

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	: عرب سرخی، ابوذر، ۱۳۶۰-
عنوان و پدیدآور	: هوش تهدید سایبری، یک نقشه راه برای تعالی سازمان های کشور در حوزه امنیت اطلاعات/ تالیف: ابوذر عرب سرخی، امین چهاردولی.
مشخصات نشر	: تهران، آراد کتاب،
مشخصات ظاهری	: ۱۳۴ ص، مصور، جدول، نمودار
شابک	: ۹۷۸-۶۰۰-۱۸۶-۷۸۱-۱
وضعیت فهرست نویسی	: فیپا
عنوان دیگر	: یک نقشه راه برای تعالی سازمان های کشور در حوزه امنیت اطلاعات
موضوع	: جرایم کامپیوتری - پیشگیری
موضوع	: امنیت اطلاعات کامپیوتری
شناسه افزوده	: چهاردولی، امین، ۱۳۶۷ -
رده بندی کنگره	: HV۶۷۷۳
رده بندی دیویی	: ۳۶۴/۱۶۸
شماره کتابخانه ملی	: ۱۰۶۱۲۵۰۲

هوش تهدید سایبری

تالیف: ابوذر عرب سرخی، امین چهاردولی	ناشر: آراد کتاب
نوبت چاپ: اول ۱۴۰۵	تیراژ: ۱۰۰ جلد
چاپ و صحافی: صدف	قیمت: ۴۴۵۰۰۰ تومان
شابک: ۹۷۸-۶۰۰-۱۸۶-۷۸۱-۱	

حق چاپ برای ناشر محفوظ است. کلیه حقوق و حق چاپ متن، طرح روی جلد و عنوان کتاب با نگرش به قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ برای انتشارات آراد کتاب محفوظ است و متخلفین تحت پیگرد قانونی قرار می گیرند.

مرکز پخش و فروش:

انتشارات آراد کتاب تلفن: ۶۶۹۷۵۲۸۵ - ۶۶۴۸۲۲۲۶ - 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، ISAC) 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 می شود به :

پدر عزیزم

شهید فتح الله عرب سرخی

و

روح رفیع شهدای تنگه ابو قریب

فہرست

عنوان	صفحه
نگاهی اجمالی بر کتاب هوش تهدید سایبری.....	۱۱
مفاهیم پایه هوش تهدید سایبری.....	۱۴
۱-۱-مقدمه.....	۱۱
۲-۱- مضامین کلیدی مرتبط با هوش تهدید سایبری.....	۱۱
۱-۲-۱- مدل سازی تهدید.....	۱۲
۲-۲-۱- پاسخگویی به حادثه.....	۱۳
۳-۲-۱- تحلیل مخاطره.....	۱۳
۴-۲-۱- فید.....	۱۴
۵-۲-۱- شکار تهدید.....	۱۵
۳-۱- آشنایی با فضای تهدیدات سایبری.....	۱۵
۴-۱- تعریف هوش تهدید سایبری.....	۱۶
۵-۱- ضرورت‌های توجه به هوش تهدید سایبری در سازمان.....	۱۷
۶-۱- منافع هوش تهدید سایبری برای سازمان.....	۱۸
۷-۱- انواع هوش تهدید سایبری.....	۱۹
۸-۱- چرخه هوش تهدید سایبری.....	۲۰
۱-۸-۱- جهت‌دهی.....	۲۱
۲-۸-۱- جمع‌آوری.....	۲۲
۳-۸-۱- پردازش.....	۲۳
۴-۸-۱- تجزیه و تحلیل.....	۲۳
۵-۸-۱- انتشار.....	۲۴
۶-۸-۱- بازخورد.....	۲۴
۹-۱- تصویر کلان از ساختار هوش تهدید سایبری در سازمان.....	۲۵
۱-۹-۱- تعیین وظایف و مسئولیت‌ها.....	۲۶

۲۷.....	۱-۹-۲- ساختار سازمانی منعطف
۲۸.....	۱-۹-۳- فرآیندها و استانداردها
۲۹.....	۱-۹-۴- فناوری و ابزارها
۳۱.....	۱-۹-۵- آموزش و توسعه
۱۱.....	منابع
۱۳.....	مروری بر ساختارها، استانداردها و چارچوب‌های پشتیبان توسعه هوش تهدید سایبری
۳۶.....	۲-۱- مقدمه
۳۶.....	۲-۲- چارچوب‌های پشتیبان هوش تهدید سایبری
۳۷.....	۲-۲-۱- چارچوب MITRE ATT&CK
۳۸.....	۲-۲-۲- چارچوب مدل الماس
۴۰.....	۲-۲-۳- چارچوب Cyber Kill Chain
۴۲.....	۲-۲-۴- چارچوب امنیت سایبری NIST
۴۴.....	۲-۲-۵- چارچوب OODA Loop
۴۷.....	۲-۲-۶- چارچوب MISP
۴۸.....	۲-۳- پلتفرم‌های مطرح پشتیبان هوش تهدید سایبری
۴۹.....	۲-۳-۱- پلتفرم اسپلانک فانتوم
۵۰.....	۲-۳-۲- پلتفرم MISP
۵۱.....	۲-۳-۳- پلتفرم ThreatConnect
۵۲.....	۲-۳-۴- پلتفرم Anomali ThreatStream
۵۴.....	۲-۳-۵- پلتفرم EclecticIQ
۵۵.....	۲-۴- ائتلاف‌های شناخته‌شده هوش تهدید سایبری در جهان
۵۵.....	۲-۴-۱- ائتلاف اشتراک‌گذاری و تحلیل اطلاعات در حوزه خدمات مالی
۵۶.....	۲-۴-۲- ائتلاف اشتراک‌گذاری و تحلیل اطلاعات
۵۷.....	۲-۴-۳- ائتلاف لیگ هوش تهدید سایبری

۵۸.....	۴-۴-۲- ائتلاف مرکز تعالی دفاع سایبری مشترک ناتو
۵۹.....	۴-۴-۵- ائتلاف تیم واکنش به حوادث اضطراری رایانه‌ای استرالیا
۶۰.....	۲-۵- استانداردهای پشتیبان هوش تهدید
۶۰.....	۲-۵-۱- پروتکل‌های عمومی هوش تهدید (پیام‌رسانی)
۶۱.....	۲-۵-۲- پروتکل‌های اختصاصی هوش تهدید
۶۲.....	۲-۵-۳- پشتیبانی از API
۶۳.....	۲-۵-۴- استفاده از زبان‌های مشترک در توصیف تهدیدات
۶۴.....	۲-۵-۵- استاندارد STIX
۶۵.....	۲-۵-۶- استاندارد TAXII
۶۶.....	۲-۵-۷- استاندارد CTISS
۶۸.....	منابع
۷۰.....	مدل‌های مرجع توسعه هوش تهدید سایبری
۷۱.....	۳-۱- مقدمه
۷۱.....	۳-۲- ضرورت نگاه معمارانه به هوش تهدید
۷۲.....	۳-۲-۱- یکپارچگی سیستم‌ها و فرآیندها
۷۲.....	۳-۲-۲- استانداردسازی و تطبیق‌پذیری
۷۳.....	۳-۲-۳- امنیت به‌عنوان یک اولویت استراتژیک
۷۴.....	۳-۲-۴- تحلیل و پیش‌بینی تهدیدات
۷۴.....	۳-۲-۵- بهره‌وری و کارایی
۷۵.....	۳-۳- نگاهی عمومی به مدل‌ها و معماری‌های مرجع هوش تهدید
۷۵.....	۳-۳-۱- مدل آمادگی محیطی هوش سایبری
۷۷.....	۳-۳-۲- مدل الماس برای تحلیل نفوذ
۷۹.....	۳-۳-۳- مدل لغت‌نامه برای ثبت رخدادها و تبادل اطلاعات حادثه
۸۰.....	۳-۳-۴- مدل مرجع لایه‌ای هوش تهدید سایبری

۴-۳- نحوه انتخاب مدل های مرجع هوش تهدید در فضای عملیاتی.....	۸۲
۴-۳-۱- مدل آمادگی محیطی هوش سایبری	۸۲
۴-۳-۲- مدل الماس برای تحلیل نفوذ	۸۲
۴-۳-۳- مدل لغت نامه برای ثبت رخدادها و تبادل اطلاعات حادثه	۸۳
۴-۳-۴- مدل مرجع لایه ای هوش تهدید سایبری	۸۳
منابع.....	۸۴
آگاهی وضعیتی به عنوان پیشران هوشمندی سایبری سازمان ها.....	۸۶
۴-۱- مقدمه.....	۸۷
۴-۲- تعاریف و مضامین پایه آگاهی وضعیتی سایبری.....	۸۷
۴-۳- نقش آگاهی سایبری در تصمیم سازی و هوش امنیت سایبری.....	۹۰
۴-۴- مدل های آگاهی وضعیتی در سازمان.....	۹۱
۴-۴-۱- مدل آگاهی وضعیتی اندسلی (سال ۱۹۹۵ میلادی)	۹۲
۴-۴-۲- مدل ادغام اطلاعات JDL (سال ۱۹۸۰ میلادی)	۹۳
۴-۴-۳- مدل آگاهی وضعیتی سایبری (سال ۲۰۰۹ میلادی)	۹۵
۴-۴-۴- مدل آگاهی وضعیتی سایبری مؤثر	۹۵
۴-۵- عوامل مؤثر در ایجاد آگاهی وضعیتی و هوش تهدید در سازمان.....	۹۷
۴-۶- مدل مرجع ایجاد آگاهی وضعیتی و هوشمندی سایبری در سازمان.....	۹۸
منابع.....	۱۰۱
نقشه راه حرکت سازمان ها به سمت هوش تهدید سایبری.....	۱۰۳
۵-۱- مقدمه.....	۱۰۴
۵-۲- کارکردهای اصلی نقشه راه امنیت سایبری.....	۱۰۴
۵-۳- ضرورت های استفاده از نقشه راه در حوزه هوش تهدید سایبری.....	۱۰۵
۵-۴- نقشه راه پایه هوش تهدید سایبری.....	۱۰۶
۵-۵- مدل مرجع نقشه راه هوش تهدید سایبری.....	۱۰۸

۱۰۹.....	۵-۵-۱- تعریف هدف
۱۱۰.....	۵-۵-۲- تحلیل و ارزیابی
۱۱۱.....	۵-۵-۳- طراحی راهکارها
۱۱۱.....	۵-۵-۴- پیاده‌سازی
۱۱۲.....	۵-۵-۵- پایش و ارزیابی
۱۱۴.....	منابع
۱۱۶.....	اصول و الزامات کلان دستیابی به هوش تهدید سایبری در سازمان
۱۱۷.....	۶-۱- مقدمه
۱۱۷.....	۶-۲- ضرورت توجه به اصول و الزامات کاری در مقوله هوش تهدید سایبری
۱۱۸.....	۶-۳- اصول دستیابی به هوش تهدید سایبری در سازمان
۱۲۰.....	۶-۴- الزامات کلان دستیابی به هوش تهدید سایبری در سازمان
۱۲۰.....	۶-۴-۱- تعیین استراتژی و سیاست‌ها
۱۲۰.....	۶-۴-۲- ایجاد زیرساخت‌های مناسب
۱۲۰.....	۶-۴-۳- توسعه مهارت‌ها و آموزش‌ها
۱۲۰.....	۶-۴-۴- همکاری و اشتراک‌گذاری اطلاعات
۱۲۰.....	۶-۴-۵- پیاده‌سازی فرآیندهای مداوم
۱۲۱.....	۶-۴-۶- مدیریت مخاطره و پاسخگویی
۱۲۱.....	۶-۵- ارزیابی و مدیریت تهدیدات سایبری با محوریت اصول و الزامات کلان
۱۲۱.....	۶-۵-۱- ارزیابی تهدیدات سایبری
۱۲۲.....	۶-۵-۲- فرآیند ارزیابی تهدید
۱۲۳.....	۶-۵-۳- تنظیم استراتژی هوش تهدید سایبری
۱۲۴.....	۶-۵-۴- تعریف قابلیت عملیاتی
۱۲۵.....	۶-۵-۵- ملاحظات مالی
۱۲۵.....	۶-۵-۶- جمع‌آوری

۶-۶- نتیجه گیری..... ۱۲۵

منابع..... ۱۲۷

لغات و علائم اختصاری..... ۱۲۹

فهرست شکل‌ها

عنوان	صفحه
شکل ۱-۱- مفاهیم کلیدی هوش تهدید سایبری.....	۱۲
شکل ۲-۱- چرخه هوش تهدید سایبری.....	۲۱
شکل ۳-۱- ساختار هوش تهدید سایبری.....	۲۶
شکل ۱-۲- تشخیص تهدید با چارچوب MITRE ATT&CK.....	۳۸
شکل ۲-۲- تشخیص تهدید با چارچوب مدل الماس.....	۴۰
شکل ۳-۲- تشخیص تهدید با چارچوب مدل Cyber Kill Chain.....	۴۲
شکل ۴-۲- تشخیص تهدید با چارچوب مدل NIST.....	۴۴
شکل ۵-۲- تشخیص تهدید با چارچوب مدل OODA Loop.....	۴۶
شکل ۶-۲- تشخیص تهدید با چارچوب مدل MISP.....	۴۸
شکل ۱-۳- مدل CIPE.....	۷۶
شکل ۲-۳- مدل DMIA.....	۷۸
شکل ۳-۳- مدل VERIS.....	۷۹
شکل ۴-۳- مدل مرجع لایه‌ای هوش تهدید سایبری.....	۸۱
شکل ۱-۴- مدل آگاهی وضعیتی ارائه‌شده توسط اندسلی در سال ۱۹۹۵ میلادی.....	۹۲
شکل ۲-۴- مدل ادغام اطلاعات JDL.....	۹۴
شکل ۳-۴- مدل آگاهی وضعیتی سایبری اوکولیکا سال ۲۰۰۹ میلادی.....	۹۵
شکل ۴-۴- مدل آگاهی وضعیتی سایبری مؤثر.....	۹۶
شکل ۵-۴- کارکردها و قابلیت‌های سامانه آگاهی وضعیتی.....	۹۹
شکل ۱-۵- مدل مرجع نقشه راه هوش تهدید سایبری.....	۱۰۸
شکل ۲-۶- خانه استراتژی هوش تهدید سایبری سازمان.....	۱۲۴

فهرست جدول‌ها

عنوان	صفحه
جدول ۱-۲ - پروتکل و استانداردهای اختصاصی هوش تهدید.....	۶۲
جدول ۱-۴ - نمونه‌هایی از تعریف‌های ارائه شده در مورد آگاهی وضعیتی.....	۸۸
جدول ۱-۶ - ارزیابی سنتی تهدید در مقابل ارزیابی پیشرفته تهدید سایبری.....	۱۲۲
جدول ۲-۶ - منابع ورودی ارزیابی تهدید.....	۱۲۳