

هوش سایبری کاربرد

چگونه هوش مبتنی بر عمل می‌تواند پاسخی مؤثر به حوادث باشد

نویسنده:

ویلسون باتیستا جی. آر.

مترجمین:

عزیز نصیرزاده

دکتر سیروس احمدی نوح‌دانی

سرشناسه	: باتیستا جی. آر.، ویلسن
عنوان و نام پدیدآور	: Wilson, Bautista Jr هوش سایبری کاربردی: چگونه هوش مبتنی بر عمل می تواند پاسخی موثر به حوادث باشد/ نویسنده ویلسون باتیستا جی. آر؛ مترجمان سیروس احمدی نوحدانی، عزیز نصیرزاده؛ ویراستار ادبی احمد ملکی؛ ویراستار فنی مهران غلامیان؛ ناظر ویراستاری حسین معین پور.
مشخصات نشر	: تهران: ارتش جمهوری اسلامی ایران، نیروی هوایی، مرکز انتشارات راهبردی، ۱۴۰۰.
مشخصات ظاهری	: ۳۵۹ ص.: مصور (رنگی).
شابک	: ۹۷۸-۶۲۲-۳۰۳-۰۱۸-۵
وضعیت فهرست نویسی	: فیا
یادداشت	: عنوان اصلی: Practical cyber intelligence : how action-based intelligence can be ۲۰۱۸an effective response to incidents,
عنوان دیگر	: چگونه هوش مبتنی بر عمل می تواند پاسخی موثر به حوادث باشد.
شناسه افزوده	: احمدی نوحدانی، سیروس، ۱۳۴۵ -، مترجم
شناسه افزوده	: نصیرزاده، عزیز، ۱۳۴۳ -، مترجم
شناسه افزوده	: ایران. ارتش. نیروی هوایی. مرکز انتشارات راهبردی
شناسه افزوده	: Iran. Army. Airforce. Strategic Publishers Centre
رده بندی کنگره	: TK۵۱۰۵/۵۹
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۸۹-۵۱۴۲
اطلاعات رکورد کتابشناسی	: فیا

مؤلف: ویلسون باتیستا جی. آر.

مترجمین: عزیز نصیرزاده، دکتر سیروس احمدی نوحدانی

ویرایش ادبی: احمد ملکی

ویرایش فنی: مهران غلامیان

ناظر ویراستاری: حسین معین پور

مدیریت چاپ و نشر: احمد ملکی

شابک: ۹۷۸-۶۲۲-۳۰۳-۰۱۸-۵

نوبت چاپ: اول

ناشر: انتشارات راهبردی نهاجا

شمارگان: ۱۰۰۰

قیمت: ۲۲۰۰۰۰۰ ریال

مطالب مندرج در این کتاب نقطه نظرات مؤلف بوده و در هنگام ترجمه سعی گردیده است به منظور رعایت حفظ اصالت اثر، دخل و تصرفی در آن صورت نپذیرد، بنابراین آنچه ترجمه گردیده است (محتوای اثر) به منزله تائید مترجمین نیست بلکه صرفاً ترجمه تحت‌اللفظی آن است.

حق چاپ و نشر برای ناشر محفوظ است

نشانی: تهران؛ خیابان پیروزی؛ ستاد نیروی هوایی ارتش جمهوری اسلامی ایران؛ مرکز

مطالعات، تحقیقات و تدوین آیین‌نامه‌های رزمی نهاجا؛

تلفن: ۰۳۵۷۴۲۳۱۲-۳۳۳۴۰۴۰-۳۳۷۸۷۰۶۵ کد پستی: ۱۷۶۵۳۴۲۴۳۱



فهرست مطالب

مقدمه ۱۷

فصل اول: نیاز به هوش سایبری ۲۳

مقدمه ۲۵

نیاز به هوش سایبری ۲۵

کاربری هوش در ارتش ۲۷

هوش در تاریخ ۲۸

جنگ انقلابی آمریکایی ۲۸

استفاده ناپلئون از هوش ۲۹

معرفی چند نوع از هوش ۳۰

هوش انسانی ۳۱

هوش تصویری ۳۱

هوش اندازه‌گیری و خاص ۳۲

هوش منبع باز ۳۲

هوش سیگنالی ۳۲

هوش ارتباطی ۳۳

هوش الکترونیکی ۳۳

هوش سیگنال‌های ابزاری خارجی یا FISINT ۳۳

هوش فنی ۳۴

هوش درمانی ۳۴

۳۵	هوش همه جانبه منابع
۳۵	هوش، پیش برنده عملیات‌ها
۴۰	تبدیل نظریه به اقدام عملی به‌سادگی نیست
۴۴	درک روحیه مانور جنگی
۴۵	روند را دنبال کن، آن روند تو را نجات می‌دهد
۴۶	مانور جنگ چیست؟
۴۷	ریتم
۴۸	حلقه او. او. دی. ای
۵۱	مرکز ثقل و آسیب‌پذیری حیاتی
۵۲	غافلگیری: ایجاد و استفاده از موقعیت
۵۳	تعامل
۵۳	انعطاف
۵۳	فرماندهی غیرمتمرکز
۵۴	خلاصه

۵۵ فصل دوم: توسعه هوش

۵۷	سلسله مراتب اطلاعات
۵۹	مقدمه‌ای بر چرخه هوش
۵۹	مراحل چرخه هوش
۶۰	قدم اول - برنامه‌ریزی و جهت‌دهی
۶۰	توسعه ملزومات
۶۱	مدیریت ملزومات

۶۲	جهت‌دهی به اقدامات هوش
۶۳	برطرف کردن ملزومات
۶۴	برنامه‌ریزی برای سیستم پشتیبانی هوش
۶۵	قدم دوم - جمع‌آوری
۶۶	قدم سوم - پردازش
۶۶	قدم چهارم - تحلیل و تولید
۶۷	قدم پنجم - انتشار
۶۷	روشها
۶۸	کانال‌ها
۶۹	حالت‌ها
۷۰	معماری انتشار
۷۰	قدم ۶- استفاده
۷۱	خلاصه

۷۳ فصل سوم: یکپارچه‌سازی هوش سایبری، امنیتی و عملیات

۷۵	نگاهی متفاوت به عملیات‌ها و امنیت
۷۶	توسعه توانایی هوش سایبری راهبردی
۷۷	درک اولویت‌های خود
۷۸	معماری کسب‌وکار
۷۸	معماری داده‌های / کاربردی
۷۸	معماری فناوری
۷۸	کاربرد معماری‌ها و هوش سایبری

نگاهی بر هوش سایبری راهبردی - سطح ۱	۸۰
مقدمه‌ای بر امنیت عملیاتی	۸۲
قدم اول امنیت عملیات - شناسایی اطلاعات مهم	۸۳
قدم دوم امنیت عملیات - تجزیه و تحلیل تهدیدات	۸۳
قدم سوم امنیت عملیات - تجزیه و تحلیل آسیب‌پذیری‌ها	۸۴
قدم چهارم امنیت عملیات - ارزیابی خطرات	۸۴
قدم پنجم امنیت عملیات - استفاده از اقدامات متقابل مناسب	۸۶
پیاده‌سازی امنیت عملیات در فضای کسب‌وکار	۸۶
نقشه‌ای برنامه هوش سایبری	۸۹
سطح راهبردی - رهبری فناوری اطلاعات	۹۰
سطح راهبردی - مسئول برنامه هوش سایبری	۹۰
سطح تاکتیکی - مدیر هوش سایبری	۹۱
سطح عملیاتی - رهبری فناوری اطلاعات	۹۲
سطح عملیاتی - تحلیل هوش سایبری	۹۲
خلاصه	۹۳

فصل چهارم: استفاده از هوش سایبری برای فعالسازی دفاع فعال ۹۵

مقدمه‌ای بر دفاع فعال	۹۸
درک زنجیره نابودسازی سایبری	۹۹
اصول کلی دفاع فعال	۱۰۱
دفاع فعال - اصل اول: آزار	۱۰۱
دفاع فعال - اصل دوم: انتساب	۱۰۳

۱۰۴..... فریب و گیرافتادن در دفاع فعال

۱۰۴..... سناریو A

۱۰۵..... سناریو B

۱۰۶..... انواع دفاع فعال

۱۰۶..... انواع دفاع فعال — مدل دستی

۱۰۷..... انواع دفاع فعال — خودکار

۱۰۸..... یک کاربرد از سطح تاکتیکی دفاع فعال

۱۱۲..... خلاصه

۱۱۵..... فصل پنجم: F3EAD برای من و شما

۱۱۸..... درک هدفگذاری

۱۲۴..... فرآیند اف.۳.ای.ای.دی

۱۲۷..... اف.۳.ای.ای.دی در عمل

۱۳۲..... اف.۳.ای.ای.دی و زنجیره نابودسازی سایبری

۱۳۲..... زنجیره نابودسازی سایبری و حلقه او.او.دی.ای

۱۳۴..... زنجیره نابودسازی سایبری و امنیت عملیات

۱۳۵..... زنجیره نابودسازی سایبری و چرخه هوش

۱۳۶..... زنجیره نابودسازی سایبری و اف.۳.ای.ای.دی

۱۳۷..... کاربرد فرآیند اف.۳.ای.ای.دی در یک فضای کسب و کار

۱۳۸..... محدودیتهای اف.۳.ای.ای.دی

۱۳۹..... خلاصه

۱۴۱..... فصل ششم: ادغام هوش تهدیدها و عملیات

- درک هوش تهدیدها ۱۴۳
- مدل قابلیت بالغ - مروری بر هوش تهدید ۱۴۶
- سطح ۱ - قابلیت جمع‌آوری هوش تهدید ۱۴۸
- فاز اولیه ۱۴۹
- مثال ۱ - انجمن تبادل تهدیدات منبع باز از شرکت الین والت ۱۴۹
- پنل الین والت ۱۴۹
- پالس‌های الین والت ۱۵۲
- مثال ۲ - شرکت تویستر ۱۵۵
- برنامه توییت دک ۱۵۶
- مثال ۳ - مراکز اشتراک‌گذاری اطلاعات و تحلیل ۱۵۹
- مثال ۴ - اختراهای هشداردهنده اخبار ۱۶۰
- مثال ۵ - خلاصه‌های وب سایت غنی ۱۶۱
- فاز A ۱۶۳
- مثال ۱ - سیسکو - پلتفرم گاسینت ۱۶۴
- مثال ۲ - پروژه پلتفرم اشتراک‌گذاری اطلاعات بدافزارها ۱۶۵
- فاز B ۱۶۵
- فاز C ۱۶۶
- سطح ۲ - ادغام داده‌های تهدید ۱۶۷
- فاز اولیه ۱۶۸
- فاز A ۱۶۹
- دسته‌بندی آنچه که برای استفاده چند تیم مفید است ۱۶۹

هنگامی که برای اولین بار از من خواسته شد این کتاب را بنویسم، قرار بود موضوع کتاب در مورد استفاده از روش هدف‌گیری نظامی برای تهدید اطلاعات باشد. با این حال، وقتی شروع به نوشتن کردم، سؤالاتی در ذهنم شکل گرفت:

✓ هوش تهدید چگونه برای سازمان‌ها مفید است؟

✓ چگونه می‌توانیم از هوش تهدید یک ارزش ایجاد کنیم؟

بنابراین، موضوع به چیزی تغییر یافت که من معتقدم در عملکرد ما به عنوان سازمان های فناوری اطلاعات گم شده است. اطلاعات تهدید اگر برای سازمان‌ها قابل استفاده نباشد، فایده‌ای ندارد. هنگامی که این مورد برای یک سازمان اجرایی شد، باید به کسی اطلاع داده شود تا نسبت به آن اقدام کند. خیلی ساده به نظر می‌رسد اما وقتی بیشتر نگاه می‌کنیم، نقاط مشترک زیادی با بخش‌های مختلف سازمان و فرایندهای مختلف بین تیم‌ها وجود دارد که سرانجام موضوع به چیزی تبدیل می‌شود که من آن را هوش سایبری می‌نامم.

اگر مدتی را به تماشای اخبار امنیت سایبری در شبکه‌های اجتماعی خود اختصاص دهید، می‌توانید در مورد آخرین بهره‌برداری، نیاز به تعداد بیشتری از متخصصان امنیت سایبری و میزان ناامنی ما مطالعه کنید. به نظر می‌رسد احساسات پر شور است و باعث آشفتگی فکر و توهم می‌شود و به عنوان «قربانی بعدی» برای رهبری ارشد شناخته می‌شود. چند بار دیده‌ایم که رهبران ارشد به دلیل نقض قدرت کنار می‌روند؟ شاید برخی از نقض‌ها به دلیل بی‌توجهی باشد، اما من مشتاقانه فکر می‌کنم که ما (به‌طور جمعی) مملو از فرآیندهای کسب و کار سنتی و بروکراتیک هستیم که اجازه انعطاف‌پذیری برای تصمیم‌گیری غیرمتمرکز را نمی‌دهد.

آیا عملیات فناوری و امنیت اطلاعات شما با استفاده از اطلاعاتی که هر یک از طرفین را تحت تأثیر قرار می‌دهد، در تصمیم‌گیری برای تصمیمات کلی فناوری اطلاعات نقش دارند؟ اگر آن‌ها این کار را کردند، پس شما باید این کتاب را کنار بگذارید زیرا محتویات این کتاب برای شما مناسب نیست. اگر این کار را نکنند، شما

درد را زمانی درک خواهید کرد که تفکیک وظایف تأثیر مستقیم روی سرعت انجام کارها خواهد داشت.

در ارتش، توانایی اطلاعاتی به فرمانده اجازه می‌دهد تا محیط اطراف خود را برای تصمیم‌گیری درک کند. این کتاب در مورد این است که چگونه می‌توانیم فرایندهای اطلاعاتی نظامی را تغییر داده و در سازمان استفاده کنیم. چه شما یک تحلیلگر سطح ابتدایی باشید و چه یک مدیر ارشد، چیزی برای شما وجود دارد که باید بلافاصله در سازمان خود یاد بگیرید و عملی کنید.

این کتاب برای چه کسانی است

مخاطبان اصلی این کتاب از متخصصین ارشد تا مدیران ارشد در مشاغل کوچک و متوسط هستند که به دنبال بهبود عملیات فناوری اطلاعات و امنیت اطلاعات خود با استفاده از فرایندها و مفاهیم متعدد نظامی هستند. همچنین برای رهبران آینده صنایع است که نگاهی دیگر به یک رویکرد جامع برای بهبود عملیات فناوری اطلاعات در سازمان‌های خود داشته باشند. هیچ تجربه قبلی مدیریتی یا فنی فرض نشده است.

آنچه این کتاب در برمی‌گیرد

فصل ۱، نیاز به هوش سایبری، مختصری از تاریخچه استفاده از اطلاعات در ارتش، انواع مختلف اطلاعات و طرز تفکر نظامی را معرفی می‌کند.

فصل ۲، توسعه هوش، مقدمه چرخه اطلاعات است و به شما نشان می‌دهد که چگونه هوش توسعه می‌یابد و چگونه می‌توان درخواست‌های اطلاعاتی دارای اولویت را ایجاد کرد.

فصل ۳، یکپارچه‌سازی اطلاعات سایبری، امنیت و عملیات، امنیت عملیاتی را پی‌ریزی می‌کند و پایه‌ای می‌شود برای درک اینکه چگونه هوش سایبری در امنیت اطلاعات و نیز در فعالیت‌های حوزه فناوری اطلاعات ادغام می‌شود.