



1 ♦

فصل اول	۱۲
آشنایی با مرکز عملیات امنیت (SOC)	۱۲
۱.۱ مقدمه	۱۲
۱.۲ آشنایی با SOC	۱۳
۱.۳ معماری SOC	۱۴
۱.۴ نتیجه‌گیری	۱۶
۱.۵ سؤالات فصل اول	۱۶
۱.۶ منابع ..	۱۶

2 ♦

فصل دوم	۱۷
فعالیت‌های مرکز عملیات امنیت (SOC FUNCTION)	۱۸
۲.۱ SIEM (Security Information and Event Management)	۱۸
۲.۲ توانمندی‌های SIEM	۱۹
۲.۳ تعامل SOC با دیگر بخش‌های شبکه	۲۰
۲.۳.۱ تعامل مرکز عملیات امنیت شبکه SOC و مسئول عملیات شبکه NOC	۲۱
۲.۳.۲ تعامل مرکز عملیات امنیت شبکه SOC و تیم پاسخگویی به فوریت‌های کامپیوتری CERT	۲۱
۲.۴ نیاز به سرویس‌های مدیریت شده	۲۲
۲.۵ انواع سرویس‌های مدیریت‌شده در SOC	۲۳
۲.۵.۱ دیوار آتش Firewall	۲۳
۲.۵.۲ سیستم‌های تشخیص حملات IDS	۲۴
۲.۵.۳ امکان فیلتر کردن محتوا	۲۵
۲.۵.۴ امکان تشخیص ویروس	۲۶
۲.۵.۵ سرویس‌های AAA	۲۶
۲.۶ پیاده‌سازی امنیت در مرکز SOC	۲۶



۲۷	Vulnerability ۲.۶.۱
۲۷	Visibility ۲.۶.۲
۲۸	Verification ۲.۶.۳
۲۸	۲.۷ سرویس‌های پیشرفته در مراکز SOC
۲۹	۲.۸ نتیجه‌گیری
۲۹	۲.۹ سؤالات فصل دوم
۳۰	۲.۱۰ منابع

3

۳۱	فصل سوم
۳۲	تعاریف رایج
۳۲	۳.۱ تعاریف رایج
۳۴	۳.۲ امنیت فناوری اطلاعات و استاندارد
۳۸	۳.۲.۱ امنیت اطلاعات
۳۹	۳.۳ اجزای راه حل ترکیبی امنیت کلان نگر
۳۹	۳.۳.۱ پایش و بررسی همه ترافیک شبکه برپایه رفتارهای نرمال
۴۱	۳.۳.۲ پایش و بررسی همه ترافیک شبکه (Each and Every Packet)
۴۱	۳.۳.۳ راهکار پویش وجود اشکال‌های امنیتی شناخته شده در شبکه (Vulnerability Assessment)
۴۳	۳.۳.۴ تشخیص نفوذ (Intrusion Detection System) و پیش‌گیری از نفوذ (Intrusion Prevention System)
۴۴	۵.۳ قرارگیری استاندارد IDS در شبکه
۴۵	۶.۳ قرارگیری استاندارد IPS در شبکه
۴۶	۳.۴ نتیجه‌گیری
۴۷	۳.۵ سؤالات فصل سوم
۴۷	۳.۶ منابع

4

۴۹	فصل چهارم
۵۰	SIEM
۵۰	۴.۱ مکانیزم گردآوری، دسته‌بندی و گزارش‌گیری (SIEM)

۴.۲	ابزارهای گردآوری و دسته بندی، ویژگی هایی مانند دو مورد زیر را فراهم خواهد نمود.....	۵۱
۴.۳	نقش عملیات امنیتی در گردش کار یک سازمان تجاری.....	۵۵
۴.۴	مرکز عملیات امنیت خروجی های زیر را در قالب گزارش ارائه می دهد.....	۵۷
۴.۵	طراحی ابزارهای مورد نیاز و فرآیند های امنیتی شامل.....	۵۷
۴.۶	طراحی، پیاده سازی، نگهداری و پشتیبانی مراکز عملیات امنیت.....	۵۸
۴.۷	SIEM.....	۵۹
۴.۸	قابلیت های SIEM.....	۶۲
۴.۹	SIEM چگونه در شبکه نصب و فعال می شود؟.....	۶۳
۴.۱۰	ویژگی های کاربردی SIEM.....	۶۵
۴.۱۱	ساختار و معماری SIEM.....	۶۶
۴.۱۱.۱	موتور عملیاتی Collector.....	۶۶
۴.۱۱.۲	موتور عملیاتی Logger.....	۶۶
۴.۱۱.۳	موتور عملیاتی Correlation.....	۶۷
۴.۱۱.۴	موتور عملیاتی گزارش ها.....	۶۷
۴.۱۲	HoneyPot.....	۶۷
۴.۱۲.۱	هانی پات ها به سه دسته تقسیم می شوند.....	۶۸
۴.۱۲.۴	نحوه قرارگیری هانی پات ها.....	۶۸
۴.۱۲.۵	Honeynet.....	۷۰
۴.۱۲.۶	مثالی کاربردی از چندین هانی پات.....	۷۰
۴.۱۳	نتیجه گیری.....	۷۰
۴.۱۴	سوالات فصل چهارم.....	۷۱
۴.۱۵	منابع.....	۷۲

5

فصل پنجم.....	۷۴
ساختار نرم افزاری SIEM.....	۷۴
ساختار نرم افزاری.....	۷۴
معرفی و شرح مختصری از چند نمونه برتر SIEM های نرم افزاری.....	۷۵
نتیجه گیری.....	۸۲
سوالات فصل پنجم.....	۸۲



6

فصل ششم.....	۸۴
ساختار سخت‌افزاری SIEM.....	۸۴
۶.۱ ساختار سخت‌افزاری.....	۸۴
۶.۲ نتیجه‌گیری.....	۹۳
۶.۳ سؤالات فصل ششم.....	۹۴
۶.۴ منابع.....	۹۴

7

فصل هفتم.....	۹۶
یک ایده.....	۹۶
۷.۱ مقدمه.....	۹۶
۷.۲ در واقع در این بخش ۵ مبحث اساسی موردبررسی قرار می‌گیرد.....	۹۷

8

فصل هشتم.....	۱۰۲
سناریو و نیازمندی‌ها.....	۱۰۲
۸.۱ نیازمندی‌های پروژه طراحی و پیاده‌سازی و تأمین تجهیزات مرکز کنترل عملیات امنیت شبکه.....	۱۰۲
۸.۱.۱ شناخت شبکه موجود.....	۱۰۲
۸.۱.۲ ارزش‌گذاری دارایی‌ها.....	۱۰۲
۸.۱.۳ سطح‌بندی امنیتی دارایی‌ها.....	۱۰۲
۸.۱.۴ بررسی نقاط آسیب‌پذیری سیستم‌عامل‌ها.....	۱۰۲
۸.۱.۵ بررسی نقاط آسیب‌پذیری برنامه‌های کاربردی.....	۱۰۳
۸.۱.۶ بررسی نقاط آسیب‌پذیری تجهیزات شبکه.....	۱۰۳
۸.۱.۷ گزارش شناخت شبکه و نتایج ارزیابی امنیتی.....	۱۰۳
۸.۱.۸ بررسی چیدمان تجهیزات.....	۱۰۳
۸.۱.۹ ارائه طرح پیکربندی فایروال‌ها.....	۱۰۴
۸.۱.۱۰ ارائه طرح پیکربندی سیستم‌های شناسایی و جلوگیری از نفوذ.....	۱۰۴

- ۸.۱.۱۱ ارائه طرح پیکربندی سیستم ثبت و جمع‌آوری وقایع..... ۱۰۴
- ۸.۱.۱۲ ارائه طرح پیکربندی امن سازی ارتباطات شبکه..... ۱۰۴
- ۸.۱.۱۳ ارائه طرح پیکربندی موتورهای ارزیابی آسیب‌پذیری..... ۱۰۴
- ۸.۱.۱۴ ارائه طرح پیکربندی نرم‌افزارهای تحلیل بدافزارها..... ۱۰۵
- ۸.۲ نیازهای نرم‌افزاری و سخت‌افزاری مرکز عملیات امنیت..... ۱۰۵



- ضمیمه اول - واژه نامه..... ۱۰۷



> CHAPTER 1

◆ آشنایی با مرکز عملیات امنیت (SOC)

فصل اول

آشنایی با مرکز عملیات امنیت (SOC)



مرکز عملیات امنیت (Security Operations Center) شامل مجموعه‌ای هماهنگ و مدیریت‌شده از ساختار و سیاست‌های امنیتی شبکه می‌باشد که به منظور یکپارچگی، مدیریت و نظارت سایر تمهیدات امنیتی موجود در هر سازمان، راه اندازی می‌شود.

۱.۱ مقدمه

در تمامی مشاغل و صنعت‌ها نیاز به کنترل و پایش وجود دارد؛ تا در هنگام بروز مشکلات به راحتی بتوان آن را حل و مسبب ایجاد مشکل را پیدا کرد.

در همه‌ی صنعت‌ها نیز این کار توسط یک سیستم مکانیزه شامل ابزارها و نیروهای انسانی انجام می‌گیرد. از این رو فناوری اطلاعات به‌عنوان یکی از صنعت‌هایی که بسیار رو به رشد و همه‌گیر می‌باشد نیازمند کنترل دقیق است.

از آنجایی که تمام نقاط جهان از طریق بستر اینترنت باهم در ارتباط هستند و تمامی سازمان‌ها و نهادها نیز دارای شبکه‌های کامپیوتری هستند، خطرات و تهدیدات نیز افزایش پیدا می‌کند.

همان‌گونه که این خطرات زیرساخت‌های سازمان‌ها را تهدید می‌کند، تأثیرات منفی و مخربی روی کاربران و مشتریان نیز می‌گذارد.

به منظور جلوگیری و مقابله با این تهدیدات و مشکلات، در تمامی زیرساخت‌ها کنترل دقیق و پایش در تمام سطوح باید انجام گیرد.

این کنترل‌ها در سطوح برنامه‌های کاربردی، شبکه، ترافیک‌های ورودی و خروجی، درخواست‌های کاربران و... انجام می‌گردد.

از چندین سال قبل بحث پیاده‌سازی این‌گونه سامانه‌ها تحت عنوان مراکز عملیات امنیت (SOC^۱) مطرح گردید. مرکز عملیات امنیت که از چندین بخش تشکیل شده است تمامی وظایف کنترلی و مقابله با تهدیدات در فضای سایبر را بر عهده دارد.

۱.۲ آشنایی با SOC

مرکز عملیات امنیت شبکه، (SOC) مکانی جهت مانیتورینگ و کنترل ۲۴ ساعته ورود و خروج اطلاعات در شبکه می‌باشد. به طور کلی هر مرکز SOC به سه سطح عمده تقسیم می‌شود که هر یک وظایف خاصی را بر عهده دارند. این سطوح عبارت‌اند از:

سطح یکم، نقطه تماس Client ها و مسئول پاسخ‌گویی به اخطارهای دریافتی از Client ها است. در این سطح به کلیه اخطارهایی که از پیچیدگی پایین‌تری برخوردارند، پاسخ داده می‌شود.

سطح دوم، در حقیقت مکمل سطح یکم است و مسئول پاسخ‌گویی به مشکلات پیچیده‌تر در سیستم‌های امنیتی شبکه می‌باشد. برای اخطارهایی که از اهمیت بالایی برخوردارند، سیستم‌های سطح دوم به‌طور کامل درگیر می‌شوند.

سطح سوم، در این سطح کارشناسان ارشد و مشاوران امنیتی شبکه قرار دارند. این سطح در حقیقت پشتیبان دو سطح پایین‌تر است. در صورتی‌که به اشکالات امنیتی در دو سطح پایین پاسخ داده نشود، کارشناسان و سیستم‌های این سطح، درگیر می‌شوند. کلیه تدابیر امنیتی و مدیریت امنیت شبکه، در این سطح اندیشیده می‌شود.

در طراحی مراکز عملیات امنیت، متدولوژی‌های مختلفی مطرح می‌باشد. با این حال پایه همه متدولوژی‌ها بر اساس ترکیب تکنولوژی، نیروی انسانی، فرآیندها در هسته فعالیت این مرکز امنیتی و احاطه آن توسط فرآیندهای اجرایی می‌باشد. این فرآیندها شامل برنامه‌ریزی، طراحی، پیاده‌سازی، عملیاتی نمودن و توسعه مرکز عملیات امنیت می‌باشد.

لایه بعدی در طراحی مرکز SOC، شامل ابزارها و معیارهایی است که از طریق آن‌ها خدمات ارائه شده ارزیابی می‌گردند. این ابزارها و معیارها شامل چشم‌انداز، منابع، زمان، هزینه، ارتباطات و ریسک‌های موجود در راه اندازی SOC می‌باشد.

^۱ Security Operations Center



نکته قابل توجه در طراحی یک SOC، انعطاف‌پذیری متدولوژی طراحی آن است که به واسطه آن می‌توان برای هر یک از مشتریان مطابق سرویس‌های مورد نیازشان راه‌حل خاصی برای مدیریت امنیت ارتباطات ارائه نمود.

در هر یک از سطوح مطرح‌شده، ابزاری برای مدیریت سیستم‌های امنیتی در نظر گرفته می‌شود. این ابزارها، امنیت شبکه را از دو دیدگاه درون سازمانی و برون‌سازمانی موردبررسی قرار می‌دهند. برای این منظور، هر SOC دارای یک سری تجهیزات در داخل شبکه و یک سری تجهیزات در خود مرکز می‌باشد. همه سرویس‌هایی که از مراکز SOC ارائه می‌گردند، مانیتورینگ و مدیریت‌شده هستند. دیگر سرویس‌هایی که از طریق این مراکز قابل ارائه می‌باشند، سرویس‌های پیشرفته‌ای به شرح زیر می‌باشد:

- توسعه سیاست‌های امنیتی
- آموزش مباحث امنیتی
- طراحی دیواره‌های آتش
- پاسخگویی آنی (CERT^۲)
- مقابله با خطرات

سرویس‌هایی که از طریق این مراکز ارائه می‌گردند، عبارت‌اند از سرویس‌های مدیریت‌شده‌ای که از تجهیزات و ارتباطات مرکز SOC محافظت می‌نمایند. این سرویس‌ها از متدولوژی و ابزارهای نرم‌افزاری و سخت‌افزاری قدرتمندی برای مدیریت امنیت استفاده می‌نمایند. اجزای سخت‌افزاری که در شبکه‌ها توسط سیستم‌های مدیریت‌شده برای اعمال سیاست‌های امنیتی مورد استفاده قرار می‌گیرند، عبارت‌اند از: سیستم‌های کشف و رفع حملات (Intrusion Detection and Prevention System)، سیستم‌های فایروال و سیستم‌های مدیریت امنیت در شبکه‌های خصوصی مجازی.

۱.۳ معماری SOC

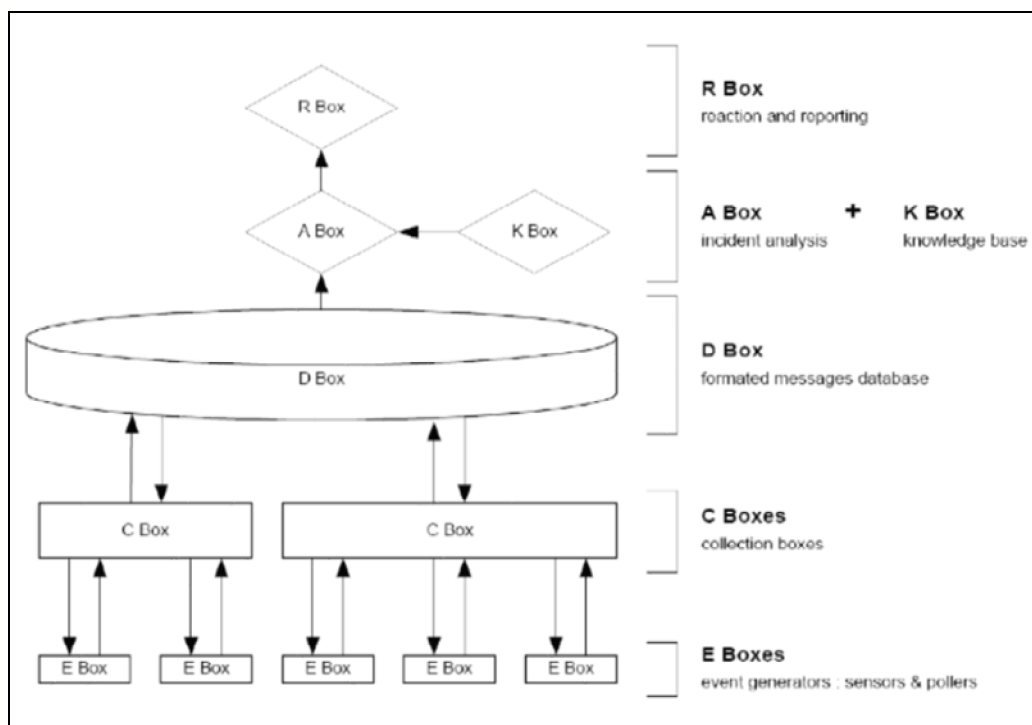
SOC بستری است که سرویس‌های کشف و واکنش را در مقابل حوادث امنیتی فراهم می‌آورد. طبق این تعریف می‌توان پنج نوع عملیات مختلف را در حوزه SOC در نظر گرفت:

- ثبت رخداد امنیتی
- جمع‌آوری

^۲ Computer emergency response team

- ذخیره‌سازی
- تحلیل
- واکنش

جهت آسان‌تر شدن مفهوم، معماری SOC را با کادرهایی نشان می‌دهیم که هر یک از این کادرها، گروه عملیاتی از ماژول‌هایی است که عملیات خاصی را انجام می‌دهند:



شکل ۱.۱ معماری مرکز عملیات امنیت

در معماری SOC چستی اطلاعات جمع‌آوری شده و چگونگی تحلیل، پردازش و ارتباط این اطلاعات مشخص می‌شود. ایجاد یک SOC با معماری مناسب مستلزم موارد ذیل است:

۱. تعیین دارایی‌ها
۲. تصمیم‌گیری در مورد اطلاعات امنیتی که بایستی جمع‌آوری گردند
۳. تعیین اطلاعات مرتبط و قابل تحلیل

۴. تحلیل پدیده‌های امنیتی مرتبط

۵. از کارشناسان امنیتی به نحو شایسته بهره گرفته شود.

۱.۴ نتیجه‌گیری

مراکز عملیات امنیت (SOC) یک مجموعه کاملاً مکانیزه و پیشرفته می‌باشند که دارای یک معماری استاندارد و کامل می‌باشند که جهت مانیتورینگ ۲۴ ساعته پیاده‌سازی می‌شوند. در این معماری ساخت‌یافته هر یک از اعضا (کارشناس) در یک بخش یا گروه عملیاتی خاص به همراه یکسری تجهیزات و ابزارها کار می‌کنند. به‌طور کلی مراکز عملیات امنیت به سه سطح نقطه تماس Clientها، مسئول پاسخ‌گویی به مشکلات و اختلالات و کارشناسان ارشد امنیتی تقسیم می‌گردند.

۱.۵ سؤالات فصل اول

۱. مرکز عملیات امنیت (SOC) را به همراه سطوح مختلف آن تعریف نمایید؟
۲. انواع سرویس‌های پیشرفته موجود در SOC را شرح دهید؟
۳. معماری یک مرکز عملیات امنیت (SOC) را توضیح دهید؟
۴. ایجاد یک مرکز عملیات امنیت موفق مستلزم رعایت چه مواردی می‌باشد؟
۵. انواع گروه‌های عملیاتی را در معماری SOC نام ببرید؟

۱.۶ منابع

- [1] <http://www.sans.org/event/security-operations-center-summit-2015>
- [2] http://www.secureworks.com/it_security_services/advantage/soc/
- [3] Security Operation Center Concepts & Implementation by Renaud Bidou
- [4] Network Intrusion Detection by Stephen Northcutt, Judy Novak
- [5] <http://h71028.www7.hp.com/enterprise/downloads/software/ESP-BWP014-052809-09.pdf>
- [6] <http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity-security-operations-centers>
- [7] <https://www.giac.org/paper/gslc/8336/security-operations-centre-soc-utility-organization/138736>