راه‌اندازی مرکز عملیات امنیت

SOC

با بودجه محدود

ترجمه: مهندس شهرام آبابایی

با مقدمه: دکتر علیرضا صالحی

عنوان و نام پدیدآور : راه‌اندازی مرکز عملیات امنیت (SOC) با بودجه محدود/نویسنده شرکت آلین والت ؛ ترجمه شهرام آبابایی ؛ زیر نظر علیرضا صالحی.
مشخصات نشر : تهران: سایبان، ۱۳۹۶.
مشخصات ظاهری : ۵۲ص.: مصور(رنگی)،جدول(رنگی)،نمودار(رنگی).
شابک : ۷-۴۲۸-۹۶۲-۶۰۰-۹۷۸: ۱۲۰۰۰۰ ریال
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی:.How to build a Security Operations Center(on a budget)
موضوع : سامانه‌های امنیتی
موضوع : Security systems
موضوع : شرکت‌های اقتصادی -- تدابیر ایمنی
موضوع : Business enterprises -- Security measures
شناسه افزوده: آبابایی، شهرام، ۱۳۵۴ - مترجم
شناسه افزوده: صالحی درجزینی، علیرضا، ۱۳۵۲ -
شناسه افزوده: شرکت آلین والت
رده بندی کنگره: ۲ر/TH۹۷۰۵
رده بندی دیویی: ۶۵۸/۴۷
شماره کتابشناسی ملی: ۴۹۵۹۵۳

این کتاب ترجمه‌ای است از: How to build a Security Operations Center
نویسنده: شرکت آلین والت
ترجمه: شهرام آبابایی
زیر نظر: علیرضا صالحی طراحی، صفحه آرایی و نظارت چاپ: هلدینگ رسانه‌ای دیده‌بان
ناشر: سایبان چاپ: یسنا صحافی: شمیم شمارگان: ۵۰۰ نسخه
چاپ اول - آذر ۱۳۹۶
شابک : ۷-۴۲۸-۹۶۲-۶۰۰-۹۷۸
نشانی: تهران - خیابان سهروردی شمالی - کوچه حاج حسنی - شماره ۵۵ - طبقه اول
تلفن: ۸۸۷۴۹۴۱۰ فکس: ۸۸۷۴۹۴۱۵
www.sayebaan.ir
فروش آنلاین: wwww.mrcenter.ir

قیمت: ۱۲۰۰۰۰ ریال

فصل اول:

افراد

گروه مرکز عملیات امنیت: باید وظایف و مسئولیت‌های کلیدی عملیات امنیتی مرکز برای ایجاد گروه بررسی شود. باید یادگیری مهارت‌ها و توانایی‌ها برای استخدام و تأمین کارکنان برای داشتن یک گروه عملیات امنیتی تهیه شود.

فصل دوم:

فرایندها

باید فرایندهای کلیدی موردنیاز ایجاد یک مرکز را ایجاد کرد. این فرایندها شامل رده‌بندی و تریاژ اولویت‌بندی و تحلیل، اصلاح و بررسی نیز ارزیابی و ممیزی است.

فصل سوم:

ابزار

بررسی ابزار ضروری نظارت امنیتی برای ایجاد مرکز که شامل استخراج دارایی‌ها، ارزیابی آسیب‌پذیری، شناسایی نفوذ، نظارت‌های رفتاری و SIEM و یا تحلیل امنیتی و شناسایی و معرفی فواید ملموس محکم‌سازی ابزار از طریق یک پلتفرم یکپارچه است، باید انجام گیرد.

فصل چهارم:

هوش

درک تفاوت میان تکنیک، استراتژی و هوش عملیاتی و روش‌های خاص مورداستفاده در این مراکز الزامی است. تهدات ترکیب جمع‌سپاری اطلاعات تهدید نیز باید موردبررسی قرار گیرد.

فصل پنجم:

دنیای واقعی

برای ایجاد مرکز در دنیای واقعی لازم است متدولوژی استفاده از فناوری ارتباطات و هوش تهدیدی موردنظر قرار گیرد.

پیش گفتار

علیرضا صالحی

مرکز عملیات امنیت یکی از مهم‌ترین و درعین‌حال شاید مظلوم‌ترین قسمت‌های چرخه تأمین امنیت است. این بخش از حفاظت، نظارت و تأمین امنیت این‌قدر مهم و جذاب هست که همه سازمان‌ها به‌نوعی درگیر پیاده‌سازی یا تلاش برای پیاده‌سازی آن هستند. به همین نحو، شرکت‌های بسیاری در کار تأمین این زیرساخت، سامانه یا [illegible] که خود از این نام برداشت می‌کنند هستند.

[illegible] به مصداق اشاره مولانا که می‌فرماید «هرکسی از ظن خود شد یار من»، هرکسی تعبیر و تفسیری از SOC دارد و طبیعی است که حاصل این تعریف‌های ناهمگون، ایجاد آشفتگی و ناهماهنگی در تأمین این بخش حیاتی از زنجیره تأمین امنیت [illegible] کشور.

خوشبختانه کتاب حاضر با بیانی ساده، موجز و با توجه به محدودیت بودجه‌ای که عملاً سازمان‌ها مبتلا به آن هستند، موضوع پیاده‌سازی مرکز عملیات امنیت را بیان کرده است. بی‌شک این کتاب مدعای آن را ندارد که همه نکات و ریزه‌کاری‌های راه‌اندازی چنین مرکزی را تبیین کرده، اما می‌تواند مرجع بسیار خوبی باشد برای همسان کردن ادبیات این موضوع در کشور و راهبری تصمیم گیران و تصمیم سازان حوزه امنیت فناوری اطلاعات کشور تا با تصویر و تصوری صحیح به این مقوله بنگرند.

نکته مهم دیگر این کتاب آ است که توسط یکی از [illegible] باسابقه فناوری اطلاعات و امنیت ترجمه‌شده که خود سال‌ها دستی بر آتشی داشته و با زیروبم‌ها و محدودیت‌های سازمان‌ها آشنا بوده است.

مطالعه این کتاب می‌تواند برای همه مدیران و کارشناسان افتای کشور مفید باشد.