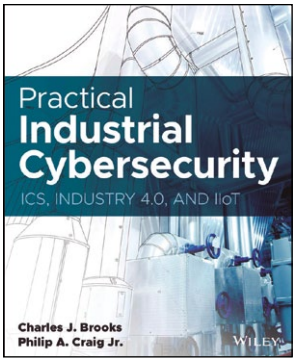
PRACTICAL INDUSTRIAL CYBERSECURITY: ICS, INDUSTRY 4.0 and IIoT

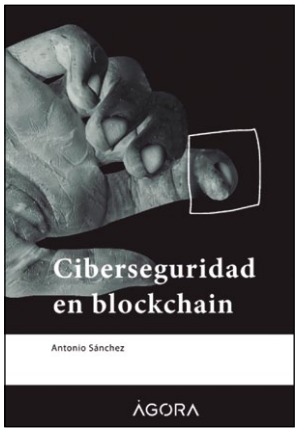


Autores: Philip A. Craig Jr. y Charles J. Brooks
Editorial: Wiley
Año: 2022 – 624 páginas
ISBN: 978-1119883029
www.wiley.com

En esta novedad bibliográfica, el veterano autor de seguridad informática, **Charles J. Brooks,** y el experto en ciberseguridad de la red eléctrica, **Philip Craig,** ofrecen abundante información y trazan los principales desafíos y cómo hacerlos frente en el ámbito de la ciberprotección industrial. Así, el lector encontrará en ella las principales herramientas y técnicas utilizadas por este tipo de profesionales, así como cuáles son las habilidades más buscadas y cómo desarrollarlas para superar con éxito el examen SANS Global Industrial Cyber Security Professional (GICSP), una de las titulaciones de referencia en este ámbito. Para ello, también se incluyen abundantes explicaciones prácticas y orientaciones.

En definitiva, los autores brindan una cobertura integral con las pautas del Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU. que rigen el establecimiento de sistemas de control industrial (ICS) seguros. Presentan explicaciones de las mejores prácticas en el diseño y la implementación de la arquitectura ICS, el endurecimiento de módulos y elementos, la evaluación y el gobierno de la seguridad, la gestión de riesgos y más.

CIBERSEGURIDAD EN BLOCKCHAIN: GUÍA BÁSICA PARA PROTEGER TUS CRIPTOACTIVOS DE FORMA SEGURA



Autor: Antonio Sánchez
Editorial: Ágora
Año: 2022 – 79 páginas
ISBN: 979-8785294196
www.agoraeditorial.com

En la actualidad, la tecnología es el impulso que nos lleva a la constante evolución de nuestro entorno. Por ello, "este libro se dirige a los creyentes de la innovadora revolución blockchain, pero no basta con creer. Hay que estar preparados para esta disruptiva transición", destaca su autor, **Antonio Sánchez**.

Para facilitar su comprensión, la obra sirve de 'manual básico' y como guía para todos aquellos que deciden adentrarse en este mundo tan apasionante. El objetivo es resolver las inquietudes en el campo de la ciberseguridad en blockchain, un elemento que cada día toma una mayor relevancia en nuestra sociedad. Además, el autor destinará los beneficios de este libro íntegramente a la fundación Fast España, que trabaja en la investigación, ensayos clínicos y divulgación científica del síndrome de Angelman. Se trata de una enfermedad neurológica rara de origen genético que afecta a una de cada 15.000 personas. Tienen epilepsia, discapacidad intelectual, ataxia, no pueden hablar, escoliosis y trastorno del sueño entre otros muchos síntomas.

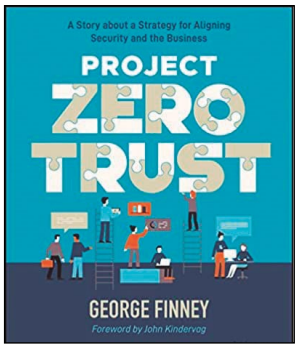
KUBERNETES PARA PROFESIONALES: DESDE CERO AL DESPLIEGUE DE APLICACIONES SEGURAS Y RESILIENTES

Autor: Rafael Troncoso
Editorial: 0xWord
Año: 2022 – 274 páginas
ISBN: 978-84-09-40450-6
https://0xword.com

La veterana editorial acaba de publicar una novedad que será de interés para muchos profesionales que precisan de esta tecnología para proteger mejor los entornos corporativos. El autor, **Rafael Troncoso**, un reconocido experto en la materia, con numerosas conferencias a sus espaldas sobre ella, pone foco en conocer a fondo cómo desplegar, de la manera más robusta, cualquier aplicación utilizando Kubernetes. Así, a lo largo de sus más de 270 páginas, el lector podrá aprender a 'fortificar' las aplicaciones. Y es que esta tecnología está llamada a convertirse, según muchos especialistas, en una especie de 'sistema operativo de la nube', ya que permite "orquestar el uso de contenedores y no tiene rival alguno", explica el autor.

Por ello, "cualquier profesional que se dedique al desarrollo de software, operaciones o a la seguridad, si se quiere mantener relevante en esta industria, debe estar familiarizado con el funcionamiento y uso de Kubernetes que se puede aprender, de forma muy práctica en esta obra que parte de los conceptos básicos para permitir ganar competencia en el despliegue de aplicaciones de forma segura y resilientes", destaca Troncoso, coautor también de otros libros de referencia como "Microhistorias: Anécdotas y Curiosidades de la historia de la informática (y los hackers)" y de "Docker: SecDevOps".

PROJECT ZERO TRUST: A STORY ABOUT A STRATEGY FOR ALIGNING SECURITY AND THE BUSINESS



Autores: George Finney, John Kindervag
Editorial: Wiley
Año: 2022 – 224 páginas
ISBN: 978-1119884842
www.wiley.com

En esta obra sobre la confianza cero, **George Finney,** director de seguridad de la Universidad Metodista del Sur, ofrece un análisis profundo y práctico de la implementación de este enfoque. Presentado en forma de una narración ficticia que involucra una brecha en una empresa, el libro rastrea las acciones del nuevo director de Seguridad de TI de dicha empresa. Los lectores aprenderán la metodología de cinco pasos de **John Kindervag** para implementar *Zero Trust*, sus cuatro principios de diseño y cómo limitar el impacto de una infracción. También, encontrarán cómo llevar a cabo estrategias concretas para alinear sus prácticas de seguridad con el negocio, qué mitos y errores comunes se comenten al aterrizar este concepto y cómo implementarlo en un entorno de nube.

Por supuesto, no falta un amplio espacio dedicado a estrategias de prevención de brechas que fomentan la eficiencia y reducción de costes en las prácticas de seguridad de una empresa. 'Project Zero Trust' es un excelente punto de referencia para los que se acercan, desde un punto de vista profesional y por primera vez, a este enfoque, así como a responsables de TI experimentados, ingenieros de redes, administradores de sistemas y gerentes de proyectos que estén interesados o vayan a adoptar la confianza cero en su compañía.