الفبای SOAR

از هماهنگ‌سازی امنیتی تا توسعه پاسخ خودکار

تالیف: محمد قنبری

انتشارات پندار پارس

سرشناسه : قنبری، محمد، ۱۳۷۰-
عنوان و نام پدیدآور : الفبای SOAR : از هماهنگ سازی امنیتی تا توسعه پاسخ خودکار/تالیف محمد قنبری.
مشخصات نشر : تهران : پندار پارس ،۱۴۰۴.
مشخصات ظاهری : ۱۶۴ص.
شابک : 978-622-7785-53-1
وضعیت فهرست نویسی : فیپا
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
Computer networks -- Security measures
کامپیوترها -- ایمنی اطلاعات -- تدابیر ایمنی
Computer security -- Security measures
رده بندی کنگره : ۵۹/TK۵۱۰۵
رده بندی دیویی : ۸/۰۰۵
شماره کتابشناسی ملی : ۱۰۲۶۹۶۳۷
اطلاعات رکورد کتابشناسی : فیپا

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۲۲۴۵۲۳۴۸ **info@pendarepars.com**

نام کتاب : الفبای SOAR، از هماهنگ‌سازی امنیتی تا توسعه پاسخ خودکار

ناشر : انتشارات پندار پارس

تالیف : محمد قنبری

چاپ اول : آبان ۱۴۰۴

شمارگان : ۵۰ نسخه

صفحه‌آرایی : حسن یعسوبی

چاپ : چاپ دیجیتال وحید

قیمت : ۲۷۰.۰۰۰ تومان شابک : ۹۷۸-۶۲۲-۷۷۸۵-۵۳-۱

فهرست

پیش‌گفتار

امروزه، فعالان حوزه امنیت سایبری در خط مقدم یک نبرد اطلاعاتی بی‌وقفه قرار دارند. اما این نبرد نه با سلاح‌های سنتی، که با هوش، سرعت و دقت پیش می‌رود. تحلیلگران امنیتی هر روز با کوهی از داده‌ها، هشدارهای متعدد و وظایف تکراری دست و پنجه نرم می‌کنند که نه تنها انرژی آن‌ها را تحلیل می‌برد، بلکه زمان ارزشمندی را که باید صرف تحلیل تهدیدهای واقعی شود، از آن‌ها می‌گیرد. این کتاب برای کسانی نوشته شده است که به دنبال راهی برای عبور از این هرج و مرج عملیاتی هستند و می‌خواهند هوشمندی و کارایی را به مرکز عملیات امنیت خود بازگردانند.

کتاب "الفبای SOAR " برای پاسخ به همین چالش نوشته شده است. عنوان کتاب تصادفی نیست؛ هدف ما این است که مفاهیم بنیادین *ارکستراسیون، خودکارسازی و پاسخ امنیتی*[1] را به زبانی ساده و ساختارمند، از اولین «الفبا» تا جملات پیچیده، برای شما تشریح کنیم.

این کتاب یک سفر است. سفری که از درک چیستی و چرایی SOAR آغاز می‌شود، با کاوش در سه ستون اصلی آن یعنی ارکستراسیون، خودکارسازی و پاسخ ادامه می‌یابد، و به قلب تپنده‌ی آن یعنی «پلی‌بوک‌ها» می‌رسد. به شما نشان خواهیم داد که چگونه می‌توانید با طراحی و پیاده‌سازی پلی‌بوک‌های هوشمند، فرآیندهای امنیتی خود را استاندارد کنید، زمان پاسخ به حوادث را به کسری از ثانیه کاهش دهید و به تحلیلگران خود فرصت دهید تا به جای غرق شدن در کارهای تکراری، بر روی تهدیدهای پیچیده و استراتژیک تمرکز کنند.

این اثر تنها مجموعه‌ای از تعاریف فنی نیست، بلکه یک راهنمای عملی است. چه شما یک مدیر امنیت باشید که به دنبال بهینه‌سازی عملیات مرکز امنیت (SOC) خود هستید، چه یک تحلیلگر تازه‌کار که می‌خواهد با ابزارهای نوین آشنا شود، و چه دانشجویی که آینده‌ی شغلی خود را در این حوزه جستجو می‌کند، الف_ب_ای SOAR چراغ راه شما خواهد بود.

امیدواریم با ورق زدن صفحات این کتاب، نه تنها دانش فنی خود را ارتقا دهید، بلکه دیدگاهی نو نسبت به مدیریت امنیت پیدا کنید؛ دیدگاهی که در آن، فناوری در خدمت توانمندسازی انسان قرار می‌گیرد تا با هم، دژی مستحکم‌تر در برابر تهدیدهای سایبری بسازیم.

---

[1] Security Orchestration, Automation, and Response

بخش ۱

مبانی و مفاهیم کلیدی SOAR

فصل ۱

مقدمه‌ای بر SOAR

با تداوم تحول جهان امروز، ما خود را در چشم‌اندازی پویا و متغیر می‌یابیم که مملو از فرصت‌ها و مخاطرات است. در میان این تحولات، صنعت امنیت سایبری به عرصه‌ای پررونق از نوآوری و حل مسائل حیاتی تبدیل شده است. ابزارهایی که برای ایمن‌سازی فضاهای مجازی مورد استفاده قرار می‌گیرند، روز به روز پیشرفته‌تر می‌شوند و یکی از راهکارهایی که به‌عنوان همراهی توانمند در مقابله با تهدیدهای سایبری پدیدار شده، استراتژی هماهنگ‌سازی (Orchestration)، خودکارسازی (Automation) و پاسخ‌دهی (Response) امنیتی که بصورت اختصار SOAR نامیده می‌شود، است.

این فصل نخست، در حکم سفری مقدماتی به دنیای SOAR است و با هدف آشنایی دو گروه طراحی شده است: نوآموزانی که به‌تازگی قدم در مسیر امنیت سایبری نهاده‌اند و همچنین متخصصان باتجربه‌ای که به دنبال ارتقای درک و به‌کارگیری مؤثرتر این راهکار هستند.

مسیر آشنایی ما با تعریفی پایه‌ای از SOAR آغاز می‌شود و سپس به بررسی اهمیت آن در منظومه امنیت سایبری معاصر می‌پردازیم. در ادامه فصل، اجزای اصلی این راهکار یعنی هماهنگ‌سازی[۱]، خودکارسازی[۲] و پاسخ‌دهی[۳] امنیتی را با دقت بررسی می‌کنیم تا دریابیم این عناصر چگونه در تعامل با یکدیگر، سامانه‌ای منسجم و جامع برای پاسخ به تهدیدات ایجاد می‌کنند.

هدف این فصل، بنیان‌گذاری دانشی مقدماتی برای بررسی عمیق‌تر SOAR در فصل‌های بعدی است؛ جایی که به تبیین اجزاء، راهبردها، شیوه‌های پیاده‌سازی و مسیرهای آینده آن خواهیم پرداخت. در پایان این فصل، خواننده باید درکی روشن از چیستی SOAR و چرایی اهمیت آن به‌عنوان ابزاری ضروری در امنیت سایبری مدرن داشته باشد.

۱-۱- (SOAR) چیست؟ تعریف، اهداف و چشم‌انداز

هماهنگ‌سازی، خودکارسازی و پاسخ‌دهی امنیتی یک رویکرد نوآورانه در حوزه‌ی امنیت سایبری به شمار می‌آید.

اساس این رویکرد، ادغام و بهره‌برداری کارآمد از ابزارها و رویه‌های مختلفی است که توانایی یک سازمان را در شناسایی، تحلیل و پاسخ‌دهی به تهدیدهای سایبری تقویت می‌کنند.

در واقع SOAR راه‌حلی است که برای پاسخ به مجموعه‌ای از چالش‌های مهم در عرصه امنیت سایبری طراحی شده است. از جمله این چالش‌ها می‌توان به موارد زیر اشاره کرد:

- ✓ حجم روزافزون هشدارهای امنیتی
- ✓ نبود هماهنگی میان ابزارهای امنیتی مختلف
- ✓ کمبود نیروی متخصص در زمینه امنیت اطلاعات

۱-۲- ارکان اصلی SOAR: هماهنگ‌سازی، خودکارسازی و پاسخ‌دهی

همان‌طور که از نام آن پیداست، SOAR از سه مؤلفه‌ی متمایز اما به‌شدت درهم‌تنیده تشکیل شده است:

- ➢ **هماهنگ‌سازی امنیتی:** فرآیند یکپارچه‌سازی و هماهنگ‌سازی ابزارها، سیستم‌ها و رویه‌های امنیتی برای ایجاد یک چارچوب منسجم عملیاتی.
- ➢ **خودکارسازی امنیتی:** استفاده از فناوری برای انجام خودکار وظایف تکراری و زمان‌بر در زمینه امنیت سایبری.
- ➢ **پاسخ‌دهی امنیتی:** اتخاذ اقدامات مشخص و مؤثر در واکنش به تهدیدات یا حوادث امنیتی، به‌صورت خودکار یا نیمه‌خودکار.

نه‌تنها SOAR به سازمان‌ها امکان می‌دهد تا تهدیدها را سریع‌تر و دقیق‌تر مدیریت کنند، بلکه باعث بهینه‌سازی منابع انسانی و کاهش زمان پاسخ‌دهی نیز می‌شود.

هماهنگ‌سازی امنیتی، فرآیند ادغام بخش‌های مختلفِ ابزارها و سیستم‌های امنیتی درون محیط یک سازمان است تا به‌صورت هماهنگ با یکدیگر کار کنند. همچنین می‌توان آن را شبیه رهبر یک ارکستر در نظر گرفت، که در آن سازهای مختلف را برای تولید یک خروجی، هماهنگ و یکپارچه می‌کند.

در زمینه‌ی امنیت سایبری[۴]، این به معنی اتصال و سازمان‌دهی سیستم‌های امنیتی گوناگون است تا آنها بتوانند مؤثرتر به‌عنوان یک واحد منسجم عمل کنند. هماهنگ‌سازی امنیتی از نقاط قوت هر ابزارِ

یکپارچه‌شده بهره می‌برد و امکان شناسایی و پاسخ‌دهی سریع‌تر و کارآمدتر به تهدیدات را فراهم می‌سازد. با انجام این کار، سایلوها[۵] را از بین می‌برد، دیدپذیری[۶] را در سراسر محیط امنیتی سازمان بهبود می‌بخشد و تصمیم‌گیری آگاهانه‌تری را ممکن می‌سازد.

خودکارسازی امنیتی دومین ستون SOAR، به استفاده از ابزارهای خودکار برای انجام وظایف تکراری و روتینی اشاره دارد که در غیر این صورت مقدار قابل‌توجهی از زمان یک تحلیل‌گر امنیتی را مصرف می‌کردند. خودکارسازی امنیتی شامل خودکارسازی وظایفی مانند جمع‌آوری داده‌ها[۷]، شناسایی تهدید[۸] ، اولویت‌بندی هشدارها[۹] و حتی برخی جنبه‌های پاسخ‌دهی به رخداد می‌شود.

خودکارسازی دو مزیت هم‌زمان دارد: افزایش بهره‌وری عملیاتی و کاهش خطاهای انسانی با واگذاری وظایف تکراری به فرآیندهای خودکار.

متخصصان امنیتی می‌توانند تمرکز بیشتری بر وظایف راهبردی و پیچیده‌ای داشته باشند که نیاز به تخصص آنها دارد. افزون بر این،خودکارسازی تضمین می‌کند که وظایف روتین، سریع‌تر و دقیق‌تر از حالت دستی انجام شوند.

در نهایت، پاسخ‌دهی در زمینه‌ی SOAR شامل اقدامات یا برنامه‌های عملی یک سازمان برای مدیریت، کاهش اثرات، و بازیابی از رخدادهای امنیتی است. این شامل شناسایی شدت رخداد، اولویت‌بندی اقدامات پاسخ‌دهی، اجرای پاسخ و یادگیری از رخداد برای پیشگیری‌های آینده می‌شود. با وارد کردن پاسخ‌دهی در چارچوب SOAR، سازمان‌ها می‌توانند زمان پاسخ‌دهی خود را تسریع بخشند و اطمینان حاصل کنند که اقدامات آن‌ها بر پایه‌ی یک استراتژی هماهنگ انجام می‌شود.

SOAR را می‌توان به‌عنوان یک چارچوب فناورانه و رویه‌ای[۱۰] در نظر گرفت که به تیم‌های امنیتی این امکان را می‌دهد که هوشمندانه‌تر فعالیت کنند، نه سخت‌تر.

ظهور SOAR را می‌توان بازتابی از پیچیدگی و پیشرفت روزافزون چشم‌انداز تهدیدات سایبری[۱۱] دانست. با افزایش کمّی و کیفی تهدیدات، رویکردهای سنتی و دستی برای تأمین امنیت دیگر کارایی لازم را ندارند. سازمان‌ها نیاز دارند که همواره یک گام جلوتر از مهاجمان باشند، و SOAR ابزارها و روش‌شناسی‌های لازم برای تحقق این هدف را در اختیار آنان می‌گذارد.

با پیاده‌سازی یک استراتژیSOAR، سازمان‌ها می‌توانند عملیات امنیتی خود را بهینه‌سازی کرده و آن را چابک‌تر، پاسخ‌گوتر و مؤثرتر سازند. مزایای SOAR فراتر از بهبود در نتایج امنیتی است. این فناوری می‌تواند منجر به صرفه‌جویی در هزینه‌ها شود، چرا که سازمان‌ها قادر خواهند بود با منابع کمتر، عملکرد بیشتری داشته باشند. افزون بر این، SOAR می‌تواند موجب افزایش رضایت شغلی در میان متخصصان امنیتی شود، زیرا آن‌ها از انجام کارهای تکراری و یکنواخت رها شده و می‌توانند تمرکز خود را بر وظایف چالش‌برانگیزتر و جذاب‌تر معطوف کنند.

بنابراین، SOAR ابزاری قدرتمند در فضای امنیت سایبری مدرن محسوب می‌شود. این فناوری بیانگر گذار از رویکردی واکنشی و پراکنده به رویکردی پیش‌دستانه و یکپارچه در حوزه‌ی امنیت است. بدون شک، مسیر درک و پیاده‌سازی SOAR فرآیندی پیچیده است، اما پاداش آن، امنیت تقویت‌شده، کارآمدی عملیاتی بیشتر و تاب‌آوری کلی بالاتر در برابر تهدیدات سایبری خواهد بود. در ادامه‌ی این کتاب و در بخش‌های بعدی که به بررسی عمیق‌تر SOAR می‌پردازد، اصول بنیادی و مزایای مطرح‌شده در این فصل مقدماتی را به‌خاطر بسپارید؛ چرا که آنها راهنمایی برای بهره‌برداری کامل از ظرفیت‌های SOAR خواهند بود.

۱-۳- اهمیت حیاتی SOAR در امنیت سایبری مدرن

در دنیای به‌شدت به‌هم‌پیوسته‌ی امروز، سازمان‌ها با چشم‌اندازی بسیار پیچیده در حوزه‌ی امنیت فضای سایبری روبه‌رو هستند. تهدیدات دیجیتال روزبه‌روز پیچیده‌تر می‌شوند، حجم هشدارهای امنیتی به‌طور بی‌سابقه‌ای افزایش یافته است و تیم‌های امنیتی اغلب برای هماهنگی با این سرعت تحولات دچار مشکل می‌شوند.

در چنین بستری، SOAR به‌عنوان راهکاری اساسی پدید آمده است که سطحی جدید از کارایی، اثربخشی و تاب‌آوری را در مدیریت امنیت سایبری ارائه می‌دهد. برای درک کامل اهمیت SOAR، باید به چالش‌های مختلفی که در حوزه‌ی امنیت سایبری با آنها روبه‌رو هستیم و SOAR در حل آنها نقش دارد، بپردازیم.

نخست، SOAR گامی مهم در مواجهه با حجم عظیم هشدارهایی است که تیم‌های امنیتی روزانه با آن مواجه‌اند. با رشد شبکه‌ها و سامانه‌های دیجیتال، سازمان‌ها روزانه با هزاران هشدار امنیتی بمباران می‌شوند. بسیاری از این هشدارها مثبت کاذب[۱۲] هستند، در حالی که برخی دیگر تهدیداتی حیاتی‌اند که نیاز به رسیدگی فوری دارند. بررسی دستی این حجم از هشدارها نه‌تنها زمان‌بر و پرزحمت است، بلکه مستعد خطای انسانی نیز هست.

راهکارهای SOAR با خودکارسازی فرآیند دسته‌بندی و اولویت‌بندی هشدارها این چالش را برطرف می‌کنند. این سیستم‌ها می‌توانند هشدارها را به‌سرعت تحلیل کرده، هشدارهای مثبت کاذب را از تهدیدات واقعی جدا کرده و آنها را بر اساس شدت، اولویت‌بندی کنند. این امر به تیم‌های امنیتی اجازه می‌دهد توجه خود را دقیقاً معطوف به نقاط بحرانی کنند.

دوم، SOAR نقشی کلیدی در پاسخ به شکاف مهارتی موجود در حوزه امنیت سایبری ایفا می‌کند. بر اساس یک نظرسنجی توسط بزرگ‌ترین نهاد غیرانتفاعی بین‌المللی در حوزه‌ی گواهی‌نامه‌های حرفه‌ای امنیت سایبری (ISC)، شکاف نیروی کار جهانی در این حوزه در سال ۲۰۲۰ حدود ۳ میلیون نفر بود. با بهره‌گیری از SOAR، حتی یک تیم کوچک از تحلیل‌گران امنیتی[۱۳] می‌توانند عملیات امنیتی سازمان را

به‌طور مؤثری مدیریت کنند؛ چرا که بسیاری از وظایف روتین به‌صورت خودکار، انجام شده و تمرکز تیم بر فعالیت‌های استراتژیک و پیچیده‌ای قرار می‌گیرد که نیازمند تخصص انسانی است.

سوم، SOAR سرعت و کارایی در پاسخ به رخدادهای امنیتی را به‌شکل چشم‌گیری افزایش می‌دهد. سرعت واکنش سازمان به یک حمله سایبری نقش تعیین‌کننده‌ای در میزان خسارت دارد. هرچه شناسایی و مهار یک نفوذ زمان بیشتری ببرد، احتمال افزایش زیان نیز بیشتر خواهد بود. راهکارهای SOAR می‌توانند با خودکارسازی مراحل مختلف فرآیند پاسخ به رخداد، از هشدار اولیه تا مهار تهدید، به‌شدت زمان واکنش را کاهش دهند. این امر نه‌تنها تأثیر حمله را به حداقل می‌رساند، بلکه موجب تقویت تاب‌آوری کلی سازمان نیز می‌شود.

فراتر از این چالش‌های مشخص، SOAR نقشی حیاتی در ارتقای کلی اثربخشی عملیات امنیتی سازمان دارد. این مهم از چند طریق محقق می‌شود. یکی از مهم‌ترین آنها بهبود هماهنگی میان ابزارها و سامانه‌های امنیتی مختلف است. زیرساخت‌های امنیتی سنتی اغلب مجموعه‌ای از ابزارهای منفصل و جزیره‌ای هستند. این نبود یکپارچگی باعث ایجاد خلأهای امنیتی و دشواری در داشتن تصویری جامع از وضعیت امنیتی سازمان می‌شود.

SOAR این مشکل را با یکپارچه‌سازی ابزارهای امنیتی در قالب یک سامانه واحد حل می‌کند. این کار دیدکلی و هماهنگی را بهبود می‌بخشد و رویکردی فعال و مبتنی بر اطلاعات را در امنیت ممکن می‌سازد.

همچنین، SOAR کیفیت تصمیم‌گیری در عملیات امنیتی را افزایش می‌دهد. این سیستم، پلتفرمی مرکزی فراهم می‌آورد که در آن داده‌ها از منابع مختلف جمع‌آوری، تحلیل و در قالبی شفاف و قابل اقدام ارائه می‌شوند. بدین‌ترتیب، تیم‌های امنیتی دیدی جامع نسبت به وضعیت امنیتی سازمان به‌دست می‌آورند و می‌توانند تصمیمات آگاهانه‌تری اتخاذ کنند؛ برای مثال، آنها قادر خواهند بود الگوها و روندهای تکرارشونده در رخدادهای امنیتی را سریعاً شناسایی کرده و متناسب با آن، راهبردهای امنیتی خود را تنظیم نمایند.

در نهایت، اهمیت SOAR فراتر از نتایج فوری در حوزه امنیت است. با خودکارسازی وظایف تکراری، فشار کاری تیم‌های امنیتی به‌طرز چشم‌گیری کاهش می‌یابد که این امر می‌تواند منجر به افزایش رضایت شغلی و کاهش احتمال فرسودگی شغلی شود.

افزون براین، SOAR با بهره‌وری بهتر منابع، منجر به صرفه‌جویی اقتصادی نیز می‌شود در جمع‌بندی می‌توان گفت که اهمیت SOAR در امنیت سایبری مدرن قابل انکار نیست. این فناوری پاسخی مؤثر به چندی از بحرانی‌ترین چالش‌های موجود در این حوزه ارائه می‌دهد؛ از حجم بالای هشدارهای امنیتی گرفته تا کمبود نیروی متخصص. با ارتقای بهره‌وری، SOAR به سازمان‌ها کمک می‌کند تا عملیات امنیتی خود را هوشمندانه‌تر، سریع‌تر و اثربخش‌تر اداره کنند.

پانویس فصل اول

[1] Orchestration
[2] Automation
[3] Response
[4] Cybersecurity
[۵] سایلوها (Sailos): ساختارهای جدا از هم در یک سازمان که به طور مستقل عمل می‌کنند و با یکدیگر ارتباط مؤثری ندارند.

[6] Visibility
[7] Data Collection
[8] Threat Detection
[۹] Alert Triage: فرآیند بررسی، طبقه‌بندی و الویت‌بندی هشدارها امنیتی به‌منظور تعیین اهمیت آن‌ها. هدف از این امر، به حداقل رساندن آسیب‌های ناشی از رخدادهای امنیتی (Security Incidents) و جلوگیری از تکرار همان یا رخدادهای مشابه در آینده است. در مجموع، این سه مؤلفه‌ی اصلی SOAR، رویکردی پیش‌دستانه، یکپارچه و کارآمد را برای مدیریت عملیات امنیتی فراهم می‌آورند.

[۱۰] procedural framework: چارچوبی که شامل مجموعه‌ای از رویه‌ها و روش‌ها برای انجام مجموعه‌ای از وظایف یا رسیدن به یک هدف مشخص است.

[۱۱] cyber threat landscape : وضعیت کلی و در حال تغییر تهدیدات موجود در فضای سایبری که سازمان‌ها با آن مواجه هستند.

[12] False positive
[13] Security analysts

فصل دوم

درک عمیق هماهنگ‌سازی امنیتی

به فصل دوم از مسیر ما در دنیای SOAR خوش آمدید. پس از آن‌که در فصل پیشین بنیان‌های اولیه‌ی SOAR و اهمیت آن در چشم‌انداز نوین امنیت سایبری مورد بررسی قرار گرفت، اکنون وارد یکی از اجزای کلیدی SOAR می‌شویم.

هماهنگ‌سازی امنیتی اغلب به رهبر یک ارکستر تشبیه می‌شود. در واقع، این مفهوم به فرآیند یکپارچه‌سازی ابزارها، سامانه‌ها و رویه‌های امنیتی مختلف با هدف ایجاد محیطی هماهنگ‌تر و کارآمدتر اشاره دارد. اما هماهنگ‌سازی امنیتی در عمل به چه معناست و چگونه کار می‌کند؟ چه مزایایی به همراه دارد و با چه چالش‌هایی مواجه است؟ اینها پرسش‌هایی هستند که در این فصل به آنها خواهیم پرداخت.

ابتدا با بررسی عمیق مفهوم هماهنگ‌سازی امنیتی آغاز می‌کنیم و به مبانی نظری و پیامدهای عملی آن می‌پردازیم. سپس مزایای این فرآیند را بررسی می‌کنیم؛ از جمله اینکه چگونه می‌تواند دیدپذیری، کارایی و تصمیم‌گیری آگاهانه‌تر را در عملیات امنیتی بهبود بخشد.

در بخش‌های بعدی، جایگاه هماهنگ‌سازی امنیتی را در چارچوب کلی SOAR تحلیل می‌کنیم و به تعامل آن با خودکارسازی امنیتی و پاسخ‌دهی می‌پردازیم. در این‌جا، تفاوت میان هماهنگ‌سازی و خودکارسازی را روشن خواهیم کرد و نشان می‌دهیم چگونه این دو در کنار یکدیگر راه‌حلی جامع و یکپارچه برای امنیت ایجاد می‌کنند.

با وجود مزایای فراوان، هماهنگ‌سازی امنیتی بدون چالش نیست. در پایان فصل، به پیچیدگی‌ها و مشکلات احتمالی در اجرای آن می‌پردازیم و راهکارهایی برای غلبه بر این چالش‌ها ارائه خواهیم کرد.

هماهنگ‌سازی امنیتی ابزاری قدرتمند در فضای امنیت سایبری مدرن است که به سازمان‌ها امکان می‌دهد عملیات امنیتی خود را به شکل مؤثرتر و کارآمدتری مدیریت کنند. هدف این فصل، تجهیز شما به دانش و درک لازم برای بهره‌گیری از قدرت هماهنگ‌سازی امنیتی در سازمان‌تان است.

به یاد داشته باشید، مسیر تسلط بر SOAR یک دوی سرعتی نیست، بلکه ماراتنی فکری است. با هر گام، درک ما عمیق‌تر و دیدگاه‌مان دقیق‌تر می‌شود و به هدف نهایی نزدیک‌تر می‌گردیم. پس بیایید گام بعدی را با هم برداریم و به دنیای جذاب هماهنگ‌سازی امنیتی وارد شویم.

۲-۱-تعریف و مفاهیم کلیدی و اصول هماهنگ‌سازی

هماهنگ‌سازی امنیتی یکی از اجزای حیاتی چارچوب SOAR به شمار می‌رود. به‌بیان ساده، این مفهوم به فرآیند یکپارچه‌سازی و هم‌راستا کردن ابزارها، فناوری‌ها و فرآیندهای امنیتی مختلف به‌منظور عملکردی هماهنگ و کارآمد اشاره دارد. اما برای درک کامل نقش و ارزش هماهنگ‌سازی امنیتی لازم است به مفاهیم کلیدی آن عمیق‌تر بپردازیم.

در قلب هماهنگ‌سازی امنیتی، ایده‌ی یکپارچه‌سازی قرار دارد. در یک سازمان معمولی، ابزارها و فناوری‌های امنیتی متعددی برای حفاظت از بخش‌های مختلف زیرساخت دیجیتال استفاده می‌شوند. این موارد می‌توانند شامل Firewalls[1]، Intrusion Detection Systems (IDS)[2]، Antivirus[۳]، Softwar[۴]، Vulnerability Scanners و ابزارهای دیگر باشند.

به‌طور سنتی، این ابزارها در سیلوها عمل می‌کردند، به این معنا که هر یک وظیفه‌ی خاص خود را بدون تعامل یا با تعامل اندک با سایر ابزارها انجام می‌دادند. نتیجه‌ی این وضعیت، چشم‌اندازی پراکنده از امنیت سازمان است که در آن دید کلی محدود بوده و تهدیدها ممکن است از شکاف‌های بین ابزارها عبور کنند.

هدف هماهنگ‌سازی امنیتی، غلبه بر این پراکندگی از طریق یکپارچه‌سازی ابزارهای گوناگون در یک سامانه‌ی امنیتی واحد است. این یکپارچه‌سازی به کمک[۵] Application Programming Interfaces(APLs) و سایر اشکال تعامل‌پذیری بین ابزارها محقق می‌شود.

پس از یکپارچه‌سازی، ابزارها می‌توانند داده‌ها را با یکدیگر به اشتراک بگذارند و بر اساس خروجی‌های یکدیگر اقدامات لازم را آغاز کنند و به‌طور کلی به‌عنوان یک واحد هماهنگ عمل کنند. این امر منجر به دیدگاهی جامع نسبت به وضعیت امنیتی سازمان و واکنشی کارآمدتر و مؤثرتر به تهدیدات می‌شود.

دومین مفهوم کلیدی در رابطه‌ای برنامه‌نویسی کاربردی، تناسب یا همان هماهنگی است. همان‌طور که یک رهبر ارکستر اطمینان حاصل می‌کند که تمامی نوازندگان، قطعه را به‌موقع و صحیح اجرا می‌کنند، هماهنگ‌سازی امنیتی نیز تضمین می‌کند که تمامی ابزارها و فرآیندهای امنیتی در هماهنگی کامل با یکدیگر عمل می‌کنند. این امر شامل تعیین قوانین، تعریف جریان‌های کاری (Workflows) و مدیریت وابستگی‌های متقابل بین ابزارها و فرآیندهاست.

برای مثال، اگر یک سیستم تشخیص نفوذ، تهدیدی احتمالی را شناسایی کند، می‌تواند به‌صورت خودکار مجموعه‌ای از اقدامات را در ابزارهای دیگر فعال کند، نظیر ایزوله کردن بخش آلوده‌ی شبکه یا آغاز یک اسکن عمیق بدافزار[۶]. چنین واکنش هماهنگی می‌تواند زمان پاسخ‌دهی به تهدیدات را به‌شکل قابل توجهی کاهش داده و خسارت احتمالی را به حداقل برساند.