

## بسمه تعالی

# پیاده سازی مرکز عملیات امنیت SOC ( Security Operation Center )

امنیت، از نیازهای اصلی انسان و بالطبع همه ابداعات و مصنوعات نرم افزاری اوست. جدیدترین این ابداعات شامل کامپیوتر، شبکه و اینترنت می شود که ضمن دیجیتالی کردن اطلاعات، باعث مبادله ساده آن نیز شده است، بنابراین امنیت آن اهمیت ویژه ای دارد لذا شایسته است جایگاه و ساختاری برای آن در نظر گرفته شود. این جایگاه در واقع مکان و سایتی است که وظیفه آن برقراری امنیت در شبکه یک سازمان بوده و نام آن، مرکز عملیات امنیت ( SOC ) است. مرکز عملیات امنیت شبکه، مکانی برای مانیتورینگ و کنترل دائم وضعیت شبکه به لحاظ ایمنی است که عموماً در سه سطح و با کمک ابزارهای متنوع امنیتی انجام می شود.

در سطح اول، کارشناسان گروه امنیت شبکه به مسائل و مشکلات امنیتی مربوط به Client های کاربران پاسخ داده و مسئولیت رفع مشکلات جزئی مربوط به امنیت سیستم های کاربران را عهده دار می باشند. در این سطح به اظهارهای دریافتی از client ها که از پیچیدگی کمتری برخوردار هستند. پاسخ داده می شود.

در سطح دوم، کارشناسان سطح بالاتر امنیت شبکه، پاسخگوی مشکلات ناشی از سیستمهای امنیتی شبکه و نرم افزارهای مربوطه می باشند و چنانچه در نرم افزار امنیتی شبکه مشکلی ایجاد شود، کارشناسان مذکور موضوع را بررسی و نسبت به رفع مشکل اقدام می نمایند. سیستمهای این سطح، برای اظهارهای پر اهمیت، کاملاً درگیر می شوند.

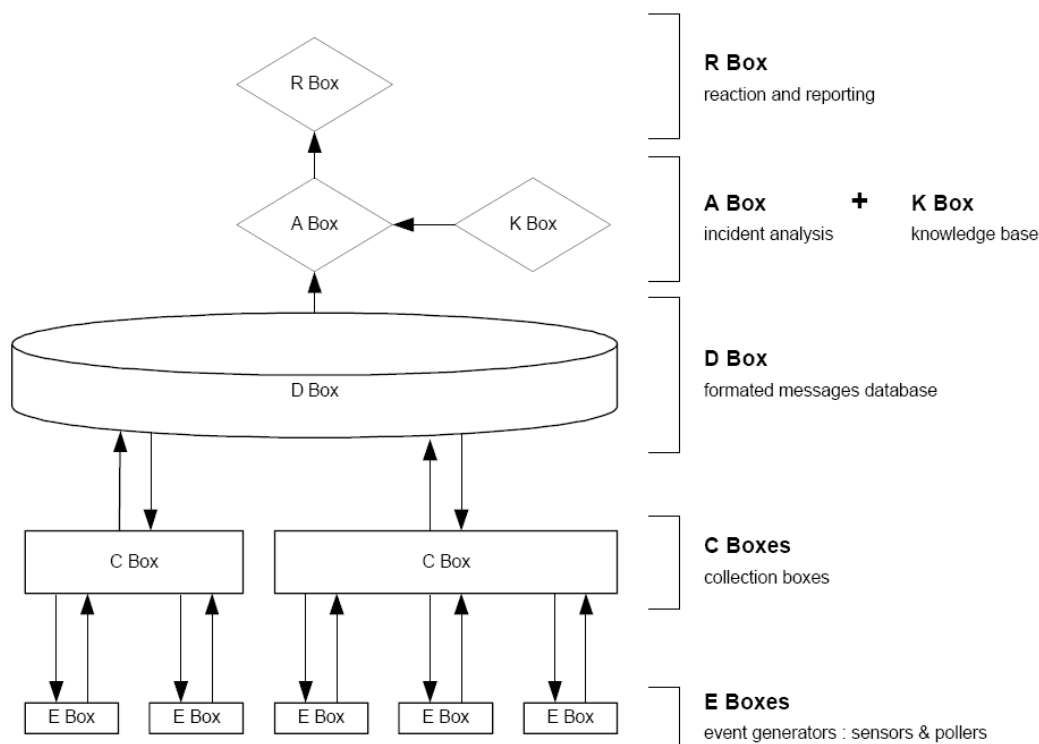
در سطح سوم، کارشناسان ارشد و مشاوران با تجربه امنیت شبکه، سیاستهای امنیت شبکه سازمان را وضع نموده و کلیه تدابیر امنیتی و مدیریتی شبکه را مشخص و تبیین می نمایند. این سطح در واقع پشتیبان دو سطح قبلی است.

با توجه به موارد فوق، واضح است که عموماً در یک مرکز امنیت شبکه، تکنولوژی، نیروی انسانی و فرایند ها، از بخشهای اصلی آن به شمار می رود و نکته قابل تامل، این است که برای هر یک از کاربران و مشتریان، مطابق با سرویس های مورد نیازشان، راه حل خاصی جهت مدیریت امنیت شبکه ارائه می گردد. این موضوع با کمک ابزارهایی انجام می شود که بایستی از دیدگاه درون سازمانی و برون سازمانی مورد بررسی قرار گیرند. گروه کارشناسان امنیت شبکه، اقدامات فوق را در SOC طبق موضوعات چهار گانه: فایر والها ( Firewall ) - شبکه خصوصی مجازی ( VPN ) - سیستم کشف حملات ( IDS ) و آنتی ویروس (Antivirus) ها انجام داده و سپس بر اساس آنها سرویسهای پیشرفته (توسعه سیاست های امنیتی، آموزش مباحث امنیتی ، طراحی دیواره های آتش، پاسخگویی آنی، مقابله با خطرات امنیتی و پیاده سازی آن ) را ارائه می دهند.

بدیهی است برای تحقق این امور نیاز به ابزارهای نرم افزاری و سخت افزاری است که برخی ابزارهای سخت افزاری بکار رفته آن عبارتند از: سیستمهای کشف و رفع حملات ( Intrusion Detection System ) سیستمهای فایروال و سیستمهای مدیریت امنیت در شبکه های خصوصی مجازی ( VPN ).

سرویس های مدیریت شده در SOC شامل: دیواره آتش یا firewall، سیستمهای تشخیص حملات یا IDS، امکان فیلتر کردن محتوی، امکان تشخیص ویروس و سرویس های AAA هستند، همچنین در مرکز عملیات امنیت، حملات به شبکه در سه رده verification حصول اطمینان از بخشهایی که کنترلا مستقیم بر روی آنها وجود ندارد ( و Visibility (مانیتورینگ امنیت تجهیزات شبکه ) و Vulnerability ( بروز رسانی تجهیزات بکار رفته در این رده به محض نصب و راه اندازی ) بررسی می شوند.

حال اگر بخواهیم SOC را به لحاظ فرایندی بررسی نمائیم باید بگوئیم که مرکز عملیات امنیت ( SOC ) از پنج ماجول ساخته شده است، که عبارتند از: تولید کننده های رویداد، تجمیع کننده های رویداد، بانک اطلاعاتی پیام ها، موتورهای تحلیل و نرم افزار مدیریت واکنش ومسئله اصلی در SOC، اجتماع این ماجول ها است. مرکز عملیات امنیت به منظور فراهم نمودن سرویس کشف و واکنش به حوادث امنیتی است. شکل زیر ارتباط بین این ماجول ها را در یک مرکز SOC نمایش می دهد. برای سادگی کار از box های ماجول استفاده شده است.



شکل (۱) معماری SOC

در شکل فوق E Box مربوط به بخشهای تولید کننده رویداد، C Box مربوط به قسمت های تجمیع رویداد ها، D Box بانک اطلاعاتی پیامهای فرمت بندی شده، A Box برای تحلیل حوادث، K Box برای استفاده از دانش و نهایتا R Box به منظور تهیه گزارش و همچنین واکنش به رویدادها است.

به عنوان مثال، مرکز JSOC یکی از بزرگترین مراکز مونیترینگ ژاپن است که چشمان خود را ۲۴ ساعته بر روی دروازه های امنیتی باز نگه می دارد و شامل firewall و IDS و سیستمهای عملیاتی و شبکه ها است و آنها را از خطرات خارجی مثل ویروس های کامپیوتری، هکهای مجازی و Worm ها محافظت می کند. در اینجا، تحلیل ساده log فایل firewall و هشدارهای IDS دسترسی های تعریف نشده و نامعتبر خطرناک را که به حوادث جدی ختم می شود را پیش بینی می کند. با استفاده از STP (Soc Technology Platform) یک تحلیل هماهنگ در الگوریتم های معین روی مقادیر زیادی از هشدارهای IDS و Log های فایر وال انجام می دهیم.

این کار به منظور حذف کشف نشده ها و کاهش دسترسی های نامعتبر است. تحلیل گر انسانی ، هر رویداد نامعتبر را که توسط STP کشف شده را دوباره تحلیل می کند و نهایتا هر گونه موضع کشف نشده ای را حذف می کند. در این روش، تنها دسترسی های نامعتبر به Client گزارش می شود. لذا با استفاده از ترکیب STP و تحلیل انسانی به سمت بهبود کارایی در کشف دسترسی های غیر مجاز پیش می رویم.

لذا ایجاد یک چنین سیستم امنیتی با اطمینان بالا (SOC)، مستلزم پرسنل کارآمد، تجهیزات نرم افزاری و سخت افزاری متناسب بدون وابستگی به محصول خاص و اتاق مونیترینگ است که در صورت صلاحدید و موافقت جنابعالی، گامهای بعدی جهت نیل به این هدف طبق استاندارد ( BS7799 ) ISMS قابل پیاده سازی خواهد بود.

علی ثاقب موفق