ثامن ارتباط عصر

خدمات مرکز عملیات امنیت (SOC)

SOC Solutions Provider

ثامن ارتباط عصر

ارائه کننده خدمات جامع
فناوری اطلاعات و ارتباطات

S.E.A

Samen Ertebat Asr

S.E.A
ثامن ارتباط عصر
ارائه کننده خدمات جامع فناوری اطلاعات و ارتباطات

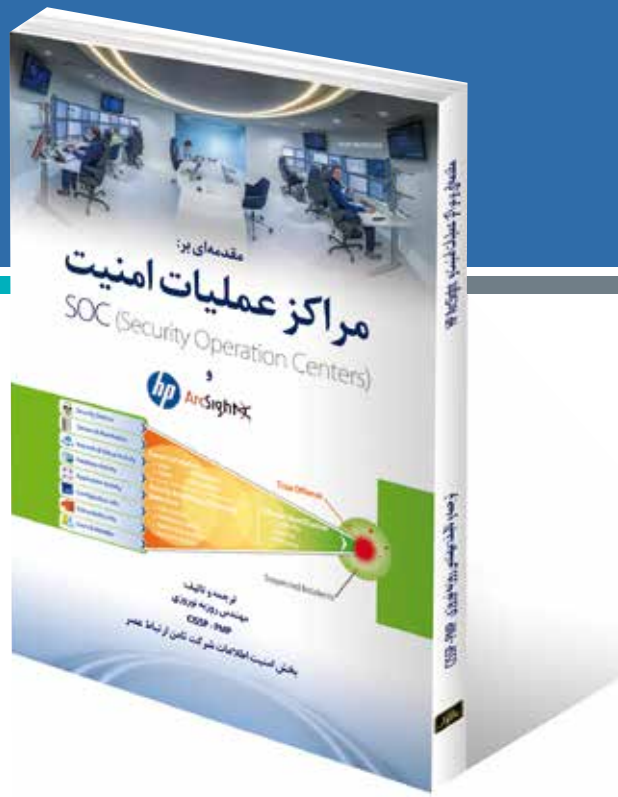
www.samenea.com

تهران، بلوار نلسون ماندلا (آفریقا)، بلوار گلشهر، پلاک ۱۲
کدپستی: ۱۹۱۵۶۶۳۴۸۱ ، تلفن: ۰۲۱-۲۴۸۷۹۰۰۰ ، فاکس: ۰۲۱-۲۶۲۰۲۸۹۸

انتشار اولین کتاب دانش‌محور در حوزه

مراکز عملیات امنیت (SOC)

شرکت ثامن ارتباط عصر بنا بر وظایف خود و تجربه عملی که در طراحی و پیاده‌سازی مراکز عملیات امنیت (SOC) داشته است، اقدام به انتشار کتابی در این زمینه نموده است. هدف از ترجمه و تألیف این کتاب، آشنایی علمی و اصولی خیل علاقمندان مرز و بوم به مقوله مراکز عملیات امنیت و پروژه‌های آن و یکی از بزرگترین راهکارهای SIEM یعنی ArcSight است تا علاوه بر پاسخ به خواست علاقمندان، انتقال دانش به داخل کشور انجام پذیرد.



توانمندی شرکت ثامن ارتباط عصر در طراحی، تامین تجهیزات، پیاده‌سازی و راهبری مراکز عملیات امنیت (SOC)

اهمیت امنیت اطلاعات امروزه برکسی پوشیده نیست چراکه با ورود به دنیای جدید در چند ساله اخیر، انباره‌ای عظیم از داده‌ها و تعداد بیشمار ارتباطات باعث شده مسایل امنیتی جدیدی علاوه برخطرات امنیتی معمول که تاکنون برای سیستم‌های رایانه‌ای مترتب بود، پدیدار شود. در نتیجه مسئولان امنیت اطلاعات سازمان‌ها، نهادها، شرکتها حتی کشورها برآن شده‌اند تا با استفاده از روش‌هایی چند و پیروی از استانداردهایی که در این حوزه ابداع شده است، ریسک مترتب برخود و سازمان خود را کاهش دهند. در این بین، ظهور و اختراع فناوری‌های نوین و روش‌های مدیریتی، کمک شایانی در پیاده‌سازی کنترل های امنیتی نموده است. اما با در نظر گرفتن خیل عظیم کنترل‌های امنیتیِ که در حوزه‌های مدیریتی، اجرایی و فنی بکار گرفته شده‌اند -که بعضاً بسیارگران قیمت هستند - دیده شده است که حملات چندی قابل شناسایی نبوده یا درصورت رخداد حادثه، مدیریت بحران، پاسخ به حادثه و پیگرد جرایم رایانه‌ای با مشکلات متعددی روبرو شده است. در این بین می‌توان از خطرات امنیتی Flame و Stuxnet که همگان آگاهند، نام برد. برای فایق آمدن به موارد فوق پیاده‌سازی مراکز عملیات امنیت یا همان SOCها در دستور کار قرار گرفته است. در بسیاری از کشورهای جهان این مراکز جزء موارد قانونی هستند که در بازرسی‌های تطابق با قوانین مورد کنترل و بازرسی قرار گرفته می‌شوند.

در ایران نیز بنا بر توصیه نهادها و ارگان‌های بالادستی و حاکمیتی، پیاده‌سازی این مراکز در برخی سازمان‌ها شروع شده است، لیکن بنا بر پیچیدگی پیاده‌سازی این مراکز، پروژهای مربوطه – به معنای واقعی کلمه - یا موفقیت نداشته‌اند یا به تمام اهداف از پیش تعیین شده نرسیده اند. هدف از پیاده‌سازی SOC تهیه و تنظیم یک یا چند نرم افزار نمی‌باشد - که حتی اگر آن را هم درنظر بگیریم - پروژه‌های انجام شده تا به حال به خوبی مورد اجرا قرا نگرفته‌اند.

بنا به ماهیت هر سازمان و بنا به قوانین کشوری و فرآیندها و قوانین سازمانی، استفاده از چهارچوبی از فناوری‌های بومی یا خارجی، مجاز و یا توصیه شده است. بدین ترتیب بایستی ابتدا اهداف سازمان ازپیاده‌سازی SOC مشخص گردد و در تطابق با قوانین بالادستی، از ابزارهای بومی یا خارجی برای پیاده‌سازی پروژه خود سود جوید.

www.samenea.com

شرکت ثامن ارتباط عصربه اهمیت پیاده‌سازی مراکز عملیات امنیت و نیاز فوری بازار ایران به پیاده‌سازی صحیح این دست از پروژه‌ها واقف شده است.
اجرای این پروژه‌ها بایستی بصورتی باشند که سریع، به موقع، با کیفیت لازم همراه با هزینه‌های معقول و کنترل شده باشند. این شرکت سعی دارد در این صنعت با استفاده از فناوری‌های نوین و با بهره‌گیری از بهینه روشها در پروژه‌های امنیت اطلاعات و کارشناسان خبره و دارای مدارک بین‌المللی نظیر CISSP، پروژه‌های مراکز عملیات امنیت را به نحو مطلوب و به طور کامل مدیریت و اجرا نماید. در این راستا از الگوهای اثبات شده فنی و مدیریتی در حوزه‌های آنالیز ریسک و مدیریت پروژه چون PMBOK، همچنین طراحی زیرساخت‌های مورد نیاز امنیتی بر اساس بهینه روش‌های جهانی، بهره‌گیری می کند تا از اشکالات فعلی در روش‌های انجام پروژه‌هایی از این قبیل جلوگیری کند.

پیاده‌سازی امنیت اطلاعات عنصرهای بسیاری را از لحاظ فنی و مدیریتی می‌طلبد که SOC یکی از مهمترین آنها است. موردی که بایستی به آن توجه داشت آن است که اصلاح زیرساخت امنیت شبکه و امنیت سیستمی، فرآیندهای مرتبط، چارت سازمانی و نظایر آن لازمه پیاده‌سازی جامع SOC است در غیر اینصورت SOC شما نمی‌تواند بصورت کارا عمل نماید.
شرکت ثامن ارتباط عصر با توجه به سابقه‌ای که در پیاده‌سازی این دست از پروژه‌ها دارد می‌تواند درکلیه مراحل طراحی، تامین تجهیزات، پیاده‌سازی و نگهداری و راهبری به یاری شما بشتابد.

توانمندی شرکت ثامن ارتباط عصر

- طراحی و پیاده‌سازی کامل‌زیرساخت فیزیکی مرکزعملیات امنیت
- طراحی و پیاده‌سازی ساختار سازمانی و فرآیندهای مرکز
- طراحی و پیاده‌سازی سخت افزارها و نرم افزارهای کشف نفوذ و واکنش به حادثه
- تهیه کلیه اقلام سخت افزاری و نرم‌افزاری مورد نیاز برای راه‌اندازی SOC
- تامین و پیکربندی کامل SIEMهای مختلف با برندهای ایرانی و خارجی
- پشتیبانی فنی و نگهداری مراکز عملیات امنیت (SOC)

S.E.A

SOC Solutions Provider