LA CLAVE PILAR (LOS TELEGRAMAS SECRETOS DEL GOBIERNO CIVIL DE MÁLAGA)

Autor: Alberto Peinado Domínguez
Editorial: Umaeditorial
Año: 2023 – 175 páginas
ISBN: 978-84-1335-230-5
www.umaeditorial.uma.es

Interesante y original obra del solvente investigador malagueño de la UMA, por su especialización y profundidad sobre telecomunicaciones, criptografía y sociedad, que son analizadas desde el prisma que ofrece la ciudad de Málaga. La histórica relación que mantiene la ciudad con las telecomunicaciones constituye el contexto perfecto para el criptoanálisis de una serie de telegramas cifrados enviados o recibidos por el Gobierno Civil entre 1934 y 1940: registros domiciliarios anteriores a la Guerra Civil, el control de la prensa durante la contienda y las órdenes recibidas de la Dirección General de Seguridad en Madrid tras el conflicto. Se presenta aquí la 'Clave Pilar', utilizada en 1940.

Su recuperación, en 2018, ha supuesto un importante hallazgo criptográfico que ha ayudado a completar el catálogo de los cifrados de cinta móvil empleados en España desde finales del siglo XIX. El análisis de éstos y otros telegramas cifrados con claves similares son también, presentados y analizados, constatando la invariabilidad con el paso del tiempo, de las relaciones entre telecomunicación, criptografía y sociedad.

Además, resulta de especial interés la recopilación de muchos de los telegramas que usaron la clave Pilar, de los que se ofrecen abundantes imágenes, un aspecto que dota al libro de relevancia académica para los que trabajan en temas, como la historia de la criptografía, la ciberseguridad y las comunicaciones secretas en el ámbito militar.

CIBERINTELIGENCIA DE LA AMENAZA EN ENTORNOS CORPORATIVOS

Autor: Mario Guerra Soto
Editorial: Ra-Ma
Año: 2023 – 772 páginas
ISBN: 978-8419857453
www.ra-ma.es

Extensa y pormenorizada obra dedicada a la inteligencia cibernética de amenazas en la que el autor destaca el valor, para cualquier empresa, de conocer minuciosamente sus activos, su exposición, sus vulnerabilidades propias o debidas a terceros, su potencial 'explotabilidad' y el impacto que ésta supondría para la continuidad de negocio.

Mario Guerra, reconocido profesional en este ámbito, plantea así una obra, dividida en ocho capítulos, para iniciados y expertos, con la que podrán desarrollar y mejorar sus capacidades como analistas de ciberinteligencia en los niveles técnico/táctico, operacional y estratégico, a través de marcos de trabajo como el de Recorded Future o Mandiant. Eso sí, dado que la ciberinteligencia de la amenaza constituye una capacidad transversal para la organización, su lectura resultará también de enorme utilidad a sus equipos de ingeniería de detección, respuesta a incidentes, *threat hunting*, forense digital, análisis de *malware*, *Red Team* y *Purple Team,* además de a responsables de SOC y a CISO. También, resultará de interés a criminólogos, periodistas, analistas antifraude, militares y miembros de las FCSE interesados en el cibercrimen en Web 2 y Web3, las operaciones de influencia, el ciberespionaje y las operaciones militares en el ámbito del ciberespacio.

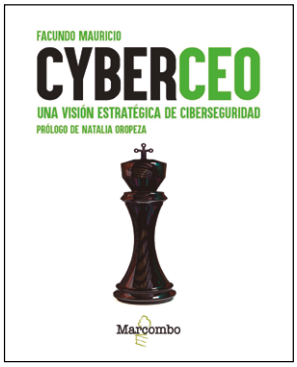
SEGURIDAD OFENSIVA EN MACHINE LEARNING. +100 PROMPTS INJECTIONS EN CHATGPT: ATACANDO Y DEFENDIENDO ORGANIZACIONES CON PROMPT ENGINEERING

Autor: Dr. Alfonso Muñoz
Editorial: Publicación independiente
Año: 2023 – 167 páginas
ISBN: 979-8399420615
www.amazon.es

El inquieto y prolífico **Alfonso Muñoz** –referente español en criptografía y temas aledaños, de la que ha impartido conferencias y publicado numerosos libros–, con esta novedad editorial en castellano, busca dar un paso más en esta disciplina para que el lector entienda la utilidad, ventajas e inconvenientes de la inteligencia artificial (IA) aplicada a la ciberseguridad. Para ello, pone foco en nuevos paradigmas y, sobre todo, en las aplicaciones prácticas de los modelos LLM (*Large Language Model*), como el popular ChatGPT. "He recopilado y organizado decenas de ejemplos, *prompt injection* y *prompt engineering*, usando más de 200 referencias de obligada lectura, para comprender de forma sencilla su utilidad real y restricciones. Espero que le resulte provechoso y le ahorre tiempo en la evaluación de esta nueva tecnología", destaca el autor.

"Llevo más de 20 años trabajando en el campo de la ciberseguridad, protegiendo organizaciones apoyándome en sinergias con disciplinas variadas y verificando (atacando) las contramedidas desplegadas. Es en este escenario donde cualquier profesional debe analizar la enorme utilidad de la IA en numerosos ámbitos de nuestra sociedad moderna, incluido la seguridad cibernética, y reflexionar sobre los riesgos inherentes de esta tecnología antigua pero vitaminada con el acceso a grandes volúmenes de información, capacidades de computación y nuevos desarrollos algorítmicos, especialmente en el campo de las redes neuronales", añade.

CYBERCEO: UNA VISIÓN ESTRATÉGICA DE CIBERSEGURIDAD

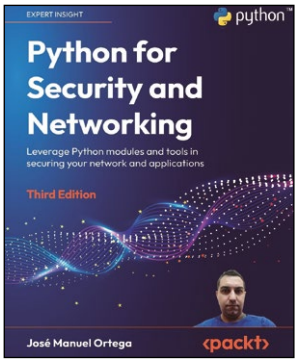


Autor: Facundo Mauricio. Natalia Oropeza (Prólogo)
Editorial: Marcombo
Año: 2023 – 324 páginas
ISBN: 978-8426735713
www.marcombo.com

"Sencillo, pragmático y desafiante". Así define este libro su autor, con un título que aunque a priori despista, trata con solvencia centrar esta disciplina como uno de los elementos intrínsecos a la alta dirección y con el que busca ofrecer un enfoque que permita "abordar la ciberseguridad de forma estratégica, integral y cerotécnica", explica. "Dirigido a ejecutivos que delegarán el cómo, pero necesitan comprender el qué y por qué", en él ofrece un recorrido amplio con una mirada histórica del impacto de la tecnología y sus consecuencias sociales, económicas, comerciales y organizacionales. Así, en sus capítulos intenta aportar "una perspectiva estratégica, propia de los líderes que buscan comprender los conflictos y las oportunidades de la era digital". "Un futuro cada vez más conectado y complejo requiere una estrategia sólida en ciberseguridad. No se trata solo de protegerse de las amenazas, sino de maximizar las potencialidades transformadoras de la digitalización, de aprovechar la IA, el *blockchain* y las posibilidades que ofrece la ciberprotección como un diferenciador y eje innovador del mañana".

El libro, además, cuenta con una invitada de referencia como es **Natalia Oropeza,** Chief Cybersecurity Officer en Siemens, prologuista del volumen y compañera del autor en la multinacional, quien destaca la necesidad en el mundo ejecutivo de dejar de ver la ciberseguridad solo como una responsabilidad técnica y comenzar a verla también, como una oportunidad.

PYTHON FOR SECURITY AND NETWORKING: LEVERAGE PYTHON MODULES AND TOOLS IN SECURING YOUR NETWORK AND APPLICATIONS



Autor: José Manuel Ortega
Editorial: Packt Publishing
Año: 2023 – 586 páginas
ISBN: 978-1837637553
www.packtpub.com

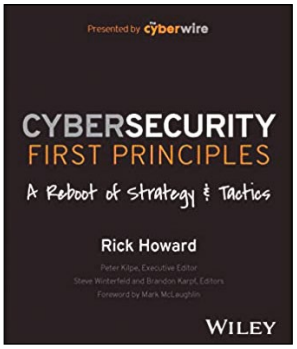
Tercera edición de esta obra con una notable actualización, tanto en nuevos capítulos como en información que, como resultado, ha sido reescrito en más del 50%, además de adaptar los *scripts* del conocido lenguaje de programación, Python, a su reciente versión 3.10. Así pues, a lo largo de este libro, de carácter técnico, el autor muestra cómo la combinación de la última versión del conocido lenguaje con un mayor enfoque en la seguridad de la red puede ayudar a mejorar las defensas contra los ciberataques.

En concreto, pretende servir de guía para construir una red segura con la ayuda de las secuencias de comandos de Python.

Para ello, ofrece amplia información de todo tipo de temas, desde la creación de una red hasta los procedimientos que debe seguir para protegerla. En su parte final, dedica un apartado a cómo crear aplicaciones seguras utilizando técnicas de criptografía y esteganografía, además de mostrar cómo proteger con este lenguaje de programación los puntos finales, entre otros aspectos de interés.

En definitiva, esta novedad editorial resultará de gran interés para ingenieros de redes, administradores de sistemas y otros profesionales de la seguridad que buscan superar problemas comunes de redes y protección con Python.

CYBERSECURITY FIRST PRINCIPLES: A REBOOT OF STRATEGY AND TACTICS



Autor: Rick Howard
Editorial: Wiley
Año: 2023 – 400 páginas
ISBN: 978-1394173082
https://onlinelibrary.wiley.com

En esta obra, **Rick Howard**, director de ciberseguridad, analista jefe y miembro principal de The Cyberwire, 'desafía' la sabiduría convencional de las mejores prácticas, estrategias y tácticas actuales de seguridad y argumenta que la profesión necesita volver al principio. Así, a lo largo del libro, muestra de manera convincente los argumentos a favor del primer principio absoluto de la ciberprotección y analiza las estrategias y tácticas necesarias para lograrlo.

La obra, además, ofrece un excelente repaso de la historia de la seguridad informática desde la década de 1960, hasta principios de la década de 2020, explicando por qué ha fallado, además de mostrar qué se debería mejorar, estrategias y tácticas que deberían adoptarse para tener mayor impacto y eficacia, así como diferentes estudios de ataques que se han producido –desde el hackeo a la empresa OPM, en 2015, hasta el de DNC, en 2016, o de Colonial Pipeline, en 2019–. A través de ello, ofrece una propuesta de cómo calcular el riesgo cibernético, tanto en grandes compañías como en medianas y pequeñas. En definitiva, se trata de un libro escrito de forma amena y que resultará de interés para los profesionales del sector en todos los niveles: desde ejecutivos de negocios hasta los sénior especializados o, incluso, los que se quieran dedicar a este ámbito y busquen las mejores oportunidades profesionales.

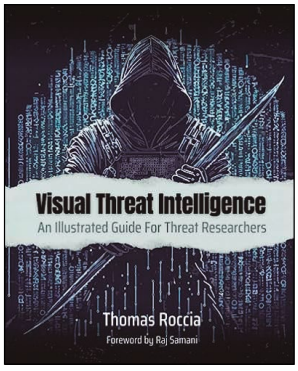
MARCO NORMATIVO DE LA UE PARA LA TRANSFORMACIÓN DIGITAL

Autor: Eloy Velasco (Coordinador)
Editorial: La Ley
Año: 2023 – 512 páginas
ISBN: 978-84-19446-36-7
https://tienda.wolterskluwer.es

Esta monografía examina el impulso regulatorio de la UE a la transformación digital de sus 27 estados miembro, promoviendo la innovación tecnológica y salvaguardando la protección de los datos personales. El resultado es un marco normativo sólido y coherente en aspectos tan transversales como la ciberseguridad, los servicios y mercados digitales, la ciberdelincuencia, la prueba digital, la identidad digital y los terceros de confianza, los criptoactivos, los medios de pago digitales, la inteligencia artificial, la privacidad y un largo etc. Este desarrollo legislativo, basado en los principios y derechos digitales en los que se enmarca, ha ayudado a fomentar la innovación y la competitividad en el mercado digital europeo, así como a proteger los derechos y libertades de los ciudadanos y las empresas.

Además, de su extensión, también destaca por su calidad con notables aportaciones de grandes especialistas como **José de la Mata**, magistrado-juez, miembro nacional de España en Eurolust; **José Luis Piñar**, catedrático de Derecho Administrativo de la USP-CEU; **Ofelia Tejerina**, abogada y presidenta de la Asociación de Internautas; **Elvira Tejada**, Fiscal de Sala del Tribunal Supremo coordinadora nacional contra la ciberdelincuencia; así como el propio **Eloy Velasco**, magistrado-juez de la Audiencia Nacional; y **Natalia Jiménez**, DPO del Canal de Isabel II, entre otros.

VISUAL THREAT INTELLIGENCE: AN ILLUSTRATED GUIDE FOR THREAT RESEARCHERS



Autor: Thomas Roccia
Editorial: Publicación independiente
Año: 2023 – 148 páginas
ISBN: 979-8373228374
www.amazon.com

Prologado por el reconocido **Raj Samani**, esta obra funciona a modo de guía mostrando los principios de la inteligencia de amenazas de forma visual y sencilla, a la vez que ofrece amplia información, con diagramas y gráficos, sobre los conceptos más complejos de este ámbito, con ejemplos prácticos.

Así, ofrece desde una buena visión de las principales motivaciones de los actores de amenazas, hasta sus metodologías de ataque más usadas, analizadas a través del ciclo de vida de la inteligencia de amenazas, el modelo diamante de análisis de intrusiones y el marco Mitre ATT&CK. También, ofrece información sobre cómo pensar como los cibercriminales, trabajar con indicadores de compromiso (IOC), y usarlo para priorizar, según el enfoque de 'pirámide del dolor', los aspectos que más exigen centrarse en ellos para lograr capacidades anticipativas a través de herramientas de inteligencia de amenazas cruciales como Yara, Sigma y MSTICpy, para rastrear *malware* y analizar datos.

No falta el análisis de algunos conocidos incidentes de los últimos años como NotPetya, Shamoon y Sunburst, con lecciones aprendidas y, también, algunos de sus aspectos más llamativos como el incremento de capacidades de los ataques para crear señales falsas para engañar a las investigaciones.