به نام خدا

اسماعیل زارع

SOC چیست و چه اهمیتی دارد؟

مخفف واژه security operations center بوده که به معنای مرکز عملیات امنیتی است. در سازمان‌ها و شرکت‌های بزرگ که نیاز به امنیت شدید سایبری به دلیل گسترده بودن شبکه حس می‌شود، مجموعه افرادی همراه با فناوری‌های نوین و خلاقانه در کنار تجهیزات امنیتی وظیفه نظارت و تجزیه‌وتحلیل ترافیک شبکه را برعهده دارند تا با پیش‌بینی خطرات احتمالی، در صورت وقوع هر نوع اتفاق بهترین واکنش را در دستور کار قرار دهند.

این تیم عملیاتی، متشکل از مهندسان امنیتی در کنار مدیران ناظر است که وظایف حیاتی بر عهده ایشان قرار دارد.

تعریفی دقیق از SOC یاsecurity operations center

در سازمان‌های بزرگ و پیشرفته زمانی که شبکه پیاده شده در حدی گسترده باشد که نیاز به امنیت سایبری در آن یک ضرورت باشد، تیمی متشکل از مهندسان مجرب و با دانش کافی زیر نظر مدیرانی آب‌دیده همراه با تجهیزات موردنیاز در مرکز سازمان مستقر خواهند شد. این تیم وظیفه نظارت و تجزیه‌وتحلیل مداوم کل زیرساخت‌ها، به‌منظور جلوگیری از وقوع هر نوع اتفاق غیرمنتظره و تهدید سایبری را برعهده دارند.

SOC روی نقاط پایانی، پایگاه‌های داده، برنامه‌ها و وب‌سایت‌ها، شبکه‌های سازمانی، سرورها و... نظارت دارند و تمامی داده‌های ورودی و خروجی از این موارد را زیر نظر می‌گیرند.

اگر بخواهیم مسئولیت اصلی security operations center را تشریح کنیم، مانند این است که تیمی متشکل از مهندسین فعال در حوزه امنیت سایبری با به دست گرفتن ذره‌بین به دنبال هر نوع فعالیت غیرعادی می‌گردند که ممکن است امنیت شبکه و زیر ساخت‌ها را به خطر بیندازد. در نتیجه تیم مرکز عملیات امنیتی مسئول است تا هرگونه حوادث امنیتی را شناسایی، تجزیه‌وتحلیل، دفاع، بررسی و گزارش کند.

۶ قطب و ستون مهم SOC

اگر در سازمان بخش فناوری اطلاعات مجزا ندارید، همیشه می‌توانید مدیریت خدمات امنیتی را برون‌سپاری کنید. اکثر MSSP ها خدمات SOC را به مشتریان خود ارائه می‌دهند تا حتی مشاغل کوچک و متوسط بتوانند از شرکت‌های خود در برابر مهاجمان محافظت کنند. در ادامه با ٦ ستون SOC برای تشکیل یک رویکرد امنیت سایبری آشنا می‌شویم.

۱ .اطلاع از دارایی‌های سازمان

مدیریت سازمان باید اطلاعات کاملی درباره دارایی‌های IT شرکت داشته باشد. فناوری‌ها، نرم‌افزارها، سخت‌افزارها و ابزارهایی که کل دارایی‌های فناوری اطلاعات را تشکیل می‌دهند، بر اساس شرکت متفاوت خواهند بود. طبیعتا فهرست این دارایی‌ها در شرکت‌های فناوری اطلاعات نسبت به شرکت‌های معمولی بلندبالاتر است.

۲ .مانیتورینگ شبکه

پیشگیری همیشه بهتر از درمان است .بنابراین انتظار می‌رود تمام تلاش خود را برای جلوگیری از نقض داده‌ها به‌کار ببندید . SOC شبکه را از نظر آسیب‌پذیری و نقض‌ها کاملا نظارت می‌کند تا فعالیت‌های مخرب شبکه را شناسایی کند.

۳ .ردیابی فعال ارتباطات و فعالیت‌ها

تحلیلگران SOC باید بتوانند در صورت نقض داده ارتباطات و فعالیت‌ها را ردیابی کنند. این یعنی لازم است تک‌تک فعالیت‌هایی که در شبکه رخ می‌دهد را ثبت کنید. تیم IT می‌تواند یک فایل گزارش از تمام ارتباطات و فعالیت‌هایی که در شبکه اتفاق می‌افتد ایجاد کند.

۴ .رتبه‌بندی هشدارهای امنیتی

اولویت همیشه باید برای هشدارهای امنیتی باشد. این‌طوری SOC می‌تواند روی هشدارهای امنیتی اصلی کار کند و قبل از پرداختن به هشدارهای معمولی، به هشدارهای اصلی پاسخ دهند.

۵ .اصلاح تنظیمات دفاع از سیستم

مسئله امنیت سایبری روزبه‌روز با گذشت زمان تغییر می‌کند و پیشرفته‌تر از قبلمی‌شود. بنابراین بهبود مستمر رویکردهای امنیتی یکی از نیازهای اساسی سازمان‌های بزرگ و شرکت‌های کوچک است. خوشبختانه SOC سیستم دفاعی شبکه را با توجه به آخرین تهدیدات اصلاح می‌کند تا هیچوقت در برابر حملات بی‌دفاع نباشید.

۶ .پیروی از انطباق‌های امنیتی

هر شرکتی باید از یک مجموعه انطباق‌های امنیتی پیروی کند. در همین راستا SOC کمک می کند از داده‌های خود در برابر هرگونه تهدید و از کسب‌وکار خود در برابر مشکلات قانونی محافظت کنید .به‌گونه‌ای که عملیات تجاری شما با آخرین مقررات مطابقت داشته باشد.

مزیت داشتن security operations center

باید به این نکته توجه داشت که برنامه‌ریزی برای یک حمله بزرگ سایبری بسیار پیچیده و پیشرفته خواهد بود و ممکن است مقدمات آن تا مدت‌ها قبل از انجام حمله اصلی صورت گیرد. پس با نظارت مداوم بر ترافیک شبکه توسط تیم security operations center می‌توان این اطمینان را پیدا کرد که تهدیدات سایبری به حداقل خواهند رسید.

تیم عملیات امنیتی با تحلیل و زیر نظر گرفتن ۲٤ ساعته نقاط پایانی، مراکز داده، سرورها و تمامی فعالیت‌ها در حال انجام در شبکه قادر هستند تا تهدیدات را به‌سرعت شناسایی و برای پاسخ و واکنش مناسب، کل سازمان را آماده کنند.

پس مهم‌ترین مزیت داشتن SOC در یک سازمان، نظارت پیشرفته و مداوم برای بهبود تشخیص حوادث امنیتی و سایبری است . گزارش‌های سالانه این تیم اطلاعات خوبی درمورد شکاف‌ها و نقص‌های موجود در شبکه را فاش می‌کند که با گذر زمان می‌توان انتظار داشت سازمان با پوشاندن این شکاف‌ها، در رأس هرم تهدیدات محیطی قرار گیرد.

نقش اعضای فعال در تیم SOC

در تیم SOC گفته شد که کارمندان در کنار سیستم‌ها و تجهیزات مختلف تمامی وظایف مربوط به نظارت بر ترافیک شبکه را بر عهده دارند. حال نیاز است تا بدانیم که هر فرد در security operations center چه نقشی را دارد و باید چه وظایفی را انجام دهد. در ادامه لیست کاملی از نقش اعضای فعال در تیم مرکز عملیات امنیتی آورده شده است:

Manager یا مدیر :رهبر و لیدر گروه که ممکن است در هر زمینه‌ای فعالیت مؤثر داشته باشد، در واقع نظارت‌کننده بر کل سیستم‌ها و رویه‌های امنیتی است.

Analyst یا تحلیلگر :مهندسینی که عهده‌دار این نقش هستند باید داده‌های یک دوره زمانی (مثلاً دوره ۳ یا ٦ ماهه) یا داده‌های مربوط بعد از یک نقص امنیتی را تحلیل و بررسی کنند.

Investigator یا بازپرس :در زمان وقوع یک حادثه امنیتی این فرد با انجام یک تحقیق رسمی با پاسخگو یا Responder در تلاش برای این است که روشن کند چه اتفاقی افتاده و چرا.

Responder یا پاسخگو :در زمان وقوع حادثه برای اتفاق افتاده اغلب پاسخ‌های ثابتی وجود دارد که یک فرد آشنا و مجرب در این زمینه می‌تواند به تیم کمک کند. در اکثر موارد بازپرس و پاسخگو در SOC یک نفر است.

Auditor یا حسابرس :فردی که تضمین می‌کند تمامی کارهای انجام شده بر اساس قوانین فعلی یا قوانینی که ممکن است در آینده وضع شود، منطبق خواهد بود.

باید افزود که بسته به‌اندازه یک سازمان ممکن است فردی بیش از یک نقش را برعهده گیرد و تیم security operations centerیک شرکت به یک یا دو نفر محدود شود.

اهمیت استفاده از تیم مرکز عملیات امنیتی(SOC)

یکی از بزرگ‌ترین موانع پیشرفت شبکه‌ها تهدیدات سایبری است. زیرا که سازمان‌ها و شرکت‌های زیادی از خطرات و حوادث موجود در این بستر ترس داشته و نمی‌توانند با اعتماد کامل زیرساخت‌های خود را در این حوزه پهن کنند. علاوه بر این موضوع مصرف‌کنندگان و مشتریان شبکه‌های بزرگ نیز در صورت وقوع یک فاجعه در نتورک سازمانی بزرگ، تا میزان زیادی نسبت به آن بدبین خواهند شد. تا جایی که در سال ۲۰۱۸ میلیاردها نفر به دلیل همین نقص‌های امنیتی آسیب دیدند.

ازاین‌رو یک تیم قدرتمند SOC می‌تواند تا حدود زیادی با خطرات و تهدیدات سایبری موجود مقابله کند و با پیش‌بینی‌های دقیق، بسیاری از حملات را دفع کند و حتی کمکی در پوشاندن شکاف‌های امنیتی دور از چشم داشته باشد. تعدادی از پراهمیت‌ترین دلایل استفاده از security operations center عبارت‌اند از:

پاسخ و واکنش سریع

در هر حوزه‌ای دقت به این موضوع که پیشگیری بهتر از درمان است باعث پیشرفت و جلوگیری از رخداد فاجعه می‌شود .با در اختیار داشتن یک تیم مرکز عملیات امنیتی می‌توان مطمئن بود که تا میزان زیادی از وقوع تهدیدات پیشگیری می‌شود و در صورت وقوع آن نیز پاسخ و واکنشی سریع در دستور کار قرار خواهد گرفت.

محافظت از اعتماد کاربران و مصرف‌کنندگان

شرکت‌های بزرگ و سازمان‌های توسعه‌یافته با به خدمت گرفتن مهندسین خبره و مجرب امنیتی علاوه بر تضمین امنیت داده‌ها و اطلاعات خود سازمان و کاربران آن، می‌توانند حس امنیت و اعتماد را نیز به مصرف‌کنندگان القا کنند. در سال‌های اخیر به دلیل حوادث رخداده در شبکه‌های مجازی شرکت‌های بزرگ، بسیاری از کاربران این سازمان‌ها اعتماد خود را نسبت به امنیت موجود ازدست‌داده‌اند.

کاهش هزینه‌ها

در وهله اول ممکن است تا فکر کنید که استخدام مهندسین امنیت سایبری به همراه تهیه ابزارها و تجهیزات موردنیاز بسیار هزینه‌بر خواهد بود. ولی باید به این نکته نیز توجه داشت که در صورت وقوع یک فاجعه ممکن است صدمات آن جبران‌ناپذیر باشد و همواره اعتماد مشتریان و اعتبار شرکت گران‌تر از هر مبلغی است.

استفاده از SIEM در بهبودSOC

هیچ فردی با هر میزان دانشی نمی‌تواند این ادعا را داشته باشد که با بررسی خط به خط داده‌ها و اطلاعات می‌تواند تهدیدات داخلی و خارجی را شناسایی کند. زیرا که داده‌های خروجی در بازه زمانی مثلاً ۳ ماهه از یک شبکه حتی کوچک، بسیار حجیم و سرسام‌آور خواهد بود. در این نقطه است که فناوری SIEM می‌تواند نتیجه بازی را تغییر دهد.

در تیم SOC با استفاده از SIEM می‌توان هر حجم از داده‌ای را به صورتی سازمان‌دهی کرد که حتی یک فرد بی‌تجربه نیز بتواند از آن استفاده کند. ازاین‌رو با به‌کارگیری این فناوری در مرکز عملیات امنیتی، می‌توانید با ساده‌تر کردن تجزیه‌وتحلیل خطرات موجود را بهتر و راحت‌تر مدیریت کنید. با security information and event management دید بالاتری نسبت به گذشته خواهید داشت. از جمله مزایای استفاده از این سیستم در security operations center عبارت‌اند از:

۱. کاهش هشدارهای نادرست

۲. یافتن رفتارهای غیرعادی در کوتاه‌ترین زمان ممکن (حتی در عرض چند ثانیه)

۳. کاهش انرژی و وقت صرف شده برای تحلیل داده‌ها و در نتیجه وقت بیشتر برای بهبود بخش‌های دیگر

٤. ارائه گزارش‌های قدرتمند و مستند

چطور سطح امنیت SOC را بالاتر ببریم؟

مواردی که در ادامه معرفی می‌کنیم، بهترین تمریناتی هستند که می‌توانید برای بالابردن سطح امنیت SOC امتحان کنید:

۱ .تمرکز بر امنیت اطلاعات و داده‌ها

در دنیای امروز اکثر شرکت‌ها برای میزبانی برنامه‌ها و داده‌های خود از محاسبات ابری استفاده می‌کنند. این امر زیرساخت اکثر شرکت‌ها را گسترش می‌دهد، روزبه‌روز ردپای اینترنت اشیا بیشتر در شرکت‌ها دیده می‌شود و تقریبا همه سازمان‌ها به فضای ابری متصل‌اند. حالا که فرصت بیشتری برای تهدیدات و حملات فراهم شده، انتظار می‌رود این فناوری‌ها و فرآیندهای جدید را در برابر تهدیدات، امن و نفوذناپذیر کنید.

۲ .جمع‌آوری هرچه بیشتر داده‌ها

اگر می خواهید رویکرد امنیت سایبری خود را بهبود بخشید، باید داده های بیشتری را جمع آوری کنید. این داده ها به شما در تصمیم گیری بهتر در مورد امنیت شبکه کمک می کند. شما باید در طول یک حادثه امنیتی داده ها را جمع آوری کنید. این به تیم SOCشما در یافتن علت اصلی نقض کمک می کند.

۳ .تجزیه و تحلیل بهتر داده‌ها

همه سازمان‌ها برای اتخاذ تصمیمات تجاری بهتر از داده‌ها استفاده می‌کنند. اما جمع آوری داده تنها زمانی ارزشمند است که بتوان آنها را به درستی تجزیه و تحلیل کرد. بنابراین انتظار می‌رود تمام داده‌های جمع‌آوری شده را وارد یک فاز تجزیه و تحلیل جامع کنید تا تیم SOCبهتر بتواند تصمیم بگیرد.

۴ .اتوماسیون امنیتی

عصر، عصر تکنولوژی و اتوماسیون است. بیراه نیست اگر برای ایمن‌سازی شبکه هم دنبال فرایندهای اتوماسیون باشید. می توانید از اسکنرهای آسیب‌پذیری برای اسکن شبکه استفاده کنید تا دیگر تیم IT درگیر یافتن آسیب‌پذیری‌ها نباشد. حتی وظایف امنیتی هم خودکارسازی می‌شوند تا افراد بتوانند روی کارهای مهم‌تر تمرکز کنند. بهتر است در این راستا از هوش مصنوعی و یادگیری ماشین هم استفاده کنید.

تفاوت بین SOC و SOC2 چیست؟

SOC for Cybersecurityو SOC2 Atestations دو چارچوب متفاوت‌اند که با مقاصد و اهداف متفاوت طراحی شده‌اند. با این حال، همپوشانی‌های خاصی نیز بین دو استاندارد گواهی و گزارش وجود دارد.

SOCبرای امنیت سایبری و کنترل‌های مدیریت ریسک سایبری گستره پوشش وسیع‌تری دارد؛ در حالی که SOC2 منحصرا برای مدیریت سازمان در نظر گرفته شده و مختص فرآیندها و کنترل‌هایی است که برای ایمن کردن داده‌های مشتری بر اساس معیاهای پنج‌گانه خدمات اعتماد (امنیت، در دسترس بودن، یکپارچگی پردازش، محرمانگی و حریم خصوصی) ارائه می‌شوند.

چالش‌های مهم SOC چیست؟

مهم‌ترین چالشی که تیم‌های SOC به‌خصوص در سال‌های اخیر با آن روبه‌رو هستید، این است که همیشه یک قدم از مهاجمان جلوتر باشند.

کمبود مهارت‌های امنیت سایبری

می‌توان گفت بیش از نیمی از تیم‌های SOC با مشکل استخدام پرسنل کارکشته مواجه‌اند. این یعنی هرکسی از عهده شناسایی و پاسخگویی به‌موقع و موثر به تهدیدات برنمی‌آید. می‌توان گفت نیروی کار امنیت سایبری راه درازی در پیش دارند تا بتوانند این شکاف مهارتی را ببندند و از سازمان‌ها دفاع کنند.

هشدارهای فراوان

تیم‌های SOC از ابزارهای جدیدی برای تشخیص تهدیدات استفاده می‌کنند. این ابزارها طوری برنامه‌ریزی شده اند که کوچک‌ترین احتمال خطر را هشدار دهند و این حجم از هشدارهای امنیتی برای تیم‌هایی امروزی که پیوسته غرق در کارند، طاقت‌فرساست. به‌علاوه بسیاری از این هشدارها اطلاعات کافی ارائه نمی‌کنند یا حتی اشتباهند! این یعنی نه فقط وقت کارکنان امنیتی را هدر می‌دهند، بلکه حواس آنها را از حوادق امنیتی اصلی منحرف می‌کنند.

سربار عملیاتی فوق‌العاده بالا

بسیاری از سازمان‌ها با یک مجموعه از ابزارهای امنیتی مجزا، سربار عملیاتی را به‌شدت بالا می‌برند. چرا که پرسنل امنیتی باید هشدارها و سیاست های امنیتی را بین محیط‌های مختلف ترجمه کنند و این به نوبه خود منجر به عملیات امنیتی پرهزینه، پیچیده و ناکارآمد می‌شود.

پیچیدگی فرایندها

ماهیت جهانی کسب‌وکار، سیال بودن محل کار، گسترش استفاده از فناوری ابری و سایر مسائل روز، پیچیدگی دفاع از سازمان و پاسخ به تهدیدات را افزایش می‌دهد. اگرچه راه‌حل‌های نسبتا ساده‌ای برای حفاظت از امنیت سیستم (مثل فایروال) وجود دارد، مسئله امنیت راه‌حل پیچیده‌تری نیاز دارد. روش‌هایی که با وجود فناوری‌ها، افراد و فرآیندهای مختلف، راه‌اندازی و نگهداری از آنها حقیقتا دشوار و پیچیده است.

هزینه هنگفت

ساخت یک مرکز عملیات امنیتی مستلزم زمان و منابع قابل توجهی است. حفظ آن سخت‌تر هم هست. چراکه چشم‌انداز تهدید دائما تغییر می‌کند و نیازمند به‌روزرسانی و ارتقاء مکرر و همچنین یادگیری و توسعه مستمر کارکنان است. گذشته از اینها، مسئله امنیت سایبری یک زمینه بسیار تخصصی است و سازمان‌های کمی استعداد درک کامل نیازهای سازمان و چشم‌انداز تهدیدات فعلی را دارند. از این‌رو ناچارند برای تضمین امنیت به ارائه‌دهندگان خدمات امنیتی روی بیاورند.

جمع‌بندی

با به‌وجودآمدن فناوری‌های نوین باید انتظار داشت که تهدیدات جدیدی نیز متولد شوند. البته شبکه و نتورک جزو تکنولوژی‌های جدید نیست ولی قدیمی نیز به شمار نمی‌آید. تهدیدات سایبری و خطراتی مانند افشای اطلاعات خصوصی کاربران و خود سازمان‌های بهره برنده از netwok، همواره یکی از مشکلات اساسی این حوزه به شمار می‌آید.

راهکارهای مختلفی برای مقابله با این مشکلات و تهدیدات موجود خلق شده که یکی از آن‌ها همین استقرار یک تیم مرکز عملیاتی امنیتی (SOC) است. در این مقاله سعی کردیم تا به‌صورت واضح و کامل به بررسی مفهوم این بخش از امنیت یک سازمان بپردازیم.