به نام خدا

معرفی نسل جدید
مراکز عملیات امنیت
Next Generation SOC

مؤلف

رضا آدینه

مؤسسه فرهنگی هنری دیباگران تهران

عنوان کتاب: معرفی نسل جدید مراکز عملیات امنیت Next Generation SOC

مولف : رضا آدینه

ناشر: موسسه فرهنگی هنری دیباگران تهران

صفحه آرایی:فرنوش عبدالهی

طراح جلد:داریوش فرسایی

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۸

چاپ و صحافی:درج عقیق

تیراژ: ۱۰۰ جلد

قیمت: ۴۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۲۲-۲۱۸-۲۱۸-۲

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهستان، پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibbook.ir

www.dibagarantehran.com

نشانی تلگرام:mftbook@ **نشانی اینستاگرام دیبا dibagaran_publishing**

سرشناسه:آدینه،رضا،۱۳۶۷-

عنوان و نام پدیدآور:معرفی نسل جدید مراکز عملیات امنیت Next generation SOC /مولف: رضا آدینه.

مشخصات نشر: تهران : دیباگران تهران :۱۳۹۸

مشخصات ظاهری:۱۱۲ص:مصور،

شابک: ۹۷۸-۶۲۲-۲۱۸-۲۱۸-۲

وضعیت فهرست نویسی: فیپا

موضوع:زیر ساخت مجازی-تدابیر ایمنی

موضوع:Cyberinfrastructure=security measures

موضوع:سامانه های امنیتی

موضوع: security systems

موضوع: شبکه های کامپیوتری

موضوع: computer networks-security measures

رده بندی کنگره: QA ۷۶/۹

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۵۹۴۱۶۴۸

هرکتاب دیباگران ،یک فرصت جدید شغلی.

هرگوشی همراه،یک فروشگاه کتاب دیباگران تهران.

از طریق سایتها و اپ دیباگران،در هر جای ایران به کتابهای ما دسترسی دارید.

فهرست مطالب

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی است که بتواند خواسته های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

هر کتاب دیباگران تهران، یک فرصت جدید شغلی

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت **"جناب آقای رضا آدینه "** و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
bookmarket@mft.info

❖ مقدمه‌مولف

نسل جدید مراکز عملیات امنیت؛

نسل جدید مراکز عملیات امنیت از سال ۲۰۱۲ تا کنون شناخته می شود. همانطور که می‌دانید مرکز عملیات امنیت همان قابلیتی است که در سازمان با استفاده از متخصصان، فرایند ها و فناوری ها اقدام به پایش امنیت سایبری کرده و به شناسایی ریسک ها و تهدیدات سازمانی می پردازد.

اما با پیشرفته‌تر شدن تهدیدات و پیچیده‌تر شدن آن ها عامل زمان در شناسایی و پاسخدهی به حوادث نقش پر رنگ تری پیدا کرده است. لذا پارادایم جدیدی از مرکز عملیات امنیت به وجود آمده که ویژگی های متفاوتی را ارائه می‌دهد. تمام تلاش سازمان ها برای کنترل ریسک بوده است و با در نظر داشتن حملات پیشرفته، همچنین نرخ رشد حملات سایبری در کمیت و کیفیت، راهکارهای سنتی به تنهایی کفایت لازم برخوردار نیستند.

همچنین بنابه انواع تهدیدات مدرن و نحوه ی حملات آن ها نقاط شناسایی تهدیدات در ساختارهای شبکه تغییر کرده است.

در این کتاب تلاش شده است ضمن مرور این ویژگی ها، وضعیت کلی یک مرکز عملیات امنیت نسل جدید را برای استفاده شما عزیزان فراهم آورد.

هدف این کتاب تنها مروری بر مفاهیم و ویژگی های جدیدی است که یک مرکز عملیات امنیت می بایست داشته باشد.