هوش امنیتی

مهری یحیائی، ساناز خلیلی

1- مقدمه

با افزایش حجم رخدادهای گزارش شده توسط سیستم‌ها و ابزارهای امنیتی، کشف و شناسایی تهدیدات و حملات داخلی و خارجی بسیار دشوار و در مواردی غیرممکن شده است، از این رو نیاز به روش متمرکزی وجود دارد تا بتوان رخدادها و داده‌های گزارش شده را مانیتور کرده و بین آنها ارتباط برقرار نمود و از این طریق تهدیدها و حملات را شناسایی کرد.
بسیاری از تحقیقات صورت گرفته بیانگر این است که از هر ده رخداد امنیتی، هفت رخداد هیچ‌وقت در سازمان‌ها گزارش نمی‌شوند و در 30 درصد مواقع، حتی خود سازمان مور حمله نیز متوجه بروز حمله نمی‌شود. همچنین یک سوم نشت اطلاعات حیاتی در سازمان‌ها، تا یک ماه بعد هم تشخیص داده نمی‌شوند و سه پنجم از رخدادهای امنیتی توسط شرکت‌های بیرونی تشخیص داده می‌شوند و نه خود سازمان قربانی و 43 درصد از حملات سایبری بر روی دارایی‌های لیست‌نشده سازمان‌ها، رخ می‌دهند.
با وجود این روند تصاعدی بروز تهدیدات جدید، محدودیت‌های فناوری در تحلیل سریع رخدادها، انبوه داده‌های غیریکپارچه در سیستم‌های مختلف یک سازمان، تغییرات سریع قوانین محلی و جهانی، منابع امنیتی محدود در سازمان از جمله نیروی متخصص، هزینه و فناوری و عدم توجه به مستندسازی اطلاعات، شرکت‌ها و سازمان‌ها را به اتخاذ تصمیمات جدی در خصوص امنیت وادار می‌کند.

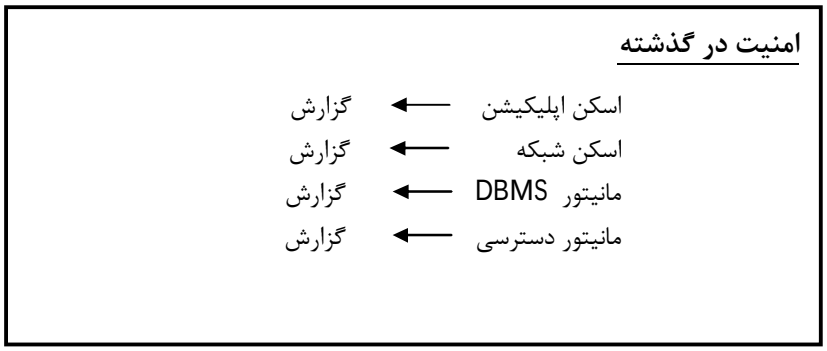
2- آشنایی با هوش امنیتی

استفاده از سخت‌افزار، نرم‌افزار، اسکنر یا سیستم‌های مانیتورینگ، هیچ‌یک به معنی احساس امن بودن نیست. راه‌کار پیشنهادی محققین امنیت اطلاعات، هوش امنیتی است که در واقع یک راه‌کار مدرن امنیتی برای مقابله با تهدیدات امروزی می‌باشد.
جمع‌آوری، هنجارسازی، همبسته‌سازی و تحلیل بزرگ‌داده‌های[1] امنیتی یک سازمان به‌منظور خودکار کردن فرآیندهای کاهش سطح مخاطرات در سازمان یا به‌عبارت دیگر تبدیل میلیون‌ها بسته اطلاعاتی به یک اقدام عملی آنی، تعاریفی از هوش امنیتی هستند.
به دو دلیل مهم Big Data و APT[2]، سازمان‌ها ناگزیرند که به سمت هوش امنیتی حرکت کنند. بزرگ داده، به مجموعه‌هایی از داده با نرخ رشد بسیار بالا گفته می‌شود که در مدت زمان کوتاهی، باعث ایجاد چنان حجمی از اطلاعات می‌شوند که ذخیره‌سازی، جست‌وجو و تحلیل آنها با ابزارهای مدیریت داده موجود در یک زمان قابل تحمل و مورد انتظار، غیر ممکن است. چهار مشخصه مهم بزرگ داده‌ها، حجم بالای داده، سرعت بالای ایجاد داده، تنوع بالای داده و سرعت بالای تغییر داده است. APT، نوعی از حملات ترکیبی و پیچیده سایبری است که هدفی خاص و دقیق دارد و از روش‌های مختلف برای پنهان ماندن از دید سامانه‌های پایش استفاده می‌کند.
همان‌طور که هوش تجاری[3] موجب کاهش ریسک در کسب و کار، تسهیل تصمیم‌گیری‌های تجاری و خودکار کردن فرآیندهای تجاری مانند خرید، پشتیبانی،ERP [4] و ... می‌شود، هوش امنیتی نیز موجب کاهش تهدیدات، کاهش سطح عدم انطباق، تسهیل تصمیم‌گیری‌های امنیتی و خودکار کردن فرآیندهای امنیتی می‌شود.
مدل امنیتی ده سال پیش سازمان‌ها، در شرایط کنونی ابدا مؤثر نیست و این مدل در بهترین حالت خود جزایر امنیتی را ایجاد می‌کند و هکرها از فاصله بین این اطلاعات استفاده می‌کنند.

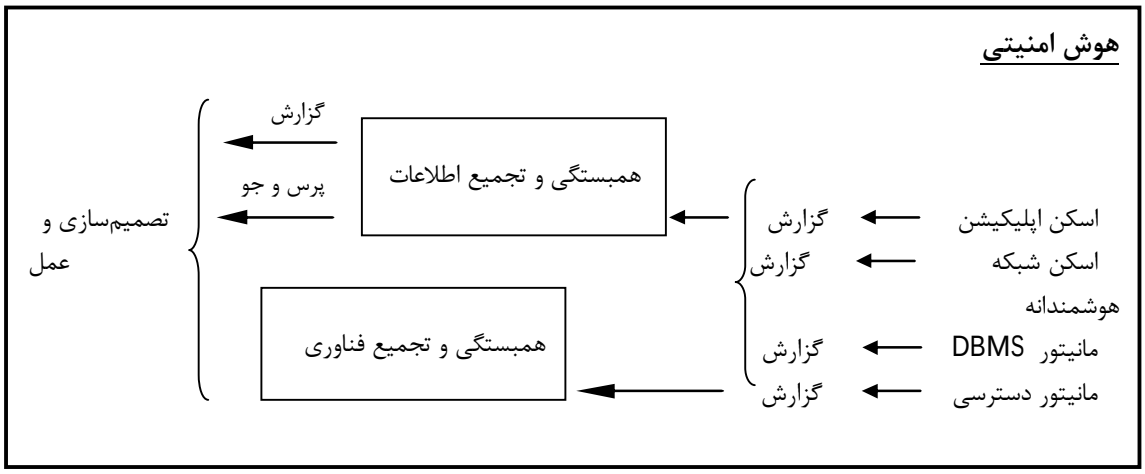
---

1 _big data
2 - Advanced Persistent Threat
3 _Business Intelligence
4 _Enterprise resource planning

جهت برقرای امنیت در روش‌های سنتی مطابق شکل زیر، از موارد مذکور گزارشی تهیه می‌شود،



اما در روش هوش امنیتی پس از تهیه این گزارشات، با استفاده از دو بخش مهم هوش امنیتی، بخش یکپارچگی اطلاعات و همبسته‌سازی و بخش برهم‌کنش تکنولوژی و همبسته‌سازی از گزارش حاصله، می‌توان تصمیم یا عمل هوشمندی را اتخاذ کرد.



مدیریت رویدادها و امنیت اطلاعات (SIEM) [5]، مدیریت مخاطرات (Risk Management) و پذیرش مقررات (Regulatory Compliance)، سه جزء اصلی یک راه‌کار هوش امنیتی هستند.

SIEM، مهمترین جزء و متفاوت با Log Management است و ترکیبی از محصولات مدیریت رویدادهای امنیتی (SEM)[6] و مدیریت اطلاعات امنیتی (SIM)[7] می‌باشد. مدیریت رخداد نگاشت‌ها (log)، نرمال‌سازی، همبسته‌سازی رویدادها، عکس‌العمل آنی به تهدیدات، امنیت عناصر انتهایی، ذخیره‌سازی وقایع و ارائه گزارش به‌صورت Web-based و راه دور، نمونه‌های از سرویس‌های SIEM هستند. قسمت زیرساخت در یک راه‌کار هوش امنیتی توسط SIEM تأمین می‌شود، وظایف نرمال‌سازی و همبسته‌سازی توسط SIEM انجام می‌شود، در بسیاری از محصولات تجاری SIEM، امکان مدیریت Compliance هم وجود دارد، محصولات تجاری SIEM عمدتاً توسعه‌پذیر[8] هستند و به دلایل مذکور SIEM، قلب یک راه‌کار هوش امنیتی است.

هدف مدیریت مخاطرات، کاهش زیان است که از طریق سه شاخص، شناسایی، ارزیابی و اولویت‌گذاری امکان‌پذیر است. بر مبنای ISO 27005، پنج قدم مهم در مدیریت مخاطرات وجود دارد که در ذیل آمده است.

5 - Security Information and Event Management
6 _Security Event Management
7 _Security Intelligence Management
8 _Expandable

قدم اول: تشخیص و شناسایی تهدیدات
قدم دوم: ارزیابی آسیب‌پذیری‌های هدف تهدیدات
قدم سوم: تشخیص زیان‌های ناشی از عملی شدن تهدیدات
قدم چهارم: تعیین راه‌کارهای کاهش مخاطرات
قدم پنجم: اولویت‌گذاری راه‌کارها

2-1 - خروجی‌های یک راه‌کار هوش امنیتی

Data silo consolidation : بدون تکنولوژی هوش تجاری، تحلیل بزرگ‌داده‌های تجاری برای تعیین مسیر حرکت یک کسب و کار عملاً ناممکن است. چنین تشبیهی در مورد هوش امنیتی نیز صادق است. بدون هوش امنیتی، دریافت log تجهیزات حتی در صورتی‌که به‌طور کامل نیز انجام گردد، باعث ایجاد یک سیلوی جدید می‌شود. در یک سازمان بزرگ این داده‌ها به اندازه‌های زتا بایت[9]، یوتا بایت[10] و هلا بایت[11] هم می‌رسد. هوش امنیتی به‌وسیله اضافه کردن Context باعث کاهش حجم اطلاعات امنیتی می‌شود.

Threat Management : از زمان ظهور اینترنت، مدل تهدیدات امنیتی از یک مدل متمرکز به یک مدل توزیع‌شده تغییر ماهیت داده است. امنیت دیگر تنها موضوع نصب فایروال نیست. امروزه تمرکز بر روی امنیت لایه‌های بالاتر مدل OSI بوده و محتوا اهمیت یافته است و حملات APT مطرح شده‌اند. فعالیتی که برای یک بخش از زیرساخت بی‌ضرر تشخیص داده می‌شود، پس از همبسته‌سازی با سایر منابع اطلاعاتی ممکن است برای بخش دیگری از زیرساخت مهلک تشخیص داده شود. وظیفه هوش امنیتی تشخیص این نوع حملات است.

Fraud Discovery : تشخیص تقلب بدون استفاده از هوش امنیتی عملاً غیرممکن است. تشخیص تقلب نیازمند جمع‌آوری Log کلیه المان‌های مسیر حرکت یک بسته اطلاعات یا تراکنش بانکی است که مجدداً با مشکل Big Data روبرو می‌شود.

Regulatory Compliance : مهمترین خروجی هوش امنیتی است که اهمیت certified بودن برای کسب و کار یک سازمان را دربردارد. در واقع یک بازرس[12] خودکار و real-time است. به‌جز حوزه‌های مربوط به منابع انسانی، سایر حوزه‌های یک استاندارد را پوشش می‌دهد و قابلیت تنظیم برای استانداردهای بومی، محلی و کشوری را دارد.

2-2- چالش‌های پیاده‌سازی هوش امنیتی

فناوری هوش امنیتی مانند سایر فناوری‌ها با چالش‌هایی روبروست که نمونه‌هایی از آنها در جهان و ایران در ادامه ذکر می‌شود. عدم پشتیبانی مدیریت ارشد، بودجه، کمبود نیروی انسانی متخصص، عدم درک درست از هوش امنیتی، پیچیدگی پیاده‌سازی و عدم توجه کافی به مدیریت ریسک نمونه‌های از چالش‌های پیاده‌سازی درجهان بوده و فرهنگ سازمانی نامناسب، عدم پشتیبانی مستقیم شرکت‌های فروشنده محصول در ایران و عدم هماهنگی بین سازمان‌های مختلف در مدیریت امنیتی نمونه‌هایی از چالش‌های پیاده‌سازی در ایران هستند.

9 - Zetta byte
10 - Yotta byte
11 - Hell byte
12 _ Auditor