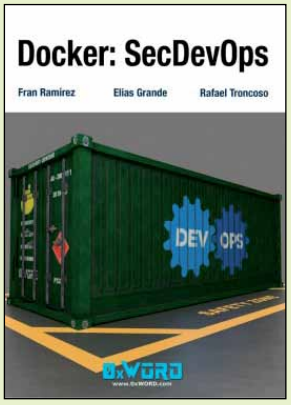


DOCKER: SECDEVOPS

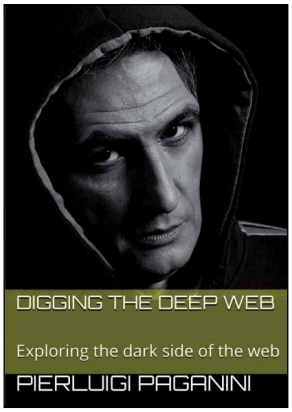
Autores: Fran Ramírez, Elías Grande y Rafael Troncoso
Editorial: 0xWord Año: 2018 – 240 páginas
ISBN: 9788469797525 0xword.com/es

Esta obra, escrita por el investigador de **ElevenPaths, Fran Ramírez**, el experto en DevOps, **Rafael Troncoso** –que trabaja para el departamento de Seguridad Nacional en EE.UU.– y **Elías Grande**, arquitecto de seguridad de **BBVA,** ofrece una visión práctica y técnica, con el paso a paso, para usar Docker y cómo solucionar los problemas de seguridad más habituales en estos entornos.

La tecnología de los contenedores –el más conocido es Docker, creado por Solomon Hykes en 2013– se ha convertido en una herramienta imprescindible tanto para los desarrolladores de aplicaciones, que buscan automatizar procesos para tener un flujo de entrega continuo –los llamados DevOps, Development & Operations–, como para los especialistas que tratan de hacerlas seguras –SecDevOps–, sin retrasar su puesta en marcha.

¿La ventaja de Docker? Es sencillo de usar y muy útil para "automatizar y desplegar aplicaciones dentro de los contenedores para su desarrollo y testeo, también en análisis de seguridad", explican los autores.

Se trata de un libro –en castellano casi es el único de este tema– que ayudará a conocer en profundidad la utilidad de Docker y comprender qué es DevOps y SecDevOps y por qué es vital que ambos trabajen juntos. Además, facilita unas recomendaciones para implementar, desde cero, buenas prácticas de seguridad en el desarrollo de aplicaciones, incluyéndose un repaso de los proyectos más conocidos y actuales en Docker como Infrakit, LinuxKit y SwarmKit.



DIGGING THE DEEP WEB: EXPLORING THE DARK SIDE OF THE WEB

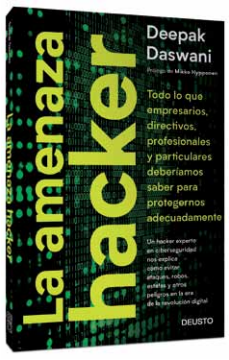
Autor: Pierluigi Paganini
Editorial: Amazon Año: 2018 – 212 páginas
ISBN: 1980532540 www.amazon.com

El conocido experto **Pierluigi Paganini** –miembro de ENISA, CTO de la empresa Cybsec, editor de CyberDefence Magazine y fundador del *blog* Security Affairs– ha publicado este nuevo libro en el que analiza qué hay de verdad y de falso en los mitos sobre la llamada web profunda –*deep web*–. Como es sabido, se trata de la parte de Internet, no indexada por los navegadores, que supone casi el 90% de la Red.

A lo largo de dos centenares de páginas, Paganini realiza una completa 'fotografía' del 'ecosistema' de la web profunda y qué uso hacen de ella cibercriminales y grupos al servicio de estados –de Rusia, China, Alemania, EE.UU, etc–. También explica cómo le sacan partido grupos cibermafiosos que viven de realizar ciberataques a empresas y obtener beneficios de robos al sector financiero o difundiendo contenidos protegidos por propiedad intelectual. Grupos delincuentes a los que se suman pederastas que intentan evadir en la *deep web* el control policial.

Paganini muestra de forma clara, pero exhaustiva, el uso de la web profunda para comercializar todo tipo de servicios y productos delictivos –como números de tarjetas de créditos robadas–. Eso sí, también es utilizada por diferentes comunidades de *hacking* que la usan para garantizar su anonimato y privacidad al margen de empresas comerciales y gobiernos.

La obra es un perfecto punto de referencia para todos los que quieran adentrarse en los 'secretos' de la *deep web* y comprender frente a qué amenazas críticas la ciberseguridad tiene que ofrecer respuestas en el día a día.



LA AMENAZA HACKER

Autor: Deepak Daswani
Editorial: Deusto Año: 2018 – 320 páginas
ISBN: 978-8423429318 www.planetadelibros.com

Daswani es uno de los *hacker* éticos más mediáticos de España como ponente habitual en eventos corporativos y de concienciación, análisis en medios de comunicación y su labor de docente. En este libro, sucinto y práctico, analiza en detalle los riesgos a los que se expone la gente usando la tecnología y explica cómo hacerles frente, evitarlos o, al menos, intentar que el impacto de su amenaza sea el mínimo. "Las noticias sobre incidentes de ciberseguridad son cada vez más habituales: a diario se roban millones de cuentas de correo, datos de tarjetas de crédito, credenciales de banca en línea y se cometen toda clase de delitos informáticos", explica el autor que ha intentado ofrecer una imagen detalla de qué, cómo y por qué ocurren estos ataques –analizando los más utilizados– a través del ciberespacio.

Escrito con un tono personal y divulgativo, el libro atrapa al lector por el gran número de ejemplos y anécdotas curiosas que aporta el autor de su experiencia personal. ¿Su reto? "Que la gente pueda comprender, incluso sin tener grandes conocimientos técnicos, los entresijos de la relación entre el mundo físico y el virtual", destaca Daswani. "En definitiva, se trata de un libro dirigido a todos los que necesitan conocer y saber cómo se originan las amenazas a las que nos exponemos". La obra, cuyo título quizá induzca al error, ha sido prologada por el conocido experto en ciberseguridad, **Miko Hypönnen,** de la firma F-Secure, y recomendada por unos de los hackers más conocidos del mundo, **Kevin Mitnick.** En definitiva, un libro perfecto para aprender de ciberseguridad… o como regalo para concienciar sobre 'buenas prácticas' en el mundo digital.