مقدمه‌ای بر:

مراکز عملیات امنیت

(Security Operation Centers)

و

HP ArcSight

ترجمه و تالیف:

مهندس روزبه نوروزی

CISSP - PMP

بخش امنیت اطلاعات شرکت ثامن ارتباط عصر

NAGHOOS
PUBLICATION

سرشناسه : نوروزی، روزبه، ۱۳۵۷-
عنوان و نام پدیدآور : مقدمه‌ای بر مراکز عملیات امنیت../ ترجمه و تالیف روزبه نوروزی.
مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۴.
مشخصات ظاهری : ۱۶۰ ص.: مصور، جدول.
شابک : ۰-۷۸۹-۳۷۷-۹۶۴- ۹۷۸ بها : ۱۶۰،۰۰۰ریال
وضعیت فهرست‌نویسی : فیپا
موضوع : تکنولوژی اطلاعات – تدابیر ایمنی
موضوع : شبکه‌های کامپیوتری—تدابیر ایمنی
موضوع : کامپیوترها—کنترل دستیابی
موضوع : پایگاه‌های اطلاعاتی—امنیت
موضوع : حفاظت اطلاعات
رده‌بندی کنگره : ۱۳۹۴ ۷م۹ن/T۵۸/۵
رده‌بندی دیویی : ۳۰۳/۴۸۳
شمارهٔ کتابشناسی ملی : ۳۹۲۷۹۳۲

انتشارات ناقوس
NAGHOOS PUBLICATION

نام کتاب : مقدمه‌ای بر مراکز عملیات امنیت Security Operation Centers و HP ArcSight
ناشر : انتشارات ناقوس
تالیف : روزبه نوروزی
چاپ اول : ۱۳۹۴
تیراژ : ۲۰۰۰ جلد
چاپ و صحافی : ۱۲۸
سرپرست صفحه‌آرا : صدف پورعبدی
صفحه‌آرا : امیر کلینی
طراح جلد : مریم اصلانی
قیمت : ۱۶۰،۰۰۰ریال
شابک : ۰-۷۸۹-۳۷۷-۹۶۴- ۹۷۸
ISBN : 978-964-377-789-0

چاپ اول

S.M.S : ۳۰۰۰۴۵۲۳۲۲

مرکز پخش: انتشارات ناقوس
۱-میدان انقلاب، خیابان کارگرجنوبی، خیابان ۱۲ فروردین- بین وحیدنظری و روانمهر- بن‌بست حقیقت- پلاک ۴
تلفن و فاکس : ۶۳۴۲۵ (۲۰خط)
۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴
۳- کتابفروشی گلریزان: ضلع جنوب‌شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰

مقدمه مترجم و مولف

اهمیت امنیت اطلاعات امروزه بر کسی پوشیده نیست زیرا با ورود به دنیای جدید در چند ساله اخیر، انباره‌ای عظیم از داده‌ها و تعداد بیشمار ارتباطات باعث شده مسایل امنیتی جدیدی علاوه بر خطرات 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 کنترل‌های امنیتی نموده است.

اما با در نظر گرفتن حجم عظیم کنترل‌های امنیتی که در حوزه‌های مدیریتی، اجرایی و فنی به‌کار گرفته شده‌اند -که بعضاً بسیارگران قیمت هستند - دیده شده است که حملات چندی قابل شناسایی نبوده یا در صورت 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 از آن آگاه هستند، 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 می‌گیرند.

در ایران نیز بنا به توصیه نهادها و ارگان‌های بالادستی حاکمیتی، پیاده‌سازی این مراکز در برخی سازمانها شروع شده است لیکن بنا به پیچیدگی‌های پیاده‌سازی این مراکز و نیاز به مدیریت پروژه توانمند، پروژهای مربوطه -به معنای واقعی کلمه- یا موفقیت نداشته‌اند یا به تمام اهداف از پیش تعیین شده نرسیده‌اند. هدف از پیاده‌سازی SOC تهیه و تنظیم یک یا چند نرم‌افزار نمی‌باشد - که حتی اگر آن را هم در نظر بگیریم- پروژه‌های انجام شده تا به حال به‌خوبی مورد اجرا قرا نگرفته‌اند.

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

هدف از ترجمه و تألیف این کتاب، آشنایی خیل علاقمندان با 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. این انتقال دانش هم می‌تواند در پیاده‌سازی ArcSight و هم در الگوبرداری برای بهینه‌سازی SIEMهای ملی مورد استفاده قرار گیرد. چراکه این SIEM تستهای کنترلی بسیاری را پشت سر گذاشته و همانطور که در کتاب ملاحظه خواهید نمود در جهان حرف بسیاری برای گفتن دارد. پس می‌توان از ایده‌های آن – بادر نظرداشتن حقوق مالکیت معنوی- برای افزایش کیفیت تولیدات داخلی بهره برد. از طرف دیگر قصد ما بر این بوده است که قابلیتهای ArcSight که آنرا به یکی از قدرتمندترین SIEMهای جهان تبدیل نموده است را مرور نماییم چرا که، اجرای نادرست و ناکامل این راهکار بصورتی که تاکنون در چند پروژه در ایران انجام شده باعث شده است درک درستی از قابلیت‌ها و توانمندی ArcSight به نمایش در نیاید.

شرکت ثامن ارتباط عصر با اهمیت پیاده‌سازی مراکز عملیات امنیت و نیاز فوری بازار ایران به پیاده‌سازی صحیح این دست از پروژه‌ها واقف شده است. اجرای این پروژه‌ها بایستی به‌صورتی باشند که سریع، به‌موقع، 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، پروژه‌های مراکز عملیات امنیت را به نحو مطلوب و به‌طور 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 می‌کند تا از اشکالات فعلی در روشهای انجام پروژه‌هایی از این قبیل جلوگیری نماید.

نکته مهم در این بین آن است که SOC قرار نیست معجزه 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، فراهم آوری نیروی انسانی متخصص و نظایر آن، لازمه پیاده‌سازی جامع SOC است، در غیر اینصورت SOC شما نمی‌تواند به‌صورت کارا عمل نماید در پایان لازم می‌دانم از حمایتهای بی‌دریغ مدیر محترم امنیت

اطلاعات شرکت ثامن ارتباط عصر جناب آقای داویدیان و همیاری‌های مجدانه جناب آقای مهندس فرخ مدیرعامل محترم شرکت در جهت مدیریت درست و عالمانه پروژه‌های SOC و تهیه این کتاب و همچنین سایر دست اندرکاران و همکاران شرکت منجمله رییس دفتر مدیرعامل محترم و مدیریت محترم آموزش جناب آقای رحمانی و روابط عمومی قدردانی نمایم. ضمناً از زحمات مهندس دنیا نوروزی که زحمت نمونه خوانی و مهندس الهه دایی که مسئولیت ویرایش ادبی را برعهده داشتند تشکر می‌گردد. خواهشمند است پیشنهادات و نظرات خود را به آدرس زیر ارسال فرمایید.

Noroozi@samenea. com
روزبه نوروزی
CISSP-PMP
www.noroozi.info
مدیر پروژه‌های مراکز عملیات امنیت (SOC) شرکت ثامن ارتباط عصر
بهار ۹۴

فهرست مطالب

عنوان — صفحه