مهر ماه ۱۴۰۱

طراحی هوشمندانه مرکز عملیات امنیتی درسازمان ها

ترجمه شده توسط شرکت مهندسی امن ارتباط سینداد

www.sindadsec

فهرست

مقدمه

در عصر ارتباطات، داده‌ها و اطلاعات ارزش بسیاری پیدا کرده‌اند. درحالی که هدف تبهکاران در قرن گذشته سرقت از بانک بود، در حال حاضر اطلاعات و داده‌های بااهمیت موردتوجه ویژه تبهکاران سایبری است. امروزه تکنیک‌هایی مانند مهندسی اجتماعی و جعل عمیق (Deepfake)، به مجموعه تهدیدهای سایبری پیوسته‌اند و باهدف نفوذ به زیرساخت‌های سازمان‌ها، همه دارایی‌ها، از جمله سرورهای ایمیل و حتی گوشی‌های موبایل را به مخاطره می‌اندازد. از همین رو امنیت داده‌ها مستلزم به‌کارگیری یک رویکرد جامع در سطحی‌ترین و عمیق‌ترین لایه‌های عملیاتی سازمان‌ها است.

فناوری‌های پیشتاز در دنیای امروز، از ابتدا تا کنون تغییرات زیادی را به خود دیده و زندگی و کسب‌وکار ما را دگرگون ساخته‌اند.عملیات امنیتی در سازمان‌ها می‌بایست مبتنی بر راهکارهای برجسته و یکپارچه امنیت سایبری باشد و در جهت انهدام انواع تهدیدها و چالش‌های امنیتی به کار گرفته شود.

باتوجه به تمام نکات امنیتی، اهمیت راه اندازی مرکز عملیات امنیتی (SOC) ضرورت بالایی دارد.

SOC ها بخش جدایی ناپذیری از تلاش بی وقفه سازمان‌ها در جهت مبارزه با تهدیدها به شمار می روند؛ اما میان آن‌ها و سیستم‌های نرم‌افزاری و سخت‌افزاری در سازمان‌ها باید حریمی ایجاد شود. SOC از یک تیم متخصص و متمرکز همراه با ابزارهای امنیتی ضروری تشکیل شده است و وظیفه تیم عملیاتی در وهله اول شناسایی انواع آسیب پذیری‌های محیط سازمان و در وهله دوم مقابله با تهدیدها از طریق تشخیص، تجزیه و تحلیل و پاسخ‌دهی فوری است.

متخصصان امنیت اطلاعات بر ضرورت راه‌اندازی این راهکار امنیتی جامع (SOC) در سازمان‌ها تاکید دارند. در سال ۲۰۱۹، یکی از موسسات بین المللی و معتبر در امور مشاوره و تحقیق امنیت سایبری پیرامون مطالعات خود در عوامل موثر بر بازدهی مرکز عملیات امنیتی، از مخاطبان پرسید:"در سازمان شما سامانه SOC تا چه اندازه اهمیت داشته؟" نزدیک به ۶۷ درصد آن‌ها پاسخ دادند که SOC برای سازمان آن‌ها یک سیستم با اهمیت به حساب آمده، و ۲۷ درصد دیگر نیز این سامانه را برای ادامه فعالیت خود حیاتی و ضرورت تلقی کرده اند. مطالعات پیشرو، میزان اهمیت راهکارهای امنیت سایبری و نیز خود مرکز عملیات امنیتی (SOC) را نزد متخصصان امنیتی روشن نموده است.

با این حال، صرفاً توجه سطحی به این موضوع پراهمیت کفایت نمی کند، زیرا سازمان‌ها همواره با شمار بالایی از چالش‌های امنیتی مواجه بوده اند که روز به روز در حال افزایش هستند.

راهبران عملیات امنیتی (SecOps) در گزارش‌ها امنیتی خود متذکر چالش‌های زیر شده اند:

- منابع در دسترس تیم امنیتی برای جلوگیری از نفوذ کافی نیستند.
- تهدیدهای مخفی و ناشناخته جدید با ابزارهای قدیمی قابل تشخیص نیستند.
- در دست‌نداشتن یک متخصص مستعد که همواره دانش خود را بروز رسانی نماید.
- بهینه‌سازی SOC بر روی زیرساخت‌های غیریکپارچه و ناهماهنگ با چالش مواجه است و نزدیک به ۸۰ درصد SOC های فعلی این مشکل را دارند.
- کشف اطلاعات و داده‌های نهفته در محیط شبکه سازمان از دشوارترین مشکلات بوده و ۵۵ درصد اکثر سازمان‌ها دارای حجم بالایی از این قبیل داده‌های نهفته هستند.

چالش‌های ذکر شده، تنها مشکلات متخصصان مرکز عملیات امنیتی نیست. برای نمونه، سازمان‌ها برای تعویض سخت‌افزارهای قدیمی و به کارگیری فناوری‌های پیشرفته با نبود بودجه کافی مواجه هستند. سایر چالش‌ها عبارتند از؛ عدم توجه تیم امنیتی به اهداف امنیتی سازمان، انتخاب سیستم‌های نامناسب، فقدان عملیات گردش کارهای مقیاس پذیر و نیز ناکافی بودن مهارت های امنیتی.

در این مقاله، نگاهی خواهیم داشت به اینکه چگونه می‌توان به‌صورت موثر SOC سازمان را بهبود بخشید، تیم امنیتی را بر روی اهداف اصلی متمرکز کرد و چگونه می‌توان فرایندهای متداول سیستم و انجام دستی عملیات امنیت را خودکارسازی کرد و یادگیری ماشین چگونه در اولویت بندی وظایف یاری رسانی می‌کند.

راهکار مدیریت رخدادها و اطلاعات امنیتی(SIEM)

رکن یکم، داشتن یک مرکز عملیات امنیتی یا SOC هوشمند، و استفاده از سامانه SIEM است. ۵ دلیل کلیدی برای نصب SIEM در مرکز عملیات امنیتی یک سازمان وجود دارد:

- ضعف مهارتی میان اعضای تیم را کاهش می‌دهد.
- فرایندهای تشخیص و پاسخ‌دهی را سرعت می‌بخشد.
- SIEM داده‌های دریافت شده از سیستم‌های مختلف، مانند برنامه‌ها و حساب‌های کاربری را به اطلاعاتی ارزشمند برای سازمان تبدیل می‌کند.
- نظارت لحظه‌ای را به منظور تشخیص تهدید، تجزیه و تحلیل رخداد و پاسخ‌دهی سریع، فراهم می‌کند.
- عملیات تیم امنیتی SOC را سهولت بخشیده و بوسیله پلتفرم متمرکز، موارد گردش کار مقیاس پذیر و داشبوردهای از پیش تعبیه شده را به کار می‌گیرد.

۱-مدیریت از طریق گردشکار و رفع حفره‌های امنیتی

اکثر تیم‌های عملیات امنیت سازمان به ابزارهای امنیتی متعددی متکی هستند که اعلان‌های کاذب و پیکربندی نامناسبی را ارائه می‌دهند. کارشناسان متخصص برای مدیریت و اولویت‌بندی رخدادهای ورودی باید وقت و انرژی زیادی را صرف کنند. این شیوه نیازمند تمامی مهارت‌های فنی، مهارت‌های نرم و خلاقانه است و پیداکردن افراد متخصص این زمینه دشوار است.

لایه ۱ مرکز عملیات (Tier ۱ SOC)، مستلزم دانش پایه‌ای و تخصصی از دانش شبکه و درک بالا از لایه‌های مختلف پروتکل‌ها است. اعضای تیم مرکز عملیات امنیتی در این لایه، به پرسمان پایگاه‌های داده، کدنویسی یا اسکریپت‌نویسی و نیز بررسی پایبندی به مقررات و سیاست‌های اجرایی و امنیتی پرداخته و توانایی عیب‌یابی و رصد آسیب‌پذیری و تجزیه‌وتحلیل اولیه امنیتی را نیز دارند.

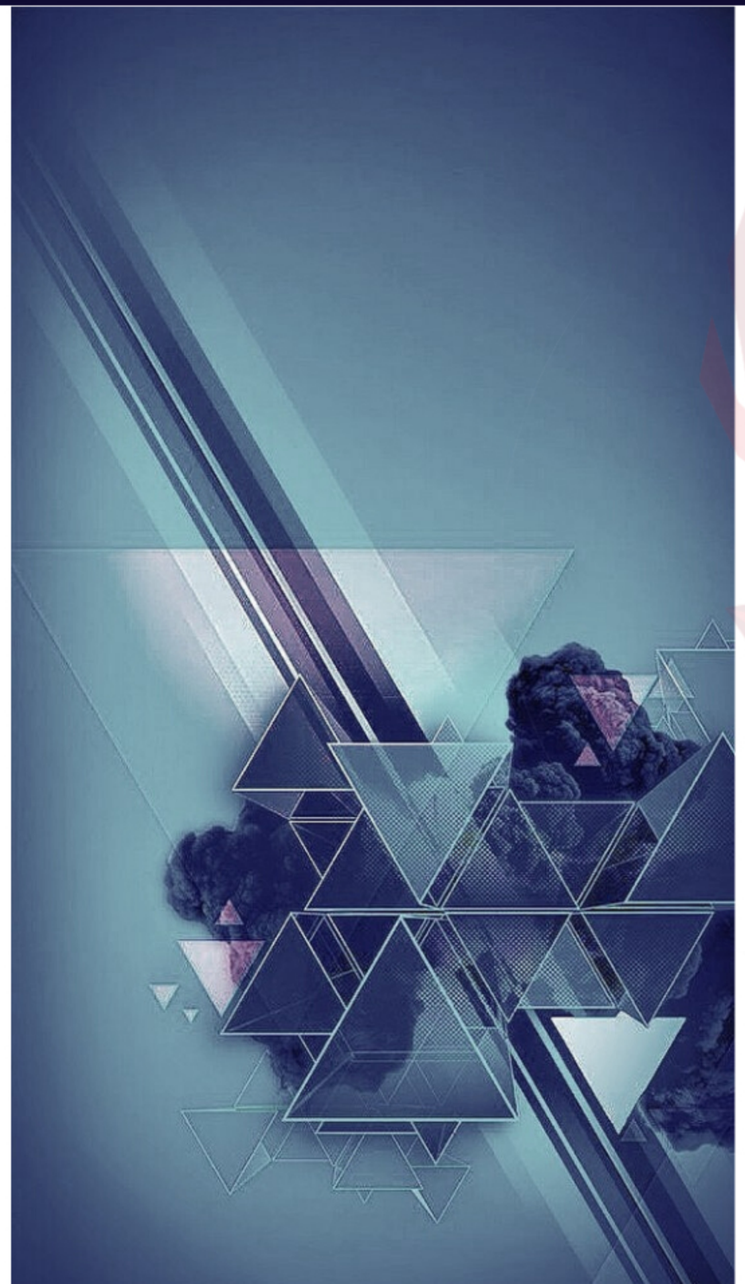
لایه ۲ مرکز عملیات (Tier ۲)، مستلزم دانش همه‌جانبه در سیستم‌عامل‌های لینوکس و ویندوز، آشنایی با مفاهیم و دستورهای خط فرمان و مهارت استفاده از ابزارهای شناسایی و توانایی عیب‌یابی است.

نیروهای امنیتی مجاز در این لایه SOC، باید دارای گواهینامه‌های معتبر امنیتی و برخوردار از مهارت تجزیه‌وتحلیل حرفه‌ای، ارتباطاتی و نوشتاری باشند.

اگر فکر می‌کنید پیداکردن این افراد خبره کار ساده‌ای است، لازم است دقت بفرمایید. طبق سالنامه رسمی CYBERSECURITY VENTURES در ارتباط با مشاغل حوزه امنیت سایبری، پیش‌بینی شده که در سال ۲۰۲۱ حدود ۳/۵ میلیون شغل در این حوزه فعال خواهد بود که این رقم در سال ۲۰۱۴، حدود ۱ میلیون نفر تخمین زده می‌شد. به همین خاطر بهینه‌سازی مرکز عملیات امنیتی، از ضروری‌ترین ماموریت‌های هر سازمان در راستای تأمین امنیت است.

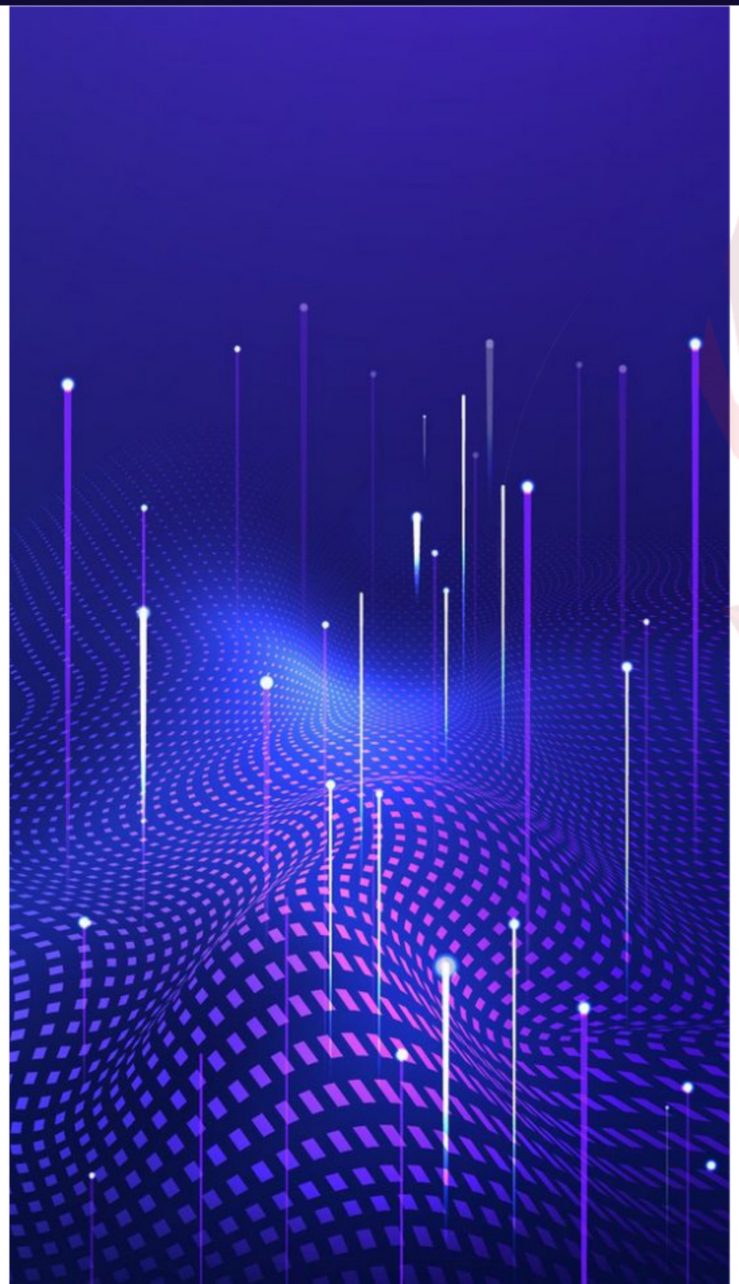
SIEM تیم امنیت را قادر به استفاده از گردشکارهای مدیریت شده و مقیاس‌پذیر می‌کند. همچنین، استفاده از SOAR، می تواند وظایف امنیتی نیروهای TIER ۱ را تا حد زیادی خودکارسازی کند و بدین ترتیب نیروها می‌توانند زمان خود را بیشتر صرف تجزیه‌وتحلیل رخدادهای بااهمیت کنند.

۲- تشخیص و پاسخ فوری



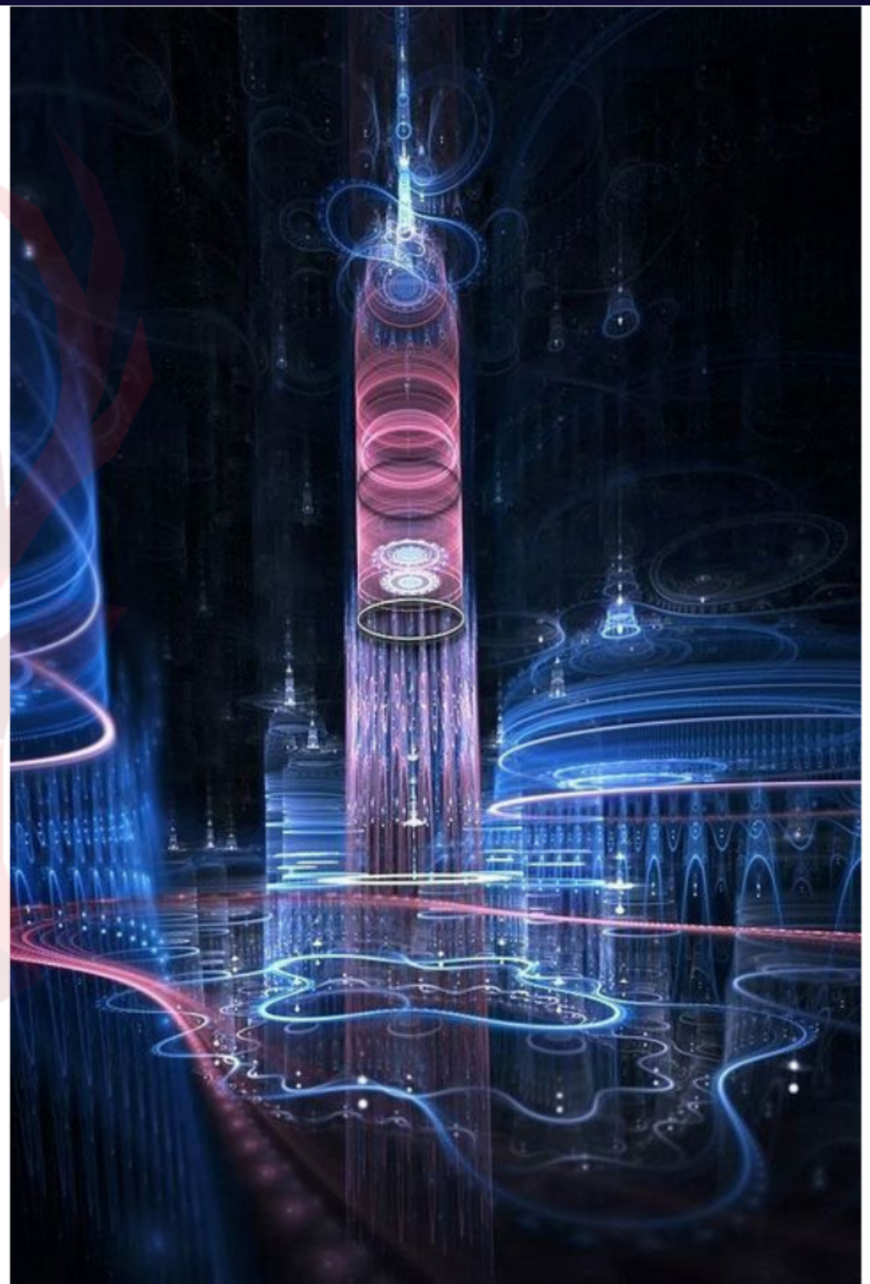
در عملیات روزانه هر سازمان، انبوهی از اطلاعات و داده‌ها تولید می‌شود که مدیریت این حجم از داده‌ها کار چندان ساده ای نیست. همچنین، استخراج اطلاعات کلیدی و استفاده موثر از آن‌ها کار دشواری است و از طرفی تهدیدهای امروزی در حمله های پی در پی خود به سازمانها، از تکنیک‌های پیچیده‌تری استفاده می‌کنند. نحوه‌ی صحیح تقابل با این تهدیدها سرعت بالا در رصد و بررسی داده‌ها است و در غیر این صورت، تمام سطوح مهم سازمان آلوده خواهد شد. فرآیند خودکارسازی نقش مهمی در مقابله با این چالش ایفا می‌کند و با حذف کارهای بدیهی و تکراری در جهت آسودگی تیم امنیتی باعث میگردد تیم SOC با تمرکز و زمان بیشتر به فعالیتهای مهم و با اولویت بالاتر بپردازد.

۳ – گردآوری و تجزیه‌وتحلیل داده‌های سراسر سازمان



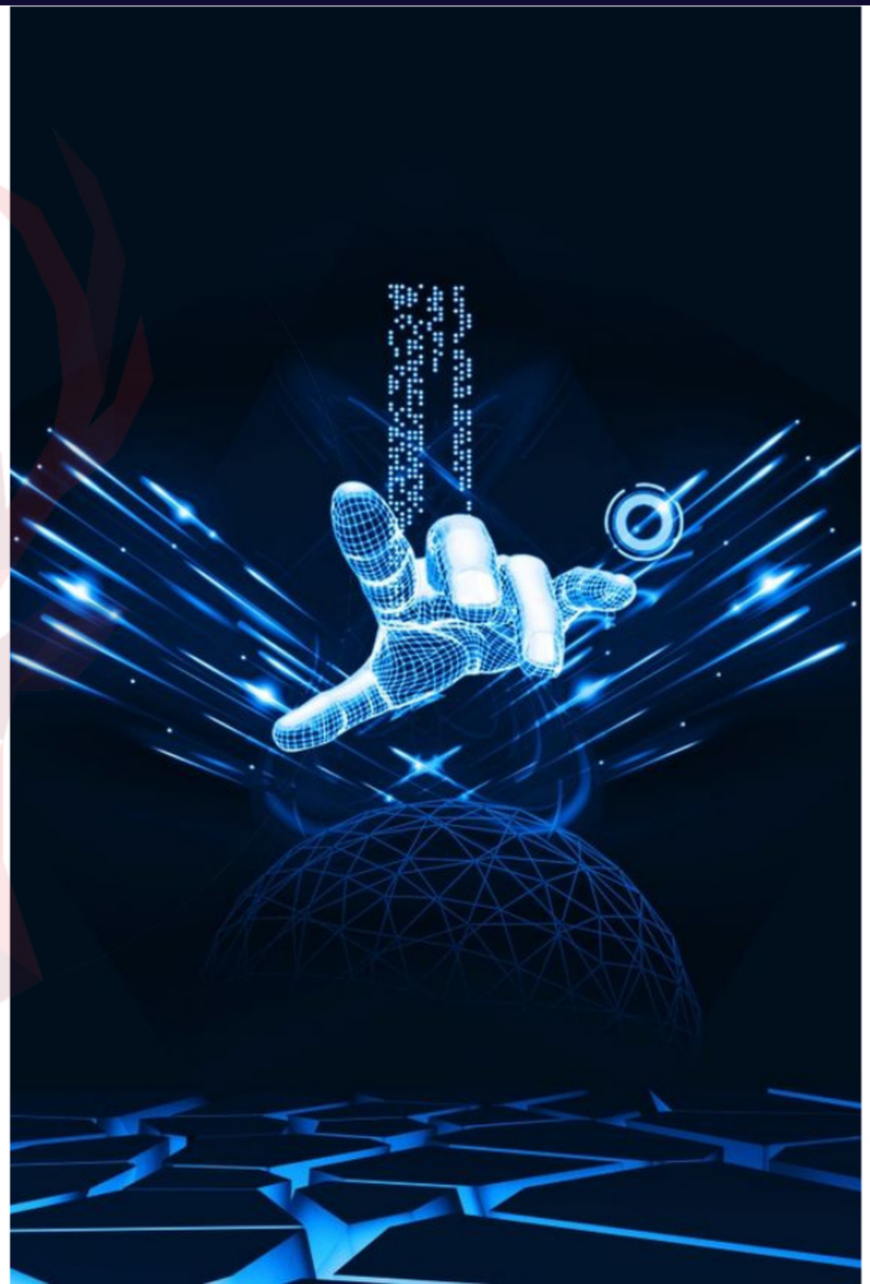
راه‌اندازی یک SOC ابری یا مدیریت شده و یکپارچه در سازمان موجب تقویت مرکز عملیات امنیتی سازمان می‌شود. SIEM در همین راستا، با دریافت و بکارگیری تمام داده‌ها و لاگ‌های خام سازمان از بخش‌های مختلف آی‌تی، اداری، سیستم‌های امنیتی، برنامه‌ها، تجهیزات و سایر موارد، تیم امنیتی را بوسیله‌ی اعلان‌های تخصصی، دقیق و در عین حال ساده از وجود تهدیدها آگاه می‌سازد. فرآیندهای تشخیص، مدیریت، بررسی، جستجو و متوقف‌سازی تهدیدها و رخدادها توسط SIEM سازمان‌دهی می‌شوند. برخی اعلان‌های امنیتی لازم است توسط نیروهای انسانی متخصص بررسی شوند و باقی آن‌ها بوسیله فناوری‌های امنیتی به انجام می رسند. حال، با ادغام قابلیت‌های ذکر شده در راهکار SIEM، سازمان‌ها می‌توانند توانایی‌های تشخیص و پاسخ به تهدیدهای امنیتی را تا حد زیادی افزایش دهند.

۴ – نظارت با سرعت بالا



هم‌زمان با رشد تجارت شما، نیاز است چشم‌انداز امنیتی شما برای مدیریت تهدیدهای جدید و ناشناخته وسعت یابد. SIEM با تجزیه و تحلیل فوری، کمک ویژه‌ای به تیم SOC می کند، که در ابتدا لازم است به ترافیک شبکه و داده‌های منابع در معرض نفوذ دسترسی پیدا کند. SIEM به عنوان بخش مهمی از SOC می‌تواند بر عمده فعالیت‌های امنیتی نظارت کند و رخدادها را مرتب و یکپارچه سازی و هشدارها را از لحاظ اعتبار سنجیده و اولویت بندی کند، و در نهایت تیم امنیتی را قادر می سازد که بهترین راه حل را پیاده سازی کند.

۵ –احداث و ایجاد گردشکار ها و داشبوردهای حرفه‌ای



کارکرد SOC به کیفیت اطلاعاتی جمع‌آوری شده بستگی دارد. تیم‌های مرکز عملیات امنیتی باید نگرشی درست از وضعیت امنیتی سازمان در دست داشته باشند و داده‌های ترافیک را به‌درستی تجزیه و تحلیل کنند. ضرورت گردش‌کارها و داشبوردها در این بخش نمایان می‌شود. مسائلی از جمله؛ پیچیدگی تاکتیک‌های تهدید، یکپارچه سازی سیستم‌های امنیتی، حجم کار اضافی تیم، عدم هماهنگی با سیاست‌های سازمان و فقدان یک راهبر ارشد SOC، همگی از جمله چالش‌هایی هستند که تیم مرکز عملیات امنیتی با آن‌ها مواجه می‌شود. تجمیع و نگهداری اطلاعات تولید شده، گردش‌کار مقیاس پذیر و محیط‌های مدیریتی کاربر پسند، از مهمترین قابلیت‌های یک SIEM حرفه‌ای است که بهره برداری از داده‌های خام و برنامه‌ریزی امنیتی را تسهیل می کند.

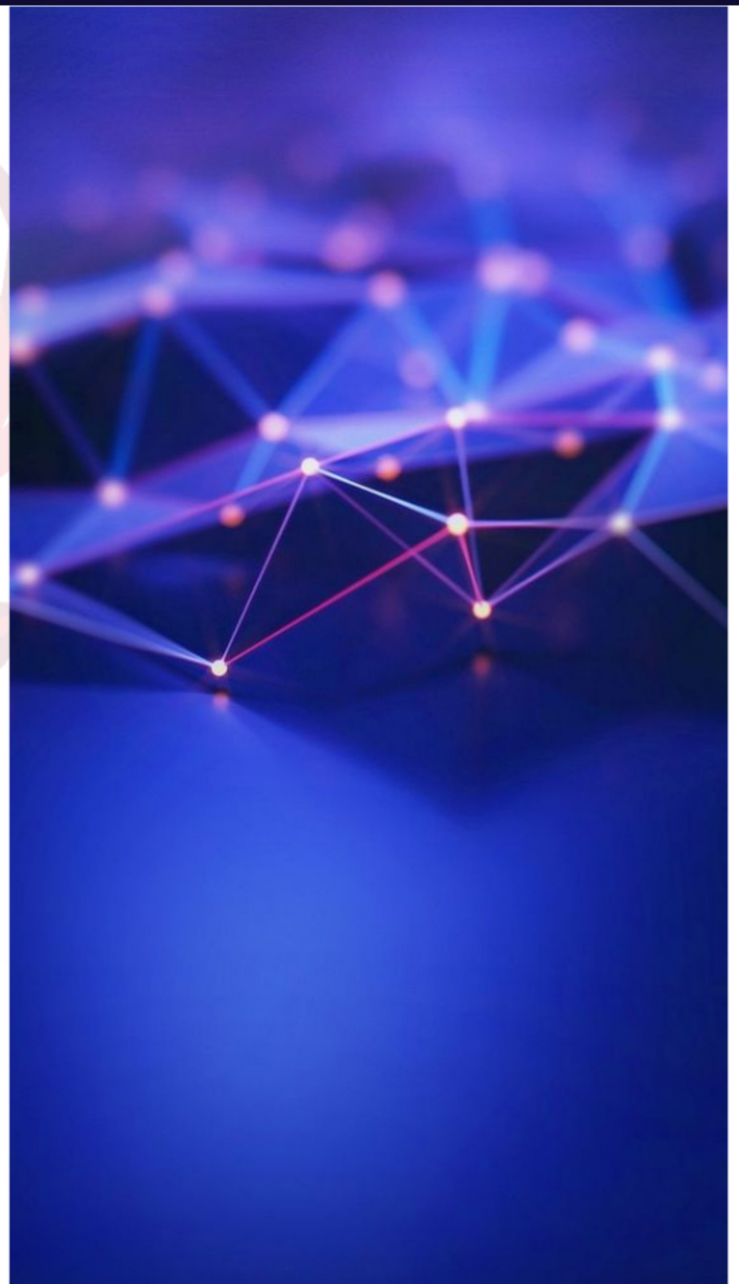
چرا باید در مرکز عملیات امنیتی از SOAR استفاده کنیم؟

جمع‌آوری داده‌ها و تجزیه‌وتحلیل آن‌ها به وسیله‌ی متخصصین به تنهایی برای تامین امنیت یک سازمان کافی نیست و فراهم سازی امکان پاسخ‌دهی لحظه‌ای در SOC ضرورت دارد. در دستیابی به اهداف امنیتی بهتر است؛ سامانه SOAR یا همان فرآیند هماهنگ‌سازی، خودکارسازی و پاسخ‌دهی (Security Orchestration، Automation and Response) را با SIEM سازمان منطبق کرد. حصول نگرش دقیق و پاسخ‌دهی سریع، در گرو ترکیب این دو سامانه است و با پیاده سازی این ابزار در SOC، فرآیندهای عملیات امنیت خودکارسازی می‌شوند.

به کمک SOAR فرآیندهای امنیتی را تحت دستورالعمل‌ها به اجرا درآورید. مدیریت برخی از رخدادها و یکپارچه سازی گردش‌کارها نیز توسط SOAR انجام می‌شود.مطابق تعاریف این دو سامانه؛ SIEM تهدیدهای پیرامون سازمان را گردآوری و یکپارچه‌سازی می‌کند و اعلان‌های امنیتی تولید میکند. SOAR در مرحله نهایی عملیات SOC اجرا می‌شود و با قابلیت تجزیه و تحلیل رفتاری (UEBA)، محدوده نظارت بر تهدیدها را وسعت می‌دهد و فرآیند بررسی امنیت را سریع‌تر کرده و منجر به بهره وری موثر می‌شود. ارزش اصلی SOAR در ارائه و ترکیب فرآیندها و استفاده از ابزارهای مرکز عملیات امنیتی است و تیم امنیت را قادر به انجام اقدامات زیر می کند:

- انجام عملیات با اولویت کمتر را به SOAR واگذار کنند.
- بر تصمیمات مهمی که اتخاذ آن‌ها صرفاً کار متخصصین است تمرکز نمایند.
- با کمک یادگیری ماشینی فرایندهای تکراری را خودکارسازی کرده و با انطباق بر دستورالعمل‌ها در جهت پاسخ‌دهی سریع استفاده نمایند.

تجزیه‌وتحلیل رفتار کاربران و رخدادها (UEBA) چیست؟

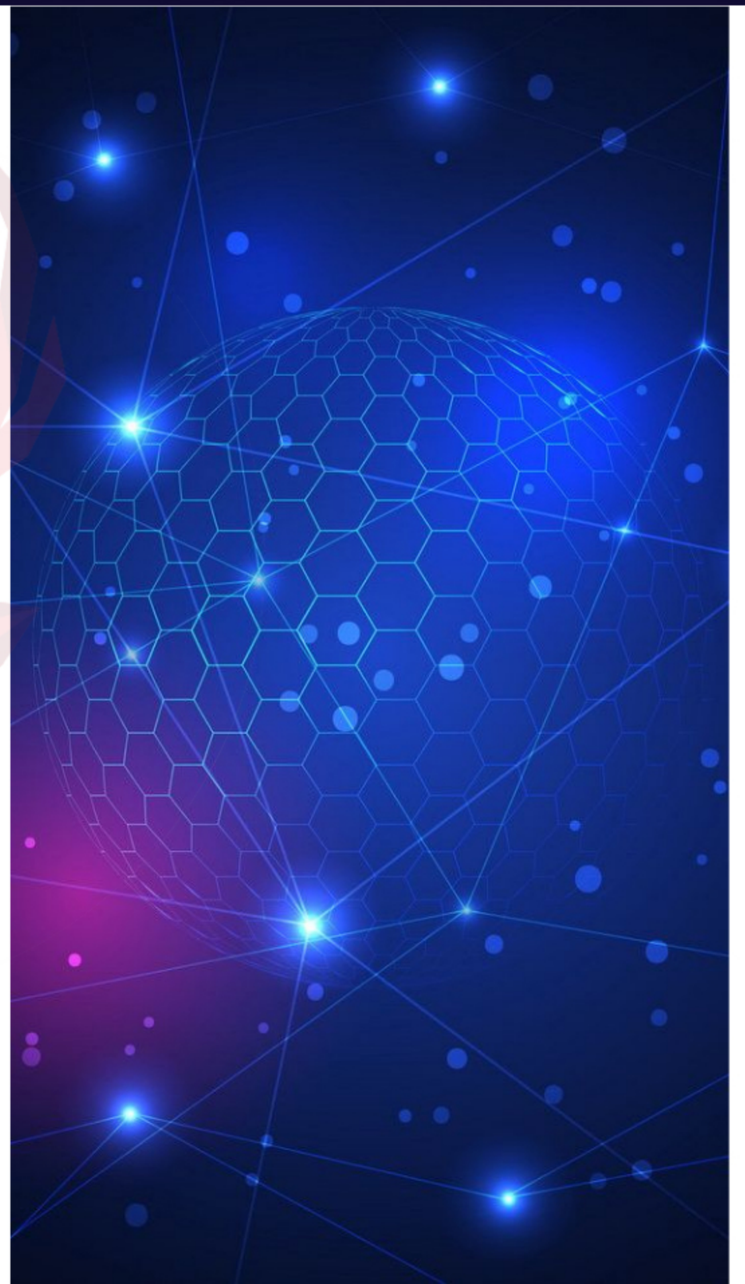


کاربردهای سامانه‌های SIEM و SOAR صرفاً در تشخیص و پاسخ خلاصه نمی‌شوند. در راهکارهای SOC نسل جدید، قابلیت‌های تجزیه و تحلیل رفتاری به SIEM اضافه شده است و رفتار کاربران و رخدادها از طریق ادغام یادگیری ماشین تجزیه و تحلیل می‌شود و نیز تهدیدهای ناشناخته به کمک ارزیابی رفتارهای غیر معمول کاربران تشخیص داده می‌شود. این ابزار به دنبال الگوهایی می‌گردد که با معیارهای رفتار عادی مطابقت نداشته و از این طریق تهدیدهای بالقوه سریع‌تر و حرفه‌ای‌تر توسط نیروهای انسانی شناسایی می‌شوند. به عنوان مثال، یادگیری ماشین میتواند در کمتر از یک دقیقه بدافزارهای منتشر شده از طریق ایمیل‌های سازمانی را شناسایی کند. در حالی که، تجزیه و تحلیل همین فرآیند توسط نیروی انسانی نیازمند زمان بسیار بیشتری است.

ادغام SIEM و UEBA مبتنی بر یادگیری ماشین، منحصرا به شناسایی و تشخیص تهدیدهای ناشناخته و رفتارهای غیر عادی نمی پردازد، بلکه با ارزیابی و اولویت بندی تهدیدها به رخدادهای امنیتی رسیدگی می‌کند. ادغام این دو راهکار به تسریع شناسایی و تجزیه و تحلیل داده‌ها در سراسر سیستم‌های سازمان کمک فزاینده ای کرده، بهره وری تیم امنیتی را بالا برده، منابع در دسترس مرکز عملیات امنیتی را افزایش داده، حجم بار وظایف متخصصین را کاهش داده، و در نهایت SOC را مقاوم سازی می‌کند.

به‌راحتی می‌توان گفت؛ پیاده‌سازی یک SOC پیشرفته، هزینه ای بالایی داشته و از اهمیت ویژه‌ای برخوردار است. SOC نسل جدید از سامانه‌های SIEM، SOAR و UEBA به صورت یکپارچه تشکیل شده و از امکاناتی همچون تجزیه و تحلیل حرفه‌ای، غنی‌سازی داده‌ها و لاگ‌ها، هوش مصنوعی، یادگیری ماشینی و سایر امکانات امنیتی بهره می‌برد و در عین حال رابط کاربری آن به صورت ساده و قابل فهم طراحی شده است.

بهینه‌سازی SOC



در واقع پویایی SOC هر سازمان به این بستگی دارد تا چه حد می‌توان از فناوری‌های امنیتی پیشرفته، ابزارها و نیروهای انسانی به‌صورت کارآمد استفاده کرد و بهره جست. چهارچوب‌های مختلفی برای طراحی SOC هر سازمان وجود دارد و نحوه‌ی اجرای هریک با هم متفاوت است.

مرکز عملیات امنیتی به‌جای واکنش‌های بی ثمر، می‌بایست هوشمندانه عمل کند و همچنین لازم است، ابزارهای ضروری خودکارسازی و یادگیری ماشین را به همراه قابلیت تجزیه و تحلیل همه جانبه در خود آماده داشته باشد. پیاده سازی SOC باید به نحوی صورت گیرد که با دیگر راهکارهای امنیتی سازگار باشد، فعالیت‌های غیر ضروری را به کمترین حالت خود برساند، وظایف امنیتی غیر مترقبه را مدیریت کند و همواره مطابق برنامه‌ای دقیق و با جزئیات در جهت متوقف سازی تهدیدها عمل نماید.

۱۰ ضرورتی که SOC باید همراه خود داشته باشد

ظرفیت بالا: یک SOC باید بتواند حجم بالایی از داده‌های بخش‌های در حال گسترش شبکه یک سازمان را از منابع مختلف و غیر مرتبط دریافت کند.
شناسایی:SOC لازم است با شناسایی و دستیابی به حجم انبوهی از داده‌های دریافتی، تهدیدهای موجود و رفتارهای ناهنجار را به‌سرعت تشخیص دهد.
پیش‌بینی: یک مرکز عملیات امنیتی (SOC) باید بتواند به طور مستمر به رصد، تجزیه و تحلیل و کنترل ابزارهای امنیتی مختلف سازمان بپردازد و آسیب پذیری‌ها و تهدیدها را به دقت زیر نظر بگیرد. بنابراین پیشگیری، یکی از قابلیت‌های اصلی مراکز عملیات امنیت کارآمد است.
خودکارسازی:همان‌طور که در بخش‌های مختلف سازمان می‌توان وظایف تکراری و ساده را به یک سیستم خودکار محول کرد و باعث بهبود بهره‌وری شد، مرکز عملیات امنیتی نیز از چنین خصوصیتی برخوردار است. بهترین استراتژی در خصوص خودکارسازی این است که هر وظیفه‌ای را بتوان به حالت خودکار درآورد. با این کار بار اضافی محول شده به گروه امنیتی کاهش می‌یابد و به طرز قابل توجهی منابع و نیروی انسانی تقویت می‌شوند.
هماهنگ‌سازی: یک SOC پیشرفته، پاسخ‌دهی به رخدادها را هماهنگ شده و سازمان‌یافته تنظیم می‌کند و اطلاعات ضروری و حائز اهمیت را، در میان انبوهی از داده‌ها، تحویل تحلیلگران امنیتی می‌دهد. این کار سبب افزایش قدرت در تصمیم‌گیری درست و پاسخ‌های لحظه ای می‌شود. هماهنگ‌سازی، فرآیندی است که در پاسخ به رخدادهای امنیتی و شامل خودکارسازی عملیات گردش‌کار، مانند بازنویسی اطلاعات احراز هویتی، patch برنامه‌ها و بروزرسانی فایروال‌ها و مقررات توسط SIEM است

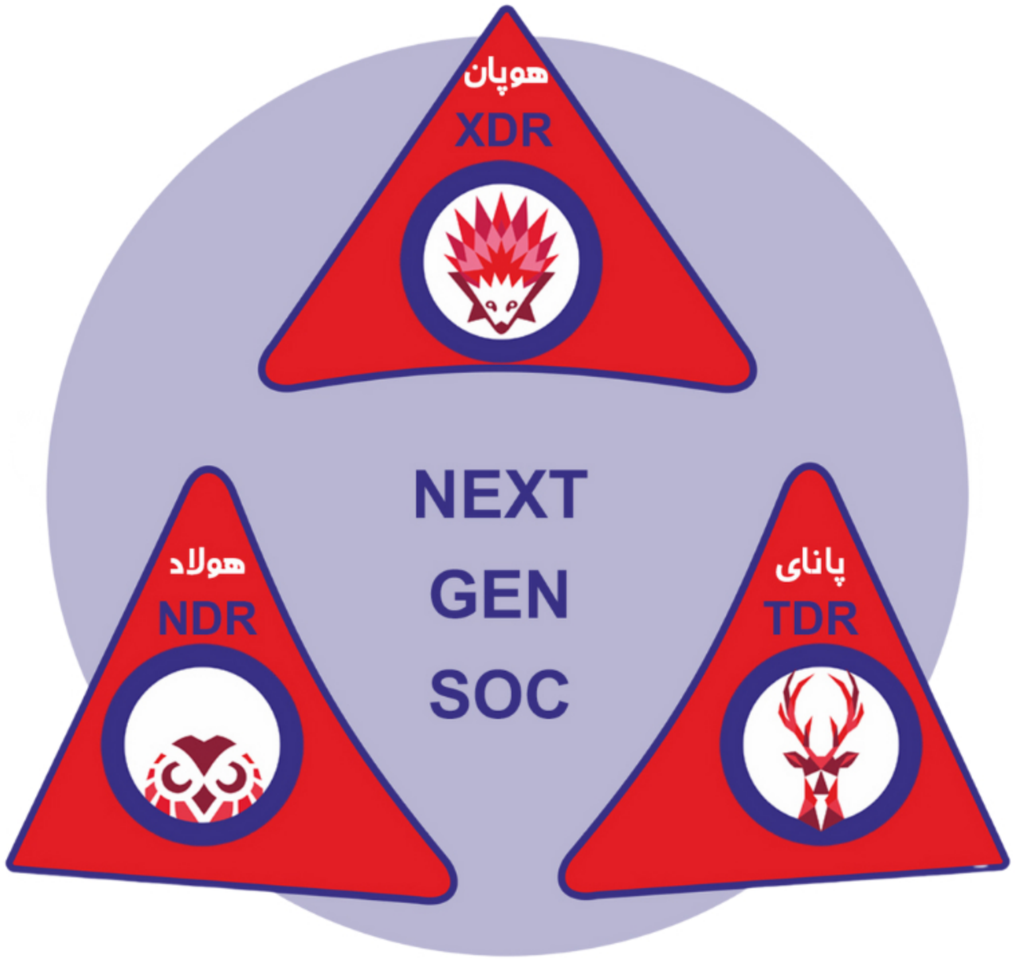
بازیابی اطلاعات و جلوگیری از نفوذ : SOC ها لازم است بتوانند اقدامات لازم امنیتی را بواسطه‌ی داده‌های گردآوری شده، تجزیه و تحلیل تهدیدها و رفتار کاربران تشخیص دهند. بعلاوه، پس از وقوع یک رخداد امنیتی این SOC موظف به بازیابی سیستم‌ها و اطلاعات مفقود شده بوده و هدف اصلی آن بازگردانی شبکه سازمان به حالت ابتدایی پیش از رخداد است.

تجزیه‌وتحلیل : SOC موظف است با شناسایی، تجزیه و تحلیل و پاسخ‌دهی به تهدیدهای سایبری از نفوذ به سازمان جلوگیری کند. پس از وقوع رخدادهای امنیتی، SOCوارد عمل می‌شود تا مشکلات بوجود آمده را در محل رخداد و درکنار علل خود شناسایی کرده و مانع وقوع دوباره آن‌ها شود.

همکاری همه‌جانبه : یک SOC باید در رأس تمامی عملیات امنیتی قرار بگیرد و نقطه‌ی آغازین کلیه تصمیم‌گیری‌ها باشد و نیز تمام رخدادهای مرتبط با سازمان را یکپارچه کند. یک مرکز عملیات امنیتی، متشکل از نیروهای متخصص، فرآیندها و فن آوری‌ها می‌باشد و هماهنگ کننده‌ی فعالیت‌های واحد آی‌تی و امنیت است تا بدین ترتیب، از وقوع اختلالات متعدد ناشی از فعالیت‌های امنیتی ممانعت گردند.

مدیریت موارد عملیاتی: مدیریت صحیح گردش‌کارها، در مراکز عملیات امنیت، امری حیاتی محسوب می‌شود. SOCها وظیفه دارند به رخدادها و فعالیت‌های بتعلیق درآمده پاسخ سریع داده و آنها را مدیریت کنند و در نهایت، نیازهای امنیتی سازمان را مترفع سازند. یک مرکز عملیات امنیتی کارآمد باید به شکل مشخص و خودکار؛ اولویت اعلان‌ها را مشخص کند، رخدادها را بررسی نماید و نیز قابلیت مدیریت بحران‌های امنیتی را داشته باشد.

گزارش‌دهی : مرکز عملیات امنیتی لازم است تهدیدهای داخلی و خارجی را جهت اطمینان سازمان در قالب یک گزارش دقیق و جزئی شرح دهد و مخاطرات مختلف را شناسایی کند. برای سازمان‌هایی که از مقررات متعددی مانند HIPAA، PCIDSS، GDPR، CCPA و ... پیروی می‌کنند ضرروت گزارش‌دهی به مراتب بالاتر است. با این قابلیت، شرکت‌های امنیتی ارائه دهنده SOC متعهد ایفای کامل امنیت می‌شوند و مخاطرات موجود در سازمان با جزئیات دقیق‌تر شناسایی می‌گردد و امنیت سازمان‌ها افزایش می‌یابد.


هوپان
XDR
هولاد
NDR
پانای
TDR
NEXT
GEN
SOC