

- Por qué ODDO, BHF pasó de las pruebas de penetración clásicas a las de colaboración colectiva
- Cómo la plataforma de pruebas de seguridad remota de Synack está ayudando a aumentar los equipos internos de ODDO-BHF
- Qué resultados y beneficios está obteniendo la empresa
- La entrevista será seguida por una demostración de nuestra plataforma

12:20 **La necesidad de talento táctico-operativo en materia de CiberInteligencia**

Enrique Ávila, Director, Centro de Análisis y Prospectiva de la Guardia Civil y Director del Centro Nacional de Excelencia en Ciberseguridad de la UAM

- Escenario actual
- Conocimiento táctico-operativo
- Plataformas de formación y entrenamiento
- Gemelos digitales
- Conclusiones

12:40 **Seminario de educación | Sesión 2**

Kenna Security

Cisco SecureX + Kenna Security: simplificación radical en la nueva era de la ciberseguridad

Stephen Roostan, VP, EMEA, Kenna Security

OPSWAT

Protección de infraestructura crítica por OPSWAT

Alessandro Porro, Vice President, Global Channels, OPSWAT

13:10 Almuerzo y networking

14:00 **Test de re-identificación: riesgos y protección del dato**

Jesús Alonso Murillo, CISO Europe, Campofrio Food Group

- Test de re-identificación
- Detalles de la valoración del riesgo
- Ejemplos de re-identificación
- Conclusiones

14:20 **El auge de los infostealers en España**

Danny Panton, Cybercrime Intelligence Analyst, Latin America, Recorded Future

- Planeando compartir información sobre la popularidad y el aumento de las variantes de los ladrones de malware de información en España que están capturando los datos privados y las credenciales de cuenta de muchas organizaciones conocidas en el país
- La presentación examinará y analizará más a fondo las variantes más habituales apalancadas en España
- La web oscura común y las fuentes del mercado clandestino donde estas variantes de ladrones de malware se utilizan más para obtener registros y datos privados

14:40 **Garantizar la preparación cibernética de sus equipos de defensa de infraestructuras acaba de entrar en una nueva era**

Rupert Collier, VP of International Sales, RangeForce

- Un enfoque de aprendizaje combinado que utiliza la educación a ritmo propio, junto con ejercicios regulares en equipo, es la mejor manera de desarrollar la memoria muscular para las ciberemergencias reales
- Los ciberdefensores pueden seguir beneficiándose de un desarrollo profesional continuo totalmente a través de un navegador, pero siempre de forma práctica
- Los CISO y los líderes de los SOC pueden supervisar y evaluar con precisión los niveles de habilidad dentro de sus equipos, con el fin de identificar cualquier posible brecha de cobertura que pueda representar una amenaza para el negocio
- La información y las métricas procesables sobre el rendimiento y los niveles de habilidad de los miembros del equipo pueden ayudar a identificar a las superestrellas de la ciberseguridad, tanto las que ya están en su organización como las que pueden querer unirse
- Todo esto está disponible a una fracción del coste del aprendizaje tradicional, con métricas de éxito mucho mejores y sin una sola clase aburrida a la vista

15:00 **El análisis forense de la evidencia de datos se ha vuelto vital**

Angel Bahamontes, Presidente y Director, ANTPJI y Presidente de delitos informáticos

- Cómo navegar de forma segura y evitar la piratería. Legal y técnicamente
- Cómo actuar ante la delincuencia informática: respuesta técnica y jurídica
- Creación de un Gabinete de Respuesta a Incidentes Tecnológicos

15:20 Descanso de networking

15:50 **Aplicar forense Cibernético para la seguridad**

Alejandro Rivas-Vásquez G, Socio, Responsable de Digital Forensics, KPMG

- Analizar el fraude de gastos y cómo las empresas pueden protegerse
- Control y gestión de incidencias
- Cómo preparar, prevenir y evitar costos

16:10 **Surviving the cybersecurity revolution**

Simon Brady, Managing Editor, AKJ Associates

- Why the return to work is a dangerous moment for security
- Why DX means no more tolerance of failure at the basics
- Left-field lessons from a year of breaches
- What our research reveals about the region's CISOs

16:30 Palabras de clausura y descanso de networking

17:00 Cierre de conferencia

Seminarios Educativos

Dentro de la agenda del día tendrán lugar una serie de seminarios, a los que podrán asistir nuestros delegados según sus preferencias, con la posibilidad de interactuar y participar activamente, aportando sugerencias y consejos prácticos personales.

Session 1: 10:20–10:50

CybelAngel

SESSION 1
10:20–10:50

Cómo romper la cadena del Ransomware

Vijay Kishnani, Lead Cyber Security Engineer, CybelAngel

Los ataques de ransomware, cada vez más frecuentes, han demostrado ser una amenaza para las cadenas de abastecimiento a nivel global, desde el petróleo, hasta la alimentación o la sanidad.

Ante el peligro, las empresas deben asumir un rol proactivo para luchar contra estos ataques.

Durante esta sesión cubriremos:

- Algunos ataques recientes – qué podemos aprender de las tácticas de prevención y la respuestas aplicadas tras los ataques
- Cómo los atacantes escogen a sus víctimas, localizan los puntos de infiltración, infectan los sistemas y chantajean a las empresas
- Buenas prácticas para prevenir los ataques de ransomware

OneLogin

SESSION 1
10:20–10:50

Aprovechamiento de IAM para una mitigación de amenazas eficaz y eficiente

Lonnie Benavides, Head of Infrastructure and Application Security, OneLogin

No hay duda de que el panorama actual de la ciberseguridad cambia y evoluciona constantemente a medida que surgen nuevas amenazas y soluciones de seguridad. El aumento de los ataques cibernéticos y las fuerzas de trabajo distribuidas han creado nuevos desafíos que requieren soluciones innovadoras.

Frente al desafío de administrar identidades y asegurar el acceso a datos y aplicaciones desde un número creciente de terminales, ¿cuáles son los controles fundamentales que las organizaciones necesitan para mantener la continuidad del negocio y proteger su fuerza de trabajo remota e híbrida?

Escuche a Lonnie Benavides, jefe de Infraestructura y seguridad de aplicaciones de OneLogin, en una charla sobre información práctica y consejos sobre la utilización de soluciones de administración de identidad y acceso para mitigar eficazmente las amenazas cibernéticas modernas en su negocio.

Conclusiones clave:

- Comprender los fundamentos clave de una postura sólida de seguridad en la nube
- Por qué las contraseñas por sí solas no son suficientes
- Mejores prácticas para construir una estrategia de ciberseguridad a escala

Session 2: 12:40–13:10

Kenna Security

SESSION 2
12:40–13:10

Cisco SecureX + Kenna Security: simplificación radical en la nueva era de la ciberseguridad

Stephen Roostan, VP, EMEA, Kenna Security

La ciberseguridad es un reto difícil. Lo que se necesita es una forma de simplificar radicalmente las operaciones de seguridad para que sean sencillas, automatizadas y democratizadas. Así pues, independientemente de la complejidad de su entorno de TI y de la cantidad de amenazas que puedan dirigirse a su organización, protegerlo no debería ser difícil.

Cisco reconoce esta necesidad y define un camino a seguir. Al integrar la aclamada plataforma de gestión de vulnerabilidades basada en el riesgo de Kenna Security, SecureX de Cisco ayudará a las organizaciones a resolver una pieza notoriamente difícil del rompecabezas de la seguridad para acelerar el tiempo de respuesta para la preparación cibernética.

En esta sesión, Stephen Roostan, vicepresidente para EMEA de Kenna Security, que ahora forma parte de Cisco, detalla por qué la adquisición de Kenna por

parte de Cisco es un movimiento fundamental para los clientes y el sector en su conjunto.

- La información sobre amenazas en el mundo real, el aprendizaje automático y el análisis predictivo ayudan a los equipos a identificar y priorizar sus vulnerabilidades más arriesgadas
- Los equipos de reparación sabrán qué arreglar y cuándo, ahorrando tiempo, dinero y recursos
- La integración de las soluciones de gestión de seguridad de la empresa en una ubicación centralizada rompe los silos y amplía las capacidades de detección y respuesta
- Los flujos de trabajo automatizados ayudan a reducir los perfiles de riesgo de la organización, a mejorar la colaboración entre la seguridad y la TI y a reducir sus superficies de ataque
- Las puntuaciones de riesgo de Kenna ayudan a las partes interesadas a evaluar claramente el riesgo relativo de una vulnerabilidad específica, una clase de activos, un grupo de trabajo o una organización en su conjunto
- Para acelerar la toma de decisiones con la priorización de los datos de vulnerabilidad basados en la inteligencia de amenazas y el valor empresarial de los activos
- La incorporación de Kenna Security a SecureX amplía las capacidades XDR más amplias del sector

OPSWAT

SESSION 2
12:40–13:10

Protección de infraestructura crítica por OPSWAT

Alessandro Porro, Vice President, Global Channels, OPSWAT

¿Cómo se pueden proteger las transferencias de archivos en toda la empresa, especialmente entre dispositivos no controlados? Alessandro Porro, Vicepresidente de ventas de canal en OPSWAT, mostrará cómo proteger la transferencia de archivos hacia, a través y fuera de entornos seguros para evitar el malware y / o la perdida de datos.

- Prevención de infracciones con escaneo múltiple
- Cumplimiento de ciberseguridad
- Control perimetral digital con bloqueo automático de dispositivos
- Transferencia de archivos segura con bloqueo de medios automatizado □

Vulnerability intel + Data science = Insight you can act on.

Modern Vulnerability Management

Focus on the threats that matter most.

Remediate faster and more efficiently with data-driven risk prioritization.

www.kennasecurity.com

Kenna and Kenna Security are trademarks and/or registered trademarks of Kenna Security, Inc. and/or its subsidiaries in the United States and/or other countries. © 2021 Kenna Security, Inc. All rights reserved.

CISCO | KENNA Security

Ponentes y Panelistas

e-Crime & Cybersecurity Spain se complace EN dar la bienvenida a los delegados, ponentes y panelistas. El evento cuenta con la asistencia de representantes de alto nivel y tomadores de decisiones en la industria.

Jesús Alonso Murillo

CISO,
Ferrovial

Jesús Alonso es un apasionado de la CiberSeguridad que cuenta con más de 15 años de experiencia en Seguridad de la Información, en empresas de consultoría, telecomunicaciones, sector financiero y de servicios. Su carácter polifacético, le ha permitido desarrollar su carrera desde el punto de vista de auditoría, control y muy especialmente en el riesgo de IT (desde áreas de riesgo y tecnología) y Ciberseguridad (desde las áreas de control y operación). Durante su dilatada experiencia ha tenido la oportunidad de defender sistemas complejos frente amenazas externas protegiendo el dato en organizaciones dónde es un activo crítico. Cuenta con las certificaciones CISA, CRISC, CDPSE, Lead Auditor 27001.

Maite Avelino

Responsable de Ciberseguridad,
Ministerio de Defensa

Es Licenciada en Matemáticas y Máster en Seguridad TIC. Es CISA, CISSP y PMP y también está especializada en Criptología Aplicada. Maite Avelino es miembro de ISACA Madrid y PMI Madrid. Ha trabajado en varias áreas y sectores de las TIC como desarrolladora, analista de sistemas, bases de datos, comunicaciones, implementación de productos en empresas como Cap Gemini, IECISA y Carrefour. En el año 2002 comenzó a trabajar en el sector de la ciberseguridad con IBM, dando servicio en su SOC. Después pasó a trabajar en el sector de la consultoría, cumplimiento normativo y auditoría de ciberseguridad en sectores variados como defensa, espacio, aeronáutica y administración pública de la mano de GMV. En el 2015 pasó como funcionaria a trabajar como Jefa de Servicio de la Oficina de Seguridad SGTIC en el Ministerio de Hacienda coordinando la implementación del Esquema Nacional de Seguridad y proporcionando consultoría y concientización en la solución de ciberincidentes. Recientemente este año se ha incorporado al Ministerio de Defensa en el Centro de Sistemas TIC. Sus funciones actuales también son la coordinación de soluciones de ciberseguridad, implementación de PKI y cumplimiento normativo.

Enrique Ávila

Director del Centro de Análisis y Prospectiva de la Guardia Civil y Director del Centro Nacional de Excelencia en Ciberseguridad de la UAM

En la actualidad, Director del Centro de Análisis y Prospectiva de la Guardia Civil y Director del Centro Nacional de Excelencia en Ciberseguridad de la UAM. Anteriormente ha dirigido el Área de Seguridad de la Información de la Guardia Civil así como múltiples proyectos de Ciberseguridad en sus destinos en el Ministerio del Interior, Tribunal Constitucional y Dirección General de la Guardia Civil. Licenciado en Derecho por la UCM, es Máster en Análisis de Evidencias Digitales y lucha contra el Cibercrimen por la UAM, Delegado de Protección de Datos acreditado por la Fundación Ortega-Marañón y Especialista Universitario en Servicios de Inteligencia por el IUGM. Además forma parte de la VI Promoción STIC del Centro Criptológico Nacional

Jose Badía López

Country Manager Spain & Portugal,
Darktrace

Jose Badía, Country Manager de España y Portugal en Darktrace, líder mundial de IA para la ciberseguridad. José lidera a los equipos en clientes de una variedad de industrias que utilizan la inteligencia artificial para la defensa de sus compañías, incluyendo entre otros, bancos, entidades gubernamentales y empresas energéticas. José dispone de una extensa carrera académica que destacan por su Grado en Comercio por la Universidad Complutense de Madrid, así cómo un MBA en Cesma Business School.

Angel Bahamontes

Presidente y Director, ANTPJI y
Presidente de delitos informáticos

Presidente y fundador de la Asociación Nacional de Tasadores y Peritos Judiciales Informáticos; ANTPJI. Director de la Cátedra de Informática Forense y Delitos Informáticos. Director del Máster de Peritaje Informático Judicial y del Máster de Comunicación y Marketing Digital CEIS y Jefe de Estudios en la

Escuela de Negocios Nieves Tapia del Máster de Marketing y Liderazgo. Asesor en el Parlamento Europeo para Peritajes Tecnológicos. Emprendedor Pro-activo. Headhunters tecnológico. Consultor, Gestor y Supervisor de negocios TICs. Dotes y larga trayectoria en Marketing, Comunicaciones, Medios de Prensa. Colaborador en programas televisivos de investigación. Conferenciante nacional e internacional en Peritaje Informático Judicial. Formador de Peritos Judiciales Informáticos. Más de 16 años capacitando a alumnos en diversos cursos especializados en Gestión, Dirección y Creación de Empresas, Marketing estratégico, Técnicos de Informática, Tasación y Valoración Informática, Peritaje y Evidencia Digital.

Miembro del Comité de expertos de SEPBLAC,MCM CORPORATION, IUICP, Plataforma Tecnológica FÉNIX, Comisión tecnológica de Bruselas. Colaboro desinteresadamente en proyectos a nivel nacional como internacional, realizando un voluntariado muy comprometido en ONGs como INFATOS dedicada a alfabetización digital de colectivos afectados por la brecha digital, Federación de Deportes de Minusválidos, Síndrome de Down, Persona rígida, Dislexia, Nuevo Proyecto Podemos y colabora activamente en varias plataformas de manera desinteresada como Haces falt.org.

Gaël Barrez

Director Comercial, Synack

Gaël Barrez es el Director Comercial de Synack. En este cargo, es responsable de supervisar las operaciones de Synack en el sur de Europa y Turquía. Gaël tiene más de 20 años de experiencia en ventas, liderazgo y desarrollo comercial de ciberseguridad. Ha ayudado principalmente a las 2000 empresas más importantes de EMEA a proteger su negocio principal contra un amplio espectro de riesgos cibernéticos y amenazas terroristas. Aporta experiencia en seguridad de aplicaciones, seguridad de redes, gobernanza y gestión de riesgos, seguridad de desarrollo de software, criptografía, soluciones antifraude, PCI-DSS, OWASP. Gaël posee un Máster en Marketing y Gestión de TI de EPITA, una escuela de ingeniería en Francia. En su tiempo libre, a Gaël le gusta bucear, viajar y aprender cosas nuevas.

Lonnie Benavides

Head of Infrastructure and Application Security, OneLogin

Lonnie Benavides is an accomplished cybersecurity leader with more than 20 years industry experience, and is currently the Head of Infrastructure and Application Security at OneLogin. Lonnie began his career as a communications encryption specialist in the US Air Force and went on to conclude his military service as a Technical Lead of the first red team in the Air National Guard. As an advanced penetration tester, Lonnie supported companies such as Washington Mutual and JP Morgan Chase, and eventually went on to launch the Boeing red team. Lonnie was responsible for leading global cybersecurity services and operations at DocuSign and McKesson, fostering his expertise in enterprise cyber-threat detection and response. Lonnie is a recognised speaker within the Phoenix education community, numerous industry conferences, and has also contributed to publications and radio shows such as TechRepublic and NPR.

Raúl Benito

Regional Sales Manager, SentinelOne

Raúl Benito, Regional Sales Manager Iberia, nos presenta su visión basada en su larga experiencia de más de veinte años en el mercado de seguridad. Raúl Benito ha formado parte de la estrategia de protección de empresas como McAfee, Trend Micro, Check Point, Qualys y actualmente forma parte de SentinelOne como responsable de poder dotar a las grandes empresas en Iberia de la mejor tecnología XDR del mercado, siempre de la mano de los mejores partners de seguridad que tenemos actualmente. La experiencia en labores de desarrollo de canal, consultoría de grandes clientes del sector financiero e industrial avalan las mejores prácticas para poder implementar una solución de seguridad avanzada en cualquier tipo de empresa.

Rupert Collier

VP of International Sales, RangeForce

Rupert Collier es el vicepresidente de ventas internacionales de RangeForce y ha trabajado en la industria de la ciberseguridad durante muchos años en una variedad de funciones de liderazgo. Rupert dará algunas pinceladas sobre los fascinantes antecedentes de RangeForce y explicará por qué el enfoque de aprendizaje combinado (individual y en equipo), utilizando técnicas de formación práctica, es tan bien recibido por las empresas corporativas de todo el mundo.

Julen Cordon

SE for Iberoamerica, Guardicore

Ligado al mundo de la ciberseguridad los últimos 20 años en diferentes fabricantes y asumiendo

diferentes roles. Actualmente dedicado a trasladar los beneficios de la segmentación definida por software con casos de uso concretos como el Ransomware.

Vijay Kishnani

Lead Cyber Security Engineer, CybelAngel

Vijay Kishnani is the Lead Cyber Security Engineer at CybelAngel. His team focuses on demonstrating the value of CybelAngel to prospective customers by leveraging our technology to identify live data leaks that can be found inside the supply chain. Vijay Kishnani has previously worked with PricewaterhouseCoopers, Merrill Lynch, and Goldman Sachs.

María Luz Garin

Responsable de Seguridad de la Información, Grupo Eroski

Responsable de Seguridad de Grupo Eroski Desde abril de 2015, ha estado en Eroski desde mayo de 2007. Con anterioridad a este cargo siempre ha estado en Procesos, proyectos y sistemas dentro del mundo de la Economía Financiera. Antes de su etapa en Eroski, estuvo vinculada al mundo de SAP - Ecofin. Licenciada en Informática por la Universidad de Deusto. Máster en Consultoría e implementación de sistemas ERP.

Danny Panton

Analista de inteligencia de ciberdelincuencia en América Latina, Recorded Future

Danny es parte del Grupo Insikt de Recorded Future, también conocido como el departamento de inteligencia de amenazas de la compañía. Está a cargo de las investigaciones de delitos cibernéticos en América Latina, pero también se utiliza a menudo como analista de inteligencia de amenazas híbridas y realiza investigaciones sobre geopolítica latinoamericana, como inestabilidad política y financiera, delitos y eventos especiales en la región que atraen la atención mundial. Además del español, también habla portugués con fluidez. Danny tiene un grado universitario en Relaciones Internacionales y actualmente está cursando su maestría en Forense Digital en la Universidad de Florida Central.

Carlos Payés

Sales Engineer, SentinelOne

Carlos Payés, SE SentinelOne Iberia; Carlos nos presenta una visión técnica del estado del arte de la seguridad en el entorno empresarial. Su gran experiencia en grandes clientes de nivel internacional, y fabricantes de seguridad como Qualys, avalan un amplio conocimiento en el mundo del EDR, gestión de vulnerabilidades y cumplimiento normativo. Actualmente desempeñando el rol de Sales Engineer en SentinelOne para la región de Iberia apoyando y fortaleciendo a partners y clientes existentes. Además colabora a nivel internacional para implementar planes de seguridad en empresas de reconocido prestigio.

Willem Peerbolt

CISO (Director de Seguridad de la Información) del Grupo ODDO-BHF

Willem Peerbolte es CISO de Grupo en ODDO-BHF, el principal grupo financiero independiente franco-alemán. Willem tiene más de 15 años de experiencia en ciberseguridad. En particular, trabajó durante más de diez años para BNP Paribas. Primero, como CISO en Arval, luego en CIB-GECD, y finalmente en la oficina central, como Director del Programa de Transformación de Seguridad Cibernética para todo el Grupo BNP Paribas. En su tiempo libre, Willem dirige su taller de modelado e impresión 3D.

Alessandro Porro

Vice President, Global Channels, OPSWAT

Alessandro ha liderado con éxito Global Channels en la industria de TI / Software durante los últimos 20 años. Recientemente, Alessandro pasó los últimos años en Ipswitch, Inc., construyendo un ecosistema mundial altamente productivo que logró un crecimiento consistente anual de más del 30% con una alta rentabilidad, que culminó con la adquisición por parte de Progress Software Corp. a principios de 2019. Posteriormente, Progress invitó a Alessandro a liderar su canal global de 300 millones de dólares/ año, donde logró una consecución de objetivo del 113% desde marzo de 2019 hasta junio de 2020.

Alejandro Rivas-Vásquez G

Socio, Responsable de Digital Forensics, KPMG

Alejandro Rivas-Vásquez G., Socio de KPMG, reconocido experto asesor de compañías multinacionales en los sectores de energía y financiero sobre la gestión de riesgo tecnológico, ciber y de fraude digital. Cuenta con una trayectoria de más de 18 años en su mayoría en Londres y, desde 2017, en Madrid. Estratégicamente, fue el arquitecto de los servicios de KPMG Ciberseguridad en UK y continúa colaborando en la innovación de servicios de

ciber y forensic a nivel global. Desde su incorporación en KPMG España, ha impulsado iniciativas de Ciber M&A, Arquitectura Segura, Cuantificación de Ciberriesgos, Ciberinteligencia, y de Informática Forense en Disputas Comerciales. A nivel técnico, Alejandro ha liderado proyectos de transformación ciber, implantación de soluciones, outsourcing, hacking ético, respuesta ante ciberincidentes, investigaciones de computer forensic y proyectos de eDiscovery, entre otros. Ha actuado como Expert Witness en diversas intervenciones criminales y civiles. Ha asesorado a consejos de administración, comités de riesgos y comisiones de auditoria de empresas en UK, Holanda y España. Fue reconocido por el Palacio de Buckingham por su participación en un programa para mejorar los conocimientos de ciber riesgos de los CEOs del FTSE350. Operacionalmente, Alejandro es responsable de nuestro equipo de Digital Forensics & Incident Response, asesorando a empresas privadas o entidades públicas a nivel internacional en la prevención, detección, respuesta e investigación de incidentes tanto de cibercriminales como de defraudadores. También, asesorando en casos de disputas comerciales y arbitrajes, directa o indirectamente según las necesidades técnicas de los encargos.

Stephen Roostan

VP EMEA,
Kenna Security

Stephen Roostan has over a decade of experience in cybersecurity and transformation projects, his role at Kenna is to rapidly grow the EMEA organisation to meet the customer demand for risk-based vulnerability management. Prior to Kenna, he held senior sales roles at Forcepoint, Citrix and Imperva, focusing on IT solutions for complex, enterprise requirements. Roostan has a passion for driving equality alongside enabling flexibility at work for modern lifestyles. He has held steering committee roles in companies looking to close the gender pay gap and develop careers for working parents, and strives to find and support equality initiatives across the workplace and industry. He believes that creating a collaborative and supportive working culture is hugely productive for both an organisation and its employees.

Fernando Vegas

Former CIO and CRO,
OHL

Fernando Vegas es un Ingeniero Civil con un doctorado. De la Universidad Politécnica de Madrid y PDD por IESE Business School. Ha sido CIO durante más de 25 años en varias empresas españolas del IBEX-35, Director de Organización durante 10 años, Responsable de Riesgos durante 3 años, y ha investigado durante 6 años escribiendo una tesis doctoral sobre una nueva metodología para evaluar la gravedad del riesgo y la resumir los escenarios de riesgo, desarrollando un sistema de gestión de riesgos completamente nuevo que se está utilizando en una empresa constructora internacional. Tiene un amplio conocimiento del campo de las tecnologías de la información, adquirido a lo largo de más de 35 años de trabajo en actividades relacionadas con las tecnologías de la información, en industrias como centrales nucleares, ferrocarriles y construcción. En 2020 fue nominado a Emerging Risk Initiative of the Year en los European Risk Management Awards 2020 y obtuvo el segundo premio en los Premios ANCI de Tesis Doctoral 2020. En 2019 ganó el premio Julio Sáez, destinado al mejor trabajo de investigación relacionado con el riesgo. Ha recibido dos premios a la Mejor Idea de Innovación relacionados con la Inteligencia Competitiva aplicada a la evaluación de riesgos (2014 y 2015). Como miembro de CIONET, ARIA, ASIS y AGERS (FERMA) ha aumentado sus conocimientos sobre otras empresas de otras industrias; como miembro del grupo de trabajo de riesgo cibernético de AGERS durante 3 años, ha participado en dos libros publicados sobre riesgos cibernéticos. Esa amplia experiencia lo ayuda a concentrarse en las necesidades de la junta con una visión general del negocio. Ha publicado artículos sobre TI y gestión de riesgos en revistas indexadas y ha impartido conferencias en PMI (Valencia Chapter), Institute for Competitive Intelligence, Agers Annual Congress, entre otros. Como profesor, ha dictado conferencias en la universidad en programas de maestría sobre TI, riesgo y la industria de la construcción, y conferencias sobre filosofía y psicología en instituciones privadas.

Matthew West

Solutions Architect,
Synack

Matthew West ha estado involucrado en ciberseguridad durante más de 20 años y ha trabajado con varias empresas y organizaciones que van desde proveedores de energía y organizaciones financieras hasta gobierno y defensa. Su enfoque ha sido la consultoría en los sectores de pruebas de penetración y gestión de vulnerabilidades. Matthew se incorporó a Synack en Mayo de 2021 como arquitecto de soluciones para el sur de Europa, Benelux y las regiones Nórdicas. □

La economía se basa en la confianza

Synack Trust Report 2021.

Par Synack

En pleno 2021, ya hemos visto cómo los ciberataques han hecho tambalear la confianza de los consumidores en los últimos meses y han provocado el pánico en las gasolineras. No solo en las gasolineras, sino también en nuestros sistemas de transporte, en nuestras escuelas y en nuestras necesidades diarias, causando un gran perjuicio a nuestra vida cotidiana.

Todo esto llega después de un año de agitación y transformación. La pandemia aceleró las iniciativas de transformación digital de las operaciones e impulsó los esfuerzos por implantar la seguridad de confianza cero en el teletrabajo. Reforzar la resiliencia cibernética sigue siendo una prioridad en nuestras organizaciones, empresas y sociedades y es algo que tiene que ir acompañado de confianza.

La Administración Biden ha hecho de la ciberseguridad una prioridad y ha publicado recientemente un memorando dirigido a los líderes empresariales en el que les exhorta a tomar medidas importantes para prevenir el ransomware y otros ciberataques, incluyendo el uso de servicios de pentesting de terceros para probar la "capacidad de defensa ante un ataque sofisticado" de empresas y sistemas. Los ejecutivos que pongan su empeño en la confianza de los accionistas y las empresas que den prioridad a las pruebas de seguridad y tomen medidas proactivas para analizar nuevos activos y aplicaciones digitales tendrán, a largo plazo, protecciones más sólidas y menos vulnerabilidades.

Clasificación de las industrias según su resistencia al atacante

Más información

La confianza sigue siendo más valiosa que nunca. La confianza no solo es crucial en nuestras relaciones comerciales y con los clientes, sino también en nuestra vida cotidiana.

El Trust Report de 2021 es la guía esencial de Synack para que los CISO, los CIO, los profesionales de la seguridad y los ejecutivos de la C-suite y de los consejos de administración entiendan cómo medir la seguridad, determinar los riesgos y crear confianza con datos y perspectivas sobre el estado de diferentes industrias y sectores de la economía.

En su cuarto volumen, el acreditado informe global comparte datos de las marcas más confiables basados en miles de pruebas de seguridad realizadas por los hackers éticos más capacitados del mundo, El Synack Red Team (SRT). El informe destaca las

Clasificación media de la industria por años (tal y como se publicó en anteriores ediciones del Trust report)

Sector	2019	2020	2021
Gobierno	47	61	64
Sanidad	60	56	61
Servicios financieros	57	59	58
Tecnología	46	55	57
Comercio electrónico	48	47	57
Venta al por menor	45	46	55
SLED	46	50	49
Consultoría/Servicios empresariales y de TI	53	48	52
Fabricación/Infraestructura crítica	70	45	50

La calificación ARS se basa en los datos del Trust Report: 2019. Datos hasta enero de 2019
Calificación de la ARS basada en los datos del Trust Report: 2020.
Datos hasta julio de 2020
Calificación de la ARS basada en los datos del Trust Report: 2021.
Datos hasta abril de 2021.

En el futuro, el papel del CISO y de los equipos de seguridad seguirá evolucionando y ampliándose. De hecho, el 55 % de los ejecutivos de las empresas planean aumentar sus presupuestos de ciberseguridad en 2021 y el 51 % está añadiendo personal cibernético a tiempo completo en 2021.

diferentes industrias y sectores de la economía y revela nuevas perspectivas sobre cómo las organizaciones críticas están preparadas para luchar contra el ransomware y otras amenazas digitales y mantenerse resilientes.

Los datos del informe se basan en el sistema patentado de Synack de Puntuación de resistencia al atacante (ARS)™ e incluyen una comparación macroindustrial que demuestra cómo las organizaciones más fiables utilizan la clasificación ARS y cómo utilizarla para comparar la resistencia al atacante con otros sectores.

Con demasiada frecuencia, las vulnerabilidades dejan a las organizaciones peligrosamente expuestas. El año pasado, la base de datos de vulnerabilidad del US-CERT registró casi 17 500 vulnerabilidades, una cifra récord por cuarto año consecutivo. Más de un tercio (el 16 %) de las vulnerabilidades detectadas entre 2020 y abril de 2021 por el Synack Red Team (SRT), nuestra red global de investigadores de seguridad altamente cualificados y sometidos a un minucioso proceso de selección, fueron consideradas "críticas". Además, el SRT observó un aumento del 14 % en los últimos dos años en las vulnerabilidades de autorización y permiso, que pueden dar a los atacantes acceso a redes y sistemas más sensibles.

Según Jay Kaplan, CEO y cofundador de Synack *"Nos enfrentamos a una crisis mundial de ciberseguridad. Algunas organizaciones están haciendo lo correcto, creando estrategias de defensa eficaces y siendo proactivas. Otras se limitan a comprobar. Pero la naturaleza de la amenaza actual requiere un enfoque agresivo y asertivo. El Trust Report y la ARS son herramientas vitales para conocer las carencias del plan de seguridad de cualquier organización, y pueden utilizarse como herramienta para que los CISO y otros responsables de seguridad prioricen los esfuerzos de seguridad y se centren primero en las amenazas y vulnerabilidades más urgentes".*

La creciente sofisticación de las amenazas actuales hace que el CISO sea aún más vital. Además de las transformaciones digitales, las organizaciones se enfrentaron a hackeos punitivos perpetrados por estados-naciones y los ciberataques siguen aumentando en 2021. En el futuro, el papel del CISO y de los equipos de seguridad seguirá evolucionando y ampliándose. De hecho, el 55 % de los ejecutivos de las empresas planean aumentar sus presupuestos de ciberseguridad en 2021 y el 51 % está añadiendo personal cibernético a tiempo completo en 2021.

"Las pruebas, cuando se trata de seguridad, protección y resiliencia, marcan la diferencia", escribió Ritesh Patel, director de seguridad de BP, en el prólogo del Synack Trust Report de 2021. "Medidas como la Puntuación de resistencia al atacante (ARS) mantienen nuestra franqueza y nuestro nivel de conocimiento sobre lo que ocurre. La ARS nos permite evaluar constantemente nuestros resultados y comparar nuestra actuación en los distintos sectores. Es un indicador sólido de que BP está actuando por encima de la media del sector, lo que envía un mensaje claro y potente dentro de la organización de que la seguridad (y la confianza) son esenciales en todo lo que hacemos en BP".

Siga leyendo para saber cómo las marcas más fiables del mundo miden la seguridad y crean confianza mientras se adentran en otros sectores e industrias de la economía.

Synack lidera la industria en la búsqueda de las vulnerabilidades más críticas y peligrosas en los activos digitales y las aplicaciones de los clientes, dándoles la información necesaria para prevenir los ataques como se indica en las conclusiones clave de nuestro informe.

El Synack Trust Report de 2021 es su guía para medir el valor de la seguridad y la resiliencia cibernética. □

Más información en:
www.synack.com

Synack®

LA PLATAFORMA DE PRUEBAS DE SEGURIDAD COLABORATIVAS MÁS CONFIABLE

SEGURIDAD A ESCALA

Un enfoque continuo y aumentado que combina lo mejor del ser humano y de la máquina para brindar una seguridad controlada, inteligente y eficiente.

¿QUÉ ELEGIRÁ USTED?

Prueba de penetración (Pentest) tradicional:

2 consultores, 80 horas de prueba

O

Synack:

ROI (rentabilidad de la inversión) 4 veces mayor

Resultados un 40% más rápidos e impactantes utilizando lo mejor en inteligencia humana y artificial

ESCALABLE. CONFIABLE. PROBADO.

OBTENGA MÁS INFORMACIÓN EN WWW.SYNACK.COM

The only universal security intelligence solution

Recorded Future – delivering relevant cyber-threat insights in real time.

Recorded Future reports

Who we are

Using a sophisticated combination of machine and human analysis, Recorded Future fuses the broadest set of open source, dark web, technical sources, and original research together to deliver relevant cyber-threat insights in real time. The Recorded Future Security Intelligence Platform aggregates this rich intelligence with any other threat data sources, which empowers security teams to collaborate on analysis and deliver intelligence wherever they need it most – including rapid integration with existing security solutions.

Security intelligence solutions

Security intelligence accelerates detection, decision-making, and response times by positioning comprehensive intelligence at the centre of your security workflows.

- *Threat intelligence:* Gain context on who is attacking you, their motivations and capabilities, and indicators of compromise to look for in your systems. This information is searchable in real time and presented in a single-pane-of-glass view and via customised alerts.
- *SecOps and response:* Discover previously unidentified threats and triage internal alerts in your SIEM based on rich external context and threat indicators correlated with internal threat data – so you can make faster, more confident decisions
- *Brand protection:* With real-time alerting, you can find things like leaked credentials, typosquat domains, social media accounts meant to impersonate an employee or brand, fake applications, threats to executives, and more. Takedown services go the last mile to simplify and expedite the removal of malicious content from the internet.
- *Vulnerability management:* Real-time risk scores based on real-life exploitability make it easy to prioritise where you should focus efforts and what you need to patch to prevent attacks. Real-time alerting on vulnerabilities affecting your tech stack provides new insights for effective risk reduction.
- *Third-party risk:* Make informed decisions to reduce your overall risk based on insights from real-time intelligence about the vendors and partner companies that form your business ecosystem – including vulnerable technologies, domain abuse, threats targeting the organisation, and more.

Intelligence-led security

Lead with intelligence across your security teams, processes, and workflows with security intelligence solutions from Recorded Future.

- Threat intelligence
- SecOps and response
- Brand protection
- Vulnerability management
- Third-party risk
- Geopolitical risk

- *Geopolitical risk:* Accelerate critical decision making with contextual data on threats, trends, sentiments, and evolving security situations – so you can protect your assets and understand shifting geopolitical dynamics in the geographic areas that matter to your organisation.

Innovative security intelligence technologies

Security Intelligence Graph

Recorded Future's unique ability to model all relevant security information available on the internet is what has set us apart since the beginning. With billions of indexed facts, and more added every day, the Recorded Future Security Intelligence Graph leverages a unique combination of patented machine learning and human analysis to provide you with unmatched insight into emerging threats that are relevant to your organisation.

Recorded Future Intelligence Cards™

Security teams gain instant context around suspicious observables and indicators with Recorded Future Intelligence Cards – with just one click. This innovation enables security teams to rapidly prioritise threats or dismiss false-positives using Recorded Future's dynamic risk scores. All of the evidence gathered by our Security Intelligence Graph is visible on these cards, allowing you to pivot quickly between indicators and attack methods, or vulnerabilities and exploits. □

For more information, please visit
www.recordedfuture.com

Recorded Future®

Recorded Future®

Elite Intelligence to Disrupt Adversaries

The World's Most Advanced Security Intelligence Platform

Powered by patented machine learning, the Recorded Future platform automatically collects and analyzes information from an unrivaled breadth of open, dark, and technical sources. Access context-rich, actionable intelligence in real time across your entire security ecosystem.

recordedfuture.com

Cuando el eslabón más débil es invisible

Todas las empresas buscan la respuesta. ¿Cuál es la mejor estrategia para luchar contra los grupos de ransomware?

Par CybelAngel

La transformación digital de las empresas es necesaria, pero comporta algunos riesgos. Según Gartner, el coste en Shadow IT de una empresa puede representar el 40% de la inversión total en tecnologías de la información.

En un mundo cada vez más complejo los ataques son también más sofisticados. Y algunos apuntan a estos blancos invisibles para las empresas. Poco a poco, los cibercriminales van rodeando a su víctima.

Primero, reconocen el terreno en busca de fallos de seguridad, de puertas abiertas para acceder a la infraestructura tecnológica de la empresa. Entre las más comunes se encuentran las Virtual Private Networks (VPNs), los Protocolos de Escritorio Remoto (RDPs), los servidores o las bases de datos.

Una vez identificados los puntos de entrada, se infiltran en el sistema utilizando una llave: un juego de credenciales, una campaña de phishing, una vulnerabilidad (CVE), etc.

Ya sólo es cuestión de introducir el malware en el sistema. Por ejemplo, vía un email de phishing con un fichero adjunto o enlace que lance una descarga automática.

El daño ya está hecho. A continuación, el ataque. Este puede consistir en suprimir o encriptar datos para luego chantajear a la víctima.

Cómo identificar los riesgos

Una forma eficaz de prevenir un ataque de ransomware es actuar a la raíz, durante las fases de reconocimiento e infiltración.

Este objetivo requiere una doble estrategia: identificar qué puertas están abiertas y proteger las llaves que permitan abrirlas.

1. Identificar las puertas de entrada

La digitalización de las empresas ha tenido un impacto directo en el número de puertas de entrada a la infraestructura y vulnerabilidades en el sistema informático de las mismas. El teletrabajo, por ejemplo, ha aumentado el uso de Protocolos de Escritorio Remoto (RDPs) y de Virtual Private Networks (VPNs).

¿Pero cómo descubrir estas puertas de entrada? Las herramientas de protección contra los riesgos digitales proponen una solución para proteger las redes informáticas. Gracias a este tipo de herramientas las empresas pueden supervisar sus activos, ya sean dispositivos físicos, sistemas de almacenamiento en la nube o los Protocolos de Escritorio Remoto (RDPs) que forman parte de la red. El objetivo, detectar esas vulnerabilidades antes que los cibercriminales.

Asset Discovery & Monitoring es la apuesta de CybelAngel en este ámbito. Se trata de un instrumento poderoso para los equipos de SOC o IT, confrontados a este tipo de riesgos a diario.

2. Proteger las llaves

Las credenciales son el arma principal utilizada en el 80% de las técnicas de hacking y pueden convertirse en la puerta de entrada al sistema de una empresa. El uso de herramientas de prevención de toma de control de una cuenta (Account Takeover Prevention) permite la detección de credenciales expuestas en las distintas capas de internet (Clear, Deep y Dark Web).

La integración de este tipo de herramientas en los procesos de Security Information and Event Management (SIEM) es fundamental para asegurar la actualización de contraseñas antiguas.

3. A por ellos

Hemos nombrado algunas herramientas que pueden ser útiles en la prevención de riesgos digitales, como Asset Discovery & Monitoring o Account Takeover Prevention.

Para llegar más lejos es necesario ir acompañado del mejor equipo. CybelAngel ha construído una plataforma concebida para acompañar a las empresas en la digitalización y protegerlas contra los riesgos que plantea. Nuestra promesa: ningún falso positivo y alertas siempre relevantes para maximizar el tiempo de tratamiento interno de tus equipos. Todo en tiempo récord, ya que nuestro tiempo de detección es un 85% más rápido. □

Más información en:
cybelangel.com

CybelAngel

CybelAngel

WWW.CYBELANGEL.COM

Protege tu mundo digital

Protección contra riesgos externos para las amenazas digitales más críticas

Gana en visibilidad y retoma el control

Ningún falso positivo. Sólo alertas accionables

Detección un 85% más rápida

Enter the raffle here!

¡Cuidado! Los ciberdelincuentes están llegando al sector financiero

Cómo los ciberataques más coordinados y el cambio repentino a una fuerza de trabajo remota hacen que sea imperativo que los profesionales de la seguridad amplíen su visión de lo que debe protegerse.

Par OneLogin

El ciberdelito es un negocio, por lo que todos debemos ser conscientes de que los ciberdelincuentes actúan igual que otras empresas. Teniendo en cuenta el entorno económico mundial y las condiciones actuales del mercado, los ciberdelincuentes, por supuesto, seguirán centrándose en sus esfuerzos para generar fuentes de ingresos. Durante 2021, es probable que veamos a individuos y grupos de delincuentes cibernéticos asociarse para tratar de maximizar el retorno de la inversión con sus ataques. Esto significa que podrán coordinar ataques contra personas de alto valor, así como contra grandes organizaciones empresariales. En particular los sistemas financieros.

Imagino que también veremos un aumento en las amenazas internas que se utilizan como vehículo de apoyo para ejecutar ataques. Forrester predice que los empleados serán responsables del 33 % de las infracciones en 2021. Un programa de seguridad integral incorpora la medición y gestión de la actividad del comportamiento accidental a un comportamiento y/o actividades de riesgo constante.

El mensaje clave aquí es que ningún individuo ni industria está exento de estas amenazas, y requiere un enfoque, evaluación y revisión constantes para garantizar que usted y sus activos de información crítica permanezcan salvaguardados y protegidos contra ataques.

La disrupción comercial causada por la COVID-19 ha acelerado la necesidad de transformación digital dentro del sector financiero, particularmente los proveedores de la industria financiera más pequeños. Aunque muchas organizaciones más pequeñas podrían haber planeado reemplazar los procesos manuales con procesos digitales, el tiempo y el dinero a menudo les impidieron avanzar. Debido a que la pandemia los obligó a abandonar sus oficinas, muchos tuvieron que ponerse al día rápidamente y acelerar su transformación digital.

El requisito de seguridad fundamental para la industria financiera es comprender quién y qué intenta acceder a los entornos de tecnología financiera y a los datos almacenados en su interior. Los bloqueos y las regulaciones de regreso al trabajo han requerido que las organizaciones implementen modelos operativos híbridos que se adapten tanto al trabajo en la oficina como a distancia. Las organizaciones que dependían de que los usuarios solo pudieran acceder a los recursos desde la oficina ya no tienen este nivel de control. A los sistemas que solo estaban disponibles dentro de la red interna ahora se debe acceder externamente. Este cambio ha resaltado aún más la importancia de la gestión de identidades y accesos para apoyar a las empresas a través de esta transformación.

Como resultado de esta necesidad de ampliar el acceso y mantener la seguridad de los datos, estamos viendo un aumento en los proveedores financieros y médicos generales que se ponen en contacto con nosotros como expertos de la industria para asociarse en la gestión de identidades y accesos. Como proveedor de administración de identidades y accesos (IAM), somos muy conscientes de que los datos financieros están sujetos a requisitos tanto normativos como de cumplimiento, y trabajamos para garantizar que nuestros clientes comprendan cómo el uso de una plataforma IAM puede ayudarles a cumplir con sus requisitos. □

OneLogin es el principal líder de valor en la administración de identidades y accesos. Nuestra Trusted Experience PlatformTM proporciona todo lo que necesita para proteger a su plantilla, clientes y socios por un precio que se ajusta a su presupuesto. Con sede en San Francisco y la sede de la UE en Dublín, OneLogin protege más de 30 millones de identidades con más de 3000 clientes en todo el mundo, incluidos Airbus, Cruz Roja Británica y Tesco.

Para obtener más información, visite **www.onelogin.com**

onelogin

onelogin

El principal líder de valor en gestión de identidades y accesos

La plataforma de experiencia fiable ó Trusted Experience Platform de OneLogin proporciona todo lo que necesita para proteger los datos de su plantilla, clientes y socios por un precio que se ajusta a su presupuesto.

OneLogin nombrado líder en el Cuadrante Mágico de Gartner 2020 para la administración de accesos

Para obtener más información o solicitar una demostración, visite

www.onelogin.com

Evitar las fugas de datos de almacenamiento y el incumplimiento de la normativa de PII

Una reciente filtración de datos en un gran minorista de ropa provocó la exposición y la filtración de datos privados de 7 millones de usuarios.

Par OPSWAT

Los actores de la amenaza piratearon un archivo de respaldo alojado en un entorno de nube externo y robaron datos críticos de PII (información de identificación personal) como números de tarjetas de crédito, contraseñas e historial encriptados, información de contacto: direcciones, números de teléfono. etc. Esta información robada se compartió en línea donde otros piratas informáticos podrían usarla.

Esto plantea el problema mucho más serio de garantizar la seguridad de los datos cuando se almacenan en proveedores de almacenamiento en la nube de terceros. La situación de Covid19 ha obligado a las empresas a utilizar capacidades de almacenamiento compartido, no solo como respaldo sino también para su almacenamiento diario, ya que se adaptan para brindar opciones de la FMH a sus empleados.

Como dice el chiste: "La nube es sólo el ordenador de otra persona" ¿Cómo puede estar seguro de que su información almacenada está totalmente segura? En definitiva...no puede.

Confiar en el proveedor de alojamiento para la seguridad es ingenuo e irresponsable. Un buen ejemplo de cómo se comparten las responsabilidades de seguridad entre el cliente propietario de los datos y el proveedor de almacenamiento en la nube se puede encontrar en Prácticas recomendadas de seguridad de Microsoft para el almacenamiento de Azure.

Una forma muy eficaz de evitar las fugas de datos de PII es escanear los archivos antes de que se carguen en la nube y tomar algunas medidas de seguridad adicionales de acuerdo con su contenido y contexto. Por ejemplo:

- Utilice DLP (protección contra la pérdida de datos) para identificar datos personales (PII) en archivos antes de que se carguen y almacenen en la nube
- Use CDR (Desarmado y Reconstrucción de Contenido) en cualquier archivo guardado en la nube para verificar que no tenga ninguna 'carga útil' maliciosa que tenga como objetivo robar información
- Realice acciones de reparación en los archivos escaneados para:
  - Ofuscar / 'enmascarar' los datos de PII: por ejemplo, reemplace o enmascare los números de tarjetas de crédito con XXXXXXXXXXX
  - Cifre todos los archivos con datos PII antes de que se carguen en cualquier almacenamiento en la nube

OPSWAT diseñó MetaDefender para almacenamiento seguro para cubrir los agujeros de seguridad de los archivos y datos cargados en los proveedores de almacenamiento en la nube más comunes como AWS (S3), OneDrive, SharePoint, Azure, Box, Dropbox, Google Drive y más.

La solución de fácil integración lo ayuda a asegurar y proteger sus datos de misión crítica (ya sea almacenados en la nube o en las instalaciones) antes de que los piratas informáticos puedan atacarlos, y lo ayuda a cumplir con los requisitos de cumplimiento normativo. □

Más información en:
www.opswat.com

OPSWAT.

OPSWAT. + ARROW

Critical Infrastructure Protection Solutions

Cross-Domain Solutions
Secure Device Access
Network Access Control
File Upload Security
Malware Analysis
Email Security
Storage Security
Developer Tools

©2021 OPSWAT, Inc. All rights reserved. OPSWAT, MetaDefender, MetaAccess, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file, Trust no device, are trademarks of OPSWAT, Inc. All other brand names may be trademarks of their respective owners.

20th e-Crime & Cybersecurity Congress

"While this e-Crime was different, it was more valuable than ever, bringing my home-desk straight to the key topics, issues, speakers and solutions, to consider e-crime risks and controls in the New Normal!"

Snr IT Risk Manager IT Infra Assurance, Diligenta Limited

"I found the event highly relevant for the issues faced across the industry. The ranges of topics and multiple viewpoints being discussed helped to confirm existing strategies, inform others underway and prompt further discussion. Overall a good two days investment; congratulations to the AKJ team."

Principal Advisors, Mastercard

"e-Crime & Cybersecurity Congress 2021 is one of the best cyber conferences on the UK circuit. This year was a first being carried out remotely and very different to the normal 2-day event in person in London due to Covid-19. I found this remote approach worked very well and there was a great selection of speakers available and some excellent educational seminars. I also found the panel discussions very informative with a great selection of representative experts from their respective fields to provide a good and balanced view. I also found the resources very useful and thought it was a great touch that you could pause a session if required and that it was also available for 20 mins or so after it started in case you needed to attend to another matter prior to attending. Very good overall as ever, fingers crossed the mid-year review will be back in person again covid depending!"

Information Security Officer, North Group

"Great job done by all involved. The virtual conference operated flawlessly given the variables of presentations given. I also enjoyed still having the ability to join with likeminded people, learn the challenges people are facing, or what is going right as well as of course the nod to the products out there."

Security Consultancy Specialist Cyber Threat Management, BT

"The e-Crime & Cybersecurity Congress is a must for people within many areas of industry, as the speakers excellent, the content very relevant, the presentations fantastic, and the event excellent. I left feeling more informed and ready for new challenges."

Senior Manager Operational Risk (IT Risk)/ Data Protection Officer, UBL

2021 Congress sponsors included:

Strategic sponsors

BeyondTrust · censornet · COFENSE · DARKTRACE · egress · illumio · INTSIGHTS (Democratizing Threat Intelligence™) · okta · OneTrust GRC (Integrated Risk Management) · Recorded Future · SentinelOne · sixgill

Education Seminar Sponsors

BARRIER · bitglass · CyGlass (by NOMINET) · INTEL471 · KENNA Security · KEYSIGHT TECHNOLOGIES · LogRhythm · ManageEngine · Menlo Security · onelogin · OPSWAT. · RANGEFORCE · Synack · tenable · tripwire

Networking Sponsors

ThreatConnect

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

¡Gracias a todos los patrocinadores!

Patrocinadores estratégicos

DARKTRACE

Guardicore

RANGEFORCE

Recorded Future®

SentinelOne™

Synack®

Patrocinadores del seminarios de educación

CybelAngel

CISCO

KENNA Security

onelogin

OPSWAT.