مدیریت یکپارچه تهدیدات

ترجمه: آسیه مددی

۱۳۹۷

مؤسسه آموزشی تألیفی کارآفرین آریا

سرشناسه	:	تایتل، اد، ۱۹۵۲ - م. Tittel, Ed
عنوان و نام پدیدآور	:	مدیریت یکپارچه تهدیدات/ [نویسنده اد تایتل]؛ مترجم آسیه مددی.
مشخصات نشر	:	آمل: آموزشی تالیفی کارآفرین آریا، ۱۳۹۷.
مشخصات ظاهری	:	۹۴ ص.
شابک	:	۹۷۸-۶۰۰-۹۶۸۴۶-۲-۵
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	عنوان اصلی: Unified threat management for dummies, 2012.
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	:	Computer networks -- Security measures
موضوع	:	فایروال (ایمن‌سازی کامپیوتر)
موضوع	:	Firewalls (Computer security)
موضوع	:	کامپیوترها -- ایمنی اطلاعات
موضوع	:	Computer se[illegible]
شناسه افزوده	:	[illegible]ددی، آسیه، ۱۳۶۷ - ، مترجم
رده بندی کنگره	:	[illegible]۴م[illegible]/TK۵۱۰۵/۵۹
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۵۱۱۶۸۶

مؤسسه آموزشی تألیفی کارآفرین آریا

■ نام کتاب:	مدیریت یکپارچه تهدیدات
■ ترجمه:	آسیه مددی
■ ناشر:	آموزشی تألیفی کارآفرین آریا
■ ویرایش:	اول
■ نوبت چاپ:	اول ۱۳۹۷
■ حروفچینی و صفحه آرایی:	www.irantypist.com
■ طراح و گرافیست:	www.irantypist.com
■ شابک:	۹۷۸-۶۰۰-۹۶۸۴۶-۲-۵
■ شمارگان:	۱۰۰۰
■ مرکز خرید آنلاین:	www.arshadan.com www.arshadan.net
■ مرکز پخش و توزیع:	۰۲۱۴۷۶۲۵۵
■ قیمت:	۲۰۰۰۰ تومان

پیشگفتار:

مدیریت تهدید یکپارچه یک راه حل جامع است که به تازگی در صنعت امنیت شبکه پدید آمده‌است و از سال ۲۰۰۴ پول گسترده‌ای را به عنوان راه حل شاهراه دفاعی شبکه‌های اصلی برای سازمان‌ها به دست آورد.

دستگاه یوتی‌ام ساده مدیریت راهبرد امنیتی یک شرکت را آسانترمی کند، فقط با یک دستگاه می‌توان مدل لایه‌های مختلف سخت افزار و نرم افزار را درنظر گرفت. همچنین بوسیله یک کنسول متمرکز، کلیه راهکارهای امنیتی میتوانند تحت نظارت باشند.یو تی ام ها انواع قابلیت های امنیتی از جمله دیواره آتش ،وی پی ان،دروازه های ضد ویروس ،ضدهرزنامه ،فیلترینگ محتوا،مدیریت پهنای باند،نرم افزار کنترل و گزارش دهی متمرکز را به عنوان ویژگی های اساسی دارند

مزایای کلیدی یو تی ام به شرح زیر است

اجتناب از نصب چند نرم‌افزار و سخت افزار و کاهش هزینه ی تعمیر و نگهداری و کاهش پیچیدگی .

. رابط کاربری گرافیکی برای مدیریت آسان مبتنی بر وب

کاهش آموزش‌های فنی مورد نیاز یک محصول برای یادگیری،چون از یک دستگاه جامع به جای چند دستگاه استفاده شده است.

فهرست مطالب

عنوان | صفحه

مقدمه

تعدادی از تکنولوژی های امنیتی در چند سال اخیر بخش های عمده ای از بازار را در اختیار دارند. مدیریت تهدید یکپارچه، که همچنین به عنوان UTM شناخته شده است، یکی از آنها است. UTM خریداران این فرصت را می‌دهد تا امنیت و عملکرد شبکه خود را بهبود بخشد و در عین حال پیچیدگی شبکه و هزینه ها را کاهش دهند.

محیط شبکه و چشم انداز تهدید به طور مداوم در حال تغییر است - دستگاه های جدید، برنامه ها و تهدید ها تقریبا روزانه ظاهر می شوند. سازمان هایی در هر اندازه برای دسترسی امن کاربران تلفن همراه در آخرین تلفن هوشمند یا رایانه لوحی، زمان مسدود کردن آخرین تهدیدهای پنهان شده داخل ترافیک برنامه ها از سایت های رسانه های اجتماعی تلاش می‌کنند. این یک مبارزه سخت است!

یک پاسخ سنتی برای تهدیدات جدید، اضافه کردن فن آوری های مستقل امنیتی به شبکه است. متاسفانه این باعث پیچیدگی و هزینه می‌شود، زیرا هر تکنولوژی جدید به معنی یک دستگاه جدید برای استقرار، یک مجموعه جدید از سیاست های پیکربندی و یک کنسول مدیریت جدید برای نظارت است. و، به این دلیل که هر محصول مستقل جدید با محصول موجود مجتمع نمی شود، باعث ایجاد لکه های بالقوه کور در یک استراتژی امنیت سازمان است، که از طریق آن تهدیدات منتقل شده کشف نمی شوند.

این کتاب ویژگی ها و مزایایی که UTM می‌تواند به شبکه شما ارائه دهد، در چارچوب شبکه های سریع در حال تحول امروز و چشم انداز تهدید ، بررسی می‌کند.

این کتاب چگونه سازماندهی شده است

فصل های این کتاب، جزئیات و فن آوری های مورد استفاده در UTM و برخی دیگر را تشخیص می‌دهند.

✓ فصل ۱: نیاز به امنیت شبکه تلفیقی توضیح می‌دهد که چالش هایی که هنگام تأمین محیط های در حال رشد شبکه با آن مواجه می‌شویم چیستند، نیاز به کنترل برنامه ها، افزایش نرم افزار جرم و غیره، مدیریت تهدید متحد برای Dummies

✓ فصل ۲: چرا فایروال های سنتی نمی توانند با تهدیدات امروز ادامه یابند؟ مشکلات فن آوری امنیت شبکه و غیره را توضیح می‌دهد.

✓ فصل ۳: UTM یا هرج و مرج دستور می‌دهد که چگونه یک رویکرد تلفیقی امنیت شبکه، حفاظت و عملکرد را بهبود می‌بخشد و هزینه و پیچیدگی را کاهش می‌دهد.

✓ فصل ۴: یک نگاه دقیق تر به مدیریت یکپارچه تهدید، جزئیات بیشتری در مورد تکنیک های بازرسی مختلف و پردازنده های سخت افزاری را ارائه می‌دهد که عضلات را برای نرم افزار UTM ارائه می‌دهند.

✓ فصل ۵: مدیریت یکپارچه تهدید در عمل، اجزای UTM را از کنترل برنامه تا فیلتر کردن وب و نحوه استفاده از UTM در سازمانهای دنیای واقعی بررسی می‌کند.

✓ فصل ۶: ده (یازده) سوال کلیدی که باید بپرسید، وقتی نوبت به ارزیابی راه حل های UTM سوالاتی را مطرح می‌کند که قبل از انجام هر گونه خرید UTM نیاز به پرسیدن آنهاست..

✓ واژه نامه: در اینجا تعاریف و اصطلاحات کلیدی را تعریف می‌کنیم.

آیکون های مورد استفاده در این کتاب

در کتاب آیکون هایی در حاشیه قرار گرفته اند تا توجه فرد را به نوشته های آن جلب کنند. این آیکون ها در این کتاب آمده است.

اینها نکاتی هستند که باید در ذهن داشته باشید وقتی که خود را در دنیای مدیریت تهدید یکپارچه غوطه ور می‌کنید.

آیکن دوم:

گاهی اوقات ما اطلاعات فنی را که از اصول اولیه فراتر رفته است به اشتراک می‌گذاریم. این آیکون به شما می‌گوید که متن مربوطه جزئیات بیشتری از UTM را از موارد کاملا ضروری ارائه می‌دهد. شما می‌توانید آن را امتحان کنید اگر دوست دارید!

آیکن سوم

این آیکون اطلاعاتی را در مورد هدف قرار می‌دهد که به شما کمک می‌کند مزایای افزایش امنیت شبکه را با استفاده از مدیریت تهدید یکپارچه به حداکثر برسانید.