آیکو بوک: فرصت یا تهدید؟

نقش هوش مصنوعی در آینده تهدیدات سایبری

بر پایه‌ی مستندات معتبر مانند گزارش‌های Sophos X-Ops، مطالعات تحقیقاتی DEF CON، داده‌های Threat Intelligence و تجربیات کارشناسان امنیت سایبری

مقدمه

در سال‌های اخیر، فناوری‌های مبتنی بر هوش مصنوعی، به‌ویژه ابزارهای مولد (Generative AI)، به‌سرعت در حال گسترش‌اند و تأثیر عمیقی بر حوزه‌های گوناگون از جمله آموزش، تولید محتوا، خدمات مشتری و سلامت داشته‌اند. اما در کنار کاربردهای مشروع، این فناوری‌ها در معرض سوءاستفاده نیز قرار گرفته‌اند.

مجرمان سایبری امروز دیگر صرفاً به ابزارهای سنتی متکی نیستند. ظهور مدل‌هایی مانند GPT-٤، Stable Diffusion، ElevenLabs و ابزارهایی مانند Auto-GPT، باعث شده تا افراد بدون دانش فنی خاص، بتوانند در عرض چند دقیقه، کمپین‌های کلاهبرداری کاملاً واقعی، قانع‌کننده و مقیاس‌پذیر راه‌اندازی کنند. این پدیده، سطح تهدید را از حملات هدفمند به یک مدل فراگیر و انبوه رسانده است که «**دموکراتیزه شدن جرم سایبری**» نام می‌گیرد.

عبارت «دموکراتیزه شدن جرم سایبری» به این معناست که دسترسی به ابزارهای پیشرفته برای انجام حملات سایبری دیگر فقط در اختیار هکرهای حرفه‌ای یا گروه‌های تخصصی نیست، بلکه افراد عادی و بدون دانش فنی خاص هم می‌توانند از این ابزارها استفاده کنند.

این کتاب با هدف بررسی نقش ابزارهای هوش مصنوعی مولد در شکل‌گیری نسل جدید حملات سایبری و تحلیل شیوه‌های مقابله با آن تدوین شده است. محتوای کتاب بر پایه‌ی مستندات معتبر مانند گزارش‌های Sophos X-Ops، مطالعات تحقیقاتی DEF CON، داده‌های Threat Intelligence و تجربیات کارشناسان امنیت سایبری تنظیم شده است.

در ادامه، ابتدا با ابزارها و زیرساخت‌های فنی آشنا می‌شویم، سپس نحوه‌ی طراحی یک کمپین واقعی کلاهبرداری بررسی می‌شود. همچنین در فصول بعدی، پیامدهای اخلاقی، حقوقی و فنی این تهدیدات بررسی شده و نهایتاً به رویکردهای دفاعی و آینده‌نگری خواهیم پرداخت.

هدف این کتاب آن است که مدیران امنیت اطلاعات، تحلیل‌گران SOC، تیم‌های پاسخ به رخداد، پژوهشگران، مدیران فناوری اطلاعات و علاقه‌مندان حوزه امنیت، درکی جامع، کاربردی و قابل اجرا از تهدیدات نوین مبتنی بر AI کسب کنند.

بخش اول: **معرفی ابزارهای کلیدی هوش مصنوعی**

در این فصل، به معرفی ابزارهایی می‌پردازیم که امروزه در ساخت، تقویت و مقیاس‌بندی حملات سایبری مورد سوءاستفاده قرار می‌گیرند. این ابزارها، در اصل برای کاربردهای مفید و سازنده طراحی شده‌اند، اما در صورت بهره‌برداری نادرست، می‌توانند تهدیدی جدی برای امنیت سایبری محسوب شوند.

۱.۱ مدل‌های زبانی بزرگ و GPT-۴ ۲.۱

مدل‌های زبانی مانند GPT-٤ قابلیت تولید متون روان، طبیعی و انسانی دارند. کاربردهای مخرب شامل:

- تولید ایمیل‌های فیشینگ متقاعدکننده
- ایجاد چت‌بات‌های جعلی برای کلاهبرداری
- تولید متن برای جعل هویت یا نفوذ اجتماعی

۱.۲ Stable Diffusion V. ۲٫۲ و DALL·E

این مدل‌ها برای تولید تصاویر خلق‌شده‌اند اما:

- قابل استفاده برای جعل لوگو، کارت شناسایی، اسکرین‌شات سیستم‌های داخلی
- ساخت تصاویر جعلی برای مهندسی اجتماعی یا رسوایی سازمانی

۱.۳ ElevenLabs V. ۲٫۳ و جعل صدا

ابزاری برای تولید صدای مصنوعی با شباهت بالا:

- جعل صدای مدیران برای فریب کارکنان مالی
- تقلید تماس‌های اضطراری یا جعلی با هدف دستکاری تصمیم‌گیری

۱.۴ Auto-GPT V. ۲/٤ و هوش عامل‌گرا

این ابزارها به مدل‌های زبان اجازه می‌دهند به صورت خودکار وظایف پیچیده را انجام دهند:

- راه‌اندازی خودکار کمپین فیشینگ
- جستجو، استخراج اطلاعات، تولید محتوا، ارسال پیام و پیگیری

۱.۵ Deepfake ۲.۵ و جعل ویدئو

ترکیب صوت، تصویر و حرکت برای تولید ویدئوهای جعلی:

- جعل سخنرانی‌های مدیران
- تولید محتوای رسواکننده یا فریب‌کارانه

در فصل بعدی، یک سناریوی واقعی فیشینگ با کمک این ابزارها بازسازی خواهیم کرد.

بخش دوم: بازسازی یک کمپین واقعی فیشینگ مبتنی بر AI

در این فصل به‌صورت عملیاتی، روند طراحی و اجرای یک کمپین کلاهبرداری فیشینگ با بهره‌گیری از ابزارهای هوش مصنوعی را بررسی می‌کنیم.

۲.۱ مرحله اول: شناسایی هدف (Recon)

مهاجم با استفاده از ابزارهایی مانند GPT و Google Dorking، اطلاعات زیر را استخراج می‌کند:

- نام و سمت مدیران
- ساختار ایمیل سازمان
- نرم‌افزارهای مورد استفاده در شرکت

۲.۲ مرحله دوم: طراحی محتوای فریبنده

با کمک GPT-٤:

- نوشتن ایمیلی رسمی از طرف مدیر مالی به کارشناس خزانه‌داری
- افزودن پیوست PDF طراحی‌شده با Stable Diffusion (شامل فاکتور ساختگی)

۲.۳ مرحله سوم: تولید صدا یا تماس تأییدکننده

مهاجم با استفاده از ElevenLabs، یک پیام صوتی تولید می‌کند که شبیه صدای مدیرعامل است و در آن از کارمند خواسته می‌شود «فوراً پرداخت را انجام دهد».

۳.۴ مرحله چهارم: ارسال ایمیل و تماس

- ایمیل از دامنه جعلی مشابه دامنه اصلی سازمان ارسال می‌شود.
- تماس تلفنی نیز از طریق شماره ناشناس و صدای جعلی انجام می‌شود.

۳.۵ مرحله پنجم: برداشت وجه و پوشش ردپا

در صورت موفقیت، وجه به کیف پول رمزارزی یا حساب واسطه انتقال داده می‌شود.

این مثال نشان می‌دهد که چطور می‌توان تنها با ابزارهای رایگان یا ارزان، در کمتر از ۲۴ ساعت، یک کمپین فیشینگ پیچیده راه‌اندازی کرد.

بخش سوم: **دموکراتیزه شدن جرم سایبری**

پیش از پرداختن به جزئیات، در این بخش قصد داریم نگاهی عمیق‌تر به یکی از تحولات بنیادین در فضای تهدیدات سایبری داشته باشیم: **دموکراتیزه شدن جرم سایبری** و ظهور مدل‌های **جرم به‌عنوان خدمت** (Crime-as-a-Service).

این تحول، مرز میان "هکرهای حرفه‌ای" و "مهاجمان معمولی" را کم‌رنگ کرده است. دیگر برای اجرای حملات پیشرفته نیازی به دانش فنی یا تجربه تخصصی نیست؛ بلکه ابزارها، راهنماها و حتی پشتیبانی لحظه‌ای (!) به‌صورت سرویس‌های آنلاین در اختیار متقاضیان قرار می‌گیرد.

3

این بخش برای مدیران امنیت، تحلیل‌گران تهدید، و حتی سیاست‌گذاران حوزه سایبری، حاوی نکات کاربردی و مبتنی بر شواهد است.

۳.۱ تغییر در نقش مهاجم

در گذشته، مهاجم سایبری یک متخصص فنی یا گروه حرفه‌ای با دسترسی به زیربنای پیچیده حمله بود. اما امروز نقش مهاجم به کسی که فقط قصد حمله دارد (نه الزاماً دانش آن را) تغییر یافته و AI این شکاف را پر کرده است.

برای یک مثال واقعی، فردی با نارضایتی شخصی یا انگیزه مالی، بدون دانش امنیت، می‌تواند با چند کلیک، عملیات اخاذی سایبری یا جعل هویت راه بیندازد.

۳.۲ حملات "آماده برای اجرا" (Plug-and-Play Attacks)

در اکوسیستم جدید جرم سایبری، افراد دیگر نیازی به ساختن بدافزار ندارند. کافی است یک مدل GPT fine-tuned برای فیشینگ، یک قالب Deepfake و یک بات کنترل از تلگرام تهیه کنند.

مثال واقعی مربوط به سال ۲۰۲۴: در انجمن‌های روس‌زبان، حمله‌ای با نام "CEO Whisperer" تبلیغ می‌شد: یک بات تلگرامی که صدا و تصویر مدیران را به‌صورت لحظه‌ای جعل می‌کرد. با قیمت فقط ۵۰ دلار!

۳.۳ گسترش آموزش‌های جرم سایبری باAI

در Crime-as-a-Service (CaaS)، صرفاً فروش ابزار مطرح نیست؛ بلکه آموزش گام‌به‌گام استفاده از آن نیز فروخته می‌شود، آن‌هم توسط چت‌بات‌هایی که با زبان ساده و بومی‌شده پاسخ می‌دهند. این مدل منجر به موارد زیر گشته است:

- افزایش سرعت یادگیری مجرمان
- کاهش خطای اجرای حمله
- افزایش تعداد حملات هم‌زمان از سوی افراد بی‌تجربه

بخش چهارم: اقتصاد جدید حمله

۴.۱ تجاری‌سازی کامل حمله

اکنون برای هر بخش از زنجیره حمله سایبری، سرویس مستقلی همراه با کسب درامد وجود دارد:

بخش حمله	سرویس فروخته‌شده
شناسایی اهداف	Botnet-as-a-Service
تولید محتوا	Phishing-Email Generator
جعل صدا/تصویر	Deepfake-as-a-Service
اجرای حمله	Ransomware-as-a-Service
پول‌شویی	Crypto Mixer API

برخی از مدل‌ها به‌صورت متن‌باز منتشر می‌شوند که اگرچه باعث نوآوری است، اما در عین حال امکان سوءاستفاده را نیز بالا می‌برد.

۴.۲ کاهش ریسک مهاجم

مدل‌های جدید CaaS به مهاجم این امکان را می‌دهند که:

- خودش در حمله دخالت نکند.
- درآمد را به صورت خودکار تقسیم کند (Smart Contracts).
- در صورت شناسایی، مسئولیت قانونی را از خود دور کند (برون سپاری مسئولیت).

۴.۳ نقش AI در توسعه این بازار

- ترجمه خودکار به زبان‌های محلی برای جذب مشتری در کشورهای مختلف
- تنظیم قیمت بر اساس منطقه جغرافیایی (مثل SaaS)
- پشتیبانی از مشتری با چت‌بات‌های شبانه‌روزی!

بخش پنجم: **راهبردهای دفاعی**

با توجه به قدرت و پیچیدگی حملات سایبری مبتنی بر هوش مصنوعی، مقابله مؤثر با آن‌ها نیازمند مجموعه‌ای از اقدامات پیشگیرانه، فنی، آموزشی و راهبردی است. در این فصل، به معرفی راهکارهای دفاعی قابل اجرا می‌پردازیم که می‌توانند در سطوح مختلف سازمان به‌کار گرفته شوند.

۵.۱ تقویت آموزش و آگاهی کارکنان

اولین و مؤثرترین خط دفاعی، نیروی انسانی آموزش‌دیده است. سازمان‌ها باید:

- آموزش‌های امنیتی مبتنی بر سناریوهای واقعی AI را اجرا کنند.
- تست‌های مهندسی اجتماعی و فیشینگ شبیه‌سازی‌شده برگزار کنند.
- آگاهی کارکنان را از روش‌های نوین جعل صوت، تصویر و پیام افزایش دهند.

5

مثال عملی: سازمانی با طراحی کمپین فیشینگ آموزشی با استفاده از GPT، توانست در یک دوره ۳ ماهه نرخ کلیک روی لینک‌های مخرب را از ٪۲۳ به ٪۶ کاهش دهد.

۵.۲ استفاده از راهکارهای امنیتی مبتنی بر AI

همان‌طور که مهاجمان از AI بهره می‌برند، ابزارهای دفاعی نیز باید هوشمند باشند:

- سیستم‌های تشخیص رفتار غیرعادی (UEBA) برای شناسایی الگوهای مشکوک
- تحلیل زبانی ایمیل‌ها با NLP برای تشخیص محتوای فیشینگ
- فیلترهای صوتی برای شناسایی صداهای جعلی

مثال عملی: یک شرکت مالی با پیاده‌سازی سیستم UEBA مبتنی بر یادگیری ماشین توانست یک تلاش داخلی برای ارسال فایل جعلی را پیش از تکمیل متوقف کند.

۵.۳ اعتبارسنجی منابع و چندلایه‌سازی احراز هویت

با گسترش جعل هویت از طریق AI ، تقویت احراز هویت اهمیت ویژه‌ای دارد:

- پیاده‌سازی MFA (احراز هویت چندعاملی)
- بررسی دامنه‌های ایمیل و گواهی‌های SSL
- استفاده از SPF، DKIM و DMARC برای ایمیل‌های سازمانی

مثال عملی: دانشگاهی با اجرای کامل SPF و DMARC توانست ارسال ایمیل‌های فیشینگ از دامنه‌های جعلی به‌طور کامل متوقف کند.

۵.۴ ایجاد مرکز عملیات امنیتی مجهز (AI-enabled SOC)

SOCهای سنتی دیگر پاسخ‌گوی سرعت حملات AI نیستند. نیاز به SOC هایی با:

- تحلیل خودکار رخدادها با استفاده از LLM
- اولویت‌بندی تهدیدات با مدل‌های یادگیری تقویتی
- تعامل انسان-ماشین برای تحلیل دقیق‌تر

۵.۵ به‌روزرسانی مستمر سیاست‌های امنیتی و پشتیبان‌گیری

- پایش پیوسته‌ی سیاست‌های امنیت اطلاعات
- بازنگری روش‌های پشتیبان‌گیری در برابر حملات باج‌افزاری تولیدشده با AI
- شبیه‌سازی دوره‌ای رخدادهای امنیتی برای تست آمادگی

بخش ششم: آینده تهدیدات سایبری

در حالی که سازمان‌ها، دولت‌ها و نهادهای بین‌المللی همچنان درگیر درک و واکنش به تهدیدات فعلی مبتنی بر هوش مصنوعی هستند، آینده امنیت سایبری با چالش‌هایی بسیار پیچیده‌تر و در عین حال فرصت‌هایی نوین روبه‌رو است.

۶.۱ مهاجمان هوشمندتر، حملات خودکارتر

پیش‌بینی می‌شود که نسل بعدی حملات سایبری نه‌تنها متکی بر مدل‌های زبانی قوی‌تری مانند **GPT-۵** یا **Claude** باشد، بلکه با بهره‌گیری از عامل‌های خودگردان (**Autonomous Agents**) قادر به موارد زیر باشند:

- شناسایی خودکار آسیب‌پذیری‌ها
- تطبیق تاکتیک حمله با توجه به واکنش هدف
- اجرای مرحله‌به‌مرحله عملیات با حداقل دخالت انسانی

۶.۲ تهدیدات بلادرنگ (Real-time Threats)

با پیشرفت پردازش زبان و تصویر در زمان واقعی، حملات بلادرنگ افزایش خواهد یافت مانند:

- تماس‌های تصویری جعلی زنده
- چت‌بات‌های تعاملی در نقش پرسنل پشتیبانی
- جعل هویت در جلسات آنلاین (Live Deepfake)

۶.۳ مدل‌های اختصاصی برای جرم

مجرمان سایبری احتمالاً مدل‌های سفارشی‌سازی‌شده خود را آموزش خواهند داد؛ مدل‌هایی که:

- فاقد محدودیت‌های اخلاقی یا فنی مدل‌های عمومی‌اند.
- با داده‌های واقعی از حملات گذشته آموزش دیده‌اند.
- هدف خاصی همچون نفوذ به بانک‌ها یا زیرساخت‌ها دارند.

۶.۴ تهدید به دموکراسی و اطلاعات عمومی

هوش مصنوعی می‌تواند در کمپین‌های اطلاعات نادرست، عملیات روانی و مهندسی اجتماعی گسترده علیه دولت‌ها و جوامع نقش ایفا کند. این تهدید، از سطح سازمانی فراتر رفته و ابعادی ملی و فراملی پیدا می‌کند.

۶.۵ پاسخ جامعه جهانی: تدوین استانداردها و چارچوب‌ها

در برابر این تهدیدات، تلاش‌هایی در حال انجام است:

- استانداردهای اخلاقی توسعه **AI** توسط **ISO**، **NIST** و **IEEE**
- ایجاد چارچوب‌های نظارتی توسط اتحادیه اروپا **(AI Act)**
- افزایش همکاری‌های بین‌المللی برای ردیابی و مقابله با حملات **AI** محور

۶.۶ ظهور امنیت سایبری مولد (Generative Cybersecurity)

در آینده نزدیک، همان‌طور که مهاجمان از **AI** استفاده می‌کنند، ابزارهای دفاعی نیز به سمت خودسازمان‌دهی، خودآموزی و تولید پاسخ‌های هوشمند سوق خواهند یافت. مفاهیمی مانند موارد زیر جای **SOC**های سنتی را خواهند گرفت.

- تشخیص تهدید با کمک **AI** بومی‌سازی‌شده
- تولید خودکار **Rule**های امنیتی
- پاسخ بلادرنگ به نفوذها

بخش هفتم: آینده‌نگری و توصیه‌های راهبردی

با ورود فناوری‌های مولد هوش مصنوعی به فضای تهدیدات سایبری، سازمان‌ها با چالش‌هایی بنیادین مواجه‌اند که فراتر از ابزار و زیرساخت، به سیاست‌گذاری، فرهنگ سازمانی، و تحول در شیوه‌های مدیریت ریسک امنیتی مربوط می‌شود. در این فصل، به‌صورت کاربردی و مرحله‌به‌مرحله به اقدامات پیشنهادی برای ارتقاء آمادگی سازمان‌ها می‌پردازیم.

۷.۱ بازنگری در مدل سنتی امنیت سایبری

سازمان‌ها باید از مدل سنتی مبتنی بر «محیط بسته و دفاع پیرامونی» به سمت امنیت داده‌محور، هوشمند و انطباق‌پذیر حرکت کنند:

- حذف اتکا صرف به فایروال‌ها و آنتی‌ویروس‌های کلاسیک
- حرکت به‌سمت Zero Trust Architecture (ZTA) از طریق امن سازی تخصصی
- اولویت دادن به رفتارشناسی (Behavioral Security) به جای سیگنالی

۷.۲ ساخت تیم‌های بین‌رشته‌ای

مقابله با تهدیدات مبتنی بر AI صرفاً فنی نیست:

- تیم امنیت باید با تیم‌های حقوقی، منابع انسانی، ارتباطات و مدیریت بحران در تعامل باشد.
- نیاز به ترکیب مهارت‌های زبان‌شناسی، تحلیل روان‌شناختی و طراحی گرافیکی در کنار تحلیل فنی

۷.۳ پیش‌بینی تهدید با تحلیل داده و مدل‌سازی سناریو

سازمان‌ها باید:

- سناریوهای فرضی از حملات مبتنی بر AI طراحی و شبیه‌سازی کنند.
- از تحلیل پیش‌بینی (Predictive Analytics) برای کشف رفتارهای مشکوک استفاده کنند.
- داده‌های SOC، فایروال و ابزارهای EDR را با الگوریتم‌های هوشمند ترکیب کنند.

۷.۴ تشکیل کمیته راهبری امنیت مبتنی بر AI

یک نهاد داخلی برای پایش پیشرفت فناوری‌های AI و ارزیابی تأثیر آن بر امنیت سازمان، باید تشکیل شود:

- تدوین سیاست‌ها و پروتکل‌های واکنش سریع به تهدیدات جدید
- ارزیابی منظم ریسک‌های نوظهور مرتبط با AI
- نظارت بر اخلاق و مسئولیت‌پذیری استفاده از AI در خودِ سازمان

۷.۵ سرمایه‌گذاری روی «آموزش مستمر» نه صرفاً ابزار

تحقیقات نشان داده‌اند که سازمان‌هایی که آموزش مستمر امنیتی داشته‌اند، ۴ برابر سریع‌تر به حملات پاسخ می‌دهند.

- طراحی محتوای آموزشی خاص تهدیدات AI
- ترکیب آموزش حضوری، شبیه‌سازی، و آموزش با محتوای تعاملی هوشمند
- ارزیابی مهارت‌های دفاعی پرسنل به‌صورت دوره‌ای

۷.۶ مشارکت در اکوسیستم امنیت

هیچ سازمانی در برابر تهدیدات هوشمند، به‌تنهایی ایمن نیست:

- عضویت در شبکه‌های اطلاع‌رسانی تهدید (Threat Intel Sharing)
- مشارکت در رویدادهای همکاری‌محور مانند DEF CON و FIRST
- ارتباط مستمر با CERT ملی یا بین‌المللی

۷.۷ تهیه و بروزرسانی دائمی «نقشه راه امنیتی»

نقشه راه سازمان باید پویا، داده‌محور و مبتنی بر سناریوهای AI باشد:

- مشخص‌کردن گلوگاه‌های فناوری، نیروی انسانی، فرایند و بودجه
- تخصیص منابع به حوزه‌های با ریسک بالا (مثلاً بخش مالی یا منابع انسانی)
- تعیین شاخص‌های پیشرفت و آمادگی (KPIs & Maturity Levels)

بخش هشتم: **جمع‌بندی**

ظهور هوش مصنوعی مولد، به‌ویژه مدل‌های زبانی بزرگ **(LLMs)** و ابزارهای تولید متن، تصویر، صدا و ویدئو، بدون تردید یکی از مهم‌ترین تحولات فناوری در دهه‌های اخیر بوده است. این فناوری‌ها، با توانمندسازی کاربران برای خلق محتوا با کیفیت بالا، موجب جهش در بهره‌وری، خلاقیت و خدمات دیجیتال شده‌اند. اما در کنار این فرصت‌ها، تهدیداتی نیز پدید آمده‌اند که به‌ویژه در حوزه امنیت سایبری، ساختاری نو و چالشی بنیادین ایجاد کرده‌اند.

همان‌طور که در فصول این کتاب مشاهده شد، استفاده مخرب از **AI** در زمینه‌هایی مانند جعل هویت، فیشینگ، تولید محتوای قانع‌کننده، جعل صوت و ویدئو، و حتی راه‌اندازی خودکار حملات پیچیده، به سطحی از «مقیاس‌پذیری تهدید» رسیده که امنیت سازمان‌ها، دولت‌ها و حتی افراد عادی را به‌طور بی‌سابقه‌ای تحت تأثیر قرار داده است.

در مسیر تحلیل این تهدیدات، دریافتیم که مقابله با آن‌ها صرفاً با ابزارهای فنی ممکن نیست. لایه‌های متعددی از آموزش، فرهنگ‌سازی، اصلاح فرآیندها، طراحی مجدد ساختارهای امنیتی، ایجاد تیم‌های چندرشته‌ای و شکل‌دهی به سیاست‌گذاری‌های هوشمندانه، برای یک دفاع مؤثر و پایدار مورد نیاز است.

ملاحظات اخلاقی و حقوقی نیز بخشی جدایی‌ناپذیر از این چالش‌هاست. نهادها و جوامع باید بتوانند همزمان با بهره‌گیری از مزایای **AI**، قواعد و استانداردهایی را تدوین کنند که مانع از سوءاستفاده‌های گسترده شود. چالش‌هایی مانند تعیین مسئولیت حقوقی تولید محتوای جعلی، رعایت حریم خصوصی در مدل‌های یادگیرنده، و تدوین مقررات شفاف برای انتشار مدل‌های متن‌باز، باید به‌شکلی جهانی و هم‌افزا حل‌وفصل شوند.

در نهایت، روشن است که چشم‌انداز آینده امنیت سایبری، عمیقاً با **AI** گره خورده است. همان‌طور که مهاجمان با سرعتی بالا در حال به‌کارگیری این ابزارها هستند، سازمان‌ها نیز باید با سرعتی مشابه، نه‌فقط ابزار، بلکه ذهنیت امنیتی خود را به‌روزرسانی کنند.

هوش مصنوعی، همچون یک چاقوی دو لبه است: یا سازمان‌ها آن را به خدمت می‌گیرند و در لبه‌ی نوآوری و امنیت باقی می‌مانند، یا از آن غافل می‌مانند و در معرض موجی از تهدیدات نوظهور قرار می‌گیرند.

این کتاب تلاشی بود برای کمک به درک این تغییر بنیادین، از طریق زبان روشن، مثال‌های کاربردی، و اتکا به منابع معتبر و روز دنیا. امید است که سازمان‌ها، مدیران، متخصصان امنیت و فعالان سیاست‌گذاری، با تکیه بر این دانش، گام‌هایی هوشمندانه، متناسب و آینده‌نگر در جهت ایمن‌سازی زیرساخت‌های خود بردارند.

تهران، شهرک غرب، بلوار گلها پلاک ۳۲

www.ayco.ir

info@ayco.ir

۰۲۱-۴۲۳۰۵۰۰۰