|  |  |
| --- | --- |
| |  | | --- | |  | |

SOC چیست؟  
  
SOC یا مرکز عملیات امنیتی به عنوان مرکز کلیه خدمات مربوط به امنیت در محیط IT سازمانها یا شرکتها می باشد. این مرکز از زیرساخت ها و داده های IT در برابر تهدیدات داخلی و خارجی محافظت می کند. زیرا به نوعی نمیشود یک شبکه را به طور کامل از حملات متعدد روی بستر آن امن کرد. از این بابت میبایست بررسی و نظارت کامل را بر روی بستر یک شبکه داشته باشیم تا درصورت رخداد مشکلات به سرعت توانایی پاسخ گویی را داشته باشیم.  
  
چه اتفاقی در SoC رخ میدهد؟  
  
اگرچه تعداد کارکنان و افراد فعال در تیم های SOC بسته به اندازه سازمان ها متفاوت است، اما تقریبا اکثر آنها یک نقش و مسئولیت یکسان را برعهده دارد.  
   
  
از این بابت SOC نیز یک عملکرد متمرکز در داخل سازمانی است که افراد، فرایندها و فناوری را برای نظارت و بهبود وضعیت امنیتی سازمان به طور مستمر و همزمان با جلوگیری، شناسایی، تجزیه و تحلیل و پاسخ به حوادث امنیت سایبری به کار می گیرد.  
  
مرکز عملیات امنیتی چه وظیفه ای دارد؟  
  
مرکز عملیات امنیتی وظیفه محافظت از زیرساخت IT یک شرکت یا سازمان را بر عهده دارد. برای اینکه بتواند این وظیفه را انجام دهد، تمام سیستم های مربوط به امنیت مانند شبکه های شرکت، سرورها، رایانه ها و … را نظارت و تجزیه و تحلیل می کند.  
علاوه بر تجزیه و تحلیل سیستم های مختلف، هشدار و اقدامات لازم برای محافظت از داده ها و برنامه ها وظایف اصلی مرکز اطلاعات امنیتی است.  
این اقدامات می توانند هم در سطح فیزیکی و هم در سطح برنامه تأثیرگذار باشند. اقدامات امنیتی فیزیکی می تواند به عنوان مثال در دیوارهای آتش یا سیستم های تشخیص نفوذ اجرا شود و از محافظت مستقیم از شبکه شرکت اطمینان حاصل کند. اقدامات حفاظتی در سطح برنامه ، راه حل های ویژه ای برای مجوز و تأیید اعتبار کاربران یا نرم افزار آنتی ویروس برای شناسایی بدافزار است.  
از طرف دیگر SOC به صورت پیشگیرانه کار می کند و تلاش می کند نقاط ضعف زیرساخت IT را در مراحل اولیه شناسایی و از بین ببرد. در صورت حملات فعلی مانند حملات DdoS ، از اقدامات محافظتی مستقیم به طور واکنش پذیر استفاده می کند. مدیریت شرکت یا سازمان در فواصل منظم از طریق گزارش در مورد کار SOC و امنیت سیستم های IT مطلع می شود.  
  
جلوگیری و کشف (Prevention And Detection)  
  
وقتی صحبت از امنیت سایبری می شود، پیشگیری همیشه نسبت به جلوگیری بسیار موثر تر میباشد. مرکز عملیات امنیتی بجای پاسخگویی به تهدیدها در هنگام وقوع، به منظور نظارت به صورت شبانه روزی بر روی یک شبکه فعالیت میکند و تمامی رخداد های متنوع توی یک شبکه را ثبت و بررسی میکند.از این بابت تیم SOC می تواند فعالیت های مخرب را شناسایی کرده و قبل از اینکه موجب آسیب و صدمه ایی به سازمان شوند از آنها جلوگیری کند.  
  
تحقیق (Investigation)  
  
در مرحله تحقیق افراد فعال در این حوزه که اغلب با نام SoC Analyst نیز شناخته میشوند به منظور کشف حملات میبایست درک کامل و جامعی از حملات متعدد و به روز دنیا داشته باشند که به سبب دانش کافی آن ها در رابطه با آن حمله بتوانند حمله را کشف و بررسی کنند.  
این افراد میبایست افکاری مانند یک هکر اخلاقی داشته باشند و از ابزار ها و تکنیک های متنوعی که برای SoC ارائه شده است نیز استفاده کنند.  
  
پاسخ (Response)  
  
پس از بررسی و کشف رخداد میبایست پاسخی را برای رفع مشکل ارائه کنند. به محض تأیید یک حادثه، مرکز SOC به عنوان اولین پاسخ دهنده عمل می کند و اقداماتی مانند جداسازی نقاط انتهایی، خاتمه بخشیدن به فرآیندهای مضر، جلوگیری از اجرای فرآیند های مضر، حذف پرونده ها و موارد دیگر را بکار میگیرد.

تا اینجای کار ما بر یک پردازشگر SOC خارجی تمرکز کردیم. در این حالت کمپانی مورد نظر به یک تامین کننده SOC خارجی پولی پرداخت می‌کند تا به نیازهای امنیت شبکه کمپانی رسیدگی کند. علاوه بر این، مدل‌های ساختاری متعدد دیگری از SOC نیز وجود دارند که به شیوه مشابهی عمل می‌کنند.

* SOC  داخلی یا اختصاصی: مجموعه یا شرکت، تیم امنیت شبکه خودش را درون نیروی سازمانی خودش تاسیس می‌کند.
* SOC مجازی: تیم امنیت شبکه امکانات و مکان اختصاصی ندارد و معمولا دورکار است.
* SOC جهانی یا بالادستی: یک گروه رده بالاست که بر فعالیت‌های تعدادی از SOC های کوچک‌تر در یک منطقه نظارت دارد.
* SOC مشارکتی: در این حالت تیم داخلی آی‌تی کمپانی در همکاری تنگاتنگ با یک شرکت خارجی به نیازهای امنیت شبکه کمپانی رسیدگی می‌کنند.

مجرمان سایبری همیشه به دنبال ابداع شکل‌های جدیدی از حمله هستند که افراد و کمپانی‌ها پیش‌بینی نمی‌کنند. تیم‌های SOC برای این که از آنها یک قدم جلوتر باشند ناچارند رویکرد مشابهی در پیش بگیرند. اگر آنها تمام زمانشان را صرف مقابله با تهدیدهای شناخته شده کنند در برابر تهدیدهای جدیدی که در راه است منفعل می‌شوند. نفوذ به شبکه و آزمایش اغتشاش عملیات حیاتی برای یک SOC هستند چرا که تیم را ناچار به جستجوی آسیب‌پذیری‌هایی که در جاهای ناشناخته پنهان شده می‌کنند.