آیکو بوک: برترین روندهای امنیت سایبری

برترین روندهای امنیت سایبری به پیشنهاد Gartner در سال ۲۰۲۵

معرفی برترین روندهای امنیت سایبری توسط تحلیلگران Gartner در همایش مدیریت امنیت و ریسک سیدنی (مارس ۲۰۲۵)

مقدمه

سال ۲۰۲۵ را می‌توان نقطه عطفی در تحول رویکردهای امنیت سایبری دانست.

بر اساس گزارش جدید Gartner، عواملی همچون پیشرفت سریع **هوش مصنوعی مولد (GenAI)**، **دگرگونی در ساختار داده‌ها**، **کمبود نیروی متخصص امنیتی** و **افزایش پیچیدگی زنجیره‌های تأمین دیجیتال**، چشم‌انداز امنیت اطلاعات را دگرگون کرده‌اند. در نتیجه، رهبران امنیت و مدیریت ریسک (SRM) ناگزیرند به‌سوی رویکردهایی حرکت کنند که علاوه بر پایداری فنی، از تاب‌آوری سازمانی و انطباق مستمر با تغییرات محیطی نیز پشتیبانی کنند.

گارتنر شش روند اصلی را برای بهبود امنیت سایبری در کنفرانس سیدنی سال ۲۰۲۵ معرفی کرده است که هر یک تأثیر گسترده‌ای بر راهبردهای امنیتی خواهند داشت. این آیکوبوک با هدف تحلیل و تبیین این شش روند کلیدی تدوین شده است.

در این کتابچه، هر روند از دو منظر موردبررسی قرار می‌گیرد: نخست، **توضیح مفهومی و تأثیر آن بر چشم‌انداز امنیت‌سازمانی** و سپس **کاربردهای عملی آن در ابزارها و زیرساخت‌های امنیت شبکه**.

روند اول: هوش مصنوعی مولد و امنیت داده‌ها

۱.۱ تعریف هوش مصنوعی مولد (GenAI)

هوش مصنوعی مولد یا عامل‌گرا، نسل جدیدی از AI است که می‌تواند به‌صورت خودکار اهداف تعیین‌شده توسط کاربران را دنبال کند و برای رسیدن به آن‌ها تصمیم‌گیری و اقدام کند. این فناوری فراتر از پردازش اطلاعات صرف است و می‌تواند عملیات پیچیده‌ای را بدون نیاز به دخالت مستقیم انسان انجام دهد. در محیط‌های سازمانی، Agentic AI می‌تواند وظایف تکراری و زمان‌بر را خودکار کرده و نیروی انسانی را به فعالیت‌های استراتژیک‌تر هدایت کند.

بااین‌حال، توانایی تصمیم‌گیری مستقل، نیازمند کنترل و چارچوب‌های اخلاقی دقیق است تا از انحراف عملکرد یا سوءاستفاده جلوگیری شود. تا پیش از ظهور GenAI، تمرکز امنیت سایبری بر داده‌های ساختاریافته مانند پایگاه‌داده‌ها بود. اما اکنون داده‌های غیرساختاریافته (متن، تصویر، صوت و ویدئو) به منبع جدید خطر و درعین‌حال دارایی حیاتی تبدیل شده‌اند. سازمان‌ها باید سیاست‌های امنیتی خود را برای حفاظت از داده‌های ورودی و خروجی مدل‌های AI بازطراحی کنند.

۲.۱ کاربرد GenAI در ابزارهای امنیت شبکه

- **DLP هوشمند (Data Loss Prevention)**: تحلیل بلادرنگ محتواهای متنی، تصویری و صوتی تولیدشده توسط کاربران برای شناسایی داده‌های حساس یا محرمانه
- **AI Shielding**: اعمال کنترل‌های امنیتی برای محدودسازی دسترسی مدل‌های زبانی به داده‌های داخلی و جلوگیری از استخراج اطلاعات حساس
- **LLM Audit Logging**: ثبت و تحلیل دقیق تعاملات کاربران با مدل‌های زبانی به‌منظور ردیابی و پیشگیری از نشت داده‌ها
- **Data Classification Automation**: استفاده از GenAI برای شناسایی خودکار نوع و حساسیت داده‌ها و اعمال سیاست‌های متناسب با سطح محرمانگی آن‌ها
- **Secure AI Gateways**: ایجاد لایه‌ای واسط میان کاربران و مدل‌های AI برای رمزنگاری، فیلتر و کنترل جریان داده‌های ورودی و خروجی در سطح شبکه

۳.۱ مزایا و معایب GenAI

مزایا	معایب
افزایش دقت در شناسایی نشت داده‌های غیرساختاریافته	پیچیدگی پیاده‌سازی و نیاز به منابع پردازشی بالا
محافظت از داده‌های آموزشی مدل‌های سازمانی	افزایش چالش در رعایت حریم خصوصی کاربران
ارتقای سیاست‌های امنیتی مبتنی بر داده‌های متنوع	هزینه بالای نگهداری و مانیتورینگ داده‌های حجیم
شفافیت در ردیابی و کنترل تعاملات AI	نیاز به تخصص ترکیبی در امنیت و یادگیری ماشین
بهبود انطباق با مقررات جدید داده و AI	وابستگی زیاد به دقت مدل‌های تحلیلی

۱.۲ تعریف مدیریت هویت‌های ماشینی

(Machine Identity Management)

امروزه مفهوم «هویت» دیگر تنها به کاربران انسانی محدود نمی‌شود. رشد چشمگیر خدمات ابری، زیرساخت‌های DevOps، اینترنت اشیا (IoT) و هوش مصنوعی مولد (GenAI) باعث شده میلیون‌ها ماشین، ربات، سرویس و فرایند نرم‌افزاری دارای هویت دیجیتال مستقل باشند. این هویت‌ها شامل کلیدها، گواهی‌ها، توکن‌ها و API Keys هستند که به سیستم‌ها امکان برقراری ارتباط امن و خودکار را می‌دهند. اما در نبود یک ساختار متمرکز برای مدیریت این هویت‌ها، سطح حمله سازمانی به طور چشمگیری گسترش می‌یابد. بسیاری از رخدادهای امنیتی اخیر ناشی از سوءاستفاده مهاجمان از گواهی‌ها یا حساب‌های ماشینی منقضی شده بوده است.

به همین دلیل، Gartner تأکید می‌کند که سازمان‌ها باید مدیریت هویت‌های ماشینی (MIM) را به‌عنوان یکی از ارکان اصلی استراتژی امنیت خود بپذیرند؛ همان‌طور که سال‌هاست احراز هویت کاربران انسانی را مدیریت می‌کنند. در این رویکرد، تمرکز بر شناسایی، کنترل، نظارت و چرخش خودکار اعتبارنامه‌های ماشینی است تا از سوءاستفاده، جعل یا دسترسی غیرمجاز در زیرساخت‌های نرم‌افزاری جلوگیری شود.

۲.۲ کاربرد مدیریت هویت‌های ماشینی

- **IAM یکپارچه (Unified Identity & Access Management)**: مدیریت و کنترل هویت‌های انسانی و ماشینی در یک بستر مشترک برای افزایش شفافیت و کاهش خطای انسانی
- **Certificate Lifecycle Automation**: خودکارسازی صدور، تمدید و ابطال گواهی‌های TLS/SSL برای جلوگیری از منقضی شدن و سوءاستفاده احتمالی مهاجمان
- **API Security Gateway**: اعتبارسنجی مداوم APIها و سرویس‌های بین سیستمی برای اطمینان از هویت معتبر ماشین‌ها در تبادل داده
- **Key Management Systems (KMS)**: رمزگذاری و مدیریت امن کلیدهای رمزنگاری، به‌ویژه در سرویس‌های ابری چند سکویی
- **Machine Identity Discovery Tools**: ابزارهای شناسایی خودکار حساب‌ها و گواهی‌های پنهان یا ناشناخته در زیرساخت سازمان برای جلوگیری از ایجاد «**نقاط کور امنیتی**»

۳.۲ مزایا و معایب مدیریت هویت ماشینی

مزایا	معایب
کاهش چشمگیر ریسک نفوذ از طریق حساب‌ها و گواهی‌های ماشینی	نیاز به ادغام گسترده با سیستم‌های متنوع و پیچیده سازمانی
افزایش شفافیت و قابلیت نظارت بر تمامی تعاملات سرویس‌ها	احتمال بروز اختلال در فرآیندهای خودکار در صورت تنظیم نادرست
بهبود انطباق با الزامات قانونی و استانداردهای امنیتی مانند NIST و ISO 27001	هزینه اولیه بالا برای طراحی، پیاده‌سازی و آموزش تیم‌ها
ارتقای امنیت در محیط‌های DevOps، Cloud و IoT	نیاز به نگهداری مستمر و به‌روزرسانی سیاست‌های دسترسی
کاهش احتمال سوءاستفاده از گواهی‌ها و کلیدهای منقضی‌شده یا سرقت‌شده	وابستگی بالا به ابزارهای خودکار و خطر ایجاد «نقطه شکست منفرد» در سامانه مرکزی

۱.۳ هوش مصنوعی تاکتیکی

(Tactical AI)

در سال‌های اخیر، بسیاری از سازمان‌ها تلاش کرده‌اند از هوش مصنوعی برای تقویت امنیت سایبری استفاده کنند، اما نتایج همیشه مطابق انتظار نبوده و گاهی ناکارآمد ظاهر شده است. ازاین‌رو، طبق تحلیل Gartner، تمرکز از «**استفاده‌ی گسترده از AI**» به سمت «**هوش مصنوعی تاکتیکی**» تغییر یافته است. یعنی استفاده هدفمند و محدود از AI در مواردی که اثرگذاری مستقیم، قابل اندازه‌گیری و سریع بر امنیت دارد.

هوش مصنوعی تاکتیکی به سازمان‌ها کمک می‌کند تا ضمن کاهش ریسک و هزینه، کارایی تیم‌های SOC و سیستم‌های تشخیص تهدید را افزایش دهند. در این رویکرد، الگوریتم‌ها به‌جای جایگزینی انسان، به‌عنوان دستیار تصمیم‌گیرنده برای تحلیل داده‌های امنیتی و تشخیص رفتارهای غیرعادی عمل می‌کنند.

۲.۳ کاربرد هوش مصنوعی تاکتیکی

- **Threat Detection & Response AI**: تحلیل خودکار الگوهای حمله و تولید هشدارهای دقیق‌تر برای کاهش آلارم‌های کاذب
- **AI-based Anomaly Detection**: تشخیص رفتارهای غیرعادی در شبکه بر اساس یادگیری الگوهای عادی سازمان
- **Incident Prioritization**: اولویت‌بندی رخدادها با استفاده از مدل‌های یادگیری ماشینی برای تمرکز منابع بر تهدیدات مهم‌تر
- **Adaptive Phishing Filters**: فیلترهای هوشمند ایمیل برای شناسایی و مسدود کردن خودکار الگوهای فیشینگ جدید
- **Automated SOC Assistant**: دستیار تحلیلی مبتنی بر LLM برای پیشنهاد پاسخ‌های سریع به هشدارهای امنیتی

۳.۳ مزایا و معایب هوش مصنوعی تاکتیکی

مزایا	معایب
بهبود سرعت و دقت در شناسایی تهدیدات پیچیده	نیاز به داده‌های باکیفیت و متنوع برای آموزش مدل‌ها
کاهش بار کاری تیم‌های امنیتی و SOC	ریسک تصمیم‌گیری نادرست در صورت تفسیر اشتباه داده‌ها
بهینه‌سازی هزینه‌ها از طریق تمرکز بر کاربردهای خاص	نیاز به نظارت انسانی مداوم برای جلوگیری از خطا
قابلیت یکپارچه‌سازی با ابزارهای موجود امنیتی	احتمال بروز حملات فریب‌دهی (Adversarial AI)
تسریع در واکنش به رخدادها با استفاده از تحلیل بلادرنگ	چالش در اثبات و ارزیابی ارزش واقعی سرمایه‌گذاری AI

روند چهارم: بهینه‌سازی فناوری‌های امنیت سایبری

۱.۴ تعریف بهینه‌سازی فناوری‌های امنیت سایبری

(Cybersecurity Technology Optimization)

گزارش Gartner نشان می‌دهد که سازمان‌های بزرگ به‌طور میانگین **از بیش از ۴۵ ابزار امنیتی** مختلف استفاده می‌کنند. این حجم از ابزارها، ضمن ایجاد تداخل عملکردی، باعث سردرگمی، هزینه‌های اضافی و کاهش بهره‌وری تیم‌های امنیتی می‌شود.

به همین دلیل، روند جدیدی در حال شکل‌گیری است: **بهینه‌سازی سبد فناوری‌های امنیت سایبری**. هدف این رویکرد، ایجاد هماهنگی، سادگی و کارایی از طریق حذف ابزارهای تکراری، تجمیع سرویس‌ها و تمرکز بر کنترل‌های اصلی امنیتی است.

این روند به رهبران امنیت (SRM Leaders) کمک می‌کند تا با معماری‌های ماژولار، تهدیدمدار و داده‌محور، کارایی سامانه‌های امنیتی را افزایش داده و هزینه‌ها را کنترل کنند.

۲.۴ کاربرد بهینه‌سازی فناوری‌های امنیت سایبری

- **Security Platform Consolidation**: ادغام ابزارهای امنیتی مشابه در یک بستر واحد برای کاهش پیچیدگی
- **Threat Modeling Integration**: استفاده از مدل‌سازی تهدید برای تعیین اولویت ابزارهای حیاتی
- **SIEM & SOAR Optimization**: بازطراحی جریان داده‌ها برای افزایش دقت تحلیل رخدادها
- **Cloud Security Posture Management (CSPM)**: ارزیابی پیوسته وضعیت امنیتی ابرها و حذف کنترل‌های تکراری
- **AI-driven Security Architecture Review**: استفاده از هوش مصنوعی برای ارزیابی و پیشنهاد حذف ابزارهای کم‌اثر

۳.۴ مزایا و معایب بهینه‌سازی فناوری‌های امنیت سایبری

مزایا	معایب
کاهش هزینه‌های نگهداری و لایسنس ابزارها	ریسک از دست دادن قابلیت‌های خاص پس از ادغام
بهبود دید کلی (Visibility) نسبت به وضعیت امنیتی	نیاز به هماهنگی بین تیم‌های متعدد IT
افزایش کارایی تیم‌های SOC با تمرکز بر ابزارهای اصلی	احتمال بروز Downtime هنگام حذف یا مهاجرت ابزارها
ارتقای قابلیت مقیاس‌پذیری در شبکه‌های بزرگ	نیاز به بازطراحی معماری امنیتی موجود
تسهیل انطباق با استانداردهای بین‌المللی	زمان‌بر بودن فرایند بهینه‌سازی و تست مجدد

۱.۵ تعریف توسعه فرهنگ و رفتار امنیتی

(Security Behavior & Culture Programs)

یکی از مهم‌ترین عوامل در هر استراتژی امنیتی، رفتار انسان‌هاست. حتی بهترین فناوری‌ها نیز بدون فرهنگ امنیتی قوی، بی‌اثر خواهند بود. **Gartner** گزارش می‌دهد که سازمان‌هایی که برنامه‌های فرهنگ و رفتار امنیتی (SBCP) را با هوش مصنوعی ترکیب کرده‌اند، تا سال **۲۰۲۶** حدود **۴۰٪** کاهش در رخدادهای ناشی از خطای انسانی خواهند داشت.

این برنامه‌ها با آموزش مستمر، بازی‌وارسازی (Gamification)، تحلیل رفتاری کارکنان و ترکیب GenAI برای تولید محتوای آموزشی تعاملی، باعث افزایش درک، تعهد و مسئولیت‌پذیری کاربران نسبت به امنیت می‌شوند. هدف نهایی، تبدیل امنیت به بخشی از DNA سازمان است، نه صرفاً مجموعه‌ای از سیاست‌ها.

۲.۵ کاربرد توسعه فرهنگ و رفتار امنیتی

- **AI-based Awareness Training**: آموزش تعاملی مبتنی بر هوش مصنوعی برای شبیه‌سازی حملات واقعی
- **Behavioral Analytics Tools**: تحلیل رفتار کاربران برای شناسایی عادت‌های پرریسک
- **Phishing Simulation Platforms**: اجرای تست‌های شبیه‌سازی فیشینگ برای افزایش هوشیاری کارکنان
- **Gamified Learning Systems**: سیستم‌های آموزشی جذاب با پاداش برای رفتارهای ایمن
- **Employee Risk Scoring**: امتیازدهی امنیتی به کارکنان بر اساس رفتار دیجیتال آن‌ها

۳.۵ مزایا و معایب توسعه فرهنگ و رفتار امنیتی

مزایا	معایب
کاهش چشمگیر خطاهای انسانی در حملات سایبری	نیاز به سرمایه‌گذاری در آموزش و فرهنگ‌سازی بلندمدت
افزایش تعهد و مسئولیت‌پذیری کارکنان نسبت به امنیت	احتمال مقاومت فرهنگی یا بی‌علاقگی کاربران
ارتقای همکاری میان تیم‌های فنی و غیرفنی	دشواری در سنجش دقیق تأثیر تغییرات رفتاری
تسهیل پیاده‌سازی سیاست‌های امنیتی سازمان	نیاز به به‌روزرسانی مداوم محتوای آموزشی
بهبود تصویر برند به‌عنوان سازمانی آگاه از امنیت	خطر بیش‌ازحد تمرکز بر آموزش و غفلت از کنترل‌های فنی

۱.۶ تعریف مقابله با فرسودگی و استرس تیم‌های امنیتی

(Cybersecurity Burnout Management)

دنیای امنیت سایبری پر از فشار، فوریت و تهدیدهای بی‌وقفه است. گزارش Gartner هشدار می‌دهد که فرسودگی شغلی (Burnout)در میان رهبران امنیت و تیم‌های SOC به یک بحران واقعی تبدیل شده است. کمبود استعداد، افزایش پیچیدگی تهدیدات و عدم حمایت مدیریتی، موجب کاهش کارایی، خطاهای تصمیم‌گیری و حتی ترک شغل متخصصان امنیتی شده است.

مدیریت مؤثر این چالش نه‌تنها مسئله‌ای انسانی بلکه یک ضرورت راهبردی است. سازمان‌هایی که به سلامت روان و تاب‌آوری تیم‌های امنیتی خود اهمیت می‌دهند، عملکرد پایدارتر و واکنش سریع‌تری در برابر رخدادها دارند.

۲.۶ کاربرد مقابله با فرسودگی و استرس تیم‌های امنیتی

- **Workload Automation**: خودکارسازی وظایف تکراری SOC برای کاهش فشار کاری
- **AI-assisted Alert Triage**: استفاده از هوش مصنوعی برای فیلتر هشدارهای غیرضروری
- **Collaborative SOC Platforms**: تسهیل همکاری و توزیع کار بین تیم‌های مختلف امنیتی
- **Mental Health Dashboards**: پایش سلامت روان و میزان استرس کارکنان امنیت با شاخص‌های قابل اندازه‌گیری
- **Rotational Duty Scheduling**: طراحی برنامه‌های نوبت‌کاری هوشمند برای جلوگیری از خستگی مفرط

۳.۶ مزایا و معایب مقابله با فرسودگی و استرس تیم‌های امنیتی

مزایا	معایب
افزایش بهره‌وری و دقت تیم‌های امنیتی	نیاز به تغییر در ساختار مدیریت منابع انسانی
کاهش نرخ ترک شغل متخصصان امنیت	هزینه‌های اولیه برای طراحی و اجرای برنامه‌های رفاهی
بهبود روحیه و انگیزه کارکنان	احتمال کاهش سرعت پاسخ‌دهی در تیم‌های کوچک
ارتقای کیفیت تصمیم‌گیری در شرایط بحرانی	دشواری در اندازه‌گیری مستقیم اثرات روانی
ایجاد فرهنگ حمایتی و پایدار در محیط‌های پرتنش	خطر بیش‌ازحد تمرکز بر آموزش و غفلت از کنترل‌های فنی

چشم‌انداز امنیت سایبری در سال ۲۰۲۵

در سال ۲۰۲۵، امنیت سایبری دیگر صرفاً به معنی «**محافظت از سیستم‌ها**» نیست، بلکه به یکی از ارکان اصلی تاب‌آوری دیجیتال و پایداری سازمانی تبدیل شده است. بر اساس تحلیل‌های Gartner، روندهای نوظهور این حوزه نشان می‌دهند که آینده‌ی امنیت سایبری بر سه محور کلیدی استوار است:

۱. یکپارچگی داده و هوش مصنوعی
۲. مدیریت پیچیدگی فناوری‌ها و هویت‌ها
۳. تمرکز بر عامل انسانی و سلامت سازمانی

در گام نخست، GenAI و سایر فناوری‌های هوش مصنوعی با ایجاد فرصت‌های جدید در تحلیل داده‌ها و شناسایی تهدیدات، به‌طور هم‌زمان چالش‌های تازه‌ای در زمینه حفظ محرمانگی، دقت و اخلاق ایجاد کرده‌اند. ازاین‌رو، سازمان‌ها باید میان نوآوری و کنترل تعادلی هوشمند برقرار کنند؛ به‌گونه‌ای که از قدرت تحلیل GenAI بهره ببرند، اما در برابر نشت داده یا سوگیری‌های الگوریتمی نیز مصون بمانند.

در مجموع، این شش روند بیانگر گذار صنعت امنیت سایبری از مرحله‌ی واکنش و ابزارگرایی به مرحله‌ی پیشگیری هوشمند و تاب‌آوری سازمانی هستند. سازمان‌هایی که بتوانند میان فناوری، فرآیند و انسان تعادل برقرار کنند، در آینده نه‌تنها از تهدیدات مصون‌تر خواهند بود، بلکه از امنیت به‌عنوان مزیت رقابتی استراتژیک نیز بهره خواهند برد.

تهران، شهرک غرب، بلوار گلها پلاک ۳۲

www.ayco.ir

info@ayco.ir

021-42305000