طراحی سامانه هوش امنیتی برای مرکز عملیات امنیت با رویکرد عامل‌بنیان

بیان مساله:

مساله اصلی این است که با توجه به پیچیدگی تهدیدات، سرعت تغییرات محیطی و رشد شتابان تکنولوژی، چگونه می توان سامانه هوش امنیتی را در مرکز عملیات امنیتِ شبکه را طراحی نمود تا ارتباط و تشخیص ناهنجاری بین انواع داده های امنیتی و به صورت بهنگام را در سازمان ایجاد نمود و از این طریق زمینه اعلام هشدار مناسب به منظور ارائه گزارش هایی بر مبنای تحلیل داده های لایه آشکار و نهان شرکت، حاصل شود؟

گام اول: در این لایه مرکز عملیات امنیت (SOC)، داده ها از طریق فایل های لاگ تجهیزات شبکه، فایروال‌ها، روترها، سویئچ‌ها، سیستم عامل، برنامه‌های کاربردی، سرورهای مهم سازمان و سامانه های اطلاعاتی مهم، قبل از همبسته‌سازی توسط موتو مرکز عملیات امنیت، جمع آوری می شوند.

گام دوم: در این لایه مرکز عملیات امنیت (SOC)، داده ها از طریق فایل های لاگ تجهیزات شبکه، فایروال‌ها، روترها، سویئچ‌ها، سیستم عامل، برنامه‌های کاربردی، سرورهای مهم سازمان و سامانه های اطلاعاتی مهم، بعد از همبسته‌سازی توسط موتو مرکز عملیات امنیت، جمع آوری می شوند.

گام سوم: در این گام، بر اساس الگوریتم های هوشمند عامل‌بنیان، تحلیل داده های جمع آوری شده حاصل از لایه اول، به منظور مقایسه و افزایش دقت تشخیص سامانه، صورت خواهد گرفت.

گام چهارم: در این مرحله، سیستم، اعلام هشدار می نماید. در این گام، پس از اعلام هشدار توسط سیستم هوش امنیتی، متناسب با شرایط نسبت به هر هشدار، تصمیمی اخذ می گردد تا آمادگی مقابله با تهدیدات، جهت ایجاد زمینه پیشگیری از بحران به وجود آید.

مدل مفهومی: مدل مفهومی پژوهش به صورت شکل زیر ارائه گردیده است: