به نام خدا

هوشمندسازی امنیت

و مقابله با تهدیدات پیشرفته

مؤلف

مهندس رضا آدینه

مؤسسه فرهنگی هنری
دیباگران تهران

عنوان کتاب: هوشمندسازی امنیت و مقابله با تهدیدات پیشرفته

مولف : مهندس 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:۹۹۰۰۰۰ ریال

شابک: ۹-۱۴۹-۲۱۸-۶۲۲-۹۷۸

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

تلفن: ۶۶۴۱۰۰۴۶-۲۲۰۸۵۱۱۱

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

www.mftdibagaran.ir

نشانی تلگرام:mftbook@

سرشناسه:آدینه،رضا،۱۳۶۷-

عنوان و نام پدیدآور: هوشمندسازی امنیت و مقابله با تهدیدات پیشرفته /مولف: رضا آدینه.

مشخصات نشر: تهران : دیباگران تهران :۱۳۹۸

مشخصات ظاهری:۲۳۴ص:مصور،

شابک: ۹-۱۴۹-۲۱۸-۶۲۲-۹۷۸

وضعیت فهرست نویسی: فیپا

موضوع:جاسوسی مجازی cyber imtelligence

موضوع: تروریسم رایانه ای -پیشگیری

موضوع:cyberterrorism-prevention

موضوع:جنگ سایبری (cyberspace operation(military sceince

موضوع:شبکه های کامپیوتری-تدابیر ایمنی

موضوع : computer networks-security measures

موضوع: کامپیوترها- ایمنی اطلاعات-تدابیر ایمنی

موضوع: computer security-security measures

موضوع: جرایم کامپیوتری-پیشگیری

موضوع: computer crimes-prevention

موضوع :امنیت ملی-نوآوری

موضوع: national security-technological innovations

رده بندی کنگره: ۶۷۷۳ HV

رده بندی دیویی: ۳۶۴/۱۸

شماره کتابشناسی ملی:۵۷۴۶۴۴۵

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.

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 **"مهندس 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

مقدمه مولف

طبق بررسی ها و تجارب حاصله سال ها فعالیت در حوزه امنیت اطلاعات سایبری تصمیم به تالیف کتابی دانشی و کاربردی و به روز برای تمامی علاقهمندان به این حوزه گرفتم . با در نظر داشتن این مسله که راهکارهای سنتی صرفا مبتنی بر پایش امروزه کارایی چندانی برای مقابله با تهدیدات پیشرفته ندارند؛ و ظهور نسل جدید راهکارهای امنیتی، جای خالی کتابی برای مفاهیم کاربردی و نوین احساس می شد. به همین خاطر این نوشتار بر همین اساس و با هدف تعریف مدلی کاربردی و مفهومی مبتنی بر هوشمند سازی و بهره برداری از مفاهیم نوین تالیف شده است.

برای تالیف این کتاب از منابع معتبر بسیاری استفاده شده است که همگی از بروزترین منابع در دسترس بوده اند. در ادامه لازم به ذکر است که در صورت وجود هرگونه نقطه نظر پیرامون کتاب پیش رو می توانید با آدرس ایمیل اینجانب در تماس باشید.

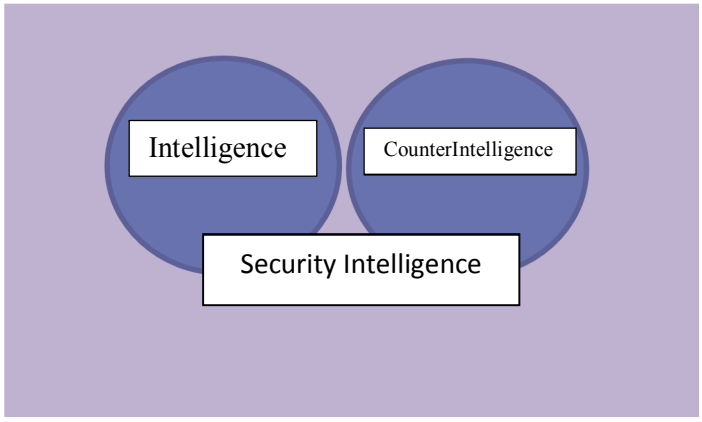
REZA_ADINEH@LIVE.COM

در این قسمت از تمامی دوستان و عزیزانی که در تالیف این کتاب اینجانب را یاری کردند تقدیر و تشکر می کنم.

پیشگفتار

در دنیای امروزی تهدیدات بسیاری برای سازمان‌ها وجود دارند. سازمان‌ها برای مقابله با تهدیدات نیازمند اطلاعات و داده‌های مفید جهت تشخیص نشانه‌های آنها می‌باشند. برای مقابله با تهدیدات که به سرعت در حال رشد و پیچیده‌تر شدن می‌باشند نیاز به راهکارهای مناسب جهت پیشگیری، تشخیص و پاسخ در بازه زمانی موثری می‌باشد تا کسب‌وکار سازمان‌ها دچار اختلال و آسیب نگردد. لذا سازمان‌ها می بایست در برنامه‌های امنیت سایبری خود از مفهومی به نام Security Intelligence به اختصار SI بهره مند شوند. SI شامل مجموعه اطلاعاتی می‌باشد که در راستای محافظت سازمان در برابر تهدیدات داخلی و بیرونی مورد استفاده قرار می‌گیرد. در SI تمامی فرایندها، سیاست‌ها و ابزار لازم جهت جمع‌آوری و تحلیل اطلاعات پیرامون تهدیدات در نظر گرفته می‌شود. در این نوشتار به معرفی مفاهیم و مضامین، بهره برداری از این مفاهیم، بررسی راهکارهای مناسب در راستای نیل به اهداف مذکور جهت مقابله و شناسایی این قبیل تهدیدات پرداخته می شود. و در نهایت مدلی برای شکار تهدیدات سایبری بر همین اساس ارائه می دهد.

هدف اصلی این نوشتار علاوه بر معرفی مفاهیم و مضامین کاربردی و مروری بر بهترین ابزارها برای محقق کردن راهکارهای ذکر شده، معرفی نظریه‌ای جدید بر مبنای بهره برداری موثر از مفهوم "هوشمندی پیرامون تهدیدات" Threat Intelligence برای اجرای (شکار تهدیدات) Threat Hunting می باشد.



دیدگاه اصلی بر محور مفهوم هوشمند سازی امنیت سایبری و بکار گرفتن این راهکار در سازمان می باشد. دو مولفه‌ی اصلی هوشمندی پیرامون تهدیدات و شکار تهدیدات از محورهای اساسی این نوشتار می‌باشد. بطور کل مفهوم هوشمندسازی امنیت متشکل از دو قسمت اساسی می‌باشد، یکی تحت عنوان Intelligence و دیگری تحت عنوان CounterIntelligence می‌باشند. تمرکز این

نوشتار بر استفاده از راهکارهای هوشمندی پیرامون تهدیدات در راستای پیشبرد فرایندهای شکار تهدیدات می‌باشد. که تلاش شده است تا تمامی جوانب موضوع مورد بررسی قرار گرفته و راهکاری مناسب و کابردی ارائه گردد. محوریت این نوشتار بر اساس تعریف، کاربرد و معرفی راهکارهای برگزیده این مضامین می‌باشد. در تمام نوشتار مفاهیم زیادی مطرح شده که سعی بر چکیده نویسی این مضامین شده است. لذا می بایست ابتدا به تعریف مفهوم هوشمند سازی امنیتی پرداخت و ضمن معرفی الزامات و مولفه های تشکیل دهنده آن، مولفه های کلیدی و چگونگی پیاده سازی این مجموعه مرور گردد.