# هوش

# تهدید سایبری

**یک نقشه راه برای تعالی سازمان‌های کشور در حوزه امنیت اطلاعات**


**تالیف:**

**ابوذر عرب‌سرخی**

**عضو هیئت علمی پژوهشگاه ارتباطات و فناوری اطلاعات**

**امین چهاردولی**



**آراد کتاب**

| | |
|---|---|
| سرشناسه | : عرب‌سرخی، ابوذر، ۱۳٦۰- |
| عنوان و پدیدآور | : هوش تهدید سایبری، یک نقشه راه برای تعالی سازمان‌های کشور در حوزه امنیت اطلاعات/ تالیف: ابوذر عرب‌سرخی، امین چهاردولی. |
| مشخصات نشر | : تهران، آراد کتاب، |
| مشخصات ظاهری | : ۱۳٤ص ، مصور، جدول، نمودار |
| شابک | : ۱-۷۸۱-۱۸٦-٦۰۰-۹۷۸ |
| وضعیت فهرستنویسی | : فیپا |
| عنوان دیگر | : یک نقشه راه برای تعالی سازمان‌های کشور در حوزه امنیت اطلاعات |
| موضوع | : جرایم کامپیوتری - پیشگیری |
| موضوع | : امنیت اطلاعات کامپیوتری |
| شناسه افزوده | : چهاردولی، امین، ۱۳٦۷ - |
| رده بندی کنگره | : HV٦۷۷۳ |
| رده بندی دیویی | : ۳٦٤/۱٦۸ |
| شماره کتابخانه ملی | : ۱۰٦۱۲۵۰۲ |

# هوش تهدید سایبری

☑ تالیف: ابوذر عرب‌سرخی، امین چهاردولی ☑ ناشر: آراد کتاب

☑ نوبت چاپ: اول ۱۴۰۵ ☑ تیراژ: ۱۰۰ جلد

☑ چاپ و صحافی: صدف ☑ قیمت: ۴۴۵۰۰۰ تومان

شابک: ۱- ۷۸۱-۱۸۶-۶۰۰-۹۷۸



مرکز پخش و فروش:

انتشارات آراد کتاب تلفن: ۶۶۹۷۵۲۸۵ ـ ۶۶۴۸۲۲۲۶ ـ ۰۹۳۵۳۰۶۲۴۵۸

خرید آنلاین از سایت: www.aradbook.com

# پیشگفتار

در دهه‌های اخیر، شتاب فزاینده تحول دیجیتال، وابستگی سازمان‌ها و دولت‌ها به زیرساخت‌های مبتنی بر فناوری اطلاعات را بیش از پیش افزایش داده است. این وابستگی اگرچه دستاوردهای بزرگی در زمینه بهره‌وری، تصمیم‌سازی سریع و چابکی عملیاتی به همراه داشته، اما در عین حال سطح جدیدی از تهدیدات سایبری پیچیده، هدفمند و بعضاً غیرقابل پیش‌بینی را نیز وارد فضای عملکردی سازمان‌ها کرده است. در چنین شرایطی، رویکردهای سنتی امنیت اطلاعات که عمدتاً بر مکانیزم‌های واکنشی و دفاعی تکیه دارند، دیگر پاسخگوی تهدیدات نوین سایبری نیستند. امروز منطق امنیتی مبتنی بر آگاهی، پیش‌بینی‌پذیری، تحلیل رفتار مهاجم و تصمیم‌سازی هوشمند بر اساس داده‌های واقعی و قابل اتکا، به ضرورتی اجتناب‌ناپذیر تبدیل شده است.

کتاب حاضر با عنوان «هوش تهدید سایبری: نقشه راهی برای تعالی سازمان‌ها در حوزه امنیت اطلاعات»، تلاشی نظام‌مند برای ارائه یک راهنمای علمی-عملی در حوزه هوشمندسازی امنیت سایبری سازمان‌ها است. این کتاب با ترسیم دقیق مبانی نظری، مدل‌های استاندارد هوش تهدید، معماری‌های مرجع، پلتفرم‌ها، چارچوب‌ها و روش‌های عملیاتی هوش تهدید، در پی آن است که مسیر حرکت سازمان‌ها از وضعیت واکنش‌محور به وضعیت پیش‌نگرانه، دانش‌محور و پیشدستانه را تسهیل کند.

در تدوین این اثر، تلاش شده است با فراهم کردن پیوندی میان مراجع معتبر بین‌المللی (مانند NIST، MITRE، ISACها و استانداردهای اشتراک‌گذاری داده‌های تهدید)، تجربه‌های عملیاتی حاصل از فعالیت مراکز عملیات امنیتی و نیازهای واقعی سازمان‌ها در بستر بومی، مرجعی قابل اتکا و کاربردی در اختیار مدیران، تحلیلگران امنیت، سیاست‌گذاران فناوری و پژوهشگران این حوزه قرار گیرد. هدف اصلی این کتاب، تقویت توانمندی سازمان‌ها در استقرار رویکردی مبتنی بر هوش تهدید، ایجاد ساختار و فرهنگ امنیت پیشگیرانه و ارتقاء بلوغ امنیتی در چارچوبی پایدار و آینده‌نگر است.

امید است این اثر بتواند گامی هرچند کوچک در مسیری بزرگ باشد؛ مسیری که به سازمان‌ها امکان می‌دهد نه تنها قربانی حملات سایبری نباشند، بلکه با داشتن تسلط اطلاعاتی و توان تحلیل رفتار مهاجمان، پیش از وقوع حادثه، تهدید را شناسایی، پیش‌بینی و خنثی کنند. موفقیت در این عرصه، نه تنها نیازمند ابزار و فناوری، بلکه متکی به دانش، راهبرد، همکاری و نگرش امنیتی پخته و یکپارچه است.

با قدردانی از تمامی پژوهشگران، تحلیلگران امنیت سایبری و کارشناسانی که با تلاش و دانش خود، افق‌های تازه‌ای در امنیت اطلاعات می‌گشایند، این کتاب تقدیم می‌شود به آنان که باور دارند قدرت واقعی امنیت نه در ایجاد دیوارهای بلند دفاعی، بلکه در فهم عمیق تهدید و آگاهی از نیت مهاجم نهفته است.

**این کتاب با احترام تمام تقدیم می‌شود به :**

**پدر عزیزم**

**شهید فتح الله عرب سرخی**

**و**

**روح رفیع شهدای تنگه ابو قریب**

# فهرست

**عنوان** **صفحه**

# فهرست شکل‌ها

عنوان صفحه

# فهرست جدول‌ها

عنوان صفحه