

بسم الله الرحمن الرحيم

مدیریت رخدادهای و اطلاعات امنیتی (SIEM)

تهیه و تألیف: نداعلینژاد، آلاله ارجمند

تهران، ۱۳۹۷



سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران

سرشناسه	: علینژاد، نداء، ۱۳۶۸ -
عنوان و نام پدیدآور	: مدیریت رخدادها و اطلاعات امنیتی (SIEM) / تهیه و تألیف نداعلینژاد، آلاله ارجمند.
مشخصات نشر	: تهران: آلاله ارجمند، ۱۳۹۷.
مشخصات ظاهری	: م، ۱۴۳ ص.؛ محور (رنگی)، جدول، نمودار (رنگی).
شابک	: 978-622-00-1828-5
وضعیت فهرست نویسی	: فیا
یادداشت	: کتابنامه: ص، ۱۴۲ - ۱۴۳.
موضوع	: شبکه های کامپیوتری -- تدابیر امنیتی
موضوع	: Computer networks -- Security measures
موضوع	: کامپیوترها -- امنیتی اطلاعات
موضوع	: Computer security
موضوع	: کامپیوترها -- کنترل دسترسی
موضوع	: Computers -- Access control
شماسه افزوده	: ارجمند، آلاله، ۱۳۶۲ -
رده بندی کنگره	: TK5۱۰۵۰۹۰۸۵۳ ۱۳۹۷
رده بندی دیویی	: ۰۰۰۰۰
شماره کتابشناسی ملی	: ۰۰۰۰۰۰۵

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

عنوان: مدیریت رخدادها و اطلاعات امنیتی (SIEM)

نویسنده: نداعلینژاد، آلاله ارجمند

ناشر مولف

شابک: ۹۷۸-۶۲۲-۰۰-۱۸۲۸-۵

تاریخ انتشار: ۱۳۹۷

نوبت چاپ: اول

تیراژ: ۱۰۰۰

چاپ: دانشگاه

حق چاپ محفوظ

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 بازل، 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 رو حاصل تحقیق در مورد تکنولوژی SIEM می‌باشد. و به ضمیمه‌ای آن در شناسایی برخی تهدیدات مخفیانه اشاره می‌کند و راه‌هایی برای مقابله با این ضلوع ما و توسعه‌ی این تکنولوژی ارائه می‌دهد.

بی‌شک هیچ کتابی خالی از اشکال نیست و ما مشتاقانه منتظر دریافت انتقادات و نظرات و پیشنهادات همکاران، دانشجویان و خوانندگان محترم می‌باشیم.

با احترام

ندا علی‌نژاد، آلاله ارجمند

Alaleh.arjmad@yahoo.com

فهرست مطالب

۱	فصل ۱. مقدمه
۱	۱-۱. مقدمه
۴	۲-۱. تعریف مساله و سئوالات اصلی تحقیق
۴	۳-۱. فرضیه‌ها
۴	۴-۱. اهداف تحقیق
۵	۵-۱. مراحل انجام تحقیق
۷	فصل ۲. مروری بر SIEM
۷	۱-۲. تعریف SIEM
۱۰	۲-۲. ویژگی‌های SIEM
۱۳	2-3. فواید SIEM
۱۴	2-4. نقاط ضعف SIEM
۱۵	۵-۲. معماری SIEM
۱۸	۶-۲. پیاده سازی SIEM
۱۹	۱-۶-۲. راه کارهای پیاده سازی SIEM
۲۰	۷-۲. نحوه ی بکارگیری SIEM
۲۴	۸-۲. توانمندی های SIEM
۲۶	۹-۲. مقایسه رهیافت‌های مدیریت فرآیندهای امنیت اطلاعات همراه با SIEM و بدون آن
۲۸	۱۰-۲. اجتناب از مشکلات SIEM

۲۹	۱۱-۲. مسائل و مشکلات احتمالی بعد از راه اندازی SIEM و راه حل آنها
۳۶	۱۲-۲. ضرورت استفاده از SIEM
۴۰	۱۳-۲. بازار SIEM
۴۱	۱۴-۲. تعریف/توصیف بازار
۴۳	۱۵-۲. نقاط قوت و ضعف فروشندگان
۴۳	۱-۱۵-۲. AlienVault
۴۵	۲-۱۵-۲. EiQ Networks
۴۶	۳-۱۵-۲. EMC-RSA
۴۹	۴-۱۵-۲. EventTracker
۵۱	۵-۱۵-۲. HP-ArcSight
۵۳	۶-۱۵-۲. IBM-Q1 Labs
۵۵	۷-۱۵-۲. LogRhythm
۵۷	۸-۱۵-۲. McAfee
۵۹	۹-۱۵-۲. McAfee
۶۱	۱۰-۱۵-۲. Sensag
۶۳	۱۱-۱۵-۲. SolarWinds
۶۵	۱۲-۱۵-۲. Symantec
۶۷	۱۳-۱۵-۲. Tenable Network Security
۶۹	۱۶-۲. بقا و حذف فروشندگان SIEM در بازار
۷۱	۱۷-۲. معیارهای ورود و خروج
۷۲	۱-۱۷-۲. معیارهای ارزیابی
	۱۸-۲. نیازمندیها مشتری - نظارت بر امنیت و انطباق گزارش برای سیستم های، کاربران،
۷۸	اطلاعات و نرم افزار
۷۹	۱۹-۲. مقیاس پذیری
۸۰	۲۰-۲. سرویسهای SIEM

فصل ۳. تهدیدات پیشرفته و مستمر ۸۳

۸۳	۱-۳	حملات مبتنی بر تهدید پیشرفته و مستمر و روشهای مقابله با آن
۸۴	۱-۱-۳	تهدید پیشرفته سمج
۹۰	۲-۳	استاکس نت
۹۰	۱-۲-۳	مقدمه
۹۰	۲-۲-۳	استاکس نت
۹۱	۳-۲-۳	نامگذاری
۹۲	۴-۳	سیستم های آسیب پذیر
۹۲	۵-۲-۳	انتشار
۹۵	۶-۲-۳	کش های آسیب دیده
۹۷	۷-۲-۳	حجوه نفوذ و بروس "استاکس نت" در نظنز
۹۸	۸-۲-۳	استاکس نت در کمین رایانه های شخصی
۹۹	۹-۲-۳	توصیه ای از رمار اتصال به اینترنت
۱۰۰	۱۰-۲-۳	اسرار صنعتی
۱۰۲	۱۱-۲-۳	ویروس شناسی
۱۰۴	۱۲-۲-۳	طراحی و سازماندهی
۱۰۵	۱۳-۲-۳	عملکرد
۱۰۶	۱۴-۲-۳	نصب
۱۰۸	۱۵-۲-۳	تغییرات در سیستم
۱۱۴	۱۶-۲-۳	طریقه انتشار
۱۱۶	۱۷-۲-۳	هدف
۱۱۸	۱۸-۲-۳	پیشگیری و پاکسازی
۱۲۲	۱۹-۲-۳	نتیجه گیری

فصل ۴. نتیجه گیری و پیشنهادات ۱۲۵

۱۲۵	۱-۴	مقدمه
۱۲۶	۲-۴	مروری کوتاه بر تکنولوژی SIEM از گذشته تا به امروز

- ۳-۴. روندهای عملیاتی SIEM ۱۲۸
- ۴-۴. SIEM Use case ۱۲۹
- ۵-۴. راه اندازی و توسعه ی موفق SIEM ۱۳۱
- ۶-۴. چند توصیه در مورد استفاده از SIEM ۱۳۴
- ۷-۴. بررسی ضعفهای تکنولوژی SIEM برای شناسایی APT ها و ارایه راهکار ۱۳۶

منابع و مآخذ

۱۴۲

www.ketab.ir