

۱۵۷۰۷۷۷
مقدمه‌ای بر:

مراکز عملیات امنیت (Security Operation Centers)

۹ HP ArcSight

ترجمه و تالیف:

مهندس روزبه نوروزی

CISSP - PMP

بخش امنیت اطلاعات شرکت ثامن ارتباط عصر



NAGHOOS
PUBLICATION

سرشناسه : نوروژی، روزبه، ۱۳۵۷-
 عنوان و نام پدیدآور : مقدمه‌ای بر مراکز عملیات امنیت./ ترجمه و تالیف روزبه نوروژی.
 مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۴.
 مشخصات ظاهری : ۱۶۰ ص.: مصور، جدول.
 شابک : ۹۷۸-۹۶۴-۳۷۷-۷۸۹-۰ : بها : ۱۶۰,۰۰۰ ریال
 وضعیت فهرست‌نویسی : فیبا
 موضوع : تکنولوژی اطلاعات - تدابیر ایمنی
 موضوع : شبکه‌های کامپیوتری - تدابیر ایمنی
 موضوع : کامپیوترها - کنترل دستیابی
 موضوع : پایگاه‌های اطلاعاتی - امنیت
 مؤثر رع : حفاظت اطلاعات
 رده‌بندی کنگره : ۳۹۴ م۷/۵ ن/۵۸/۵
 رده‌بندی دیویی : ۳۰۳/۴۸۳
 شماره کتابشناسی ملی : ۳۹۲۷۹۳۲



**NAGHOOS
PUBLICATION**

این کتاب Online به آدرس زیر مراجعه کنید:

www.naghoospress.ir

انتشارات ناقوس

مقدمه‌ای بر مراکز عملیات امنیت HP ArcSight و Security Operation Centers :

چاپ اول

S.M.S : ۳۰۰۰۴۵۲۳۲۲

کلیه حقوق این سرمایه‌گذار محفوظ
 است. تکثیر تمامی یا قسمتی از این اثر
 به‌صورت حروفچینی یا چاپ مجدد،
 چاپ افست، پلی‌کپی، فتوکپی و انواع
 دیگر چاپ ممنوع است و پیگرد قانونی
 دارد.

نام کتاب :
 ناشر : انتشارات ناقوس
 تالیف : روزبه نوروژی
 چاپ اول : ۱۳۹۴
 تیراژ : ۲۰۰۰ جلد
 چاپ و صحافی : ۱۲۸
 سرپرست صفحه‌آرا : صدف پورعبدی
 صفحه‌آرا : امیر کلینی
 طراح جلد : مریم اصلانی
 قیمت : ۱۶۰,۰۰۰ ریال
 شابک : ۹۷۸-۹۶۴-۳۷۷-۷۸۹-۰
 ISBN : 978-964-377-789-0

مرکز پخش: انتشارات ناقوس

۱- میدان انقلاب، خیابان کارگر جنوبی، خیابان ۱۲ فروردین - بین وحیدنظری و روانمهر - بن‌بست حقیقت - پلاک ۴

تلفن و فاکس: ۶۳۳۲۵ (۲۰ خط)

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 بر خود 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 خیل عظیم کنترل‌های امنیتی که در حوزه‌های مدیریتی، اجرایی و فنی به کار گرفته شده‌اند - که بعضاً سیارگران 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 فائق آمدن به موارد فوق پیاده‌سازی مراکز عملیات امنیت یا همان SOA ها 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 و حمایتی، پیاده‌سازی این مراکز در برخی سازمانها شروع شده است لیکن بنا به پیچیدگی پیاده‌سازی این مراکز و نیاز به مدیریت پروژه توانمند، پروژه‌های 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 به خوبی مورد اجرا قرار 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 نظر داشتن 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 ر 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 داده و مدیریت پروژه چون PMBOK، همچنین طراحی زیرساخت‌های مورد نیاز امنیتی را در 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 آنهاست. 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 به- صورت 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

بخش اول: اصول و مبانی مراکز عملیات امنیت	۱۵
۱- اهمیت و ضرورت مرکز عملیات امنیت	۱۸
۲- مدیریت مؤثر رخدادها	۲۰
۳- پایش و واکنش سریع به وقایع امنیتی	۲۰
۴- مدیریت مؤثر وصله‌های امنیتی و به‌روزرسانی نرم‌افزارها	۲۱
۵- تحلیل مخاطرات و پیگرد جرم	۲۱
بخش دوم: نکاتی در طراحی و پیاده‌سازی پروژه‌های مراکز عملیات امنیت	۲۳
۱- فاز صفر: تعریف پروژه	۲۵
۲- فاز اول: شناخت	۲۶
۳- فاز دوم: طراحی مرکز عملیات امنیت	۲۶
۴- فاز سوم: خرید و تأمین تجهیزات بر اساس خریدی فاز دوم	۲۷
۵- فاز چهارم: پیاده‌سازی و اجرای مرکز عملیات امنیت	۲۸
۶- فاز پنجم: تهیه مستندات	۲۹
۷- فاز ششم: آموزش	۲۹
۸- فاز هفتم: انتقال	۳۱
۹- فاز هشتم: پشتیبانی سیستم	۳۱
نکته آخر این فصل، انتخاب SIEM	۳۲
بخش سوم: بررسی مقدماتی HP ArcSight	۳۳
۱- فصل اول: ArcSight ESM چیست؟	۳۵
۲- نقش‌ها و مسئولیت‌ها	۳۷
۳- کاربر تجاری	۳۸
۴- فصل دوم: ساختار و معماری ArcSight	۴۱
۵- برخی اصطلاحات پایه‌ای در ArcSight	۴۲
۶- اجزای ArcSight	۴۳
۷- SmartConnector ها	۴۴
۸- دستگاه سخت‌افزاری Connector ها	۴۵
۹- توانمندی‌های دستگاه Connector	۴۵
۱۰- Flex Connector	۴۷
۱۱- Forwarding Connector	۴۸
۱۲- HP Reputation Security Monitor Solution	۴۸
۱۳- RepSM چگونه کار می‌کند؟	۴۸

۴۸	ArcSight Manager
۴۹	ذخیره ساز CORR-Engine
۴۹	بررسی رابط‌های کاربری ArcSight
۴۹	۱. کنسول ArcSight
۴۹	۲. کنسول Manager
۴۹	ArcSight Interactive Discovery (AID)
۵۰	Pattern Discovery
۵۰	فوائد Pattern Discovery
۵۱	Logger
۵۱	ArcSight NCM/TRM
۵۱	توانایی‌های دستگاه NCM/TRM
۵۳	فصل سوم: چرخه حیات، جمع‌آوری داده‌ها و پردازش رویدادها در ArcSight Express
۵۴	بررسی تفصیلی نحوه جمع‌آوری داده‌ها
۵۴	نرمال‌سازی داده‌های رویدادها
۵۶	اعمال دسته‌بندی رویدادها
۵۷	ابزار دسته‌بندی رویداد
۵۸	اضافه نمودن اطلاعات Zone و مشتری
۵۹	فیلترها و رویدادهای تجمیع شده
۵۹	تنظیم SmartConnector برای تجمیع رویدادها
۶۰	انجام تنظیمات SmartConnector برای اجرای دستورات
۶۱	مدیریت تنظیمات SmartConnector ها
۶۳	فصل چهارم: برآورد اولویت و اعمال مدل شبکه‌ای
۶۳	یافتن و تخصیص مدل شبکه
۶۴	محاسبه فرمول اولویت‌بندی
۶۴	فاکتورهای اولویت‌بندی
۶۵	درجه‌بندی اولویت
۶۶	بررسی زیرساخت اولویت‌بندی
۶۹	فصل پنجم: جریان کاری
۷۱	حاشیه‌نویسی
۷۲	پرونده
۷۳	کاربران و گروه‌های کاری ArcSight
۷۴	اطلاع‌رسانی
۷۴	عملکرد اطلاع‌رسانی چگونه است؟
۷۵	پایگاه دانش
۷۶	Reference Page

۷۷.....	فصل ششم: تلفیق
۷۷.....	مرور عملیات تلفیق
۷۹.....	فیلترها
۸۰.....	استفاده از فیلترها در Active Channel
۸۰.....	دیبگ فیلتر
۸۰.....	Rule
۸۱.....	Rule ها چگونه کار می کنند؟
۸۲.....	تجمیع Rule
۸۲.....	ارزیابی Rule ها به چه شکل است؟
۸۳.....	اعمال Rule ها و زمان ها
۸۴.....	رویدادهای تلفیق شده توسط Rule ها
۸۴.....	چگونه Rule ها از Active List استفاده نمایند؟
۸۵.....	مثالی از واکنش دو Rule نسبت به یکدیگر
۸۵.....	Active List ها چگونه کار می کنند؟
۸۵.....	مثالی دیگر
۸۷.....	چگونه Rule ها از Session List استفاده می کنند؟
۸۸.....	انجام تست Rule ها در Rule Channel
۸۹.....	Data Monitor
۸۹.....	سه نوع Data Monitor وجود دارد
۹۰.....	خلاصه ای از انواع رویدادها
۹۳.....	فصل هفتم: انجام پایش، بررسی و تحقیق
۹۵.....	شرح عناصر Active Channel
۹۶.....	Rules Channel
۹۶.....	Resource Channel
۹۷.....	دشبوردها
۹۸.....	Event Graph Data Monitor
۹۹.....	استفاده از نمودار رویداد به عنوان ابزار پایش
۱۰۰.....	چگونه از گراف رویداد به عنوان ابزار تحقیق و تحلیل استفاده کنیم؟
۱۰۲.....	داشبورد نگاه به صورت دلخواه
۱۰۲.....	Query Viewer
۱۰۴.....	بررسی Query Viewer به عنوان ابزار جستجو و تحقیق و تحلیل
۱۰۵.....	دستورات تجمعی برای اجرای نتیجه یک تحلیل

۱۰۷	فصل هشتم: تحلیل یک واقعه و تهیه گزارش
۱۰۸	Query ها
۱۰۹	روند
۱۰۹	Snapshot Trend
۱۱۰	Interval Trend
۱۱۱	روندها چگونه کار می کنند؟
۱۱۲	قالب
۱۱۳	گزارش ها
۱۱۳	Data Report
۱۱۴	Focused Report
۱۱۴	Job Scheduler
۱۱۴	Scheduled Job Manager
۱۱۵	ArcSight Pattern Discovery
۱۱۵	خروجی های Pattern Discovery
۱۱۶	ArcSight Interactive Discovery (AID)
۱۱۹	فصل نهم: CORR-Engine
۱۲۰	مدت زمان نگهداری فعال
۱۲۱	آرشیو
۱۲۱	Time- and Space-Based Storage Retention
۱۲۱	مدیریت CORR-Engine
۱۲۳	فصل دهم: شیمای رویداد
۱۲۳	فیلدهای داده ای ArcSight
۱۲۴	دستگاه و دارایی در شیمای رویدادها
۱۲۴	یک دستگاه در شیمای رویداد چیست؟
۱۲۵	دارایی در شیمای چیست؟
۱۲۶	کارت شبکه دوم و شیمای رویداد
۱۲۸	Point Event
۱۲۹	فصل یازدهم: مدل شبکه و مدل Actor
۱۲۹	مدل شبکه:
۱۳۲	تعریف برخی مفاهیم:
۱۳۳	Assets\ Zone Tab
۱۳۴	Networks
۱۳۵	Customer

۱۳۷.....	روش‌های تکمیل مدل شبکه
۱۳۸.....	بررسی روش ۱- الف:
۱۳۸.....	بررسی روش ۱- ب:
۱۳۹.....	بررسی روش ۲- الف:
۱۳۹.....	بررسی روش ۲- ب:
۱۳۹.....	بررسی روش ۳:
۱۳۹.....	استفاده از منبع Graph (نمایش) برای تأیید صحت مدل تولید شده
۱۴۱.....	مدل دارایی
۱۴۵.....	Actor Model
۱۴۵.....	قابلیت Actor چگونه کار می‌کند؟
۱۴۷.....	فصل دوازدهم: مدیریت منبع Content های استاندارد
۱۴۷.....	منبع چیست؟
۱۴۸.....	Content چیست؟
۱۴۸.....	Package ها
۱۴۹.....	Package View
۱۵۰.....	File Resource
۱۵۰.....	ابزار آرشیو ArcSight
۱۵۰.....	Resource Graph
۱۵۱.....	URI چیست؟
۱۵۳.....	Resource ID
۱۵۴.....	لیست کنترل دسترسی (ACL)
۱۵۴.....	تعریف سطوح دسترسی
۱۵۵.....	Standard Content
۱۵۶.....	Standard Content Foundation
۱۵۶.....	شرح Foundation ها
۱۵۸.....	Use Case ها
۱۵۹.....	انجام تنظیم Use Case