بسم الله الرحمن الرحیم

مدیریت رخدادها و اطلاعات امنیتی(SIEM)

تهیه و تألیف: نداعلینژاد، آلاله ارجمند

تهران،۱۳۹۷

سرشناسه : علینژاد، ندا، ۱۳۶۸ -
عنوان و نام پدیدآور : مدیریت رخدادها و اطلاعات امنیتی (SIEM)/ تهیه و تالیف نداعلینژاد، آلاله ارجمند.
مشخصات نشر : تهران: آلاله ارجمند، ۱۳۹۷.
مشخصات ظاهری : ۱۴۳ ص.: مصور (رنگی)، جدول، نمودار (رنگی).
شابک : 978-622-00-1828-5
وضعیت فهرست نویسی : فیپا
یادداشت : کتابنامه: ص. ۱۴۲ - ۱۴۳.
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع : Computer networks -- Security measures
موضوع : کامپیوترها -- ایمنی اطلاعات
موضوع : Computer securi
موضوع : کامپیوترها -- کنترل دسترسی
موضوع : Computers -- Access co
شناسه افزوده : رجمند، آلاله، ۱۳۶۳-
رده بندی کنگره : TK۵۱۰۵
رده بندی دیویی : ۰۰۵
شماره کتابشناسی ملی : ۰۰۸۵

تاریخ درخواست : ۱۳۹۷/۰۹/۱۱
تاریخ پاسخگویی :
کد پیگیری : 5468502

عنوان: مدیریت رخدادهاواطلاعات امنیتی(SIEM)

نویسنده: نداعلینژاد،آلاله ارجمند

ناشرمولف

شابک:۵-۱۸۲۸-۰۰-۶۲۲-۹۷۸

تاریخ انتشار:۱۳۹۷

نوبت چاپ: اول

تیراژ: ۱۰۰۰

چاپ: دانشگاه

مقدمه

مباحث مرتبط با امنیت عمری به اندازه پیدایش مفهوم ارتباطات و فناوری اطلاعات دارند. سال‌هاست که مدیران شبکه و امنیت به دنبال ایجاد سازوکارهای تامین امنیت شبکه و مقابله با تهدیدات امنیتی هستند. از سویی انتشار ویروس‌های مخربی چون Stuxnet و Flame ثابت کرد که هنوز راه درازی در حصول اطمینان به روشهای امن سازی موجود در کشور وجود دارد. آنچه مسلم است بکارگیری انواع فایروال ها، آنتی ویروس ها و تجهیزات امنیتی گوناگون به تنهایی نمی‌تواند پاسخی بر نیاز امنیتی سازمان‌ها و شبکه‌ها باشد. یکی از قطعات بسیار مهم این پازل، بحث مدیریت رخدادها و تهدیدات قابل کشف از رخدادهای ایجاد شده توسط تجهیزات، کاربران و ترافیک موجود در شبکه است.

سامانه‌های "مدیریت رخدادها و اطلاعات امنیتی" که به اختصار به SIEM معروف هستند از مهمترین ابزارهای مدیریت امنیت در سازمان‌ها محسوب می‌گردند. کتاب پیش روحاصل تحقیق در مورد تکنولوژی SIEM می باشد. و به ضرورت های آن در شناسایی برخی تهدیدات مخفیانه اشاره می کندوراه هایی برای مقابله با این ضرورت ها و توسعه ی این تکنولوژی ارائه می دهد.

بی شک هیچ کتابی خالی از اشکال نیست و ما مشتاقانه منتظر دریافت انتقادات ونظرات و پیشنهادات همکاران، دانشجویان و خوانندگان محترم می باشیم.

بااحترام

نداعلینژاد،آلاله ارجمند

Alaleh.arjmad@yahoo.com

فهرست مطالب