مرکز عملیات امنیت

فهرست

مقدمه

امروزه بکارگیری مراکز داده برای میزبانی داده، خدمات و اتصال به اینترنت توسط شرکت‌ها و سازمان‌های مختلف در سراسر دنیا به نیازی اساسی تبدیل شده است. مدیریت رویدادهای امنیتی در چنین محیط‌های بزرگ و پیچیده‌ای یک مسأله اساسی برای محافظان امنیت است. اگرچه بکارگیری راهکارهای امنیتی نظیر استفاده ازضدبدافزارها، فایروال‌ها، IPS[1]ها، IDS[2]ها و سامانه‌های احرازهویت و کنترل دسترسی تا حدی می‌تواند شبکه را از حالت انفعالی و بدون نظارت نجات داده و به تأمین امنیت آن کمک کند، ولی باید به این نکته مهم توجه داشت که بکارگیری این تجهیزات امنیتی، خود باعث تولید حجم عظیمی‌از رخدادهای امنیتی در قالب‌های متفاوت می‌شود. این حجم بالایداده‌های امنیتی تولید شده، باعث سردرگمی‌و سلب امکان مدیریت و استفاده از آن‌ها می‌شود.

امروزه با توجه به افزایش قابل توجه ارزش و اهمیت دارایی‌ها و داده‌های موجود در مراکز داده و پیرو آن افزایش انواع مختلفی از تهدیدهای امنیتی، استفاده از راهکارهای مدیریت و رصد امنیتی به ضرورتی اجتناب ناپذیر جهت افزایش امنیت و پایداری شبکه و سامانه‌های اطلاعاتی و ارتباطی تبدیل شده است.

مرکز عملیات امنیت[3] سامانه ای است که تمامی‌فعالیت‌های امنیتی شبکه را زیر نظر گرفته، رخدادهای امنیتی را جمع آوری و تحلیل کرده و مخاطرات امنیتی رخ داده و یا در حال وقوع را کشف کرده و اقدام مقتضی را صورت می‌دهد.رصد امنیتی یکپارچه و جامع شبکه علاوه بر اینکه موجب می‌شود در مقابل تهدیدات بهترین عکس العمل صورت گیرد؛ باعث می‌شود تا مدیران تحلیل دقیق تری از وضعیت

---

[1] Introduction Protection System

[2] Introduction Detection System

[3] Security Operation Center

امنیتی شبکه و میزان خطرپذیری آن داشته باشند. این روند نهایتاً منجر به اصلاح روش‌ها، سیاست‌ها و راهکارهای امنیتی و به طور کلی بهبود محسوس و قابل توجه امنیت خواهد شد.

فصل ۱

اهمیت و ضرورت مرکز عملیات امنیت

امروزه زیرساخت‌های اطلاعاتی سازمان‌های دولتی، شرکت‌های خصوصی و همچنین مراکز عمومی، داده‌های بسیار ارزشمندی را میزبانی می‌کنند و بسیاری از مراکز داده، خدماتی را به مشتریان و کاربران خود ارائه می‌کنند که چه بسا خرابی هرچند کوتاه و توقف ارائه خدمات توسط آن‌ها، باعث ایجاد خسارات مالی و اعتباری قابل توجه خواهد شد. از سوی دیگر انواع مختلفی از حملات و تهدیدها از حملات ویروس‌ها و کرم‌های اینترنتی گرفته تا حملات ممانعت از سرویس[۱] و نفوذ در شبکه همواره زیرساخت‌های اطلاعاتی را تهدید می‌کند. این تهدیدها می‌تواند لطمات و خسارات جبران ناپذیری را به داده‌ها و خدمات تحمیل کند.

با رشد روز افزون تهدیدهای امنیتی، اهمیت پرداختن به امنیت زیرساخت‌های اطلاعاتی بیشتر نمایان می‌شود. به همین دلیل طی سالیان اخیر راهکارهای امنیتی

[۱] Denial of Service

متعددی مورد توجه سازندگان، تولیدکنندگان، کاربرهای شبکه و مدیران سازمان‌ها و مراکز داده و همچنین محققان مراکز تحقیقاتی قرار گرفته است. تولید تجهیزات امنیتی به روز با قابلیت‌های پیشرفته تر و تجمیع برخی محصولات این حوزه به منظور مدیریت مؤثر تهدیدات و آسیب پذیری‌ها از جمله این راهکارها است.

روش‌های مورد اشاره عمدتاً، مبتنی بر حفاظت است و در آن‌ها سعی می‌شود با بکارگیری مکانیزم‌هایی جلوی حملات گرفته شود. آنچه در این میان توجه بدان دارای اهمیت است، این نکته است که اگرچه بکارگیری راهکارهای حفاظتی در جلوگیری از برخی حملات و تهدیدهای امنیتی مؤثر است، ولی به تنهایی تأمین کننده امنیت نخواهد بود. راهکاری که اخیراً مورد توجه قرار گرفته است، پیاده سازی مرکز عملیات امنیت است.

SOC یک سامانه رصد و مدیریت امنیتی یکپارچه است که با توجه به بهره مندی از مقداری هوشمندی امکان مدیریت حجم عظیم رویدادها و رخدادهای تولیدشده توسط دیگر راهکارهای حفاظتی را فراهم می‌آورد. سامانه مرکز عملیات امنیت می‌تواند حملات و تهدیدهای کشف شده را بی درنگ اعلان و ثبت کند. این اعلان می‌تواند از طریق واسط‌های مختلف از قبیل کنسول مرکز داده، به صورت صوتی، ارسال پست الکترونیکی و یا ارسال پیامک صورت گیرد. با اعلان خطر، کارشناسان مرکز عملیات و یا سایر مراکز مسئول می‌توانند وارد عمل شده و در کوتاه ترین زمان ممکن بهترین واکنش را به حمله یا تهدید نشان دهند. این واکنش می‌تواند شامل ریشه یابی حمله، جلوگیری از انتشار حمله و در صورت نیاز برگرداندن سامانه‌ها به وضعیت قبلی باشد.

اهمیت پیاده سازی SOC در زیرساخت‌های اطلاعاتی

امروزه راهکارهای حفاظت در مقابل حملات، تضمین کننده امنیت زیرساخت اطلاعاتی نیست. آنچه امروزه به نیاز اساسی تبدیل شده است، رصد امنیتی شبکه از طریق پیاده سازی یک مرکز عملیات امنیت است. پیاده سازی SOC در یک زیرساخت اطلاعاتی از جنبه‌های مختلف دارای اهمیت است. در ادامه این بخش به بررسی برخی از قابلیت‌های اساسی مرکز عملیات امنیت که باعث اهمیت یافتن پیاده سازی آن می گردد، خواهیم پرداخت.

- مدیریت مؤثر رخدادها

با افزایش حجم داده و خدمات میزبانی شده مراکز داده، میزان ترافیک دسترسی به این مراکز و به تبع آن میزان رخدادهای امنیتی تولید شده به شدت افزایش یافته است. به عنوان مثال کارگزارهای وب حجم بسیار زیادی از رخدادها را که مربوط به دسترسی کاربران به منابع کارگزار است ثبت می کنند.

فایروال‌ها، IDSها و مسیریاب‌های شبکه به صورت خودکار رخدادهای زیادی مرتبط با دسترسی کاربران (دسترسی‌های مجاز و دسترسی‌های غیر مجاز جلوگیری شده) را ثبت می کنند. رخدادهای تولیدی در فایل‌های متنی و یا باینری، بسته به سامانه مربوطه، ذخیره و نگهداری می‌شوند. البته فایل‌های رخدادها تنها منابع SOC نیستند. تغییر فایل های پیکربندی سامانه‌ها، تغییر سیاست‌های امنیتی، تغییر محتوای کارگزارهای وب، عبور متغیرهای رصد شده از آستانه‌های تعریف شده و سایر مؤلفه‌های زیرساخت اطلاعاتی که توسط ابزارهایی رصد می‌شوند نیز از منابع تولید رخداد به حساب می آیند.

هدف از مدیریت رخدادها، جمع آوری، تحلیل و گزارش آن‌ها است. مدیریت بهینه رخدادها از قابلیت‌های اصلی SOC است.

مدیریت رخدادها در یک شبکه با چالش‌های متعددی روبرو است. از جمله این چالش‌ها می‌توان به حجم بسیار زیاد رخدادهای تولیدی و همچنین پراکندگی و تنوع آنها اشاره کرد. SOC با جمع آوری رخدادها و انجام پیش پردازش و حذف رخدادهای تکراری و اضافی و تحلیل و بررسی همبستگی بین رخدادها، تعدادی رویداد[1] تولید می‌کند که این رویدادها می‌توانند نمایانگر حملات و یا تهدیدهای واقعی باشند. پیرو تولید و اعلان رویدادها مدیران امنیتی شبکه می‌توانند با بررسی و ردیابی حملات، واکنش نشان داده و از حملات و گسترش دامنه آن‌ها جلوگیری کنند و یا در صورت خسارت دیدن سامانه‌ها، آن‌ها را با استفاده از پشتیبان‌های تهیه شده به حالت قبلی برگردانند.

- رصد امنیتی متمرکز و بی درنگ ترافیک شبکه

داده‌ها و خدمات میزبانی شده در زیرساخت‌های اطلاعاتی از دارایی‌های اصلی آن‌ها محسوب می‌شود. حفاظت از داده و خدمات مرکز داده در مقابل انواع مختلف حملات از دغدغه‌های مهم مدیران سازمان‌ها و مراکز داده است. پیاده سازی SOC این امکان را ایجاد می‌کند که کلیه فعالیت‌های انجام گرفته در مرکز داده به صورت متمرکز و بی درنگ رصد شده و حملات و تهدیدها در کمترین زمان، کشف و اعلام شده و واکنش در کوتاه ترین زمان صورت پذیرد. مرکز عملیات امنیت با رصد بیدرنگ کل زیرساخت، این امکان را فراهم می‌سازد که قبل از وقوع بسیاری از حملات، سامانه‌های

[1] Incident

خطرپذیر شناسایی و اصلاحات لازم در شبکه و سامانه‌های زیرساخت انجام گردد.

- مدیریت مؤثر وصله‌های امنیتی و بروز رسانی نرم افزارها

سیستم‌های عامل، کاربردها و تجهیزات شبکه همواره دارای آسیب پذیری‌هایی هستند که معمولاً پس از کشف آن‌ها، وصله[1]های امنیتی جهت اصلاح توسط تولیدکننده‌ها و سازندگان تهیه و منتشر می‌گردد. برای داشتن یک زیرساخت امن اطلاعاتی انجام به موقع بروز رسانی کلیه نرم‌افزارها و به ویژه ضدبدافزارها، و اعمال وصله‌های امنیتی اهمیت بالایی دارد. به دلیل تنوع و کثرت تعداد کارگزارها، کاربردها، سیستم عامل‌ها و سایر نرم افزارها، بروزرسانی و اعمال وصله‌ها و مدیریت آن‌ها از کارهای مشکل در مدیریت امنیتی است. مدیریت وصله‌های امنیتی و همچنین بروز رسانی کلیه سیستم عامل‌ها و نرم افزارها از قابلیت‌های مهم SOC است.

- تحلیل ریسک شبکه

مدیران سازمان تا زمانی که اطلاعات دقیقی از میزان مخاطرات امنیتی شبکه خود نداشته باشند، نمی‌توانند گامی‌در جهت بهبود وضعیت امنیتی بردارند. مرکز عملیات امنیت با رصد سراسری شبکه و کلیه اجزای آن، و تحلیل و گزارش مشاهدات خود، اطلاعات دقیقی از وضعیت امنیتی شبکه و میزان ریسک آن ارائه می‌دهد. بر اساس گزارش‌های تولیدی توسط SOC می‌توان پیکربندی امنیتی تجهیزات، سامانه‌ها، کاربردها و همچنین سیاست‌های امنیتی را مورد بررسی و بازنگری قرار داده و در صورت نیاز راهکارهای حفاظتی را بهبود و یا ارتقاء بخشید.

---

[1] Patch

فصل ۲

اهداف، وظایف و اجزای مرکز عملیات امنیت

مرکز عملیات امنیت ابعاد امنیتی کل شبکه را از یک نقطه مرکزی رصد و اداره می‌کند، رویدادها را کشف و درجه بندی کرده و میزان ریسک هر رویداد، نقاط و دارایی‌های تحت حمله آن را بر اساس تجزیه و تحلیل اطلاعات دریافتی سامانه‌های مختلف امنیتی موجود در شبکه تعیین می‌کند. سپس گزارش و فرامین جزء به جزء مربوطه را به سطوح مختلف شبکه فرستاده و بدین ترتیب امکان یک مدیریت بی‌درنگ و بازرسی[۱] کامل را فراهم می آورد. وظیفه کلیدی SOC تهیه اطلاعات موقعیتی[۲] و ارائه تصویر متحد و جامع از وضعیت امنیت در شبکه بصورت لحظه ای است. SOC با جمع آوری اطلاعات از ابزارهای مختلف مستقر در سراسر شبکه و سپس همسان سازی این اطلاعات و یکپارچه کردن آن‌ها یک گزارش بلادرنگ از

---

۱ Audit

۲ Situational Awareness

آنچه در حال رخ دادن در شبکه است تولید می‌کند. مسئول شبکه می تواند با استفاده از این اطلاعات، حملات را پیش از آنکه آسیبی به شبکه بزنند مدیریت و پاسخدهی کند.

اهداف پیاده سازی مرکز عملیات امنیت

بطورکلی در راه اندازی هر مرکز عملیات امنیت اهداف زیر دنبال می‌شود.

۱. برخورد مناسب و مؤثر با رویدادهای امنیتی و تأمین امنیت شبکه در مقابل تهدیدهای احتمالی
۲. ارتقاء امنیت و پایداری داده‌ها و خدمات بوسیله حفاظت از زیرساخت‌های اطلاعاتی، ترافیک، سرویس‌ها و داده‌های مشتریان
۳. کاهش زمان اختلال در ارائه خدمات به مشتری
۴. بهبود و تسریع در پاسخ‌ها و واکنش‌های امنیتی
۵. بهبود کارآیی شبکه
۶. کاهش هزینه‌های ناشی از تهدیدها و حملات امنیتی

SOC جهت نیل به اهداف بیان شده، خدمات ذیل را ارائه می‌کند.

۱. مدیریت و رصد بلادرنگ ترافیک شبکه، فایروال‌ها، IDSها،IPSها، کارگزارها، کاربردها، ضدبدافزارها و دیگر اجزای شبکه
۲. تحلیل رویدادها، رخدادهای امنیتی، اطلاعات آسیب پذیری‌ها[۱] و اعلام خطر فوری
۳. واکنش فوری به تهدیدهای بالقوه و رفع سریع مشکل
۴. حفاظت از ترافیک شبکه، کارگزارها و کاربردهای سازمان و مشتریان آن در مقابل حملات و تهدیدها

[۱] Vulnerabilities

۵. تهیه و ارائه انواع گزارش‌های امنیتی در سطوح فنی و مدیریتی

ساختار و وظایف مرکز عملیات امنیت

رخدادهای امنیتی در یک زیرساخت اطلاعاتی توسط حسگرهای شبکه آن تولید می‌گردند. حسگرهای شبکه شامل کلیه سیستم عامل‌ها، کاربردها، نرم افزارها و تجهیزات سخت افزاری شبکه است. رخدادهای امنیتی به روش‌های مختلف از حسگرها جمع آوری و با قالب یکسانی در بانک اطلاعاتی رخدادها ذخیره می‌گردند. رخدادهای جمع آوری شده توسط تحلیلگر SOC مورد تحلیل قرار گرفته و پس از بررسی همبستگی بین رخدادها، حملات و تهدیدهای امنیتی زیرساخت اطلاعاتی مربوطه به صورت رویداد اعلام می‌شود.

تحلیلگر SOC جهت تحلیل و تشخیص همبستگی مابین رخدادها از دانش ذخیره شده در پایگاه دانش مرکز عملیات امنیت بهره می‌برد. معیار اصلی کشف حملات و تهدیدها، اطلاعات پایگاه دانش است. اطلاعات مربوط به آسیب‌پذیری‌های سامانه، سیاست‌های امنیتی تعریف شده و همچنین وضعیت فعلی سامانه‌ها از اطلاعات مهم ذخیره شده در پایگاه دانش است که توسط واحدی در SOC باید به طور مرتب بروز شود.

در بالاترین لایه مرکز عملیات امنیت که کاربر SOC با آن سروکار دارد، پورتال و کنسول قرار دارد. پورتال به صورت داشبورد SOC عمل کرده و امکان مشاهده و مرور وضعیت امنیتی زیرساخت اطلاعاتی بصورت گرافیکی، تهیه انواع مختلفی از گزارش‌ها و همچنین تنظیم مؤلفه‌های SOC را فراهم می‌سازد. در ادامه این بخش عملکرد و وظایف هر یک از بخش‌های اصلی سامانه SOC را مورد بررسی قرار می‌دهیم.

- حسگرها

حسگرها در SOC منابع جمع آوری رخدادهای امنیتی هستند. از جمله حسگرهای مهم و معمول جهت جمع آوری رخدادها می‌توان به IDSها، IPSها، فایروال‌ها، تجهیزات شبکه شامل سوئیچ‌ها و مسیریاب‌ها، سیستم‌عامل‌ها، سرویس‌های اینترنت و ضدبدافزارها اشاره کرد.

IDSها بسته‌های عبوری از شبکه را شنود کرده و با تحلیل بسته‌های شنود شده بر اساس الگوی حملات شناخته شده و یکسری قواعد، برخی از حملات، تهدیدها و وضعیت غیرعادی در شبکه مرکز داده را کشف و نتایج را به صورت رخدادهایی ثبت می‌کنند. یک IDS، روزانه حجم زیادی از رخدادها را تولید می‌کند. به عنوان مثال، در یک مرکز داده ممکن است به طور متوسط روزانه چندین میلیون رخداد توسط IDS تولید شود، که بخش عمده آنها بلا استفاده خواهد بود. بررسی این حجم عظیم رویدادهای تولیدشده توسط IDSها و کشف حملات و تهدیدهای واقعی از چالش‌های بزرگ مدیریت امنیتی مراکز داده است.

فایروال‌ها به منظور کنترل دسترسی به منابع، بر اساس قواعد و سیاست‌های امنیتی تعریف شده به پایش بسته‌های شبکه می‌پردازند. این دستگاه‌ها رخدادهای مربوط به پایش ترافیک شبکه را ثبت می‌کنند. این رخدادها یکی از منابع مهم جمع آوری داده در SOC هستند. البته امروزه به دلیل پیچیده شدن روش‌های حملات، معمولاً مهاجمان، فایروال‌ها را دور می‌زنند. با این حال اطلاعات ثبت شده توسط این تجهیزات هنگامیکه در کنار سایر اطلاعات قرارگرفته و تحلیل می‌شود، به کشف حملات توسط SOC کمک می‌کند.

منبع دیگر جمع آوری رخدادهای امنیتی، تجهیزات شبکه هستند. از آنجا که تمام ترافیک یک شبکه از سوئیچ‌ها و مسیریاب‌های اصلی می‌گذرد، مؤلفه‌های مختلف مدیریتی بر روی این تجهیزات قابل دسترسی هستند و از ابزارها و معیارهای مهم کشف بسیاری از حملات هستند.

سیستم عامل‌ها، کاربردها و نرم افزارهای مختلف نصب شده بر روی کارگزارها انواع مختلفی از رخدادها را تولید می‌کنند. اطلاعات مربوط به دسترسی کاربران به منابع، احراز هویت کاربران، تغییرات پیکربندی، خطاهای رخ داده و غیره، توسط این منابع ثبت می‌شوند.

- واحد تجمیع رخدادها

جمع آوری رخدادهای امنیتی از حسگرها توسط این واحد انجام می‌شود. بطورکلی این واحد رخدادها را از منابع مختلف و با استفاده از روش‌ها و پروتکل‌های مربوطه جمع آوری و پس از انجام عمل پیش پردازش و پایش، آنها را در بانک اطلاعاتی رخدادها ذخیره می‌کند. از آنجاکه رخدادهای مربوط به حسگرهای مختلف دارای قالب‌های متفاوتی هستند، قبل از ذخیره شدن توسط واحد تجمیع رخدادها به قالب یکسانی تبدیل می‌شوند.

- واحد تحلیل و تشخیص همبستگی رخدادها[1]

هر یک از سامانه‌های یک زیرساخت اطلاعاتی، روزانه حجم بسیار زیادی از رخدادها را تولید می‌کنند که لزوماً تمامی آنها به طور مستقیم یا غیرمستقیم به مسائل امنیتی مربوط نمی‌شوند. با افزایش تعداد کارگزارها، خدمات و در نتیجه ترافیک شبکه، بررسی بی‌درنگ رخدادهای تولیدشده توسط نیروی انسانی غیر ممکن می‌شود. تنها راه حل پیش‌رو، انتقال دانش و مهارت‌های کارشناسان امنیتی خبره به یک برنامهٔ هوشمند است که بتواند با تحلیل گزارش‌ها و رخدادهای دریافتی از اجزای موجود، اقدام به تشخیص حملات و تهدیدها و یا خلاصه کردن رخدادها کند، همچنین در صورت تشخیص هر نوع حملهٔ احتمالی بتواند نسبت به آن واکنش مناسب نشان دهد. این واکنش بسته به شرایط، ممکن است تغییر در پیکربندی یک فایروال یا مسیریاب، از کار انداختن موقت یک یا چند سامانه و یا سرویس، و یا اعلان خطر از طریق روش‌های ارتباطی تعبیه شده در سامانه (مانند پست الکترونیک،پیامک، ارتباط تلفنی، اخطار صوتی و ...) باشد.

---

[1] Correlation که بصورت «برقراری یا پیدا کردن ارتباط میان موجودیت‌ها» تعریف می‌شود، روشی شناخته شده در امنیت اطلاعات است که با ترکیب اطلاعاتی که از منابع مختلف بدست می‌آورد، کارایی فرآیند تحلیل و شناسایی تهدیدها را بهبود می‌بخشد

این واحد در مرکز عملیات امنیت، وظیفه تحلیل رخدادهای جمع‌آوری شده از سراسر زیرساخت اطلاعاتی را بر عهده دارد. تحلیل رخدادها به منظور کشف تهدیدها، بر اساس اطلاعاتی است که در پایگاه دانش ذخیره و نگهداری می‌شود.

روش‌ها و الگوریتم‌های تحلیل رخدادها و تشخیص حملات، در حال حاضر از موضوعات روز تحقیقاتی در سراسر دنیا است. از آنجا که هر کدام از الگوریتم‌های تحلیل و Correlation دسته‌های خاصی از حملات را تشخیص می‌دهند، باید ماژول‌های متعددی جهت تحلیل رخداد در SOC طراحی و پیاده سازی گردد. سامانه SOC باید همواره امکان اضافه کردن ماژول جدید تحلیل را به سهولت فراهم کند.

زیرسامانه دیگری در واحد تحلیل رخدادها وجود دارد که وظیفه واکنش به رویدادهای تولید شده را بر عهده خواهد داشت. این زیر سامانه نسبت به برخی از رویدادهای امنیتی کشف شده توسط موتورهای تحلیل، درصورت اضطرار و بر اساس قواعد تعریف شده در SOC، واکنش‌های لازم رانشان می‌دهد.

- واحد مدیریت وصله‌ها و مرور پیکربندی

یکی از وظایف مهم مرکز عملیات امنیت، مدیریت مؤثر وصله‌های نرم‌افزاری و همچنین پیکربندی وضعیت فعلی کلیه سامانه‌ها است.

آسیب‌پذیری‌های امنیتی مربوط به سیستمعامل‌ها و همچنین کاربردهای مختلف پس از کشف آنها توسط تولیدکننده با ارائه وصله نرم افزاری ترمیم می‌شود. مدیریت صحیح وصله‌ها و اعمال به موقع آن‌ها، علاوه بر اینکه درجه امنیتی سامانه‌ها را ارتقا می‌بخشد، کشف

حملات و تهدیدات در فرآیند تحلیل رخدادها و همچنین واکنش به رویدادهای تولید شده توسط مدیران امنیتی را بهبود می‌بخشد.

علاوه بر مدیریت وصله‌ها، مدیریت پیکربندی و نگهداری آخرین وضعیت سامانه‌ها (مشخصات سخت افزاری، سیستم عامل، سرویس‌های فعال ، نرم افزارهای نصب شده ، پورت‌های باز و پیکربندی) نیز از وظایف این واحد SOC است. وضعیت سامانه‌ها به عنوان دانش در تحلیل رخدادها مورد استفاده قرار می‌گیرد. از آنجا که کلیه پیکربندی اجزاء و همچنین آخرین وضعیت سامانه‌ها توسط این واحد بروز و نگهداری می‌شود، امکان مرور اطلاعات آن‌ها از طریق پورتال SOC فراهم خواهد بود. این اطلاعات جهت کشف ریشه حملات و آسیب‌های امنیتی و همچنین انجام بهترین واکنش هنگام وقوع رویدادهای امنیتی بسیار سودمند خواهد بود.

پیاده سازی سامانه مدیریت مؤثر وصله‌ها در SOC به دلایل متعددی دارای اهمیت است: نخست اینکه حجم بالای وصله‌هایی که منتشر می‌شوند، عملاً کنترل دستی آنها را ناممکن میکند. دوم اینکه فرآیند استفاده از یک وصله جدید پیچیده بوده و شامل مراحل ارزیابی، دریافت، آزمایش، نصب و نگهداری وصله است که مدیریت کل این فرآیند به صورت دستی خطازا خواهد بود. سوم اینکه سرعت از ملزومات مدیریت وصله‌های منتشر شده است، چراکه نفوذگران بسرعت از رخنه‌های امنیتی کشف شده سوءاستفاده می‌کنند و باید این زمان را از آنان گرفت.

- واحد پورتال و کنسول

به طور کلی پورتال و کنسول مرکز عملیات امنیت وظایفی از قبیل اعلان بی درنگ رویدادهای امنیتی، تنظیم پارامترهای مربوط به هر کدام از زیر سامانه‌های SOC و تهیه انواع مختلف گزارش‌ها از وضعیت امنیت شبکه، رخدادها و رویدادهای امنیتی تولید شده و همچنین گزارش‌های تحلیل مخاطرات امنیتی را بر عهده دارد.

فصل ۳

ویژگی‌های ساختاری مرکز عملیات امنیت

تعیین و انجام عکس‌العمل صحیح و به موقع از مهمترین دلایل راه اندازی سامانهمرکز عملیات امنیت و یکی ازموضوعاتمهم در زمان طراحی آن است. مرکز عملیات امنیت باید ویژگی‌های عمومی‌زیر را داشته باشد.

مقیاس پذیری

امروزه به طور معمول در یک مرکز داده با اندازه متوسط روزانه چندین میلیون رخداد تولید می‌شود. بنابراین پارامتر مقیاس پذیری باید در طراحی مرکز عملیات امنیت و بخش‌های مختلف آن مورد توجه قرار گیرد. سامانه SOC باید به نحوی طراحی گردد که با افزایش میزان ترافیک و رخدادهای تولیدی، بتواند با کارآیی بالا وظیفه خود را انجام دهد.

ماژولار بودن

کارگزارها، خدمات، کاربردها و تجهیزات شبکه منابع جمع آوری رخدادها در سامانه SOC هستند. این منابع معمولاً در زیرساخت‌های مختلف، متنوع و گوناگون بوده و در طی زمان افزایش یافته و یا جایگزین می‌شوند. بنابراین، منابع جمع آوری رخدادها در یک مرکز عملیات امنیت در دوره‌های زمانی مختلف دچار تغییر و تحول می‌گردند. SOC باید به نحوی طراحی شود که براحتی بتوان منابع و الگوریتم‌های تحلیل و همبستگی جدید را به سامانه اضافه کرد و یا تغییر داد. به طور کلی باید طراحی ماژولار در کلیه بخش‌ها و زیرسامانه‌های مرکز عملیات امنیت مورد توجه قرار گیرد.

کارآیی بالا

هدف از طراحی و پیاده سازی مرکز عملیات امنیت در یک زیرساخت اطلاعاتی نظارت بر امنیت کل شبکه (امنیت داده‌ها ، امنیت خدمات و غیره) وکشف حملات و تهدیدهای واقعی در کوتاهترین زمان ممکن است. به این منظور SOC باید پوشش کاملی روی زیرساخت مربوطه داشته باشد. بدین معنی که تمام اجزای شبکه شامل کلیه کارگزارها، نرم افزارها، تجهیزات و ترافیک شبکه را رصد و همچنین الگوریتم‌های تحلیل، همبستگی و همچنین اطلاعات مربوط به آسیب‌پذیری‌ها، الگوی حملات، سیاست‌های امنیتی و وضعیت سامانه‌ها را بروز کند.

امنیت

از آنجا که هدف SOC تأمین و تضمین امنیت و پایداری داده و خدمات است، پیاده سازی آن نباید خود منجر به بروز مخاطرات امنیتی جدید در بستر اطلاعاتی گردد. لذا لازم است که در تمام بخش‌های SOC مسائل امنیتی مورد توجه جدی قرار گیرد. با توجه به دسترسی مرکز عملیات امنیت به کلیه تجهیزات امنیتی، ترافیک و سیاست‌های شبکه و اجزای آن، استفاده از دانش و سامانه‌های بومی‌و مطمئن در طراحی و پیاده سازی آن در زیرساخت‌های کشور از اهمیت قابل توجهی برخوردار است. از نکات مهم در طراحی و پیاده سازی مرکز عملیات امنیت می‌توان به موارد ذیل اشاره کرد.

۱. جمع آوری رخدادها از منابع مختلف باید از طریق کانال‌های امن صورت گیرد.
۲. حتی المقدور باید از نصب عامل‌ها بر روی سامانه‌ها جهت جمع‌آوری رخدادها اجتناب کرد. چرا که خود عامل‌ها می‌توانند باعث بوجود آمدن شکاف‌های امنیتی در سامانه‌ها گردند.
۳. نگهداری رخدادها، رویدادها، پیکربندی سامانه‌ها، سیاست‌های امنیتی و دسترسی به آنها باید کاملاً امن باشد.
۴. دسترسی کاربران به پورتال باید بر اساس نقش آن‌ها بوده و تمامی‌فعالیت‌های انجام گرفته توسط هر کاربری باید ثبت گردد.

ارتباط با گروه‌های واکنش هماهنگ رویدادهای رایانه ای

از دیگر ویژگی‌های حائز اهمیت ارتباط و همبستگی مرکز عملیات امنیت و مراکز امداد و نجات رایانه ای و گروه‌های واکنش هماهنگ رویدادهای رایانه ای است، به گونه‌ای که مرکز عملیات امنیت جهت بروز رسانی و جامع کردن پایگاه دانش خود از خروجی‌های حاصل از اقدامات مراکز امداد ونجات رایانه ای استفاده می‌کنند و مراکز امداد و نجات رایانه ای نیز جهت تحلیل و کشف حوادث و حملات روز نیازمند اطلاعات جامعی هستند که تنها از طریق مراکز عملیات امنیت بدست می‌آید.