

عباس معلم

آشنایی با فناوری امنیت سایبری

راهنمای انتخاب ابزارهای مناسب

دکتر مؤید محسنی

انتشارات ترجمک

ترجمک
Tarjomak

آشنایی با فناوری های امنیت سایبری

راهنمای انتخاب ابزارهای امنیت سایبری صحیح

توجه :

کتاب حاضر حاصل زحمات دکتر مؤید محسنی می باشد. فایل کتاب حاوی اطلاعات DRM (مدیریت حقوق دیجیتال) است. وقتی برای اولین بار فایل را باز می کنید، کد شناسایی کتاب به همراه آدرس IP سیستم شما ذخیره شده و زمانیکه آنلاین شوید، به سرور انتشارات ترجمک انتقال می یابد.

خواهشمند است به حقوق نگارنده و انتشارات ترجمک احترام گذاشته و از توزیع بدون مجوز فایل کتاب اجتناب نمایید. شما با خرید و دانلود این کتاب موافقت نموده اید که اطلاعات فایل DRM به سرور انتشارات ترجمک انتقال یابد و در صورت محرز شدن نقض حقوق صاحب اثر، کلیه خسارات حاصله در طی فرآیند حقوقی و مطابق قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان و ناشران جمهوری اسلامی (مصوب دوازده اسفند ۱۳۶۵ یا بعد از آن) از شما دریافت شود.

از اینکه با عرضه مقرون به صرفه کتاب های الکترونیک و شکوفایی انتشارات ترجمک همیاری می کنید، سپاسگزاریم.

انتشارات ترجمک

<https://tarjomac.ir/>

عباس معلم

آشنایی با فناوری‌های امنیت سایبری:

راهنمای انتخاب ابزارهای امنیت سایبری مناسب

ترجمه

دکتر مؤید محسنی

ویراست اول

زمستان ۱۴۰۳

انتشارات ترجمک

شماره کتابشناسی ملی	: ۹۸۷۸۵۵۹
شابک	: ۳۵۰۰۰۰۰ : ۹۷۸-622-7855-89-0
عنوان و نام پدیدآور	: آشنایی با فناوری‌های امنیت سایبری: راهنمای انتخاب ابزارهای امنیت سایبری مناسب / عباس معلم؛ ترجمه موید محسنی.
مشخصات نشر	: همدان، ترجمک، ۱۴۰۳
مشخصات ظاهری	: ک، [۱۹۶] ص.: مصور.
شناسه افزوده	: عنوان اصلی: a : Understanding cybersecurity technologies : a guide to selecting the right cybersecurity tools, 2022.
شناسه افزوده	: شبکه‌های کامپیوتری -- تدابیر ایمنی (-- Computer networks (Security measures), امنیت کامپیوتر (Computer Security)
شناسه افزوده	: محسنی، موید، ۱۳۵۶-، مترجم
رده بندی کنگره	: TK5105/59
رده بندی دیویی	: ۰۰۵/۸

شناسنامه کتاب

نام کتاب: آشنایی با فناوری‌های امنیت سایبری: راهنمای انتخاب ابزارهای مناسب

ترجمه: دکتر موید محسنی

ناشر: انتشارات ترجمک

صفحه آرای: انتشارات ترجمک

طراحی جلد: محمدحسین گیوی

نوبت چاپ: اول، ۱۴۰۳

قیمت (چاپی): ۳۵۰۰۰۰ تومان

قیمت (ایبوک): ۱۲۵۰۰۰ تومان

چاپ: گروه نشر الکترونیک ترجمک

شابک (پرینت): ۹۷۸-۶۲۲-۷۸۵۵-۸۹-۰

شابک (ایبوک): ۹۷۸-۶۲۲-۷۸۵۵-۹۰-۶

تلفن تماس: ۰۹۱۸۱۵۰۶۱۰۰

تارنمای اینترنتی: <https://tarjomac.com>

ISBN : 978-622-7855-89-0



9 786227 855890

ISBN : 978-622-7855-90-6



9 786227 855906

نویسنده:

دکتر عباس معلم

Abbas Moallem

مترجم:

دکتر موید محسنی

Moaied Mohseni

شابک اورجینال:

ISBN: 978-0-367-45745-7 (hbk)

ISBN: 978-1-032-15784-9 (pbk)

ISBN: 978-1-003-03842-9 (ebk)

شابک ترجمه فارسی:

شابک (پرینت): ۹۷۸-۶۲۲-۷۸۵۵-۸۹-۰

شابک (ایبوک): ۹۷۸-۶۲۲-۷۸۵۵-۹۰-۶

سال انتشار: ۲۰۲۳ - سی آر سی. پرس (چاپ اول)

کلیه حقوق این اثر برای انتشارات ترجمک محفوظ است. این اثر شامل کلیه قوانین حمایت حقوق مؤلفان و مصنفان و هنرمندان و ناشران جمهوری اسلامی می باشد (مصوب دوازده اسفند ۱۳۶۵ یا بعد از آن)، و بهره برداری بدون مجوز از آن به هر شکلی ممنوع است.

انتشارات ترجمک: سال ۱۴۰۳

tarjomac@gmail.com

همدان، صندوق پستی ۱۱۷-۶۵۹۱۵

مقدمه

حملات سایبری به شرکت‌ها، موسسات دولتی و افراد به طور تصاعدی در حال افزایش است. در عین حال، تعداد شرکت‌های کوچک و بزرگی که انواع راه‌حل‌ها را پیشنهاد می‌دهند نیز رو به افزایش است. از آنجایی که شرکت‌ها برای محافظت از خود در مقابل حملات سایبری به راه‌حل‌های تکنولوژیک تکیه می‌کنند، شناخت و انتخاب راه‌حلی مناسب از میان همه راه‌حل‌های ارائه‌شده، متخصصان، مدیران شرکت‌ها و تازه‌واردان حوزه امنیت سایبری را با چالش مهمی مواجه می‌سازد.

در کنفرانس RSA 2019، یک نماینده امنیت اطلاعات که در سانفرانسیسکو، کالیفرنیا برگزار شد، بیش از ۷۰۰ شرکت محصولات خود را در زمینه امنیت سایبری به نمایش گذاشتند. آیا این بدان معناست که آنها بیش از ۷۰۰ فناوری منحصر به فرد را ارائه می‌دهند؟ بدیهی است که نه. تعداد فناوری‌های واقعی مرتبط با امنیت سایبری بسیار کمتر از تعداد شرکت‌هایی است که آنها را ارائه می‌دهند. بسیاری از این شرکت‌ها از فناوری‌های یکسانی استفاده می‌کنند و آن‌ها را به صورت بسته‌بندی متفاوتی برای فروش عرضه می‌کنند، که گاهی اوقات حتی تفاوت‌های خیلی جزئی با هم دارند. مثلاً شرکت‌های زیادی وجود دارند که راه‌حل‌های آنتی‌ویروس ارائه می‌دهند. آیا آنها از فناوری‌های مشابه یا متفاوتی استفاده می‌کنند؟ اگر متفاوت است، پس آن تفاوت‌ها در چیست؟ اگر کسی بخواهد یک راه‌حل آنتی‌ویروس را انتخاب کند، مهمترین معیار این است که بفهمد چه راه‌حل‌های تکنولوژیکی در محصول استفاده می‌شود. در طول تحقیقی درباره راه‌حل‌های فناوری امنیت سایبری، من کتاب‌ها، مجلات، وبلاگ‌ها، مقالات و وبسایت‌های شرکت مربوط به فناوری امنیت سایبری را برای توضیحات محصول بررسی کردم. پس از صرف زمان قابل توجه برای پیمایش، مرور و خواندن این منابع، آموختم که:

- اکثر کتاب‌هایی که توسط کارشناسان مختلف نوشته شده‌اند، فوق‌العاده فنی هستند و برای همه سطوح حرفه امنیت سایبری چندان قابل درک نیستند.
- کتاب‌های موجود اغلب به دلیل تغییرات سریع حوزه امنیت سایبری قدیمی هستند.
- کتاب‌ها اغلب بیش از حد کلی هستند و شامل توصیف آسان برای درک فناوری‌ها نیستند.

- مجلات فنی، مقالات یا وبلاگ‌ها عمدتاً توسط تأثیرگذاران نوشته می‌شوند، به این معنی که اطلاعات ارائه شده همیشه عینی یا قابل اعتماد نیستند. این منابع اغلب شرکت‌ها، راه‌حل‌ها را رتبه‌بندی می‌کنند و بر ارائه توضیحات کلی از راه‌حل‌ها تمرکز می‌کنند.
- شرکت‌ها تنها توضیحات راه‌حل را با مواد بازاریابی عمومی و بدون توضیح عمیق و قابل درک از فناوری‌ها ارائه می‌دهند. گاهی اوقات توضیحات عمومی هستند و به سادگی ویژگی‌های محصول را فهرست می‌کنند - نه فناوری مورد استفاده برای ارائه آن ویژگی‌ها.

پس از مطالعه مطالب شرکت‌های مختلف حاضر در کنفرانس، تصمیم گرفتم از هر یک از فروشندگان در نمایشگاه محصولات امنیت سایبری توضیح شفاهی بخواهم. در حالی که به نمایش‌های بازاریابی آنها در سالن‌های نمایشگاه گوش می‌دادم، متوجه شدم که اکثر افرادی که در این سخنرانی‌ها شرکت می‌کردند برای به دست آوردن اطلاعات با مشکل مواجه بودند. این یک تجربه بسیار ناامیدکننده بود.

ارائه‌ها بسیار عمومی بودند، حتی بیشتر از خواندن مطالب. گاهی اوقات نیز محتوا توسط افرادی ارائه می‌شد که خودشان متخصص فناوری نبودند. اسلاید پاورپوینت‌های عمومی اغلب با چند سؤال مسابقه همراه بود که به شما امکان می‌داد جایزه نمادین دریافت کنید.

پس از آن تجربه، من در جلسات مدیریت شرکت‌های مختلف درباره راه‌حل‌های امنیت سایبری تحقیق کردم و به این نتیجه رسیدم که در بسیاری از موارد، تنها مدیران امنیتی شرکت‌های مربوطه کاملاً آگاه و مسلط بوده و درک قوی از موضوع دارند. در بقیه مواقع، آشکار بود که متصدیان به خوبی آگاه نبودند و دانش عمیقی از فناوری‌های واقعی نداشتند.

به دنبال این تجربه، تصمیم گرفتم خودم را به چالش بکشم و یک راهنمای قابل درک از فناوری‌های امنیت سایبری ایجاد کنم که بر فناوری‌های موجود و در راه‌حل‌های مختلف استفاده می‌شود، بدون تمرکز بر شرکت‌هایی که چنین فناوری‌هایی را ارائه می‌کنند.

اولین قدم ارائه دسته‌بندی و توصیف قابل اعتماد و قابل درک برای هر گروه از فناوری‌ها است.

نیت این کتاب کمک به همه متخصصان تازه‌کار در زمینه امنیت سایبری، دانشجویان و متخصصان است، تا از محتوا برای آموزش مخاطبان خود در مورد مبانی راه‌حل‌های ارائه شده استفاده کنند.

پس از طبقه‌بندی مختصر فناوری‌های اصلی (فصل ۱)، هر فصل صرفاً بر روی یک نوع یا گروهی از فناوری‌ها تمرکز خواهد کرد. هدف ایجاد فصول مختصر و قابل هضم، اجتناب از اصطلاحات فنی تا حد امکان و تمرکز بر فناوری‌های منبع‌باز است. محتوای هر فصل منسجم است: پس از مقدمه و پیشینه تاریخی، نحوه عملکرد فناوری‌ها را شرح می‌دهم، فناوری‌های اصلی را در هر گروه توضیح می‌دهم، مزایا

و معایب اصلی آن فناوری‌ها را بیان می‌کنم، محصولاتی را که از آن فناوری‌ها استفاده می‌کنند (در صورت لزوم) فهرست می‌کنم. و با یک نتیجه‌گیری کوتاه فصول ختم می‌شوند. برای کمک به درک فناوری‌ها، از تمثیل‌ها و یک تصویر بصری (نقشه درختی با شاخه‌های مختلف) برای کمک به خوانندگان غیر فنی و ارائه یک تصویر ذهنی استفاده می‌کنم. علاوه بر این، به منظور شفاف‌سازی اصطلاحات، کلیه اصطلاحات و تعاریف فنی استفاده شده در هر فصل به همراه نام افراد ذکر شده در کتاب در بخش واژه‌نامه گنجانده شده است.

عباس معلم

نویسنده

دکتر عباس معلم (Abbas Moallem)، دکتری حرفه ای، مشاور و استاد کمکی در دانشگاه ایالتی سن خوزه، کالیفرنیا است که در آنجا تعامل انسان و کامپیوتر، امنیت سایبری، تجسم اطلاعات و عوامل انسانی را تدریس می کند. او رئیس برنامه HCI-CPT، کنفرانس بین المللی HCI برای امنیت سایبری، حریم خصوصی و اعتماد است.

دکتر معلم ویراستار کتاب تعامل انسان با کامپیوتر و امنیت سایبری و نویسنده کتاب آگاهی از امنیت سایبری در میان دانشجویان و اساتید دانشگاه است. او همچنین ویراستار یک سری کتاب از CRC Press با عنوان عنصر انسانی در سیستم‌های اسمارت و هوشمند است.

فهرست مندرجات در یک نگاه

عنوان

صفحه

فصل ۱- دسته‌بندی فناوری‌های امنیت سایبری.....	۱
فصل ۲- رمزگذاری.....	۵
فصل ۳- احراز هویت.....	۱۸
فصل ۴- بیومتریک.....	۳۲
فصل ۵- فناوری فایروال.....	۴۷
فصل ۶- شناسایی ویروس.....	۵۹
فصل ۷- شناسایی فیشینگ.....	۶۹
فصل ۸- محافظت نقطه پایانی.....	۸۳
فصل ۹- فناوری حفاظت درمقابل بدافزار.....	۹۶
فصل ۱۰- اینترنت اشیا (IoT).....	۱۰۷
فصل ۱۱- امنیت شبکه.....	۱۲۱
فصل ۱۲- ردیابی مکان.....	۱۳۵
فصل ۱۳- نظارت و مراقبه.....	۱۴۷
فصل ۱۴- محافظت در مقابل تهدید داخلی.....	۱۶۰
فصل ۱۵- تشخیص تهاجم.....	۱۶۹
فصل ۱۶- اسکن آسیب پذیری.....	۱۷۷
فصل ۱۷- تست نفوذ.....	۱۸۶
فصل ۱۸- جمع بندی پایانی.....	۱۹۶

فهرست مندرجات کتاب

صفحه	عنوان
ب	مقدمه.....
۱	فصل ۱- دسته‌بندی فناوری‌های امنیت سایبری.....
۱	۱-۱ مقدمه.....
۱	۲-۱ دسته‌های مختلف فناوری سایبری.....
۳	۳-۱ دسته‌بندی فناوری.....
۵	فصل ۲- رمز گذاری.....
۵	۱-۲ مقدمه.....
۶	۲-۲ مروری بر پیشینه تاریخی.....
۸	۳-۲ چگونه فناوری های رمز گذاری کار می کنند.....
۱۰	۴-۲ فناوری های رمز گذاری.....
۱۴	۵-۲ مزایا و معایب رمز گذاری BLOWFISH و RSA.....
۱۵	۶-۲ کدام محصولات از رمز گذاری استفاده می کنند.....
۱۶	۷-۲ جمع بندی.....
۱۸	فصل ۳- احراز هویت.....
۱۸	۱-۳ مقدمه.....
۱۸	۲-۳ مروری بر پیشینه تاریخی.....
۲۰	۳-۳ چگونه فناوری های احراز هویت کار می کنند.....
۲۴	۴-۳ فناوری های احراز هویت.....
۲۵	۵-۳ مزایا و معایب فناوری های احراز هویت.....
۲۸	۶-۳ چه محصولاتی از احراز هویت استفاده می کنند.....
۲۹	۷-۳ جمع بندی.....

فصل ۴- بیومتریک ۳۲

۱-۴ مقدمه..... ۳۲

۲-۴ مروری بر پیشینه تاریخی..... ۳۲

۳-۴ فناوری بیومتریک چگونه عمل می کند..... ۳۳

۴-۴ فناوری های بیومتریک..... ۳۷

۵-۴ مقایسه صفات بیومتریک..... ۳۸

۶-۴ مزایا و معایب فناوری های بیومتریک..... ۴۰

۷-۴ چه محصولاتی از بیومتریک استفاده می کنند..... ۴۳

۸-۴ جمع بندی..... ۴۵

فصل ۵- فناوری فایروال..... ۴۷

۱-۵ مقدمه..... ۴۷

۲-۵ مروری بر پیشینه تاریخی..... ۴۷

۳-۵ فناوری فایروال چگونه کار می کند..... ۵۰

۴-۵ فناوری های فایروال..... ۵۲

۵-۵ مزایا و معایب فناوری های فایروال..... ۵۶

۶-۵ جمع بندی..... ۵۷

فصل ۶- شناسایی ویروس..... ۵۹

۱-۶ مقدمه..... ۵۹

۲-۶ مروری بر پیشینه تاریخی..... ۶۰

۳-۶ چگونه فناوری های تشخیص ویروس کار می کنند..... ۶۱

۴-۶ فناوری های تشخیص ویروس..... ۶۴

۵-۶ مزایا و معایب فناوری های تشخیص ویروس..... ۶۵

۶-۶ رویکردهای مورد استفاده در شناسایی ویروس..... ۶۶

۷-۶ جمع بندی..... ۶۷

فصل ۷- شناسایی فیشینگ..... ۶۹

۱-۷ مقدمه..... ۶۹

۲-۷ مروری بر پیشینه تاریخی..... ۷۰

۳-۷ فناوری های تشخیص فیشینگ چگونه کار می کنند..... ۷۱

۷۳.....	۴-۷ فناوری های تشخیص فیشینگ.....
۷۸.....	۵-۷ مزایا و معایب فناوری های تشخیص فیشینگ.....
۸۰.....	۶-۷ در چه محصولاتی از تشخیص فیشینگ استفاده می شود.....
۸۱.....	۷-۷ جمع بندی.....
۸۳.....	فصل ۸- محافظت نقطه پایانی.....
۸۳.....	۱-۸ مقدمه.....
۸۴.....	۲-۸ مروری بر پیشینه تاریخی.....
۸۵.....	۳-۸ چگونه فناوری های حفاظت نقطه پایان کار می کنند.....
۸۸.....	۴-۸ فناوری های حفاظت نقطه پایان.....
۹۰.....	۵-۸ مزایا و معایب فناوری های حفاظت نقطه پایان.....
۹۲.....	۶-۸ چه محصولاتی از محافظت نقطه پایانی استفاده می کنند.....
۹۳.....	۷-۸ جمع بندی.....
۹۶.....	فصل ۹- فناوری حفاظت درمقابل بدافزار.....
۹۶.....	۱-۹ مقدمه.....
۹۷.....	۲-۹ مروری بر پیشینه تاریخی.....
۹۹.....	۳-۹ فناوری های حفاظت از بدافزار چگونه کار می کنند.....
۱۰۱.....	۴-۹ فناوری های حفاظت در مقابل بدافزار.....
۱۰۳.....	۵-۹ مزایا و معایب حفاظت در مقابل بدافزار.....
۱۰۵.....	۶-۹ چه محصولاتی از محافظت در برابر بدافزار استفاده می کنند.....
۱۰۵.....	۷-۹ جمع بندی.....
۱۰۷.....	فصل ۱۰- اینترنت اشیا (IoT).....
۱۰۷.....	۱-۱۰ مقدمه.....
۱۰۸.....	۲-۱۰ مروری بر پیشینه تاریخی.....
۱۰۹.....	۳-۱۰ فناوری های IoT چگونه کار می کنند.....
۱۱۲.....	۴-۱۰ فناوری های امنیت اینترنت اشیا.....
۱۱۷.....	۵-۱۰ مزایا و معایب فناوری های امنیت اینترنت اشیا.....
۱۱۸.....	۶-۱۰ چه محصولاتی از فناوری های IoT استفاده می کنند.....
۱۱۸.....	۷-۱۰ جمع بندی.....

فصل ۱۱- امنیت شبکه..... ۱۲۱

۱-۱۱ مقدمه..... ۱۲۱

۲-۱۱ مروری بر پیشینه تاریخی..... ۱۲۱

۳-۱۱ فناوری های امنیت شبکه چگونه کار می کنند..... ۱۲۳

۴-۱۱ فناوری های امنیت شبکه..... ۱۲۶

۵-۱۱ مزایا و معایب امنیت شبکه..... ۱۲۷

۶-۱۱ کدام محصولات از امنیت شبکه استفاده می کنند..... ۱۲۹

۷-۱۱ جمع بندی..... ۱۳۲

فصل ۱۲- ردیابی مکان ۱۳۵

۱-۱۲ مقدمه..... ۱۳۵

۲-۱۲ پیشینه تاریخی مختصر..... ۱۳۶

۳-۱۲ فناوری های ردیابی مکان چگونه کار می کنند..... ۱۳۷

۴-۱۲ فناوری های ردیابی مکان..... ۱۳۹

۵-۱۲ کدام محصولات از ردیابی مکان استفاده می کنند..... ۱۴۳

۶-۱۲ جمع بندی..... ۱۴۵

فصل ۱۳- نظارت و مراقبه ۱۴۷

۱-۱۳ مقدمه..... ۱۴۷

۲-۱۳ مروری بر پیشینه تاریخی..... ۱۴۸

۳-۱۳ چگونه فناوری نظارت کار می کند..... ۱۴۹

۴-۱۳ فناوری های نظارتی..... ۱۵۱

۵-۱۳ مزایا و معایب فناوری های مراقبه..... ۱۵۴

۶-۱۳ کدام محصولات از سیستم مراقبه استفاده می کنند..... ۱۵۶

۷-۱۳ جمع بندی..... ۱۵۸

فصل ۱۴- محافظت در مقابل تهدید داخلی..... ۱۶۰

۱-۱۴ مقدمه..... ۱۶۰

۲-۱۴ مروری بر پیشینه تاریخی..... ۱۶۱

۳-۱۴ فناوری های حفاظت از تهدیدات داخلی چگونه کار می کنند..... ۱۶۳

۴-۱۴ فناوری های تشخیص تهدید داخلی..... ۱۶۴

۱۶۶	۵-۱۴ نظارت بر فعالیت کاربر و تجزیه و تحلیل رفتار.....
۱۶۶	۶-۱۴ مزایا و معایب شناسایی تهدیدات داخلی.....
۱۶۷	۷-۱۴ جمع بندی.....
۱۶۹	فصل ۱۵- تشخیص تهاجم.....
۱۶۹	۱-۱۵ مقدمه.....
۱۶۹	۲-۱۵ مروری بر پیشینه تاریخی.....
۱۷۰	۳-۱۵ چگونه فناوری های تشخیص تهاجم کار می کنند.....
۱۷۲	۴-۱۵ فناوری های تشخیص نفوذ.....
۱۷۳	۵-۱۵ مزایا و معایب سیستم های تشخیص تهاجم.....
۱۷۴	۶-۱۵ از کدام محصولات برای تشخیص تهاجم استفاده شود.....
۱۷۵	۷-۱۵ جمع بندی.....
۱۷۷	فصل ۱۶- اسکن آسیب پذیری.....
۱۷۷	۱-۱۶ مقدمه.....
۱۷۸	۲-۱۶ مروری بر پیشینه تاریخی.....
۱۷۸	۳-۱۶ چگونه فناوری های اسکن آسیب پذیری کار می کنند.....
۱۸۲	۴-۱۶ فناوری های اسکن آسیب پذیری.....
۱۸۳	۵-۱۶ مزایا و معایب اسکن آسیب پذیری.....
۱۸۴	۶-۱۶ جمع بندی.....
۱۸۶	فصل ۱۷- تست نفوذ.....
۱۸۶	۱-۱۷ مقدمه.....
۱۸۷	۲-۱۷ مروری بر پیشینه تاریخی.....
۱۸۷	۳-۱۷ چگونه فناوری های تست نفوذ کار می کنند.....
۱۸۸	۴-۱۷ فناوری های تست نفوذ.....
۱۹۲	۵-۱۷ مزایا و معایب تست نفوذ.....
۱۹۳	۶-۱۷ جمع بندی.....
۱۹۶	فصل ۱۸- جمع بندی پایانی.....

دسته‌بندی فناوری‌های امنیت سایبری

۱-۱ مقدمه

امنیت سایبری^۱ یک حوزه علمی رو به رشد است که از انواع بسیار متنوعی از فناوری‌ها تشکیل شده است که برای محافظت از سیستم‌ها در برابر انواع مختلف حملات، برخی آشنا و برخی ناشناخته، استفاده می‌شود. به دلیل پیچیدگی جنبه‌های در حال تحول این حوزه، هیچ دسته‌بندی استاندارد از فناوری‌های حفاظتی وجود ندارد. دسته‌بندی فناوری‌های سایبری به درک بهتر نحوه عملکرد این فناوری‌ها کمک می‌کند. در این فصل، پس از مرور برخی از دسته‌بندی‌های مختلف موجود، روشی را ارائه می‌دهم که فناوری‌های سایبری محافظ بازنگری شده در این کتاب را طبقه‌بندی کرده‌ام.

۲-۱ دسته‌های مختلف فناوری سایبری

فناوری‌های مورد استفاده در امنیت سایبری به طرق مختلفی دسته‌بندی شده است. از دیدگاه تحقیقاتی، موضوعات امنیت سایبری به شرح زیر طبقه‌بندی می‌شوند [۱]:

۱. امنیت سایبری کاربردی
۲. علم داده‌های امنیت سایبری
۳. آموزش و تعلیم امنیت سایبری
۴. وقایع امنیت سایبری
۵. مدیریت و سیاست امنیت سایبری
۶. فناوری امنیت سایبری
۷. امنیت سایبری انسانی و اجتماعی
۸. نظریه‌ها در امنیت سایبری

¹ Cybersecurity

از نقطه نظر عملی، یک نوع طبقه بندی معمولاً بر اساس نوع تهدیدات و اثرات مورد نظر آنها است. در این دسته، تهدیدها به دو گروه طبقه بندی می شوند [۲]:

۱. تکنیک های حمله

۲. اثرات تهدید

نوع دیگری از طبقه بندی بر اساس نوع محافظت سایبری است. سپس فناوری های حفاظتی را می توان به چهار گروه طبقه بندی کرد:

۱. سیستم معماری

۲. نوع شناسایی (تشخیص)

۳. اکوسیستم

۴. نوع داده

فناوری های امنیت سایبری را می توان بر اساس مؤلفه هایی که هر فناوری قرار است از آنها محافظت کند نیز طبقه بندی کرد. این طبقه بندی شامل گروه های اصلی زیر است:

۱. شبکه (Network)

۲. اپلیکیشن (Application)

۳. نقطه پایان (Endpoint)

۴. داده (Data)

۵. هویت (Identity)

۶. دیتابیس (Database)

۷. فراساختار (Infrastructure)

۸. موبایل (Mobile)

۹. ابر (کلود) (Cloud)

۱۰. پشتیبان (Backup)

نوع دیگری از دسته بندی بر اساس انواع راه حل های امنیتی است. طبقه بندی مبتنی بر راه حل یک شیوه تجربی تر برای دسته بندی فناوری های سایبری است. در این دسته بندی راه حل ها به گروه های زیر دسته بندی می شوند:

۱. مدیریت هویت و دسترسی

۲. مدیریت ریسک و رعایت

۳. رمزگذاری
۴. پیشگیری از بین رفتن داده (DLP)
۵. مدیریت واحد تهدید (UTM)
۶. دیوار آتش (فایروال)
۷. راه حل های آنتی ویروس / ضد بدافزار
۸. سیستم تشخیص تهاجم (IDS)/سیستم جلوگیری از تهاجم (IPS)
۹. بازیابی سوانح
۱۰. کاهش حملات انکار توزیع شده خدمات (DDoS).
۱۱. فیلتر کردن وب

۱-۳ دسته‌بندی فناوری

برای این کتاب، من از طبقه بندی بر اساس راه حل های تکنولوژیک موجود استفاده می‌کنم. آنها به ۱۶ دسته اصلی گروه‌بندی می‌شوند. در هر فصل، من نمای درختی فناوری‌های هر گروه پیشرو را ارائه می‌دهم. دسته‌بندی در این کتاب شامل گروه‌های زیر است (شکل ۱-۱):

- | | |
|-----------------------------------|----------------------------|
| ۱. رمزگذاری | ۸. محافظت در مقابل بدافزار |
| ۲. احراز هویت | ۹. اینترنت اشیا |
| ۳. بیومتریک | ۱۰. امنیت شبکه |
| ۴. فایروال | ۱۱. ردیابی مکان |
| ۵. حفاظت نقطه پایان | ۱۲. نظارت یا مراقبه |
| ۶. شناسایی فیشینگ | ۱۳. تهدید داخلی |
| ۷. شناسایی ویروس (معمولاً با دسته | ۱۴. تشخیص تهاجم |
| حفاظت نقطه پایان در یک گروه واحد | ۱۵. اسکن آسیب پذیری |
| گذاشته می‌شود) | ۱۶. تست نفوذ |



شکل ۱-۱ دسته بندی فناوری امنیت سایبری بر اساس راه حل های تکنولوژیک موجود