Nota de prensa

M2i Formación y EC-Council, impulsoras de la formación CCISO en España

- **Ambas compañías reforzaron su parnership en un encuentro celebrado en Madrid, en el que evidenciaron las necesidades formativas tanto de los directivos IT, como de los perfiles más técnicos y pusieron el foco en la importancia de contar con certificaciones como Computer Hacking Forensic Investigator (CHFI), Certified Ethical Hacker (CEH) o Certified Chief Information Security Officer (CCISO)**
- **El amplio catálogo de cursos y certificaciones ofrecidos por la alianza conformada hace más de 10 años entre EC-Council y Alhambra-Eidos, a través de su área M2i Formación, cubre las necesidades y creciente demanda de profesionales en relación a la gestión de los riesgos y las vulnerabilidades de sus estructuras frente a ciberataques**

Madrid, 24 de abril de 2019.- M2i Formación, líder en capacitación IT, Multimedia y Management en modalidad presencial, e-Learning, Blended-Learning, aula virtual y COOC, evidencia, junto a su partner EC-Council, las necesidades formativas relativas a la ciberseguridad de los profesionales IT y la importancia de la formación en Certified Chief Information Security Officer (CCISO) en las compañías españolas.

En un desayuno tecnológico, bajo el lema "Formación en Ciberseguridad ante una nueva era", participaron diferentes expertos del ámbito de la ciberseguridad y de la formación, quienes explicaron cuáles son los riesgos reales, cómo y por qué se generan y qué formación deben tener los profesionales IT para poder combatirlos. "Resulta fundamental conocer el riesgo, para tomar las medidas oportunas y gestionar la seguridad. España es el tercer país más atacado del mundo, sin embargo, seguimos siendo muy inmaduros en el ámbito de la seguridad tanto a nivel personal como profesional", advirtió José María Ochoa, Area Manager de OneseQ y Co-Director de LAB SEC Blockchain.

Durante el encuentro, se recalcó la importancia de mantener seguras las infraestructuras en cualquier compañía, puesto que se mostró cómo las incidencias en ciberseguridad no solo conciernen a las multinacionales o grandes compañías. Y es que las pymes son mucho más vulnerables y pueden verse abocadas al cierre más fácilmente tras sufrir un ataque. "Solo alrededor del 24% de los ataques se detectan a tiempo, muchas compañías sufren daños irreparables tras un ataque, debido a que no consiguen recuperarse y acaban echando el cierre", asegura Ochoa.

Con respecto a los ataques, Jaime Álvarez, Red Team de Aiuken, expuso los diferentes tipos de atacantes a los que se enfrentan las compañías en la actualidad y los motivos por los que se realizan, concluyendo que "los atacantes malos" van siempre un paso por delante de "los buenos", razón por la cual muchos de ellos consiguen sus propósitos.

Además, a lo largo de la mañana, fueron enumeradas las brechas a las que se enfrentan las entidades: fugas de información, robo de datos, de planificación, incapacidad de detección, etc. Y en general, los ponentes coincidieron en que, en muchos de los casos, se deben a la inexistencia de planes de gestión y a la falta de formación y concienciación, todo ello por no invertir tiempo y recursos en ciberseguridad.

Ante esta situación, se puso sobre la mesa la figura del CISO, persona encargada de conocer las estrategias de seguridad y saber cómo gestionar los incidentes en los tiempos adecuados. Son muchas las cuestiones a tener en cuenta: gestión de incidentes, gestión de la normativa, gestión del equipo de ciberseguridad, gestión la seguridad IT de la compañía. Todo ello, necesita una estrategia que impulse la detección temprana y acorte los tiempos de respuesta. "No podemos seguir trabajando con los mismos recursos si queremos nuevos y mejores resultados —aseguró Ochoa — formemos a los gestores (CCISO), a los técnicos (CEH y CHFI) y a los usuarios (cursos de concienciación) para conseguir compañías más seguras".

En este sentido, Guillermo Hernández, Trainer de Ciberseguridad y CCISO de M2i Formación, habló sobre cómo las posibles vulnerabilidades hacen necesario tener a todos los miembros de una organización concienciados de los riesgos y de la necesidad de llevar a cabo buenas prácticas, así como de recibir un protocolo de actuación adecuado por parte de los responsables para saber cómo proceder. Además, destacó la importancia de tener la capacidad de rastrear el ataque para poder realizar una estimación real de los daños, para así poder presentar evidencias y llevar a los sistemas por una senda segura. Todo ello, con la figura del CISO en el centro, que lidere, conciencie y dirija todas las acciones y además demuestre el ROI.

"La tecnología y la fuerza de seguridad técnica por parte de TI ha dejado de ser suficiente. Hoy en día la organización debe conocer cómo protegerse a sí misma. Y, como mínimo, el responsable de la ciberseguridad de una organización ha de saber qué hacer si, por ejemplo, un sábado de madrugada recibe un mensaje con una amenaza estilo hacker de robo de información o datos y una petición de rescate económica con un plazo de 24horas. Suena a película, pero es real y más habitual de lo que podría imaginarse y la mayoría de las organizaciones y sus profesionales no sabría cómo actuar ni quién es el responsable que debe tomar la decisión sobre qué hacer en ese caso", señaló Hernández.

Además de la certificación del CCISO, ofrecida de forma exclusiva en España por M2i Formación y EC-Council, se destacaron las formaciones en Computer Hacking Forensic Investigator (CHFI) y el Certified Ethical Hacker (CEH). Claire Kemp, EC-Council Representative in South Europe & Africas Owner, habló en concreto sobre la importancia del hacking ético, debido a que, pensar como un hacker nos ofrece capacidades para poder evitar el cibercrimen. Del mismo modo, Mario Farias-Elinos, Trainer experto en ciberseguridad, mediante una práctica forense realizada en remoto, remarcó la importancia de conocer cómo se producen los ataques para evitar que se vuelvan a repetir, así como de disponer de un buen esquema de manejo de incidencias, conocimientos que se imparten en el curso CHFI.

Por último, Guido Peterssen, Director Operacional de M2i Formación, recalcó su posición de Centro Oficial Formador y Examinador de EC-Council, lo que les permite abordar un amplio abanico formativo que posibilita a las organizaciones construir una red de protección y

seguridad con la interrelación de todos los agentes y roles existentes, para los que se ofrece una formación y certificado de calidad: Chief Information Security Officer, Aplication Security Engineer, Network Defender, Secure Computer User, Application Security Engineer, Threat Intelligence Analyst, Incident Handler, Computer Hacking Forensic Investigator, Ethical Hacker, Security Analyst y Penetration Tester. Además de estos programas, también ofrecen certificaciones en formaciones técnicas especializadas en tecnologías de los principales fabricantes: Microsoft, Cisco, VMware, Mikrotik, etc.

Sobre M2i Formación

M2i Formación facilita la especialización en diferentes tecnologías, marcos de trabajo y estándares a perfiles del área IT como desarrolladores, analistas, responsables de servicios, jefes de proyecto y especialistas en bases de datos, mandos intermedios y directivos.

Tras la integración del área de formación de Alhambra-Eidos con M2i Formation, M2i Formación España ofrece el catálogo de cursos que aúna la experiencia de Alhambra-Eidos, basada en su larga experiencia como partner de los principales fabricantes (Microsoft, PMI, Axelos, EXIN, EC-Council, VMware entre otros) y a sus instructores certificados y la experiencia de una organización tan reconocida en Francia como M2i. Gracias, además, a sus instructores certificados, M2i ofrece cursos oficiales de gran calidad, además de cursos a medida.

www.M2iFormacion.com

Sobre Alhambra-Eidos

Más allá de su área de formación, M2i. Alhambra-Eidos es una compañía que, desde su creación, en 1991, ha desarrollado una gran experiencia como socio tecnológico que diseña, integra, personaliza y gestiona los Servicios TIC aplicados a los objetivos de su cliente, haciéndolos simples y accesibles.

Además, garantizan la calidad en todas sus áreas de actividad, teniendo certificados todos sus Servicios Gestionados, Cloud Computing y Redes Multiservicio bajo la norma de Gestión de Servicios ISO20001 y de Gestión de la Seguridad ISO27001. Por otro lado, más de 10 años adoptando los mejores modelos de Desarrollo de Software han permitido obtener el nivel de madurez 3 en CMMI© para desarrollo de software. Además, todos los procesos operativos de la organización están certificados ISO9001 desde el año 2005. A finales de 2016 obtuvo la certificación ISO14001 en Gestión Ambiental. Por último, en 2017, ha obtenido la norma 22301 de Continuidad de Negocio y la 27018 de Gestión de Datos de Carácter Personal en servicios en la nube.

www.Alhambra-Eidos.com

Para más información:

Alhambra-Eidos– Tel.: 91 787 23 00
Sergio Lumbreras
sergio.lumbreras@a-e.es

Art Marketing – Tel.: 91 351 31 51
Leire Navaridas
leire@artmarketing.es

Los datos personales que Ud. nos haya facilitado y, especialmente su dirección de correo electrónico, figuran incorporados a un fichero con el fin de gestionar nuestras relaciones y cuya responsabilidad corresponde a ART MARKETING COMUNICACIÓN Y ARTE, S.L. que garantiza el tratamiento de sus datos de carácter personal de conformidad con la Ley Orgánica 15/1.999 de Protección de Datos de Carácter Personal. Ud. podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante ART MARKETING COMUNICACIÓN Y ARTE, S.L. en Carretera de Húmera, 19 28224 Pozuelo de Alarcón Madrid. De conformidad con la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico, le solicitamos el consentimiento para el envío de comunicaciones publicitarias o promocionales, consentimiento que entenderemos otorgado, salvo que Ud. nos indique, por este mismo medio y en el plazo de siete días naturales, su oposición al tratamiento de sus datos con fines promocionales.