شناخت و بررسی SOCو مطرح ترین SIEMها در جهان

مولف
پیمان فیروزیان

سرشناسه	:	فیروزیان، پیمان، ۱۳۶۹- Firooziyan, Payman
عنوان و نام پدیدآور	:	شناخت و بررسی SOC و مطرح ترین SIEMها در جهان / پیمان فیروزیان.
مشخصات نشر	:	تهران: میعاد اندیشه، ۱۳۹۹.
مشخصات ظاهری	:	۲۲۲ ص.
شابک	:	978-622-2312-23-7
وضعیت فهرست نویسی	:	فیپا
موضوع	:	سامانه‌های امنیتی
موضوع	:	Security systems
موضوع	:	شبکه‌های کامپیوتری – تدابیر ایمنی
موضوع	:	Computer networks -- Security measures
موضوع	:	پایگاه‌های اطلاعاتی – امنیت
موضوع	:	Database security
رده بندی کنگره	:	TH۹۷۰۵
رده بندی دیویی	:	۶۵۸/۴۷۳
شماره کتابشناسی م	:	۶۱۲۵۲۹۵

انتشارات میعاد اندیشه

www.miadpub.ir

عنوان کتاب: شناخت و بررسی SOC و مطرح ترین SIEMها در جهان

مولف : پیمان فیروزیان

ناشر : میعاد اندیشه

نوبت چاپ: اول - ۱۳۹۹

شمارگان: ۱۰۰۰ نسخه

قیمت: ۵۴۰/۰۰۰ ریال

شابک: ۷- ۲۲۳- ۲۳۱ - ۶۲۲ - ۹۷۸

پیشگفتار

امنیت یک اصل برای زندگی تمام انسان ها در قالب خانواده، شهر، کشور و حتی کره زمین است و برای این اصل هر لحظه میکوشیم تا بهترین شرایط را فراهم کنیم. دنیا ما امروزه درگیر اطلاعات مهم و حیاتی بر بستر فناوری اطلاعات است و برای پیاده کردن اصل امنیت باید توان و تخصص خود را در این حوزه بالا ببریم تا بتوانیم شرایط مناسبی را برای حریم خصوصی خود ایجاد کنیم. نقض امنیت بر بستر فناوری اطلاعات دلایل زیادی دارد که برای بررسی این موارد باید به طور شبانه روزی بر این بستر نظارت کنیم. اما تحلیل تمام داده‌ها و رویداد ها تولید شده از تجهیزات شبکه کار دشواریست. وظیفه این تحلیل های گسترده که در مراکز عملیات امنیت صورت میگیرد بر عهده سیستم های امنیت اطلاعات و مدیریت رویداد است که به صورت شبانه روزی این بستر را پایش می‌کند. اما این سیستم با تمام مزایایی که در اختیار ما قرار می دهند مهمانان بلند مدتی در شبکه ما خواهند بود و همچنین از مهمترین داده های ما که همان رویداد های امنیتی هستند باخبراند، تمام این موارد میزان اهمیت غیر قابل انکار این سیستم ها را نشان می‌دهد و بررسی دقیقی را برای انتخاب هر یک این سیستم ها می‌طلبد. در این کتاب برآن شدم تا با بررسی اصول و قواعد امنیت و تحلیل مراکز عملیات امنیت به معرفی مطرح ترین سیستم های امنیت اطلاعات و مدیریت رویدادها بپردازم و پارامتری های ارزیابی این محصولات را معرفی کنم تا راه را برای انتخاب کارآمدتر این محصولات بر حسب نیازهای سازمانی هموار سازم. کلیه منابع ارائه شده در این کتاب دارای ترجمه کامل توسط مولف است و هرگونه کپی برداری از آن بدون قید نام مولف خارج از اخلاق تالیف کتب است. زمان صرف شده برای تهیه این اطلاعات ۱۹ ماه بوده است که امیدوارم شناخت مناسبی را برای شما از محصولات به همراه داشته باشد.

فهرست مطالب

چکیده

از دیرباز مسئله امنیت اطلاعات و مدیریت رویداد ها جزو اساسی‌ترین بخش‌های حوزه فناوری اطلاعات به حساب می‌آید که طراحی سیستم‌های امنیتی زیادی برای پایش ترافیک و سطح امنیت داده ها شده‌اند. از جمله این نمونه‌ها سیستم‌های امنیت اطلاعات و مدیریت رویدادها (SIEM) هستند که در هسته مرکز عملیات امنیت قرار دارند و به حیث میزان دسترسی و بازه زمانی استفاده طولانی، از اهمیت بسیار بالایی برخوردارند؛ لذا شناخت درست و دقیق برای بررسی و مقایسه هر نوع از این سیستم‌ها احساس می‌شود. از آنجایی که پارامترهای ارزیابی این سیستم‌ها بسیار گسترده و متنوع است در این کتاب میتوان به مواردی از آن اشاره کرد. این در حالی است که برای انتخاب، تعیین سطح امنیت سازمانی، ابعاد سازمان و نیازهای سازمان مشخص کننده محدوده انتخاب محصول برای آن سازمان است که بنا به تعداد تجهیزات تولید کننده رویداد، نیازهای هر سازمان میتوان مواردی را برای انتخاب بهتر در اولویت قرار داد. در این میان نیز سازمان‌هایی هستند که برحسب محدودیت‌های مالی و یا تصمیمات مراتب بالادستی ملزم به استفاده از یک محصول خاص می‌شوند. از آنجایی که این کتاب به دنبال گستره محصولات مطرح را مورد بررسی قرار داده است چند نمونه از محصولات بومی را نیز در این لیست قرار دارند که به بررسی آن ها می‌پردازد.