۱۷۱۰۸۸۲

پیاده‌سازی مرکز عملیات امنیت
با استفاده از رویکردهای برتر SIEM

مولف:
مهندس علی نایب پور
مهندس تورج رهنما

www.ketab.ir

سر شناسه	: نایب پور،علی،۱۳۶۵
عنوان و نام پدیدآور	: پیاده سازی مرکز عملیات امنیت با استفاده از رویکرد های برترSIEM مولف/علی نایب پور،تورج رهنما
مشخصات نشر	: تهران: ناقوس،۱۳۹۷
مشخصات ظاهری	: ۲۰۲ص
شابک	:978-600-473-113-3
وضعیت فهرست نویسی	: فیپا
یادداشت	: سامانه های امنیتی
موضوع	: Security systems
موضوع	: شبکه های کامپیوتری—تدابیر ایمنی
موضوع	: Computer networks—Security measures
وضوع	: حفاظت داده ها
موضوع	: Data protection
موضوع	: پایگاه اطلاعاتی—امنیت
موضوع	: Data base security
موضوع	: سیستم های روی تراشه
موضوع	: Systems on a chip
شناسه افزوده	: رهنما،تورج،۱۳۵۷-
رده بندی کنگره	: TH۹۷۰۵/ ن ۲ پ ۹ ۱۳۹۷
رده بندی دیویی	: ۶۵۸/۴۷۳
شماره کتابشناسی ملی	: ۵۱۳۶۰۸۵

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoospress.ir

انتشارات ناقوس

NAGHOOS PUBLICATION

نام کتاب	: پیاده سازی مرکز عملیات امنیتی با استفاده از رویکردهای برتر SIEM
ناشر	: انتشارات ناقوس
مولفین	: علی نایب پور, تورج رهنما
چاپ اول	: ۱۳۹۷
تیراژ	: ۱۰۰
چاپ و صحافی	: نارنجستان
صفحه آرا	: ثریا صفرزاده
قیمت	: ۱۹۰۰۰۰ریال
شابک	: ۹۷۸ -۶۰۰-۴۷۳-۱۱۳-۳
ISBN	: 978-600-473- 113-3

S.M.S : ۳۰۰۰۴۵۲۳۲۳

کلیه حقوق برای ناشر محفوظ است. تکثیر تمام یا قسمتی از این اثر به صورت الکترونیکی یا چاپ مجدد، چاپ افست، پلی‌کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

مرکز پخش: انتشارات ناقوس

۱-خیابان بلوار کشاورز-خیابان ۱۶آذر-کوچه پارسی-پلاک ۱۰

تلفاکس-۶۶۴۷۸۹۵۷-۶۶۴۷۸۹۵۸

کتابفروشی الیاس :انقلاب نبش فروردین-تلفن۶۶۴۶۶۳۴۴

کتابفروشی گلریزان:میدان انقلاب تلفن ۶۶۹۷۶۲۳۲-۶۶۹۷۶۲۳۱

www.ketab.ir

فهرست مطالب

پیشگفتار..... ۱۳

فصل اول: مفاهیم مقدماتی امنیت

۱,۱. مقدمه..... ۱۵

۱,۲. تعاریف عملیاتی امنیت اطلاعات..... ۲۰

۱,۳. انواع حملات سایبری..... ۳۱

۱,٤نشانه‌های حملات سایبری..... ۳۵

فصل دوم: مرکز عملیات امنیت

۲,۱. مقدمه..... ۱٤

۲,۲. سرویس‌ها، مؤلفه‌ها و فرآیندهای مرکز عملیات امنیت..... ٤٤

۲,۳. ساختار سازمانی..... ۵۵

۲,٤. معماری مرکز عملیات امنیت..... ۵۹

۲,۵. طراحی و پیاده‌سازی مرکز عملیات امنیت..... ٦۲

۲,٦. مانیتورینگ چند لایه..... ٦۷

فصل سوم: سیستم مدیریت رخداد و اطلاعات امنیتی

۳,۱. مقدمه..... ۷۱

۳,۲. اهداف و دامنه اجرا از استقرار SIEM..... ۷۵

۳,۳. معماری SIEM..... ۸۲

۳,٤. مشکلات راه‌اندازی SIEM..... ۸۸

فصل چهارم: بررسی رویکردهای برتر SIEM

٤,۱. مقدمه..... ۱۰۵

www.ketab.ir

۲,٤. مقایسه رویکردهای SIEM از ۲۰۱۵ الی ۲۰۱۷.....۱۰٦
۳,٤. آشنایی با رویکردهای برتر SIEM.....۱۱۳

فصل پنجم: قواعد پیاده‌سازی واحد امنیت اطلاعات

۱,٥. مقدمه.....۱۵۹
۲,٥. اهداف و مأموریت‌ها.....۱٦٤
۳,٥. مراحل پیاده‌سازی واحد امنیت اطلاعات.....۱۸۱
٤,٥. آموزش و تامین پرسنل واحد امنیت اطلاعات.....۱۸۸

www.ketab.ir

پیش گفتار

امروزه داده‌های بسیار ارزشمندی توسط زیرساخت‌های اطلاعاتی سازمان‌های دولتی، شرکت‌های خصوصی و همچنین مراکز عمومی میزبانی می‌شود. علاوه براین، بسیاری از مراکز داده خدماتی را به مشتریان و کاربرهای خود ارائه می‌کنند که توقف هرچند کوتاه مدت ارائه خدمات، خسارت سنگینی مالی و اعتباری به همراه دارد. این خسارات می‌تواند شامل از دست‌دادن داده‌های ارزشمند، مشتریان و اعتبار سازمان باشد. لذا با رشد روز افزون تهدیدهای امنیتی، اهمیت توجه به امنیت زیرساخت‌های اطلاعاتی بیشتر نمایان می‌شود. بنابراین در سال‌های اخیر راهکارهای امنیتی متعددی مورد توجه سازندگان، تولیدکنندگان، اپراتورهای شبکه و مدیرهای سازمان‌ها، مراکز داده، شرکت‌های ارائه‌دهنده خدمات پرداخت، بانک‌ها و همچنین محقق‌های مراکز تحقیقاتی قرار گرفته است. آنچه در این میان قابل توجه است، این نکته می‌باشد که اگرچه بکارگیری راهکارهای حفاظتی در پیشگیری از برخی حملات و تهدیدهای امنیتی مؤثر است، ولی به تنهایی تامین‌کننده امنیت نخواهد بود. راهکاری که اخیراً مورد توجه قرار گرفته است، پیاده‌سازی مرکز عملیات امنیت است.

ایجاد مرکز عملیات امنیت یا «SOC» به منظور تحلیل و پایش مستمر تهدیدات و مقابله با حملات سایبری در کنار مرکز عملیات شبکه یا «NOC» و نیز تیم واکنش اضطراری رخدادهای کامپیوتری یا «CERT» جهت پاسخ-گویی بلادرنگ به حملات و رخدادهای امنیتی می‌تواند دامنه سرویس‌های کسب‌وکار و افزایش سطح امنیت و در دسترس‌پذیری سامانه‌های حیاتی سازمان‌ها و شرکت‌ها را تضمین کند. لذا هدف اصلی ایجاد مرکز عملیات امنیت، محافظت از اصلی‌ترین دارایی‌های غیر فیزیکی یک سازمان یعنی اطلاعات و داده‌های حساس است.

طراحی و پیاده‌سازی مرکز عملیات امنیت برای سازمان‌هایی که تا کنون به صورت جامع به پیاده‌سازی آن فکر نکردند، کاری بسیار دشوار است اما نکته قابل توجه این است که می‌توان با یک برنامه راه مناسب، جهت دستیابی به این هدف گام‌های مؤثری را طی کرد. هدف اصلی از نقشه راه برای ایجاد مرکز عملیات امنیت، طرح‌ریزی و اجرای مرحله به مرحله فازهای عملیاتی، بر اساس تحلیل شکاف موجود بین وضعیت کنونی و وضعیت دلخواه و نیز الویت‌بندی فازهای مورد نیاز جهت حصول وضعیت مطلوب با در نظر گرفتن زمان، هزینه و اهداف مورد نظر است. بدیهی است این فازها در صورت برنامه‌ریزی مناسب شامل صرف هزینه‌های بالا نمی‌شود و سازمان بر اساس تحلیل میزان بودجه، پرسنل عملیاتی کارآمد، محدودیت‌های سازمانی و نیز تکنولوژی‌ها و فرآیندهای مورد نیاز به یک مرکز عملیات امنیت کارا دست پیدا کند.

سیستم مدیریت امنیت اطلاعات و وقایع یا «SIEM» فن‌آوری جدیدی است که می‌تواند تمام زیرساخت‌های حساس را به هم متصل کند و یک دیدگاه جامع از امنیت اطلاعات ارائه دهد. امنیت فناوری اطلاعات معمولاً از چند فن‌آوری مختلف مانند فایروال‌ها، سیستم‌های پیشگیری از نفوذ، حفاظت از پایانه‌ها و غیره تشکیل شده است که برای حفاظت از شبکه و داده‌های حساس سازمان از هکرها و سایر تهدیدات همکاری می‌کنند. با این وجود

www.ketab.ir

اتصال همه این سیستم‌های متفرقه چالشی دیگر است و SIEM می‌تواند در این زمینه کمک کند. سیستم SIEM مدیریت و تشخیص ورودی‌های امنیتی را از انواع دستگاه‌ها انجام می‌دهد و از طیف وسیعی از توابع، از جمله تهدیدهای پنهان، از رخدادها قبل از وقوع آنها، شناسایی رخدادهای امنیتی و ارائه اطلاعات قانونی برای تعیین وقوع یک حادثه و همچنین تاثیر احتمالی، جلوگیری می‌کند. از سویی همین‌طور نیاز به ایجاد و بکارگیری مراکز عملیات امنیت، بکارگیری سامانه‌های SIEM را کاملاً توجیه‌پذیر می‌کند.

در این پژوهش ابتدا به بیان مفاهیم مقدماتی و تعاریف پایه امنیت، انواع و نشانه‌های حملات سایبری می‌پردازیم. همچنین در ادامه به بررسی جزئیات مرکز عملیات امنیت هم‌چون سرویس‌ها، مؤلفه و فرآیندهای مورد نیاز، ساختار سازمانی، معماری و روش‌های طراحی و پیاده‌سازی می‌پردازیم و در خصوص رویکرد مانیتورینگ چند لایه بحث می‌کنیم. در ادامه ضمن بررسی SIEM، اهداف و دامنه اجرا، معماری و در نهایت مشکلات راه‌اندازی و پیاده‌سازی SIEM را بررسی می‌کنیم و ضمن بحث در خصوص مرکز پژوهش گارتنر، گزارش گارتنر در سال ۲۰۱۷ و ۲۰۱۸ در خصوص رویکردها برتر SIEM را بررسی می‌کنیم. در نهایت ضمن بیان اصول و قواعد راه‌اندازی واحد امنیت به عنوان متولی مرکز عملیات امنیت، ابتدا حالات سازمانی واحد امنیت، اهداف و ماموریت-ها، مراحل پیاده‌سازی و در نهایت بحث آموزش و تامین پرسنل واحد امنیت مورد بررسی قرار می‌گیرد.

لازم به ذکر است در تدوین این کتاب تلاش شده است که علاوه بر ارائه مطالب کاربردی و قابل فهم برای عموم علاقه‌مندان به حوزه امنیت، تجربیات کاربردی شخصی نیز به بهترین شکل ارائه شود. لازم به ذکر است که نظرات و پیشنهادات خوانندگان عزیز می‌تواند بر افزایش کیفیت کار ما موثر باشد، لذا برای ارتباط و بیان نظرات و پیشنهادات می‌توانید از آدرس ایمیل [illegible]pr@yahoo.com استفاده نمایید.

مهندس علی نایب‌پور

مهندس تورج رهنما

www.ketab.ir