

شناخت و بررسی SOC و مطرح ترین SIEM ها در جهان

مؤلف

پیمان فیروزبان

www.ketab.ir

سرشناسه	: فیروزیان، پیمان. ۱۳۶۹-
عنوان و نام پدیدآور	: Firoozian, Payman
مشخصات نشر	: شناخت و بررسی SOC و مطرح ترین SIEM ها در جهان / پیمان فیروزیان.
مشخصات ظاهری	: تهران: میعاد اندیشه، ۱۳۹۹.
شابک	: ۲۳۲ ص.
وضعیت فهرست نویسی	: 978-622-2312-23-7
موضوع	: فیبا
موضوع	: سامانه های امنیتی
موضوع	: Security systems
موضوع	: شبکه های کامپیوتری - تدابیر ایمنی
موضوع	: Computer networks -- Security measures
موضوع	: پایگاه های اطلاعاتی - امنیت
موضوع	: Database security
رده بندی کنگره	: TH۹۷۰۵
رده بندی دیویی	: ۶۵۸/۲۷۲
شماره کتابشناسی	: ۶۱۲۵۲۹۵



www.midadpub.ir

عنوان کتاب: شناخت و بررسی SOC و مطرح ترین SIEM ها در جهان

مؤلف : پیمان فیروزیان

ناشر : میعاد اندیشه

نوبت چاپ: اول - ۱۳۹۹

شمارگان: ۱۰۰۰ نسخه

قیمت: ۵۴۰/۰۰۰ ریال

شابک: ۷-۲۲۳-۲۳۱-۶۲۲-۹۷۸

همه ی حقوق مادی و معنوی این اثر برای مؤلف محفوظ است.

تکثیر و انتشار این اثر به هر صورت، از جمله بازنویسی، فتوکپی، ضبط الکترونیکی

و ذخیره در سیستم های بازیابی و پخش، بدون دریافت مجوز کتبی و قبلی از نویسنده

به هر شکلی ممنوع است.

این اثر تحت حمایت «قانون حمایت از حقوق مولفان، مصنفان و هنرمندان ایران» قرار دارد

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 داده ها و رویداد ها تولید شده از تجهیزات شبکه را از شوازیست. وظیفه این تحلیل های گسترده که در مراکز عملیات امنیت - رزنت میگیرد بر عهده سیستم های امنیت اطلاعات و مدیریت رویداد است که به صورت شبانه روزی این بستر را پایش می کند. 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 به عنوان رویداد های امنیتی هستند با خبراند، تمام این موارد میزان اهمیت غیر قابل انکار این سیستم ها را نشان می دهد و بررسی دقیقی را برای انتخاب هر یک این سیستم ها می طلبد. 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. پانزده متری 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

۱	چکیده
۲	مقدمه
۳	فصل اول: آشنایی با مفاهیم اولیه
۴	۱-۱ مفاهیم امنیت اطلاعات
۴	۱-۱-۱ مفهوم ISMS
۵	۱-۱-۲ مفهوم SOC
۸	۱-۱-۳ مفهوم NCC
۱۰	۱-۱-۴ مفهوم SIEM
۱۰	۲-۱ اصول و قواعد امنیت اطلاعات
۱۰	۱-۲-۱ مدیریت ریسک
۱۱	۲-۲-۱ نقش ها و مسئولیت ها
۱۱	۳-۲-۱ مستندسازی امنیت اطلاعات
۱۲	۴-۲-۱ اعتباربخشی سامانه ها
۱۲	۵-۲-۱ مانیتورینگ امنیت اطلاعات
۱۳	۶-۲-۱ رخدادهای امنیت سایر
۱۳	۷-۲-۱ تعامل با صنعت و برون سپاری
۱۴	۸-۲-۱ امنیت فیزیکی
۱۴	۹-۲-۱ امنیت کارکنان
۱۶	۱۰-۲-۱ زیرساخت ارتباطات
۱۷	۱۱-۲-۱ ابزارها و سامانه های ارتباطی
۱۷	۱۲-۲-۱ نیازمندی های الزامی چارچوب سیاست امنیتی ممانعتی
۱۸	۱۳-۲-۱ محصول امنیتی

- ۱۹-۲-۱ امنیت رسانه های ذخیره ساز..... ۱۹
- ۲۰-۲-۱ امنیت نرم افزار..... ۲۰
- ۲۱-۲-۱ امنیت ایمیل..... ۲۱
- ۲۲-۲-۱ کنترل دسترسی..... ۲۲
- ۲۳-۲-۱ مدیریت امن..... ۲۳
- ۲۴-۲-۱ رمزنگاری..... ۲۴
- ۲۶-۲-۱ امنیت شبکه..... ۲۶
- ۲۷-۲-۱ امنیت دامنه های متقاطع..... ۲۷
- ۲۸-۲-۱ انتقال داده و فیلترینگ محتوا..... ۲۸
- ۲۸-۲-۱ کارکردن خارج از محل کار..... ۲۸
- ۳۲-۲-۱ مرکز عملیات امنیت..... فصل دوم: ۳۲
- ۳۳-۲-۱ مقدمه..... ۳۳
- ۳۴-۲-۱ تعریف مرکز عملیات امنیت..... ۳۴
- ۳۵-۲-۱ تاریخچه..... ۳۵
- ۳۶-۲-۱ نسل اول مرکز عملیات امنیت..... ۳۶
- ۳۷-۲-۱ نسل دوم مرکز عملیات امنیت..... ۳۷
- ۳۸-۲-۱ نسل سوم مرکز عملیات امنیت..... ۳۸
- ۳۸-۲-۱ نسل چهارم مرکز عملیات امنیت..... ۳۸
- ۳۹-۲-۱ نسل پنجم مرکز عملیات امنیت..... ۳۹
- ۴۰-۲-۱ نسل بعدی مرکز عملیات امنیت..... ۴۰
- ۴۱-۲-۱ اجزای مرکز عملیات امنیت..... ۴۱
- ۴۲-۲-۱ افراد (People)..... ۴۲
- ۴۲-۲-۲ روند (Process)..... ۴۲

۵۹	۳-۴-۲ فناوری (Technology)
۶۲	۵-۲ مزایای مرکز عملیات امنیت (SOC)
۶۴	۶-۲ سرویس SIEM (هسته مرکز عملیات امنیت)
۶۵	فصل سوم: امنیت اطلاعات و مدیریت رویدادها
۶۶	۱-۳ مقدمه
۶۷	۲-۳ امنیت اطلاعات و مدیریت رویداد
۶۷	۲-۳ مفهومی LMS
۶۷	۲-۲-۳ مفهومی SLM یا SLM
۶۸	۳-۲-۳ مفهومی SIEM
۶۸	۴-۲-۳ مفهومی SEC
۶۹	۳-۲ وظایف اصلی SIEM
۶۹	۱-۳-۳ عادی سازی
۶۹	۲-۳-۳ طبقه بندی
۷۰	۳-۳-۳ مطابقت
۷۰	۴-۳-۳ شناسایی تهدیدها
۷۰	۵-۳-۳ بررسی شواهد قانونی (Forensics)
۷۱	۶-۳-۳ اولویت بندی
۷۱	۷-۳-۳ تحلیل آماری
۷۱	۸-۳-۳ تحلیل تاریخی
۷۲	۹-۳-۳ مدیریت لاگ و گزارشگیری
۷۲	۴-۳ عوامل موثر در عملکرد سیستم امنیت اطلاعات و مدیریت رویدادها
۷۲	۱-۴-۳ عواملی که موجب بهبود عملکرد SIEM
۷۳	۲-۴-۳ عواملی که موجب ضعف عملکرد SIEM

۷۳	۵-۳ پارامترهای ارزیابی
۷۴	۱-۵-۳ شش نکته در ارزیابی SIEM از دیدگاه سائیس جگو
۷۷	۲-۵-۳ معیارهای غیر قابل اجتناب از زبان Mike Mahoney
۷۸	۳-۵-۳ معیارهای ارزیابی از نگاه گارتنر
۸۳	۶-۳ فروشندگان SIEM از دیدگاه گارتنر
۸۴	۱-۶-۳ رهبران
۸۴	۲-۶-۳ چالشگرها
۸۵	۱-۶-۳ آینده نگرها
۸۵	۴-۶-۳ بازیچان ذخیره
۸۶	۷-۳ خلاصه و بازنگری
۸۸	۸-۳ هر آنچه برای ارزیابی SIEM باید بدانیم
۸۸	۱-۸-۳ شرکت و محصول
۸۹	۲-۸-۳ معماری
۹۰	۳-۸-۳ نصب و پیکربندی
۹۱	۴-۸-۳ جمع آوری رویدادها
۹۱	۵-۸-۳ ذخیره سازی رویدادها
۹۲	۶-۸-۳ رابط کاربری و تجربه کاربری
۹۳	۷-۸-۳ گواهینامه ها و دوره های آموزشی
۹۴	فصل چهارم: SIEM های مطرح بومی و غیر بومی
۹۵	۱-۴ مقدمه
۹۵	۲-۴ بررسی محصولات SIEM مطرح
۹۷	۱-۲-۴ Alien Vault
۱۰۳	۲-۲-۴ BlackStratus

107	 (RSA) Dell 2-2-2
109	 Exabeam 2-2-2
111	 Fortinet 5-2-2
112	 IBM 7-2-2
118	 LogPoint 7-2-2
120	 LogRhythm 8-2-2
123	 ManageEngine 9-2-2
126	 McAfee 10-2-2
130	 HP ArcSight Micro Focus 11-2-2
133	 NetScout EventTracker 12-2-2
136	 Rapid7 13-2-2
138	 Securonix 14-2-2
142	 SolarWinds 15-2-2
145	 Splunk 16-2-2
149	 Venustech 17-2-2
152	 LayerX Technologies 18-2-2
155	 LogLogic-Tibco 19-2-2
157	 Tenable 20-2-2
159	 FairWarning Data Protection 21-2-2
170	 LookWise S21 SEC 22-2-2
171	 Tripwire Log Center 23-2-2
172	 Tango/04 SIEM Tool 24-2-2
175	 Huntsman Enterprise SIEM Tool 25-2-2

- ۱۶۷ Symantec SIEM ۲۶-۲-۴
- ۱۶۸ Alert Logic ۲۷-۲-۴
- ۱۶۹ CorreLog – CA Technologies ۲۸-۲-۴
- ۱۷۰ Sophos SIEM ۲۹-۲-۴
- ۱۷۱ EiQ Networks ۳۰-۲-۴
- ۱۷۲ Extreme Networks SIEM Tool ۳۱-۲-۴
- ۱۷۷ GFI LanGuard ۳۲-۲-۴
- ۱۷۹ Juniper Secure Analytics ۳۳-۲-۴
- ۱۸۰ ARMA SIEM (محصول شرکت آریا همراه سامانه) ۳۴-۲-۴
- ۱۸۶ APK SIEM (محصول شرکت امن پردازان کویر) ۳۵-۲-۴
- ۱۸۸ Eavi SIEM (محصول شرکت پیام پرداز) ۳۶-۲-۴
- ۲۰۳ CoreLog® (محصول شرکت بهین راهکار توسعه پیشرو) ۳۷-۲-۴
- ۲۱۰ Douran SEIM (محصول امن شرکت داده پردازی دوران) ۳۸-۲-۴
- ۲۱۸ منابع

چکیده

از دیرباز مسئله امنیت اطلاعات و مدیریت رویدادها جزو اساسی‌ترین بخش‌های حوزه فناوری اطلاعات به حساب می‌آید که طراحی سیستم‌های امنیتی زیادی برای پایش ترافیک و سطح امنیت داده‌ها 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 اساسی 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 این ب، 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 رویدادها از برای 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 بررسی گستره محصولات مطرح را مورد بررسی قرار داده است چند نمونه از محصولات بومی را نیز در این لیست قرار دارند که به بررسی آن‌ها می‌پردازد.